



Guía para desarrolladores

Controlador de recuperación de aplicaciones de Amazon Route 53



Controlador de recuperación de aplicaciones de Amazon Route 53: Guía para desarrolladores

Copyright © 2024 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 Route 53 ARC?	1
Compare las capacidades multizona de disponibilidad y multirregión	4
Recuperación en zonas de disponibilidad múltiples	6
Cambio de zona	6
Cómo funciona un cambio zonal	7
Regiones de AWS	9
Componentes de cambio de zona	13
Planos de datos y control	15
Precios	16
Prácticas recomendadas	16
Operaciones de la API	19
Ejemplos de uso de las operaciones de la CLI	20
Recursos admitidos	23
Iniciar, actualizar o cancelar un turno zonal	25
Registro y monitorización	27
IAM para cambio zonal	35
Cambio automático de zona	47
Cómo funciona el cambio de zona	49
Acerca del cambio automático zonal	55
Regiones de AWS	56
Componentes del cambio automático de zona	56
Planos de datos y control	59
Precios	60
Prácticas recomendadas	60
Operaciones de la API	65
Ejemplos de uso de las operaciones de la CLI	66
Habilitar el cambio automático zonal y trabajar con él	72
Registro y monitorización	76
Identity and Access Management	84
Recuperación multirregional	101
Control de enrutamiento	101
Acerca del control de enrutamiento	102
AWS Regiones	105
Componentes	106

Planos de datos y control	109
Etiquetado	110
Precios	111
Cómo empezar con la recuperación multirregional	111
Prácticas recomendadas	114
Operaciones de la API	117
Ejemplos de uso de las operaciones de la CLI	122
Trabajar con componentes de control de enrutamiento	140
Registro y monitorización	161
Identity and Access Management	165
Cuotas	181
Verificación de preparación	182
¿Qué es la verificación de disponibilidad?	183
AWS Regiones	192
Componentes	192
Planos de datos y control	195
Etiquetado	196
Precios	197
Configure una aplicación resiliente	197
Prácticas recomendadas	198
Operaciones de la API	198
Ejemplos de uso de las operaciones de la CLI	202
Trabajar con grupos de recuperación y comprobaciones de preparación	212
Monitorear el estado de preparación	218
Obtención de recomendaciones de arquitectura	219
Crear autorizaciones entre cuentas	221
Reglas de preparación, tipos de recursos y ARNS	224
Registro y monitorización	245
Identity and Access Management	260
Cuotas	276
Ejemplos de código	278
Acciones	278
GetRoutingControlState	279
UpdateRoutingControlState	281
Seguridad	285
Protección de datos	286

Cifrado en reposo	287
Cifrado en tránsito	287
Identity and Access Management	287
Público	287
Autenticación con identidades	288
Administración de acceso mediante políticas	292
Cómo funcionan las capacidades de Route 53 ARC con IAM	294
Ejemplos de políticas basadas en identidades	295
AWS políticas administradas	295
Resolución de problemas	302
Registro y monitorización	304
Validación de conformidad	305
Resiliencia	306
Seguridad de la infraestructura	307
Historial de documentos	308
.....	cccxi

Qué es el controlador de recuperación de aplicaciones de Amazon Route 53

El controlador de recuperación de aplicaciones Amazon Route 53 (Route 53 ARC) le ayuda a preparar y completar una recuperación más rápida de las aplicaciones en ejecución AWS. Route 53 ARC ofrece dos conjuntos de capacidades: la recuperación en múltiples zonas de disponibilidad (AZ), que incluye el cambio zonal y el cambio automático zonal, y la recuperación en múltiples regiones, que incluye el control de enrutamiento y la verificación de disponibilidad. Con Route 53 ARC, puede aprovechar las herramientas de recuperación de alta disponibilidad para mitigar rápidamente las deficiencias que afectan a sus aplicaciones multirregionales o multizona de disponibilidad. También puede utilizar la verificación de preparación para obtener información sobre si sus aplicaciones y recursos están preparados para la recuperación.

La infraestructura de nube AWS global ofrece resistencia y tolerancia a los errores, y cada una de ellas Región de AWS está compuesta por varias zonas de disponibilidad completamente aisladas. Route 53 ARC funciona dentro de esta AWS estructura para ayudar a que sus aplicaciones sean resilientes.

Recuperación en zonas de disponibilidad múltiples

Si tiene aplicaciones diseñadas para aprovechar las zonas de disponibilidad AWS, puede aislarlas rápidamente y recuperarse de las deficiencias de las zonas de disponibilidad mediante el cambio zonal. El cambio zonal le permite recuperarse de las deficiencias en las zonas de disponibilidad (AZ), ya que desplaza temporalmente el tráfico de un recurso compatible desde una zona de disponibilidad hacia zonas de disponibilidad en buen estado. Región de 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 sola zona de disponibilidad. Al reducir el tráfico, reduce el impacto para los clientes que utilizan su aplicación cuando se produce un problema en una zona de disponibilidad.

Puedes iniciar un cambio zonal para cualquier recurso compatible de tu cuenta en una región. AWS los servicios registran automáticamente AWS los recursos compatibles con el cambio zonal en Route 53 ARC, de modo que puede iniciar un cambio zonal en cualquier momento.

El cambio automático zonal es una capacidad de Route 53 ARC que puede habilitar AWS para autorizar el traslado del tráfico de una zona de disponibilidad para los recursos compatibles, en su nombre, a zonas de disponibilidad en buen estado. Región de AWS AWS inicia un cambio

automático cuando la telemetría interna indica que hay una avería en una zona de disponibilidad de una región 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.

Los cambios zonales y los cambios automáticos son temporales. Al iniciar un turno zonal manual, debe especificar una caducidad (ampliable), inicialmente de hasta tres días. Si desea seguir manteniendo el tráfico alejado de una zona de disponibilidad, puede actualizar el cambio zonal y establecer un nuevo vencimiento. Con el cambio automático zonal, AWS finaliza un cambio automático cuando los indicadores muestran que ya no hay ningún problema o problema potencial.

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

- [Cambio de zona en el controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Cambio automático de zona del controlador de recuperación de aplicaciones de Amazon Route 53](#)

Recuperación multirregional

Si tiene una aplicación que ha diseñado para funcionar desde otra Región de AWS para continuar con las operaciones, puede utilizar el control de enrutamiento para la conmutación por error. El control de enrutamiento le permite conmutar por error el tráfico de una Región de AWS a otra cuando hay un problema, de modo que puede garantizar que su aplicación permanezca disponible. El control de enrutamiento incluye reglas de seguridad, que ayudan a protegerlo de resultados imprevistos, al imponer barreras que usted defina. Con estas reglas, puede asegurarse, por ejemplo, de que solo una de las réplicas de su aplicación, activa o en espera, esté habilitada y en uso a la vez.

Para la recuperación en varias regiones, Route 53 ARC puede ayudarlo a conmutar por error el tráfico de DNS entre Regiones de AWS ellas. Los controles de enrutamiento extremadamente confiables de Route 53 ARC le permiten recuperar su aplicación al desviar el tráfico de una región con problemas a una región en buen estado.

Con la comprobación de disponibilidad, Route 53 ARC monitorea continuamente las cuotas de AWS recursos, la capacidad y las políticas de enrutamiento de la red, y puede notificarle los cambios que podrían afectar su capacidad de conmutación por error a una réplica y de recuperación. Las comprobaciones continuas 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. La comprobación de disponibilidad resulta útil al configurar Route 53 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:

- [Control de enrutamiento del controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Comprobación de disponibilidad del controlador de recuperación de aplicaciones de Amazon Route 53](#)

Compare las capacidades de recuperación multizona y multirregión de Amazon Route 53 Application Recovery Controller

El cambio zonal, el cambio automático zonal y el control de enrutamiento de Amazon Route 53 Application Recovery Controller pueden lograr una recuperación rápida y ayudarlo a garantizar la resiliencia de sus aplicaciones. Estas opciones 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 opciones 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 se centra principalmente en AWS las aplicaciones que se encuentran en varias AWS regiones (multirregiones), mientras que el cambio zonal y el cambio automático zonal solo admiten el cambio de tráfico para los balanceadores de carga con aplicaciones multizona de disponibilidad. También hay otras diferencias, tal y como se describe en esta sección.

La información de la siguiente tabla incluye algunas de las características clave del control de cambio zonal, automático zonal y enrutamiento, y una comparación de las opciones entre sí. Estas descripciones pueden ayudarle a comprender mejor cómo una opción específica puede ser la mejor opción para las necesidades de recuperación ante desastres de su organización.

Control de enrutamiento	Cambio de zona	Cambio automático de zona
Regional	De zona	De zona
Redirige el tráfico de una AWS región a otra (principalmente)	Aleja el tráfico de una zona de disponibilidad	Aleja el tráfico de una zona de disponibilidad
También se puede usar para redirigir las distintas zonas de disponibilidad	El tráfico se dirige a otras zonas de disponibilidad de la región, no a un objetivo específico	El tráfico se dirige a otras zonas de disponibilidad de la región, no a un objetivo específico
Requiere configuración	Disponible sin configuración	Requiere una configuración de ejecución de práctica

Control de enrutamiento	Cambio de zona	Cambio automático de zona
Requiere configuración y puesta en marcha	Los servicios compatibles lo habilitan automáticamente Application Load Balancers y Network Load Balancers	Disponible para los servicios compatibles Application Load Balancers y Network Load Balancers
Iniciado por el cliente	Iniciado por el cliente	Iniciado por AWS
El cliente determina cuándo redirigir el tráfico	El cliente determina cuándo comenzar un cambio de zona	AWS desvía el tráfico de aplicaciones de una zona de disponibilidad en su nombre
De pago	Incluido con los servicios	Incluido con los servicios
Requiere cargos separados para el control de rutas	La creación de cambios de zona para desviar el tráfico de las zonas de disponibilidad se incluye en los equilibradores de carga compatibles	El inicio de cambios automático de zona para desviar el tráfico de las zonas de disponibilidad en su nombre se incluye en los equilibradores de carga compatibles
No caduca	Temporal	Temporal
El tráfico se puede redirigir a una réplica indefinidamente	Todos los cambios zonales deben estar configurados para que caduquen	AWS inicia y finaliza los cambios automáticos

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

- [Cambio de zona en el controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Cambio automático de zona del controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Control de enrutamiento del controlador de recuperación de aplicaciones de Amazon Route 53](#)

Utilice el cambio zonal y el cambio automático zonal para recuperar aplicaciones en Amazon Route 53 Application Recovery Controller

En esta sección se explica cómo utilizar las capacidades de Amazon Route 53 Application Recovery Controller para recuperar de forma fiable AWS la aplicación en caso de un problema en una zona de disponibilidad (AZ). Estas capacidades, el cambio zonal y el cambio automático zonal, alejan temporalmente el tráfico de una zona de disponibilidad para un recurso de Elastic Load Balancing, a fin de reducir el tiempo de recuperación de sus 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, mueve manualmente el tráfico de un recurso de Elastic Load Balancing administrado dentro y Región de AWS fuera de una zona de disponibilidad.
- Con el cambio automático zonal, el tráfico de Elastic Load Balancing se desplaza automáticamente de una zona de disponibilidad deteriorada a una zona de disponibilidad sana de una región durante los eventos, en su nombre.

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

Temas

- [Cambio de zona en el controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Cambio automático de zona del controlador de recuperación de aplicaciones de Amazon Route 53](#)

Cambio de zona en el controlador de recuperación de aplicaciones de Amazon Route 53

Con el cambio zonal en Amazon Route 53 Application Recovery Controller, puede mover el tráfico de un recurso de Elastic Load Balancing fuera de una zona de disponibilidad en una Región de AWS, a fin de mitigar un problema y recuperar rápidamente la aplicación. Tenga en cuenta que los recursos

de Elastic Load Balancing deben tener desactivado el equilibrio de carga entre zonas para poder utilizar esta capacidad.

Al implementar y ejecutar AWS aplicaciones en balanceadores de carga en varias zonas de disponibilidad (normalmente tres) de una región, puede recuperar rápidamente una aplicación en una zona de disponibilidad deteriorada iniciando un cambio zonal. Trasladar el tráfico de aplicaciones a zonas de disponibilidad en buen estado reduce la duración y la gravedad del impacto provocado por cortes de energía o problemas de hardware o software en una zona de disponibilidad.

Puede optar por cambiar el tráfico, por ejemplo, porque una mala implementación provoca problemas de latencia o porque la zona de disponibilidad está deteriorada. Un cambio zonal no requiere pasos de configuración previos, pero su AWS configuración debe permitir gestionar la carga de clientes sin la zona de disponibilidad de la que se está desplazando. Los recursos de balanceador de carga compatibles se registran automáticamente en Amazon Route 53 Application Recovery Controller para que pueda iniciar un cambio zonal para el balanceador de carga cuando sea necesario.

El inicio de un cambio zonal no requiere ningún tipo de instalación ni configuración. Una vez que se asegure de que tiene la capacidad suficiente para desviar el tráfico de una zona de disponibilidad, elija la zona de disponibilidad de la que desea alejarse y el recurso al que desviar el tráfico y, a continuación, inicie el cambio zonal. Puede cancelar el turno en cualquier momento para que el tráfico comience a regresar a la zona de disponibilidad.

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

Tenga en cuenta que, en algunos escenarios específicos, el cambio zonal no desplaza el tráfico de la zona de Arizona. Para obtener más información acerca de la asistencia con el cambio de zona, consulte [Recursos compatibles para el cambio de zona y el cambio automático de zona](#).

Cómo funciona un cambio zonal

Al iniciar un cambio zonal para un recurso del balanceador de cargas, el tráfico del recurso se aleja de la zona de disponibilidad que especificó. Para iniciar el cambio, Amazon Route 53 Application Recovery Controller solicita que la comprobación de estado del balanceador de carga de la zona de disponibilidad se establezca en mal estado, de modo que no pase la comprobación de estado. Una comprobación de estado defectuosa, a su vez, hace que Amazon Route 53 retire automáticamente 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.

Es importante tener en cuenta que el cambio zonal no utiliza las comprobaciones de estado de la forma habitual, ya que una comprobación de estado monitorea el estado subyacente de los balanceadores de carga o las aplicaciones. En cambio, Route 53 ARC utiliza comprobaciones de estado como mecanismo para alejar el tráfico de una zona de disponibilidad. El mecanismo solicita que una comprobación de estado se establezca explícitamente como insalubre y, después, vuelva a estar en buen estado para cambiar la forma en que fluye el tráfico.

El tráfico comienza a cambiar: al iniciar un cambio zonal en Route 53 ARC, debido a los pasos que implica el flujo de tráfico, es posible que el tráfico no salga inmediatamente de la zona de disponibilidad. Las conexiones existentes y en curso en la zona de disponibilidad también pueden tardar poco en completarse, según el comportamiento del cliente y 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, consulta [Cómo garantizar que los cambios de tráfico finalicen rápidamente](#).

Finaliza el turno de tráfico: cuando vence un turno zonal o lo cancelas, Route 53 ARC toma medidas para detener los cambios de tráfico. Invierte el proceso para iniciar un cambio de tráfico y solicita que los controles de estado de Route 53 vuelvan a configurarse en buen estado. Los controles de estado correctos dan como resultado la restauración de las direcciones IP zonales originales. Ahora, la zona de disponibilidad recuperada vuelve a incluirse en el enrutamiento del balanceador de cargas y el tráfico comienza a volver a fluir hacia la zona de disponibilidad.

Debe configurar todos los turnos zonales para que caduquen al comenzar 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 aleja

En algunas situaciones específicas, el cambio de zona no desvía el tráfico de la zona de disponibilidad. Por ejemplo, si los grupos objetivo del equilibrador de carga de las zonas de disponibilidad no tienen ninguna instancia o si todas las instancias están en mal estado, el equilibrador de carga se encuentra en un estado de apertura por error. Si inicias un cambio zonal para un balanceador de cargas en este escenario, el cambio zonal no cambiará las AZ que utilice el balanceador de cargas, ya que el balanceador de cargas ya está en un estado de apertura por

error. Este es el comportamiento esperado. El cambio zonal no puede forzar a una de las AZ a estar en mal estado y a desplazar el tráfico a las demás AZ de una región si todas las AZ están fallando al abrirse (en mal estado). Un segundo escenario es si se inicia un cambio zonal para un Application Load Balancer que es un punto final para un acelerador en AWS Global Accelerator. Los balanceadores de carga de aplicaciones, que son los puntos finales de los aceleradores de Global Accelerator, no admiten el cambio de zona.

Para obtener más información acerca de la asistencia con el cambio de zona, consulte [Recursos compatibles para el cambio de zona y el cambio automático de zona](#).

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 Route 53 Application Recovery Controller, consulte los [puntos de enlace y las cuotas de Amazon Route 53 Application Recovery Controller](#) en la Referencia general de Amazon Web Services.

El cambio zonal está disponible actualmente en la Regiones de AWS lista aquí. El cambio de zona también está disponible en las regiones de China, es decir, las regiones de China (Pekín) y China (Ningxia).

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
Este de EE. UU. (Norte de Virginia)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Norte de	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
California)			
Oeste de EE. UU. (Oregón)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Bombay)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com	HTTPS

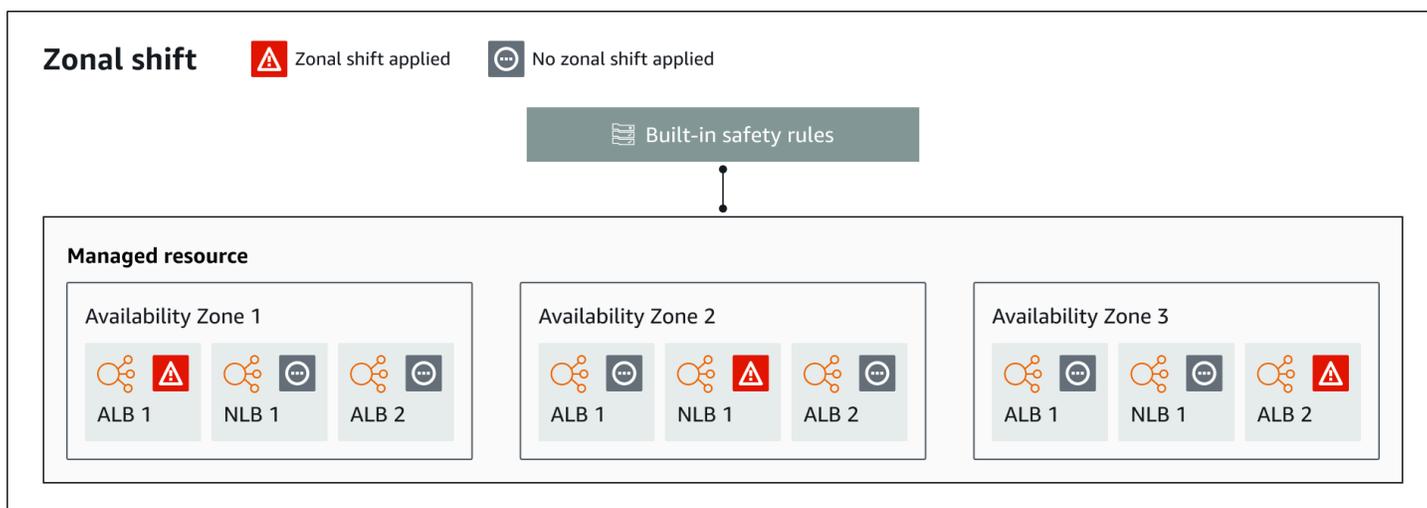
Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Osaka)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Londres)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com	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
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	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 en Route 53 ARC.

Cambio de zona

Se inicia un cambio zonal para un recurso administrado de su AWS cuenta con el fin de alejar temporalmente el tráfico de una zona de disponibilidad en una zona de disponibilidad y llevarla a zonas de disponibilidad en buen estado de la región, a fin de recuperarse rápidamente de un problema en una zona de disponibilidad. Región de AWS Actualmente, solo puede iniciar un cambio zonal para los balanceadores de carga de red y los balanceadores de carga de aplicaciones que no tengan configurado el balanceo de carga entre zonas. Los balanceadores de carga compatibles se registran automáticamente en Route 53 ARC.

Controles de seguridad integrados

Las comprobaciones integradas en Route 53 ARC evitan que se produzca más de un cambio de tráfico para un recurso a la vez. Es decir, solo un cambio de zona iniciado por el cliente, un cambio de zona de ejecución de práctica o un cambio automático del 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 [Cambio automático de zona del controlador de recuperación de aplicaciones de Amazon Route 53](#) 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).

Para un cambio zonal, solo puede elegir los recursos de su cuenta para un AWS servicio compatible con Route 53 ARC. El servicio registra automáticamente los recursos compatibles en esos AWS servicios en Route 53 ARC. AWS

Note

Actualmente, solo se puede iniciar un cambio zonal para los balanceadores de carga de red y los balanceadores de carga de aplicaciones con el balanceo de carga entre zonas desactivado.

Administrar recursos

AWS los servicios registran los recursos automáticamente con Route 53 ARC para el cambio zonal. Un recurso que se ha registrado es un recurso administrado en Route 53 ARC.

Nombre del recurso

El nombre de un recurso en Route 53 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.

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. Para un cambio de zona iniciado por el cliente, inicialmente puede configurar un cambio de zona para que esté activo durante un máximo de tres días (72 horas).

Cuando inicia un cambio zonal, especifica cuánto tiempo desea que esté activo, que Route 53 ARC convierte en tiempo de caducidad (tiempo de caducidad). También puede cancelar un cambio de zona iniciado por el cliente 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.

Con el cambio automático zonal, puede cancelar tanto los turnos zonales iniciados por el cliente como los que AWS comiencen para una sesión de práctica.

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.

Precios para el cambio zonal en Amazon Route 53 Application Recovery Controller

Para el cambio zonal, puede iniciar un cambio zonal para obtener 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.

Solo paga por lo que utilice en Amazon Route 53 Application Recovery Controller. Para obtener información detallada sobre los precios de Route 53 ARC y ejemplos de precios, consulte los [precios de Amazon Route 53](#) y desplácese hacia abajo hasta Amazon Route 53 Application Recovery Controller.

Prácticas recomendadas para los cambios de zona en Route 53 ARC

Recomendamos las siguientes prácticas recomendadas para utilizar cambios de zona para la recuperación de varias zonas de disponibilidad en Route 53 ARC. Los cambios de zona suelen reducir la capacidad de una aplicación activa, por lo que es importante tener cuidado al utilizarlos en producción.

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.

Al iniciar un cambio de zona para un único recurso de equilibrador de carga, por ejemplo, la capacidad de una zona de disponibilidad se eliminará temporalmente desde detrás del equilibrador de carga. En función de los cambios de zona que inicie y de la configuración de los equilibradores de carga, debe asegurarse de haber planificado detenidamente la gestión del aumento de carga en las zonas de disponibilidad restantes.

Limite el tiempo que los clientes permanecen conectados a sus terminales

Cuando el controlador de recuperación de aplicaciones Amazon Route 53 desvía el tráfico de una zona afectada, por ejemplo, mediante el cambio zonal o el cambio automático zonal, el mecanismo que utiliza Route 53 ARC para mover el tráfico de las aplicaciones es una actualización de 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. 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.

Pruebe los cambios 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 objetivos de los equilibradores de carga de las aplicaciones estén en buen estado y capturen tráfico de forma activa 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 representar mejor 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 (“destino compartido”).

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 puedes 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 de Route 53 ARC que puede usar mediante cambios de zona, que desvían el tráfico de una zona de disponibilidad para 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 del AWS CLI cambio zonal](#).

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Comenzar un cambio de zona	Consulte Comenzar un cambio de zona	Consulte Shift StartZonal
Actualizar un cambio de zona	Consulte Actualizar o cancelar un cambio zonal	Ver UpdateZonalShift
Enumere los cambios zonales	Consulte Cambio de zona en el controlador de recuperación de aplicaciones de Amazon Route 53	Ver ListZonalturnos
Descripción de recursos administrados	Consulte Recursos compatibles para el cambio de zona y el cambio automático de zona	Ver ListManagedrecursos
Obtenga un recurso gestionado	Consulte Recursos compatibles para el cambio de zona y el cambio automático de zona	Ver GetManagedrecurso

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Cancelar un cambio de zona	Consulte Actualizar o cancelar un cambio zonal	Ver CancelZonalShift

Ejemplos de uso del AWS CLI cambio zonal

En esta sección, se describen ejemplos de aplicaciones sencillas sobre el uso del cambio zonal AWS Command Line Interface para trabajar con la capacidad de cambio zonal en Amazon Route 53 Application Recovery Controller 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 Route 53 ARC le permite mover temporalmente el tráfico de los recursos compatibles fuera de una zona de disponibilidad para que su aplicación pueda seguir funcionando normalmente con otras zonas de disponibilidad de una. Región de AWS El cambio de zona actualmente es compatible con el Equilibrador de carga de red y el Equilibrador de carga de aplicación con el equilibrador de carga de varias zonas desactivado.

Veamos un ejemplo de cómo iniciar un cambio de zona mediante la AWS Command Line Interface. También puede usar la AWS CLI para actualizar un cambio de zona, por ejemplo, para establecer un nuevo vencimiento. 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:testservice::111122223333:ExampleALB123456890" \
  --away-from="usw2-az1" \
  --expires-in="5m" \
  --comment="Shifting traffic away from USW2-AZ1"
```

```
{
  "zonalShiftId": "2222222-3333-444-1111",
  "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
  "awayFrom": "usw2-az1",
  "expiryTime": 2022-11-14T01:40:42+00:00,
  "startTime": 2022-11-14T01:35:42+00:00,
  "status": "ACTIVE",
  "comment": "Shifting traffic away from USW2-AZ1"
}
```

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:testservice::111122223333:ExampleALB123456890"
```

```
{
  "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
  "name": "TestResource",
  "appliedWeights": {
    "usw2-az1": 1.0,
    "usw2-az2": 1.0,
    "usw2-az3": 1.0
  },
  "zonalShifts": []
}
```

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": [
    {
      "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
      "name": "TestResource",

```

```

        "availabilityZones": [
            "usw2-az1",
            "usw2-az2",
            "usw2-az3"
        ]
    }
]
}

```

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": [
    {
      "zonalShiftId": "2222222-3333-444-1111",
      "resourceIdentifier":
"arn:aws:testservice::111122223333:ExampleALB123456890",
      "awayFrom": "usw2-az1",
      "expiryTime": 2022-11-15T09:10:42+00:00,
      "startTime": 2022-11-13T01:35:42+00:00,
      "status": "ACTIVE",
      "comment": "Shifting traffic away from USW2-AZ1"
    }
  ]
}

```

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="arn:aws:testservice::111122223333:ExampleALB123456890" \
  --expires-in="1h" \
  --comment="Still shifting traffic away from USW2-AZ1"

```

```
{
```

```

"zonalShiftId": "2222222-3333-444-1111",
"resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
"awayFrom": "usw2-az1",
"expiryTime": 2022-11-15T10:35:42+00:00,
"startTime": 2022-11-15T09:35:42+00:00,
"status": "ACTIVE",
"comment": "Still shifting traffic away from USW2-AZ1"
}

```

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="arn:aws:testservice::111122223333:ExampleALB123456890"

```

```

{
  "zonalShiftId": "2222222-3333-444-1111",
  "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
  "awayFrom": "usw2-az1",
  "expiryTime": 2022-11-15T10:35:42+00:00,
  "startTime": 2022-11-15T09:35:42+00:00,
  "status": "CANCELED",
  "comment": "Shifting traffic away from USW2-AZ1"
}

```

Recursos compatibles para el cambio de zona y el cambio automático de zona

El controlador de recuperación de aplicaciones Amazon Route 53 admite actualmente los siguientes recursos para el cambio zonal y el cambio automático zonal:

- Equilibrador de carga de red
- Equilibrador de carga de aplicación

Los recursos de equilibrio de carga compatibles se registran automáticamente en Route 53 ARC para que pueda usarlos con el cambio zonal (y el cambio automático zonal). Puedes iniciar un cambio zonal para un balanceador de carga en la consola de Elastic Load Balancing (en la mayoría de los casos Regiones de AWS) o en Route 53 ARC.

Revise las siguientes condiciones para trabajar con cambios y recursos zonales en Route 53 ARC:

- El equilibrio de carga entre zonas no se admite con cambios de zona. Para registrar un balanceador de cargas en Route 53 ARC, asegúrate de haber desactivado el balanceo de cargas entre zonas para el balanceador de cargas en Elastic Load Balancing.
- en algunos escenarios específicos, el cambio zonal no desplaza el tráfico desde la zona de disponibilidad. 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 son incorrectas, el equilibrador de carga se encuentra en un estado de apertura por error y no puede desviar ninguna de las zonas de disponibilidad.
- Se admiten equilibradores de carga de red públicos e internos (privados) y equilibradores de carga de aplicación.
- Un recurso debe estar activo y aprovisionado por completo para desplazar el tráfico hacia él. Antes de iniciar un cambio zonal para un recurso, asegúrese de que se trata de un recurso administrado en Route 53 ARC. Por ejemplo, puede ver la lista de recursos gestionados en la AWS Management Console operación o utilizar la `get-managed-resource` operación con el identificador del recurso.
- Los equilibradores de carga de aplicaciones, que son los puntos finales de los aceleradores de Global Accelerator, no admiten el cambio de zona.
- Cuando un Equilibrador de carga de aplicación sea el destino de un Equilibrador de carga de red, comience 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 continúa enviando tráfico al Equilibrador de carga de aplicación.
- El recurso para un cambio zonal debe ser un recurso administrado que un AWS servicio haya registrado en Route 53 ARC. Elastic Load Balancing se registra automáticamente en los balanceadores de carga de red ARC y en los balanceadores de carga de aplicaciones Route 53 con el balanceo de carga entre zonas desactivado.
- Para iniciar un cambio zonal con un recurso, debe implementarse en la zona de disponibilidad y en el Región de AWS lugar donde se inicia el turno. Asegúrese de iniciar un cambio de zona en la misma región en la que se encuentra la zona de disponibilidad del turno y de que el recurso al que va a transferir el tráfico también esté en la misma zona y región.
- Asegúrese de que el usuario cuente con los permisos de IAM correctos para utilizar el cambio de zona con un recurso. Para obtener más información, consulte [IAM y permisos para el cambio de zona](#).

Iniciar, actualizar o cancelar un turno 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

En los pasos de esta sección se explica cómo iniciar un cambio de zona iniciado por el cliente en la consola del controlador de recuperación de aplicaciones de Amazon Route 53. 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 Route 53 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 de Route 53 en <https://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 desea transferir el tráfico.
5. Seleccione un balanceador de carga de la tabla Recursos para alejar 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 de zona que inicie, o cancelarlo, en la consola del controlador de recuperación de aplicaciones de Amazon Route 53. 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 AWS se inicien para un recurso para una sesión de práctica para 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 de Route 53 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 de Route 53 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 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 Route 53 Application Recovery Controller

Puede usar AWS CloudTrail Amazon EventBridge para monitorear el cambio zonal en Amazon Route 53 Application Recovery Controller, analizar patrones y ayudar a solucionar problemas.

Temas

- [Registro de llamadas a la API de cambio zonal mediante AWS CloudTrail](#)
- [Cómo usar el cambio zonal con Amazon EventBridge](#)

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

El controlador de recuperación de aplicaciones Zonal Shift for Amazon Route 53 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 Route 53 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 de Route 53 y llamadas en código a las operaciones de la API ARC de Route 53 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 que se realizó a Route 53 ARC para el cambio zonal, 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 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 actividad en Route 53 ARC para 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 tener un registro continuo de los eventos en su zona Cuenta de AWS, incluidos los eventos relacionados con el cambio de zona en Route 53 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 Route 53 ARC se registran CloudTrail y documentan en la [Guía de referencia de la API de control de enrutamiento para Amazon Route 53 Application Recovery Controller](#). Por ejemplo, las llamadas a las ListManagedResources acciones StartZonalShift y 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 lo 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 [CloudTrail UserIdentity](#).

Visualización de eventos de Route 53 ARC en el historial de eventos

CloudTrail 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 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": "VGXG4ZUE7UZTVCM TJGIAF_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": "ARO33L3W36EXAMPLE",
        "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": "OP40YXZ54HUPMIPGWH_EXAMPLE",
    "eventID": "0bca6660-e999-43a5-9008-EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
    "eventCategory": "Management"
}
}
```

Cómo usar el cambio zonal con Amazon EventBridge

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

Puedes crear reglas en Amazon EventBridge para actuar en caso de cambio zonal. Un evento de cambio zonal especifica información sobre el estado de los cambios zonales. Por ejemplo, se crea un evento al iniciar un cambio zonal.

Para capturar eventos de cambio zonal específicos que le interesen, defina patrones específicos de eventos que EventBridge pueda utilizar para detectar los eventos. 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 Route 53 ARC hasta casi EventBridge en tiempo real, 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 zonal con EventBridge

Con EventBridge, puede crear reglas que definan las acciones que se deben realizar cuando Route 53 ARC emita eventos para sus recursos. Por ejemplo, puede crear una regla que envíe un mensaje de correo electrónico al iniciar un cambio zonal.

Para escribir o copiar y pegar un patrón de eventos en la EventBridge consola, seleccione la opción 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 zonal](#).

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

1. Abra 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. Elija Create rule.
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.

Ejemplo de patrón de evento de Route 53 ARC

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.

- Seleccione todos los eventos del cambio zonal ARC de Route 53.

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

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-policies](#) CLI 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. Abra 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 Route 53 ARC, consulte las secciones anteriores de este tema.

4. En la página Seleccione el destino, elija CloudWatch como destino.
5. Elija un grupo de CloudWatch registros en el menú desplegable.

Identity and Access Management para el cambio zonal en Amazon Route 53 Application Recovery Controller

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 estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Route 53 ARC. La IAM es una Servicio de AWS herramienta 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 Amazon Route 53 Application Recovery Controller](#)

Cómo funciona el cambio zonal con IAM

Antes de usar IAM para administrar el acceso al cambio zonal en Amazon Route 53 Application Recovery Controller, conozca qué funciones de IAM están disponibles para usar con el cambio zonal.

Características 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
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí

Característica de IAM	Soporte de cambio zonal
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 basadas en identidades de Route 53 ARC

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 adjunto. Para 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 basadas en identidad de Route 53 ARC, consulte [Ejemplos de políticas basadas en identidad en Amazon Route 53 Application Recovery Controller](#).

Políticas basadas en recursos en Route 53 ARC

Compatibilidad con las políticas basadas en recursos	No
--	----

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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

Admite acciones de política	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 las acciones ARC de Route 53 para el cambio zonal, consulte [Acciones definidas por Amazon Route 53 Zonal Shift](#) en la Referencia de autorización de servicio.

Las acciones políticas en Route 53 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 de Route 53 para el cambio zonal, consulte. [Ejemplos de políticas basadas en la identidad para el cambio zonal en Amazon Route 53 Application Recovery Controller](#)

Recursos de políticas para el cambio zonal

Admite 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 puede 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 \(ARN\)](#). Puede 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, utilice 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 ARN, así como las acciones que puede especificar con el ARN de cada recurso, consulte el tema siguiente en la Referencia de autorización de servicio:

- [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 de Route 53 para el cambio zonal, consulte. [Ejemplos de políticas basadas en la identidad para el cambio zonal en Amazon Route 53 Application Recovery Controller](#)

Claves de condición de la política para el cambio zonal

Admite 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 puede 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. Puede crear expresiones condicionales que utilicen [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 puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte [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 ARC basadas en la identidad de Route 53 para el cambio zonal, consulte. [Ejemplos de políticas basadas en la identidad para el cambio zonal en Amazon Route 53 Application Recovery Controller](#)

Listas de control de acceso (ACL) en Route 53 ARC

Admite las ACL

No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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 Route 53 ARC

Admite 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 [¿Qué es 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.

Route 53 ARC incluye el siguiente soporte parcial para ABAC:

- El cambio de zona admite ABAC para los recursos administrados que están registrados en Route 53 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 Route 53 ARC

Compatible con el uso de credenciales temporales	Sí
--	----

Algunos 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 más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) 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 más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos de entidades principales entre servicios de Route 53 ARC

Admite Forward access sessions (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 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](#)

Servicio de roles de Route 53 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.

Roles vinculados a servicios de Route 53 ARC

Compatible con roles vinculados al servicio	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 Route 53 Application Recovery Controller, especialmente si trabaja con la función desde otro AWS servicio, como Elastic Load Balancing. Para obtener información sobre cómo funcionan las funciones ARC de Route 53 con la IAM y los permisos en general, consulte la información del tema de información general, [Identity and Access Management para el cambio zonal en Amazon Route 53 Application Recovery Controller](#).

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 cambio de zona en Route 53 ARC. Para obtener más información, consulte el acceso a la [consola de turnos zonales y el acceso a las operaciones por turnos zonales](#).
- No necesita añadir permisos adicionales de Elastic Load Balancing con IAM para trabajar con cambios zonales para los recursos del equilibrador de carga gestionado en su cuenta de Route 53 ARC.
- Una política AWS administrada 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 Amazon Route 53 Application Recovery Controller

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Route 53 ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la API. AWS 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.

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](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Route 53 ARC, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición del controlador de recuperación de aplicación de Amazon Route 53 ARC](#) en la Referencia de autorizaciones de servicio.

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 identidades determinan si alguien puede crear, acceder o eliminar los recursos de Route 53 ARC de la 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, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) 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, consulte [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, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.

- Utilice 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 [Política de validación de Analizador de acceso de IAM](#) en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [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 del controlador de recuperación de aplicación de Amazon Route 53, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de Route 53 en su 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 conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite 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 de zona del controlador de recuperación de aplicaciones de Amazon Route 53

Con el cambio automático zonal, usted 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. 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. 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 Route 53 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 de zona que Route 53 ARC inicia para las ejecuciones de práctica le ayudan a garantizar que el desvío del tráfico de una zona de disponibilidad durante un cambio automático sea seguro para la 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

completan 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.

Para garantizar que las pruebas con 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. 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 monitorearlas. Según el tiempo que el servicio y los clientes reutilicen las conexiones, es posible que el tráfico continúe hacia la zona de la que te has alejado durante más tiempo del esperado. Para obtener más información, consulte [Limitar el tiempo que los clientes permanecen conectados a sus puntos de conexión](#).

Después de comprobar, al iniciar y evaluar un cambio zonal, que su aplicación puede seguir funcionando normalmente con el tráfico desplazado fuera de una zona de disponibilidad, la práctica habitual que realiza Route 53 ARC le ayuda a confirmar, de forma continua, que tiene suficiente capacidad para un cambio automático.

Además de habilitar el cambio automático zonal para un recurso de balanceador de carga en la consola Arc de Route 53, tiene la opción de habilitar el cambio automático zonal para un balanceador de carga específico en la consola Amazon EC2. 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 Route 53 Application Recovery Controller 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 que se escale previamente en todas las zonas de disponibilidad de una Región de AWS, de modo que una aplicación pueda funcionar con normalidad si se pierde una zona de disponibilidad.

Con el cambio automático de zona, es necesario configurar ejecuciones de práctica, en las que Route 53 ARC desvía periódicamente el tráfico del recurso de zona de disponibilidad. Route 53 ARC programa ejecuciones de práctica aproximadamente una vez por semana para cada recurso que tenga una configuración de ejecución de práctica asociada. Las ejecuciones de práctica para cada recurso se programan de forma independiente.

En cada ejecución de práctica, Route 53 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](#).

Temas

- [¿Cuándo se AWS inicia y se detiene el cambio automático?](#)
- [Cuando Route 53 ARC programa, inicia y finaliza ejecuciones de práctica](#)
- [Prioridad para los cambios de zona, las ejecuciones de práctica y los cambios automáticos](#)
- [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 \(UTC\)](#)

Cuándo AWS arranca y 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 escalado 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 Route 53 ARC programa, inicia y finaliza ejecuciones de práctica

Route 53 ARC programa semanalmente una ejecución de práctica para un recurso, durante unos 30 minutos. Route 53 ARC programa, inicia y administra las ejecuciones de práctica de cada recurso de forma independiente. Route 53 ARC no agrupa las ejecuciones de práctica de los recursos de la misma cuenta.

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 algunas situaciones en las que Route 53 ARC interrumpe una ejecución de práctica y la finaliza. Por ejemplo, si se inicia un cambio automático durante una ejecución de práctica, Route 53 ARC interrumpe dicha ejecución 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 esta situación, Route 53 ARC también interrumpe la ejecución de práctica y la finaliza.

Además, hay varias situaciones en las que Route 53 ARC no inicia una ejecución de práctica programada para un recurso.

En respuesta a las ejecuciones de práctica interrumpidas o bloqueadas de un recurso, Route 53 ARC hace lo siguiente:

- Si una ejecución de práctica de un recurso se interrumpe mientras está en curso, Route 53 ARC considera que la ejecución de práctica semanal ha finalizado y programa una nueva ejecución de práctica del 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 de bloqueo cuando se programa el inicio de una ejecución de práctica de un recurso, Route 53 ARC no iniciará la ejecución de práctica. Route 53 ARC continúa con la supervisión habitual para determinar si aún hay una o varias restricciones de bloqueo. Si no hay ninguna restricción de bloqueo, Route 53 ARC iniciará la ejecución de práctica del recurso.

A continuación se proporcionan ejemplos de restricciones de bloqueo que impiden que Route 53 ARC inicie una ejecución de práctica de un recurso, o continúe con ella.

- Route 53 ARC no inicia ni continúa las carreras de práctica cuando hay un AWS Fault Injection Service experimento en curso. Si un AWS FIS evento está activo cuando Route 53 ARC ha programado el inicio de una carrera de práctica, Route 53 ARC no inicia la carrera de práctica. Route 53 ARC monitorea durante las sesiones de práctica para detectar restricciones de bloqueo, incluido un AWS FIS evento. Si un AWS FIS evento comienza mientras hay una carrera de práctica activa, Route 53 ARC finaliza la carrera de práctica y no intenta iniciar otra hasta la siguiente carrera de práctica programada regularmente para el recurso.
- Si hay un AWS evento actual en una región, Route 53 ARC no inicia las carreras de práctica para obtener recursos y finaliza las carreras de práctica activas en la región.

Cuando la ejecución de práctica finalice sin interrupciones, Route 53 ARC programa la próxima ejecución de práctica en una semana, como de costumbre. Si una carrera de práctica no se inicia debido a una restricción de bloqueo, como un AWS FIS experimento o un intervalo de tiempo bloqueado que haya especificado, Route 53 ARC seguirá intentando iniciar una carrera de práctica hasta que se pueda iniciar la carrera de práctica.

Prioridad para los cambios de zona, las ejecuciones de práctica y los cambios automáticos

No puede haber más de un cambio de tráfico para un recurso que esté en vigor a la vez, es decir, solo se puede realizar un cambio de zona de ejecución de práctico, un cambio de zona iniciado por el cliente o un cambio automático para el recurso. Cuando hay más de un cambio de tráfico en curso, Route 53 ARC sigue una prioridad para determinar qué cambio de tráfico está en vigor para un recurso.

El principio general de prioridad es que los turnos zonales que se inician como cliente tienen prioridad sobre los cambios automáticos, que tienen prioridad sobre las sesiones de práctica. Es decir, cambios de zona iniciados por el cliente > cambios automáticos > cambios de zona de ejecución de práctica.

Para ilustrar esto, a continuación se explica cómo funciona la prioridad en algunas situaciones de ejemplo:

- Si hay un cambio automático activo y se inicia un cambio de zona de un recurso que tiene el cambio automático habilitado, el cambio de zona que se inicie será APPLIED. El recurso ahora se desvía de la zona de disponibilidad a la que se aplica el cambio de zona. Si el cambio de zona finaliza antes de que AWS finalice el cambio automático, el cambio automático se convertirá en el cambio APPLIED. Por lo tanto, el recurso se aleja de la zona de disponibilidad en la que se está realizando el cambio automático AWS .
- Si se ha iniciado un cambio zonal activo para un recurso que tiene activado el cambio automático e AWS inicia un cambio automático, el cambio automático existe para ese recurso. Sin embargo, el cambio de zona se establece en APPLIED y el cambio automático se establece en NOT APPLIED hasta que el cambio de zona finalice. A continuación, el estado del cambio automático se actualiza a APPLIED y desvía el tráfico hacia el recurso hasta que finalice el cambio automático. AWS
- Si hay una ejecución de práctica activa para un recurso y se inicia un cambio de zona para el recurso que desvía el tráfico hacia la misma zona de disponibilidad, la ejecución de práctica se interrumpirá. Si se inicia un cambio de zona que desvíe el tráfico de una zona de disponibilidad diferente, la ejecución de práctica continuará como de costumbre.
- Si hay un cambio de zona activo para un recurso y Route 53 ARC tiene previsto iniciar una ejecución de práctica, esta se aplaza durante una hora. A continuación, Route 53 ARC intenta de nuevo iniciar la ejecución de práctica. Route 53 ARC sigue comprobando cada hora hasta que se pueda iniciar una ejecución de práctica.

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 se establecen en ACTIVE.

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

Para detener un cambio automático en curso para un recurso, deshabilite el cambio automático de zona del recurso.

Al deshabilitar el cambio automático de zona, la configuración de la ejecución de práctica del recurso no se ve afectada. 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 de zona requiere ejecuciones de práctica, al eliminar una configuración de ejecución de práctica mediante la consola Route 53 ARC, esta acción también deshabilita el cambio automático de zona 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 detener una ejecución de práctica activa, cancele el cambio de zona de la ejecución de práctica. Para obtener más información, consulte [Cancelación de un cambio de zona de ejecución de práctica](#).

Cómo se desvía el tráfico

Para los cambios automáticos y los cambios de zona de ejecución de práctica, el tráfico se desvía de una zona de disponibilidad mediante el mismo mecanismo que Route 53 ARC utiliza para los cambios de zona iniciados por el cliente. Para desviar el tráfico de una zona de disponibilidad para los equilibradores de carga que tienen desactivado el equilibrio de carga entre zonas, Route 53 ARC establece la comprobación de estado del equilibrador de carga de la zona de disponibilidad en estado incorrecto, por lo que no pasa la comprobación de estado. A su vez, una comprobación de estado incorrecta hace que Amazon Route 53 retire del DNS las direcciones IP correspondientes al recurso, por lo que el tráfico se redirige desde la zona de disponibilidad. En su Región de AWS lugar, las nuevas conexiones ahora se enrutan a otras zonas de disponibilidad.

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

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. Route 53 ARC utiliza las comprobaciones de estado para desviar el tráfico de las zonas de disponibilidad, solicitando que estas comprobaciones se establezcan en el estado incorrecto y, después, se vuelven a restaurar al estado normal cuando finaliza un cambio automático o cambio de zona.

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 [Prácticas recomendadas al configurar el cambio automático zonal](#).

La alarma de resultados también proporciona información sobre el resultado de la ejecución de práctica que Route 53 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)

Tiene la opción de bloquear las ejecuciones de práctica para fechas específicas del calendario o para periodos 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.

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.

Puede habilitar un cambio automático de zona para los equilibradores de carga de red y los equilibradores de carga de aplicaciones con el equilibrio de carga entre zonas desactivado.

Al implementar y ejecutar AWS aplicaciones en balanceadores de carga en varias zonas de disponibilidad (normalmente tres) de una región y realizar un escalado previo para garantizar la estabilidad estática, se AWS pueden recuperar rápidamente las aplicaciones de los clientes en una zona de disponibilidad al desviar el tráfico mediante un cambio automático. Al desviar el tráfico de recursos a otras zonas de disponibilidad de la región, AWS se pueden reducir la duración y la gravedad del posible impacto provocado por cortes de energía, problemas de hardware o software en una zona de disponibilidad u otros problemas.

Cuando se AWS inicia un cambio automático para un recurso de equilibrio de carga, Route 53 ARC establece las comprobaciones de estado de Amazon Route 53 en estado incorrecto para las direcciones IP correspondientes del recurso de equilibrio de carga, de modo que el tráfico del recurso ya no se dirige a la zona de disponibilidad. Cuando AWS determina que la AZ está lista para que regrese el tráfico de la aplicación, Route 53 ARC restablece las comprobaciones de estado de Route 53 y se restauran las direcciones IP zonales originales.

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 de destino del equilibrador de carga de las zonas de disponibilidad no tienen ninguna instancia o si todas las instancias son incorrectas, el equilibrador de carga se encuentra en un estado de apertura por error y no puede desviar ninguna de las zonas de disponibilidad.

Para obtener más información sobre el cambio automático de zona, consulte [Cambio automático de zona del controlador de recuperación de aplicaciones de Amazon Route 53](#).

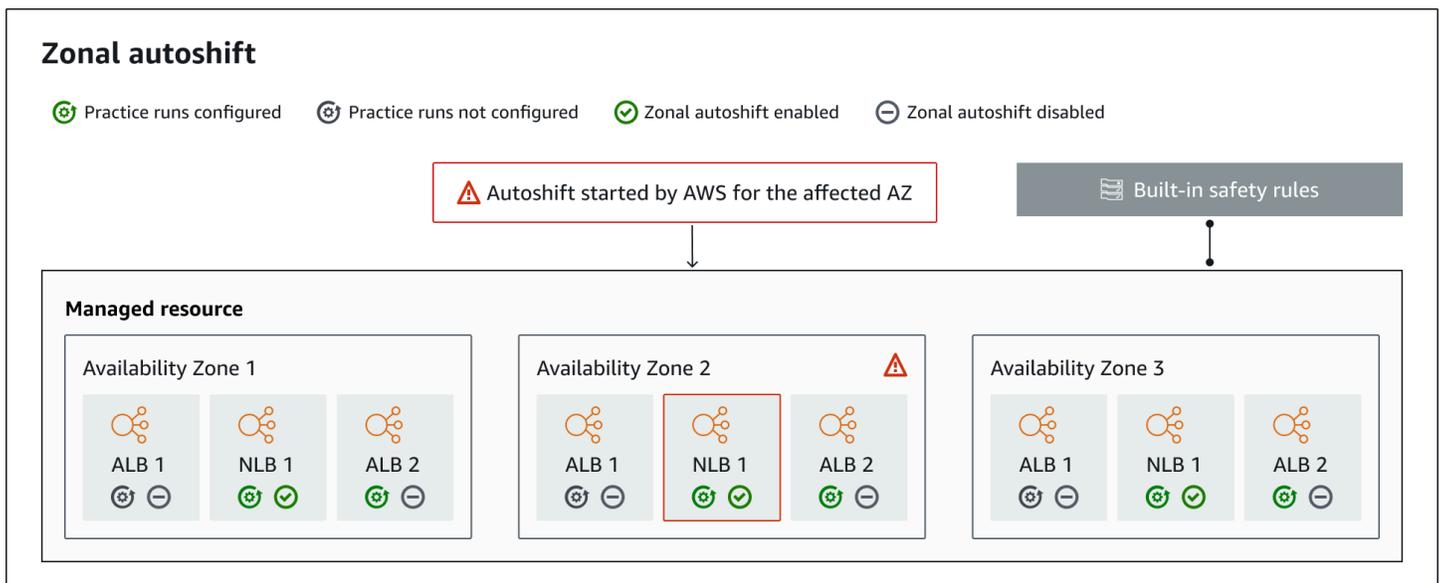
Región de AWS disponibilidad para el cambio automático zonal

El cambio automático zonal está disponible actualmente en el mercado. Regiones de AWS

Para obtener información detallada sobre el soporte regional y los puntos de enlace de servicio para Amazon Route 53 Application Recovery Controller, consulte los [puntos de enlace y las cuotas de Amazon Route 53 Application Recovery Controller](#) 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 un deterioro en la zona de disponibilidad que podría afectar a los clientes.



Los siguientes son componentes de la capacidades de cambio automático de zona de Route 53 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 capacidad de Route 53 ARC que 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. 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. Las ejecuciones de práctica garantizan que la aplicación pueda ejecutarse con normalidad sin una zona de disponibilidad. En una sesión 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 finalice la sesión 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 la ejecución de la práctica de un recurso con cambio automático zonal. Puede modificar una ejecución de práctica en cualquier momento para añadir o cambiar las fechas o periodos de tiempo bloqueados o para actualizar las alarmas de la ejecución de práctica.

Para habilitar el cambio automático de zona, debe tener una configuración de ejecución de práctica para un recurso; también puede eliminar una ejecución 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 se especifique pasa a un estado de ALARM, Route 53 ARC finaliza el cambio de zona de la práctica, de modo que el tráfico para el recurso ya no se desvía 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

Route 53 ARC informa de un resultado para cada ejecución 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.

Reglas de seguridad integradas

Las reglas de seguridad integradas en Route 53 ARC impiden que entre en vigor más de un cambio de tráfico para un recurso a la vez. Es decir, solo un cambio de zona iniciado por el cliente, un cambio de zona de ejecución de práctica o un cambio automático del 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 [Resultados de las sesiones de práctica](#).

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 Route 53 ARC. El servicio registra automáticamente los recursos compatibles en esos AWS servicios en Route 53 ARC. AWS

 Note

Solo puede configurar el cambio automático zonal para los balanceadores de carga de red y los balanceadores de carga de aplicaciones con el balanceo de carga entre zonas desactivado.

Administrar recursos

AWS los servicios registran los recursos automáticamente con Route 53 ARC para el cambio automático zonal. Un recurso que se ha registrado es un recurso administrado en Route 53 ARC.

Nombre del recurso

El nombre de un recurso administrado en Route 53 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.

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 Amazon Route 53 Application Recovery Controller

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.

Solo paga por lo que utilice en Amazon Route 53 Application Recovery Controller. Para obtener información detallada sobre los precios de Route 53 ARC y ejemplos de precios, consulte los [precios de Amazon Route 53](#) y desplácese hacia abajo hasta Amazon Route 53 Application Recovery Controller.

Prácticas recomendadas al configurar el cambio automático zonal

Tenga en cuenta las siguientes prácticas recomendadas y consideraciones al habilitar el cambio automático zonal en Amazon Route 53 Application Recovery Controller.

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.
- Con las carreras de práctica, Route 53 ARC inicia un cambio zonal en tu nombre. El cambio zonal desplaza el tráfico de una zona de disponibilidad hacia un recurso y viceversa, con 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 cambios 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 el controlador de recuperación de aplicaciones Amazon Route 53 desvía el tráfico de una zona afectada, por ejemplo, mediante el cambio zonal o el cambio automático zonal, el mecanismo que utiliza Route 53 ARC para mover el tráfico de las aplicaciones es una actualización de 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. Cuando elija 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 capacidad de cambio automático zonal de Route 53 ARC le ayuda a recuperarse rápidamente de AWS los eventos en una zona de disponibilidad cuando tiene una aplicación con recursos que están preescalados para funcionar normalmente con 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. 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 de zona en el controlador de recuperación de aplicaciones de Amazon Route 53](#).

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 general, son compatibles los equilibradores de carga de red y los equilibradores de carga de aplicación con el equilibrador de carga de varias zonas desactivado. 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).

Un segundo escenario es si se AWS inicia un cambio automático para un Application Load Balancer que es un punto final para un acelerador de entrada. AWS Global Accelerator Al igual que con el cambio de zona, el cambio automático no es compatible con los equilibradores de carga de aplicación, que son los puntos de conexión de los aceleradores de Global Accelerator.

Para obtener más información sobre los recursos compatibles, incluidos todos los requisitos y excepciones que debe tener en cuenta, consulte [Recursos compatibles para el cambio de zona y el cambio automático de zona](#).

Especifique las alarmas para las sesiones de práctica

Se configura al menos una alarma (la alarma de resultado) para las carreras de práctica con cambio automático zonal. De forma opcional, 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 (KPI) 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 en el estado de ALARM, Route 53 ARC inicia las ejecuciones de práctica la próxima vez que se programe una ejecución de práctica para el recurso.
- En el caso de la alarma de bloqueo de ejecuciones de 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 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

Route 53 ARC informa de un resultado para cada ejecución 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.

- **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 de Route 53 ARC que puede usar con el cambio automático de zona. Para ver ejemplos del uso de operaciones de la API de cambio automático zonal con el AWS CLI, consulte.

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 de Route 53 ARC	Uso de la API de Route 53 ARC
Creación de una configuración de ejecución de práctica	Consulte Habilitar o deshabilitar el cambio automático de zona	Consulte CreatePracticeRunConfiguration
Eliminación de una configuración de ejecución de práctica	Consulte Configuración, modificación o eliminación de una configuración de ejecución de práctica	Ver DeletePracticeRunConfiguration
Enumeración de cambios automáticos	Consulte Cambio automático o de zona del controlador de recuperación de aplicaciones de Amazon Route 53	Consulte ListAutoshifts .
Enumeración de los recursos para el cambio automático de zona	Consulte Recursos compatibles para el cambio de zona y el cambio automático de zona	Ver ListManagedrecursos
Obtención de los recursos para el cambio automático de zona	Consulte Recursos compatibles para el cambio de zona y el cambio automático de zona	Ver GetManagedrecurso

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Modificación de una configuración de ejecución de práctica	Consulte Configuración, modificación o eliminación de una configuración de ejecución de práctica	Ver UpdatePracticeRunConfiguration
Habilitar o deshabilitar el cambio automático de zona	Consulte Habilitar o deshabilitar el cambio automático de zona	Ver UpdateZonalAutoshiftConfiguration

Ejemplos de uso del cambio AWS CLI automático zonal

En esta sección, se describen ejemplos de aplicaciones sencillas sobre el trabajo con el cambio automático zonal y el uso de la AWS Command Line Interface función de cambio automático zonal en Amazon Route 53 Application Recovery Controller 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 Route 53 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. El cambio automático zonal incluye recorridos de práctica, que también alejan el tráfico de las zonas de disponibilidad, para ayudar a comprobar, de forma continua, que los cambios automáticos son seguros para su aplicación.

El cambio automático de zona actualmente es compatible con el Equilibrador de carga de red y el Equilibrador de carga de aplicación con el equilibrador de carga de varias zonas desactivado.

Para obtener más información, consulte [Recursos compatibles para el cambio de zona y el cambio automático de zona](#).

En esta sección se proporcionan los siguientes ejemplos para ilustrar cómo empezar a utilizar el cambio automático de zona y cómo trabajar con él:

- Cree una configuración de ejecución de práctica para un recurso.
- Habilite y deshabilite los cambios automáticos para un recurso.

- Finalice una ejecución de práctica en curso mediante la cancelación del cambio de zona iniciado por la ejecución de práctica.
- Finalice un cambio automático en curso deshabilitando la característica de cambio automático de zona de un recurso.
- Edite la configuración de una ejecución de práctica de un recurso para cambiar las alarmas especificadas o las fechas o ventanas bloqueadas.
- Elimine una configuración de ejecución de práctica para un recurso.

[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 cambio automático de zona y enlaces a más información, consulte [Operaciones de la API de cambio automático de zona.](#)

Cree 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" \  
  --alarm-name=ExampleAlarm
```

```

--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"  
}
```

Cancelación de un cambio automático en curso

Finalice un cambio automático en curso para un recurso, deshabilite la característica de cambio automático de zona. Este es el mismo comando que se utiliza para deshabilitar el cambio automático de zona en general, de modo que cuando se deshabilite el cambio automático de zona para cancelar un cambio automático en curso, el recurso tampoco se ve afectado por los cambios automáticos futuros. Puede actualizar el cambio automático de zona para volver a habilitarlo en cualquier momento.

Tenga en cuenta que puede deshabilitar el cambio automático de zona para un recurso sin eliminar la configuración de ejecución de práctica del recurso.

Para cancelar un cambio automático con la CLI, deshabilite el cambio automático de zona mediante el comando `update-zonal-autoshift-configuration`. Por ejemplo, para finalizar un cambio automático 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="DISABLED"
```

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

Cancelación de una ejecución de práctica en curso

Puede cancelar una ejecución de práctica en curso con la CLI mediante la cancelación del cambio de zona que la ejecución de práctica inició para el recurso. Para cancelar una ejecución de práctica, utilice el comando `cancel-zonal-shift`.

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

```
aws arc-zonal-shift cancel-zonal-shift \  
  --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 Started"  
}
```

Modificación de una configuración de ejecución de práctica

Puede modificar 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 Route 53 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 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.

- 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 recurso, 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

Esta sección proporciona los procedimientos para trabajar con los cambios automáticos zonales en Amazon Route 53 Application Recovery Controller, incluida la activación y desactivación del cambio

automático zonal, la configuración de las ejecuciones de práctica y la cancelación de las ejecuciones de práctica en curso.

Habilitar o deshabilitar el cambio automático de zona

En los pasos de esta sección se explica cómo habilitar o deshabilitar un cambio automático de zona en la consola del controlador de recuperación de aplicaciones de Amazon Route 53. 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 de Route 53 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, seleccione Habilitar el cambio automático de zona o Deshabilitar el cambio automático de zona y, a continuación, siga 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.

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

En los pasos de esta sección se explica cómo modificar o eliminar una configuración de ejecución de práctica en la consola del controlador de recuperación de aplicaciones de Amazon Route 53. 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 de Route 53 en <https://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. Elija deshabilitar 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 [Prácticas recomendadas al configurar el cambio automático zonal](#).

7. También puede especificar fechas o periodos de tiempo bloqueados. Elija fechas o periodos de tiempo (días y horas) para impedir que Route 53 ARC inicie ejecuciones de práctica para 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 de Route 53 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, 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.
 - Para la alarma de resultado que monitorea los entrenamientos, puede especificar que se utilice una CloudWatch alarma diferente. 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 Guardar.

Para eliminar una configuración de ejecución de práctica

1. Abra la consola ARC de Route 53 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, seleccione Eliminar la configuración de la ejecución de práctica.
5. En el cuadro de diálogo modal de confirmación, escriba De1ete 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 de zona de ejecución de práctica

En los pasos de esta sección se explica cómo cancelar un cambio de zona en la consola del controlador de recuperación de aplicación de Amazon Route 53. 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 cancelar los cambios zonales que inicie usted mismo. También puede cancelar los cambios zonales que se AWS inician para un recurso para una prueba de cambio automático zonal.

Para cancelar un cambio de zona de ejecución de práctica

1. Abra la consola ARC de Route 53 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 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 automático zonal en Amazon Route 53 Application Recovery Controller

Puede usar AWS CloudTrail Amazon EventBridge para monitorear el cambio automático zonal en Amazon Route 53 Application Recovery Controller, 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 controlador de recuperación de aplicaciones Zonal Autoshift for Amazon Route 53 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 Route 53 ARC. CloudTrail captura todas las llamadas a la API para el cambio de zona como eventos. Las llamadas capturadas incluyen llamadas desde la consola ARC de Route 53 y llamadas en código a las operaciones de la API ARC de Route 53 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 que se realizó a Route 53 ARC para el cambio zonal, 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 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 actividad en Route 53 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 tener un registro continuo de los eventos en su zona Cuenta de AWS, incluidos los eventos del cambio automático zonal en Route 53 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 Route 53 ARC se registran CloudTrail y documentan en la [Guía de referencia de la API de control de enrutamiento para Amazon Route 53 Application Recovery Controller](#). Por ejemplo, las llamadas a las ListManagedResources acciones StartZonalShift y 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 lo 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 [CloudTrail UserIdentity](#).

Visualización de eventos de Route 53 ARC en el historial de eventos

CloudTrail 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 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": "ARO33L3W36EXAMPLE",
        "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": "VGXG4ZUE7UZTVCM TJGIAF_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 que actúen en el cambio automático zonal. Un evento de cambio automático zonal especifica información sobre el estado de los cambios automáticos de las prácticas, por ejemplo, cuando se está realizando una ejecución de práctica.

Para capturar eventos de cambio automático zonal específicos que le interesen, defina patrones específicos para cada evento 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 Route 53 ARC hasta casi EventBridge en tiempo real, 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 EventBridge, puede crear reglas que definan las acciones que se deben realizar cuando Route 53 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. Elija Create rule.
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

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

- Selecciona 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

El siguiente es un ejemplo de un evento de una acción de cambio automático zonal:

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

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-policies](#) CLI 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 Route 53 ARC, consulte las secciones anteriores de este tema.

4. En la página Seleccione el destino, elija CloudWatch como destino.
5. Elija un grupo de CloudWatch registros en el menú desplegable.

Identity and Access Management para cambio automático zonal

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 estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Route 53 ARC. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Contenido

- [Cómo funciona el cambio automático zonal en el controlador de recuperación de aplicaciones Amazon Route 53 con IAM](#)
- [Ejemplos de políticas basadas en la identidad para el cambio automático zonal](#)
- [Uso de la función vinculada al servicio para el cambio automático zonal en Route 53 ARC](#)
- [AWS políticas administradas para el cambio automático zonal en Amazon Route 53 Application Recovery Controller](#)

Cómo funciona el cambio automático zonal en el controlador de recuperación de aplicaciones Amazon Route 53 con IAM

Antes de usar IAM para administrar el acceso al cambio automático zonal en Amazon Route 53 Application Recovery Controller, conozca qué funciones de IAM están disponibles para usar con el cambio automático zonal.

Funciones de IAM que puede utilizar con el cambio automático zonal en Amazon Route 53 Application Recovery Controller

Característica de IAM	Soporte de cambio automático 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
ACL	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 basadas en identidades de Route 53 ARC

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 adjunto. Para 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 basadas en identidad de Route 53 ARC, consulte [Ejemplos de políticas basadas en identidad en Amazon Route 53 Application Recovery Controller](#).

Políticas basadas en recursos en Route 53 ARC

Compatibilidad con las políticas basadas en recursos	No
--	----

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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 Route 53 ARC

Admite acciones de política	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 las acciones ARC de Route 53 para el cambio automático zonal, consulte [Acciones definidas por Amazon Route 53 Zonal Shift](#) en la Referencia de autorización de servicio.

Las acciones políticas en Route 53 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 de Route 53 para el cambio automático zonal, consulte. [Ejemplos de políticas basadas en la identidad para el cambio automático zonal](#)

Recursos de políticas para el cambio automático zonal en Route 53 ARC

Admite 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 puede 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 \(ARN\)](#). Puede 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, utilice 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 ARN, así como las acciones que puede especificar con el ARN de cada recurso, consulte el tema siguiente en la Referencia de autorización de servicio:

- [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 de Route 53 para el cambio automático zonal, consulte. [Ejemplos de políticas basadas en la identidad para el cambio automático zonal](#)

Claves de condición de la política para el cambio automático zonal en Route 53 ARC

Admite 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 puede 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. Puede crear expresiones condicionales que utilicen [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 puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte [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 de Route 53 para el cambio automático zonal, consulta 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 de Route 53 para el cambio automático zonal, consulte. [Ejemplos de políticas basadas en la identidad para el cambio automático zonal](#)

Listas de control de acceso (ACL) en Route 53 ARC

Admite las ACL

No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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 Route 53 ARC

Admite 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 [¿Qué es 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 Route 53 ARC incluye el siguiente soporte parcial para ABAC:

- El cambio automático zonal es compatible con ABAC para los recursos gestionados que están registrados en Route 53 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 Route 53 ARC

Compatible con el uso de credenciales temporales	Sí
--	----

Algunos 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 más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) 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 más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos de entidades principales entre servicios de Route 53 ARC

Admite Forward access sessions (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 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](#)

Servicio de roles de Route 53 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.

Roles vinculados a servicios de Route 53 ARC

Compatible con roles vinculados al servicio	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 acerca de cómo crear o administrar roles vinculados a servicios de Route 53 ARC, consulte [Uso de la función vinculada al servicio para el cambio automático zonal en Route 53 ARC](#).

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte [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

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Route 53 ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la API. AWS 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.

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](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Route 53 ARC, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición del controlador de recuperación de aplicación de Amazon Route 53 ARC](#) en la Referencia de autorizaciones de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)

- [Ejemplo: acceso zonal a la consola de cambio automático](#)
- [Ejemplos: Acciones de la API de Route 53 ARC](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Route 53 ARC de la 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, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) 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, consulte [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, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice 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 [Política de validación de Analizador de acceso de IAM](#) en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [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 del controlador de recuperación de aplicación de Amazon Route 53, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de Route 53 en su 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 conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite 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 Route 53 ARC. Para obtener más información, consulte [Uso de la función vinculada al servicio para el cambio automático zonal en Route 53 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 de Route 53 ARC

Puede utilizar una política para garantizar que un usuario pueda utilizar las acciones de la API ARC de Route 53 para el cambio automático zonal a fin de configurar el cambio automático zonal de modo que AWS desvíe el tráfico de recursos de la aplicación de una zona de disponibilidad, en su nombre, a las AZ en buen estado de la misma Región de AWS, a fin de reducir el 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 que está asociado a Route 53 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 Route 53 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 Route 53 ARC

[El cambio automático zonal de Amazon Route 53 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 de (en este caso, Route

53 ARC). Route 53 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 simplifica la configuración de Route 53 ARC porque ya no tendrá que añadir manualmente los permisos necesarios. Route 53 ARC define los permisos para la función vinculada al servicio y, a menos que se defina lo contrario, solo Route 53 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 adjuntar 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 ARC de Route 53 porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Yes (Sí) en la columna Service-Linked Role (Rol vinculado 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 `AWSServiceRoleForZonalAutoshiftPracticeRun`

Route 53 ARC usa el rol vinculado al servicio denominado `AWSServiceRoleForZonalAutoshiftPracticeRun` para hacer lo siguiente:

- Supervisar 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 `AWSServiceRoleForZonalAutoshiftPracticeRun`

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

El rol `AWSServiceRoleForZonalAutoshiftPracticeRun` vinculado al servicio confía en que el siguiente servicio asuma el rol:

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

Para ver los permisos de esta política, consulte la Referencia [AWSZonalAutoshiftPracticeRunSLRPolicy](#) de políticas AWS administradas.

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 AWSServiceRoleForZonalAutoshiftPracticeRunvinculado al servicio para Route 53 ARC

No es necesario crear manualmente el rol vinculado al AWSServiceRoleForZonalAutoshiftPracticeRunservicio. Al crear la configuración de la primera ejecución de práctica en el AWS Management Console AWS CLI, el o un AWS SDK, Route 53 ARC crea el rol vinculado al servicio automáticamente.

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 configuración de ejecución de práctica, Route 53 ARC vuelve a crear el rol vinculado al servicio.

Edición del rol AWSServiceRoleForZonalAutoshiftPracticeRunvinculado al servicio para Route 53 ARC

Route 53 ARC no le permite editar el rol AWSServiceRoleForZonalAutoshiftPracticeRunvinculado al servicio. 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 AWSServiceRoleForZonalAutoshiftPracticeRunvinculado al servicio para Route 53 ARC

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree 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 de zona en el controlador de recuperación de aplicaciones de Amazon Route 53](#).

Note

Si el servicio Route 53 ARC está utilizando el rol cuando intenta eliminar los recursos, la eliminación del rol de servicio podría producir un error. En tal caso, espere unos minutos e intente eliminar de nuevo el rol.

Eliminación manual del 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. `AWSServiceRoleForZonalAutoshiftPracticeRun` 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 de Route 53 para el cambio automático zonal

Para ver las actualizaciones de las políticas AWS administradas para las funciones vinculadas al servicio de Route 53 ARC, consulte la [tabla de actualizaciones de políticas AWS administradas](#) de Route 53 ARC. También puede suscribirse a alertas RSS automáticas en la [página del historial de documentos](#) ARC de Route 53.

AWS políticas administradas para el cambio automático zonal en Amazon Route 53 Application Recovery Controller

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 por AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: AWSZonalAutoshiftPracticeRunSLRPolicy

No puede asociar AWSZonalAutoshiftPracticeRunSLRPolicy a sus entidades IAM. Esta política está asociada a un rol vinculado a un servicio que permite a Amazon Route 53 Application Recovery Controller 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)

Para obtener más información, consulte [Uso de la función vinculada al servicio para el cambio automático zonal en Route 53 ARC](#).

Actualizaciones de las políticas AWS gestionadas para el cambio automático zonal

Para obtener más información sobre las actualizaciones de las políticas AWS administradas para el cambio automático zonal en Route 53 ARC desde que este servicio comenzó a rastrear estos cambios, consulte. [Actualizaciones de las políticas AWS administradas para Amazon Route 53 Application Recovery Controller](#) Para obtener alertas automáticas sobre cambios en esta página, suscríbese a la fuente RSS en la [página de historial de documentos](#) de Route 53 ARC.

Utilice el control de enrutamiento para recuperar aplicaciones de varias regiones en Amazon Route 53 Application Recovery Controller

En esta sección, se explica cómo utilizar la capacidad de control de enrutamiento de Amazon Route 53 Application Recovery Controller 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 preparación, una función de Route 53 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 del controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Comprobación de disponibilidad del controlador de recuperación de aplicaciones de Amazon Route 53](#)

Control de enrutamiento del controlador de recuperación de aplicaciones de Amazon Route 53

Para conmutar por error el tráfico a varias réplicas de aplicaciones Regiones de AWS, puede utilizar los controles de enrutamiento de Amazon Route 53 Application Recovery Controller 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 Route 53 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 Route 53 ARC crea para el 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 Route 53 ARC es un plano de datos de puntos finales en cinco Regiones de AWS.

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 Route 53 ARC para redirigir el tráfico como parte de un plan de conmutación por error para su aplicación en un escenario de desastre, consulte [Mejores prácticas para el control de enrutamiento en Route 53 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 Route 53 ARC lo actualice para configurarlo como correcto o incorrecto, según el estado del 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 un estado de control de enrutamiento y poder redirigir el tráfico, debe conectarse a uno de los puntos finales del clúster en Route 53 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 configurar los 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 mediante el control de enrutamiento de Route 53 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 Route 53 Application Recovery Controller, 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, consulta [Cómo garantizar que los cambios de tráfico finalicen rápidamente](#).

Cómo utilizar el control de enrutamiento

Un control de enrutamiento de Route 53 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 instancias de Amazon EC2, en función de las comprobaciones de estado en el 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.

A continuación, se muestra 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 Route 53 Application Recovery Controller, consulte los [puntos de enlace y las cuotas de Amazon Route 53 Application Recovery Controller](#) en la Referencia general de Amazon Web Services.

Note

El control de enrutamiento de Amazon Route 53 Application Recovery Controller 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 de Regional Route 53. Es decir, cuando crea recursos como clústeres, paneles de control o controles de enrutamiento.

Un control de enrutamiento ARC de Route 53 es un conmutador de encendido/apagado que cambia el estado de una comprobación de estado del ARC de Route 53, que luego 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 de Route 53, altamente confiables, para realizar consultas de control de enrutamiento y actualizaciones de estado del control de enrutamiento, puede confiar en Route 53 ARC para la conmutación por error durante los escenarios de recuperación ante desastres. Para obtener más información, consulte [Obtener y actualizar los estados de control de enrutamiento mediante la API de Route 53 ARC \(recomendado\)](#).

Route 53 ARC mantiene los estados de control de enrutamiento en un clúster, que es un conjunto de cinco puntos finales regionales redundantes. Route 53 ARC propaga los cambios de estado del control de enrutamiento en todo el clúster, que se encuentra en una flota de Amazon EC2, para conseguir quórum en cinco regiones. AWS Tras la propagación, cuando consulta a Route 53 ARC para obtener un estado de control de enrutamiento mediante la API y el plano de datos de alta confiabilidad, 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, `Off On`. Luego, Route 53 ARC propaga la actualización en 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.

Route 53 ARC ofrece una confiabilidad extrema con su plano de datos para que pueda conmutar manualmente su aplicación entre celdas. Route 53 ARC garantiza que siempre pueda acceder al menos a tres de los cinco puntos finales del clúster para realizar cambios de estado del control de enrutamiento. Tenga en cuenta que cada clúster ARC de Route 53 es de un solo inquilino, para garantizar que no se vea afectado por «vecinos ruidosos» que puedan ralentizar sus patrones de acceso.

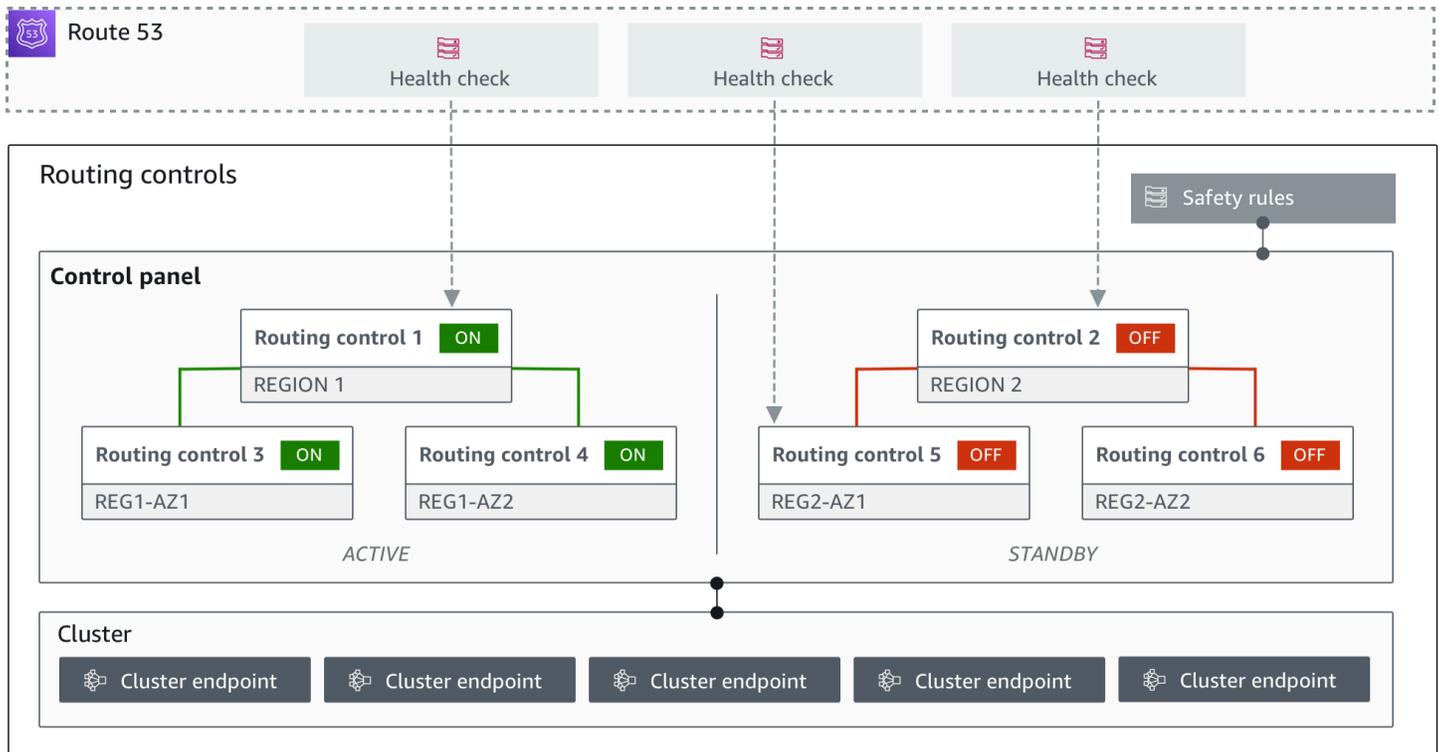
Al realizar cambios en los estados del control de enrutamiento, se basa en los tres criterios siguientes, que es muy poco probable que no den resultado:

- 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 en Route 53 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, Route 53 ARC cambia las comprobaciones de estado de 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 Route 53 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 sencillo conmutador de encendido/apagado, alojado en un clúster, que se utiliza para controlar el enrutamiento del tráfico de clientes que entra y sale de las celdas. Cuando crea un control de enrutamiento, agrega una verificación de estado ARC de Route 53 en Route 53. Esto le permite redirigir el tráfico (mediante las comprobaciones de estado, configuradas con registros DNS para sus aplicaciones) al actualizar el estado del control de enrutamiento en Route 53 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, Route 53 ARC actualiza las comprobaciones de estado correspondientes, que redirigen el tráfico, por ejemplo, a la conmutación 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, Route 53 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 Route 53 ARC tiene cinco puntos finales regionales que puede usar para configurar y recuperar los estados de control de enrutamiento. Su proceso de acceso a los puntos finales debe suponer que Route 53 ARC sube y baja los puntos finales con regularidad

para realizar tareas de mantenimiento, por lo que debe probar cada punto final sucesivamente hasta que se conecte a uno. 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, consulte [Mejores prácticas para el control de enrutamiento en Route 53 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 Route 53 Application Recovery Controller

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 de Route 53 ARC:

- Clústeres
- Paneles de control
- Normas de seguridad

El etiquetado en Route 53 ARC solo está disponible a través de la API, por ejemplo, mediante. 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 [TagResource](#) de referencia de la API de configuración de control de recuperación para Amazon Route 53 Application Recovery Controller.

Precios para el control de enrutamiento en Route 53 ARC

Con el Controlador de recuperación de aplicaciones de Amazon Route 53, solo paga por lo que configura para usarlo en el servicio. Para el control de enrutamiento en Route 53 ARC, 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 Route 53 ARC](#).

Para obtener información detallada sobre los precios de Route 53 ARC y ejemplos de precios, consulte los [precios de Amazon Route 53 Application Recovery Controller](#) y desplácese hacia abajo hasta Amazon Route 53 Application Recovery Controller.

Introducción a la recuperación multirregional en Amazon Route 53 Application Recovery Controller

Para realizar la conmutación por error de sus aplicaciones mediante el control de enrutamiento de Amazon Route 53 Application Recovery Controller, debe tener AWS aplicaciones que estén en varias 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 Amazon Route 53 Application Recovery Controller](#).

Para poder usar el control de enrutamiento ARC de Route 53 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, proporcionamos 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 Route 53 Application Recovery Controller 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 del control de enrutamiento en el AWS Management Console tráfico de conmutación por error, pero le recomendamos que, en su lugar, utilice las acciones ARC de Route 53, 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 usar la acción de la API para establecer el estado de to y to. `update-routing-control-state 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 plantillas descargables AWS CloudFormation y de HashiCorp Terraform con una aplicación de ejemplo para que pueda explorar rápidamente la configuración y el uso de Route 53 ARC por sí mismo.

Después de implementar la aplicación de ejemplo, puede usar las plantillas para crear componentes de Route 53 ARC y, a continuación, explorar el uso de los controles de enrutamiento para administrar el flujo de tráfico hacia la aplicación. Puede adaptar las plantillas y el proceso a sus propios escenarios y aplicaciones.

- AWS CloudFormation: Para empezar con un ejemplo de aplicación y AWS CloudFormation plantillas, consulte las instrucciones de README que aparecen aquí en este [bucket de Amazon](#)

[S3](#). Puede obtener más información sobre el uso de AWS CloudFormation plantillas leyendo [AWS CloudFormation los conceptos](#) de la Guía del AWS CloudFormation usuario.

- HashiCorp Terraform: Para empezar con una aplicación de muestra y plantillas de Terraform, consulte las instrucciones README que aparecen aquí en este bucket de [Amazon S3](#). [Puede obtener más información sobre el uso de las plantillas de Terraform leyendo la documentación.](#) [HashiCorp](#)

Mejores prácticas para el control de enrutamiento en Route 53 ARC

Recomendamos las siguientes prácticas recomendadas para la preparación de la recuperación y la conmutación por error para el control de enrutamiento en Amazon Route 53 Application Recovery Controller.

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 sus cinco puntos finales del clúster regional y los ARN de control de enrutamiento](#)
- [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 Route 53 ARC con la API del plano de datos del clúster de recuperación, puede adjuntar una política de IAM de Route 53 ARC a su usuario. Para obtener más información, consulte [Ejemplos de políticas basadas en identidad en Amazon Route 53 Application Recovery Controller](#).

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 utiliza los controles de enrutamiento para cambiar de uno Región de AWS a otro, el mecanismo que Amazon Route 53 Application Recovery Controller utiliza para mover el tráfico de las 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 que esté en línea con el 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.

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

Le recomendamos que guarde una copia local de los puntos finales del clúster regional de Route 53 ARC, en marcadores o guardada en el código de automatización que utilice para volver a intentar los puntos de enlace. Durante un caso de error, es posible que no pueda acceder a algunas operaciones de la API, incluidas las operaciones de la API de Route 53 ARC que no están alojadas en el clúster del plano de datos extremadamente confiable. Puede enumerar los puntos finales de sus clústeres ARC de Route 53 mediante la operación de [DescribeCluster](#) API.

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

Le recomendamos que, cuando necesite realizar una conmutación por error, actualice (y recupere) los estados del control de enrutamiento mediante un punto de conexión aleatorio de los cinco puntos de conexión regionales del clúster. Si se produce un error en ese punto de conexión, vuelva a intentarlo con cada uno de los demás puntos de conexión regionales. 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 SDK](#)

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 de Route 53, consulte los controles y estados de enrutamiento con la operación [ListRoutingControls](#) y actualice los estados del control de enrutamiento para redirigir el tráfico y realizar la conmutación por error con la [UpdateRoutingControlState](#) operación. Puedes usar el código AWS CLI ([como en estos ejemplos](#)) o el que escribas con uno de los AWS SDK. Route 53 ARC ofrece una fiabilidad 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 de conexión regionales del clúster para que Route 53 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 Route 53 ARC

Pruebe la conmutación por error con regularidad con el control de enrutamiento de Route 53 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 de Route 53 ARC que has agregado estén alineadas con los recursos correctos de tu pila y de que todo funcione como esperabas. Debe probar esto después de configurar Route 53 ARC para el entorno y continuar realizando pruebas periódicamente para que el entorno de conmutación por error esté preparado antes de que se produzca una situación de error en la que necesite que el sistema secundario esté listo y funcionando rápidamente para evitar el tiempo de inactividad de los usuarios.

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 Route 53 Application Recovery Controller, 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 de Route 53 con AWS CLI](#).

En la siguiente tabla, se enumeran las operaciones de la API ARC de Route 53 que puede usar para la configuración del control de enrutamiento, con enlaces a la documentación relevante.

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Crear un clúster	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte CreateCluster .
Describir un clúster	Consulte Creación de componentes del control de	Consulte DescribeCluster .

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
	enrutamiento de Route 53 ARC	
Eliminar un clúster	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte DeleteCluster .
Listar los clústeres de una cuenta	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte ListClusters .
Creación de un control de enrutamiento	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte CreateRoutingControl
Describa un control de enrutamiento	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte DescribeRoutingControl
Actualización de control de enrutamiento	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte UpdateRoutingControl
Eliminación de un control de enrutamiento	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte DeleteRoutingControl

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Listar los controles de enrutamiento	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte ListRoutingControles
Creación de un panel de control	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Consulte el CreateControlpanel
Describa un panel de control	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Ver DescribeControlpanel
Actualización de un panel de control	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Ver UpdateControlpanel
Eliminación de un panel de control	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Ver DeleteControlpanel
Descripción de paneles de control	Consulte Creación de componentes del control de enrutamiento de Route 53 ARC	Ver ListControlpaneles
Creación de una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Ver CreateSafetyregla

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Describa una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Ver DescribeSafetyregla
Actualice una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Ver UpdateSafetyregla
Eliminación de una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Ver DeleteSafetyregla
Enumere las reglas de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Consulte ListSafetylas reglas
Enumere comprobaciones de estado asociadas de Route 53	Consulte Creación de una comprobación de estado de control de enrutamiento de Route 53 ARC	Ver ListAssociatedRuta 53 HealthChecks
Enumere las políticas AWS IAM de recursos para compartir clústeres	Consulte Support multicuenta para clústeres en Route 53 ARC	Consulte la GetResourcepolítica

En la siguiente tabla, se enumeran las operaciones comunes de la API ARC de Route 53 que puede usar para administrar la conmutación por error de tráfico con el plano de datos de control de enrutamiento, con enlaces a la documentación relevante.

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Obtener el estado de un control de enrutamiento	Consulte Obtener y actualizar los estados de control de	Consulte GetRoutingControlState

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
	enrutamiento en el AWS Management Console	
Listar los controles de enrutamiento	N/A	Consulte ListRoutingControles
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	Ver UpdateRoutingControlStates

Uso de este servicio con un AWS SDK

AWS Los kits de desarrollo de software (SDK) 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 for C++	AWS SDK for C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK for Go	AWS SDK for Go ejemplos de código
AWS SDK for Java	AWS SDK for Java ejemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código

Documentación de SDK	Ejemplos de código
AWS SDK for .NET	AWS SDK for .NET ejemplos de código
AWS SDK for PHP	AWS SDK for PHP ejemplos de código
AWS Tools for PowerShell	Herramientas para ejemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) ejemplos de código
AWS SDK for Ruby	AWS SDK for 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 SDK](#).

 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 de Route 53 con AWS CLI

En esta sección, se describen ejemplos de aplicaciones sencillas que muestran cómo trabajar con el control de enrutamiento y cómo AWS Command Line Interface trabajar con la capacidad de control de enrutamiento de Amazon Route 53 Application Recovery Controller 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 Route 53 Application Recovery Controller, 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 de Route 53 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

Route 53 ARC es un servicio global que admite varios Regiones de AWS puntos finales. Sin embargo, debe especificar la región EE.UU. Oeste (Oregón), es decir, especificar el parámetro, en la mayoría de los comandos `--region us-west-2` ARC CLI de Route 53. Por ejemplo, utilice el `region` parámetro cuando cree grupos de recuperación, paneles de control y clústeres.

Al crear un clúster, Route 53 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 del 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 de Route 53 es un conjunto de cinco puntos finales, uno en cada uno de los cinco diferentes Regiones de AWS. La infraestructura ARC de Route 53 permite que estos puntos finales funcionen de forma coordinada para garantizar la alta disponibilidad y la coherencia secuencial de las operaciones de conmutación por error.

1. Crear un clúster

1a. Cree un clúster.

```
aws route53-recovery-control-config --region us-west-2 create-cluster --cluster-name
NewCluster
```

```
{
  "Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
    "Name": "NewCluster",
    "Status": "PENDING"
  }
}
```

La primera vez que crea un recurso de Route 53 ARC, tiene el estado de 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::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
    "ClusterEndpoints":[
      {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
      {"Endpoint": "https://host-bbbbbbb.ap-southeast-2.example.com",
"Region":"ap-southeast-2"},
      {"Endpoint": "https://host-ccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
      {"Endpoint": "https://host-ddddd.us-west-2.example.com", "Region":"us-
west-2"},
      {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
"Region":"ap-northeast-1"}
    ]
    "Name": "NewCluster",
```

```

    "Status": "DEPLOYED"
  }
}

```

Cuando el estado es IMPLEMENTADO, Route 53 ARC ha creado correctamente el clúster con el conjunto de puntos de conexión 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
```

```

{
  "Clusters": [
    {
      "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/1234abcd-abcd-1234-abcd-1234abcdefg",
      "ClusterEndpoints": [
        {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region": "us-
east-1"},
        {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
"Region": "ap-southeast-2"},
        {"Endpoint": "https://host-ccccc.eu-west-1.example.com", "Region": "eu-
west-1"},
        {"Endpoint": "https://host-ddddd.us-west-2.example.com", "Region": "us-
west-2"},
        {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
"Region": "ap-northeast-1"}
      ],
      "Name": "AnotherCluster",
      "Status": "DEPLOYED"
    },
    {
      "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefg",
      "ClusterEndpoints": [
        {"Endpoint": "https://host-ffffff.us-east-1.example.com", "Region": "us-
east-1"},
        {"Endpoint": "https://host-gggggg.ap-southeast-2.example.com",
"Region": "ap-southeast-2"},
        {"Endpoint": "https://host-hhhhhh.eu-west-1.example.com", "Region": "eu-
west-1"},

```

```

        {"Endpoint": "https://host-iiiiii.us-west-2.example.com", "Region": "us-
west-2"},
        {"Endpoint": "https://host-jjjjjj.ap-northeast-1.example.com",
"Region": "ap-northeast-1"}
    ],
    "Name": "NewCluster",
    "Status": "DEPLOYED"
}
]
}

```

2. Creación de un panel de control

Un panel de control es una agrupación lógica para organizar los controles de enrutamiento de Route 53 ARC. Al crear un clúster, Route 53 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-5678abcdefg",
      "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/0123456bbbbbbb0123456bbbbbbb0123456",  
    "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-  
abcd-5678-abcd-5678abcdefgh",  
    "DefaultControlPanel": false,  
    "Name": "NewControlPanel2",  
    "RoutingControlCount": 0,  
    "Status": "PENDING"  
  }  
}
```

La primera vez que crea un recurso de Route 53 ARC, tiene el estado PENDING mientras se crea. 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/0123456bbbbbbb0123456bbbbbbb0123456
```

```
{  
  "ControlPanel": {  
    "ControlPanelArn": "arn:aws:route53-recovery-  
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",  
    "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 de Route 53 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/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
  "RoutingControl": {
    "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",
    "Name": "NewRc1",
    "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/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/0123456bbbbbbb0123456bbbbbbb0123456
```

```
{
  "RoutingControls": [
    {
      "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",
      "Name": "Rc1",
      "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
abcdefg1234567",
      "Status": "DEPLOYED"
    },
    {
      "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",
```

```

        "Name": "Rc2",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/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 protecciones, 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 On 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 [AssertionRule](#) la Guía de referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53.

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 `RoutingControls` 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 [GatingRule](#) la Guía de referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53.

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 [0123456bbbbbbb0123456bbbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbbb0123456333333444444

```

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 de Route 53 configura la comprobación de estado para que falle, de modo que Route 53 redirija 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 Route 53 ARC para crear un control de enrutamiento para cada celda.
2. Use la CLI de Route 53 para crear una verificación de estado de Route 53 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-5678abcdefg
```

```
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-5678abcdefg
```

5b. Cree una comprobación de estado para cada control de enrutamiento.

 Note

Las comprobaciones de estado de Route 53 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/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
  "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
  "HealthCheck": {
    "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
    "CallerReference": "RoutingControlCell1",
    "HealthCheckConfig": {
      "Type": "RECOVERY_CONTROL",
      "Inverted": false,
      "Disabled": false,
      "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/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/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
  "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
  "HealthCheck": {
    "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
    "CallerReference": "RoutingControlCell2",
    "HealthCheckConfig": {
      "Type": "RECOVERY_CONTROL",
      "Inverted": false,
      "Disabled": false,
      "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/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 comandos de Amazon Route 53 para el AWS CLI comando [change-resource-record-sets](#). 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": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx"
}

```

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 Route 53 Application Recovery Controller, 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, Route 53 ARC le proporciona un conjunto de puntos de conexión de clúster, uno de cada cinco Regiones de AWS. Debe especificar uno de estos puntos de enlace regionales (el punto de enlace 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 `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 finales regionales y estén preparados para volver a intentarlo con cada uno de los puntos finales disponibles. Para ver ejemplos de código que ilustran cómo probar los puntos de conexión de un clúster de forma secuencial, consulte [Acciones para el controlador de recuperación de aplicaciones mediante AWS SDK](#).

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. Route 53 ARC ofrece una fiabilidad extrema con el plano de datos de control de enrutamiento de Route 53 ARC para redirigir el tráfico y conmutar por

error entre las celdas. Para obtener más recomendaciones sobre el uso de Route 53 ARC para la conmutación por error, consulte [Mejores prácticas para el control de enrutamiento en Route 53 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 `ClusterEndpoint` incluye una región y el punto final correspondiente que puede usar para obtener o actualizar los estados del control de enrutamiento. [DescribeCluster](#) es una operación de API de configuración de control de recuperación. Le recomendamos que guarde una copia local de los puntos finales del clúster regional de Route 53 ARC, en marcadores o codificada en el código de automatización que utilice para volver a probar los puntos de enlace.

1. Listar los controles de enrutamiento

Puede ver sus controles de enrutamiento y sus estados de control de enrutamiento utilizando los puntos finales del plano de datos de Route 53 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/0123456bbbbbbb0123456bbbbbbb0123456 \  
    --region us-west-2 \  
    --endpoint-url https://host-ddddd.us-west-2.example.com/v1
```

```
{  
  "RoutingControls": [{  
    "ControlPanelArn": "arn:aws:route53-recovery-  
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",  
    "ControlPanelName": "ExampleControlPanel",  
    "RoutingControlArn": "arn:aws:route53-recovery-  
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/  
abcdefg1234567",
```

```

    "RoutingControlName": "RCOne",
    "RoutingControlState": "On"
  },
  {
    "ControlPanelArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",
    "ControlPanelName": "ExampleControlPanel",
    "RoutingControlArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
zzzzxxxxyyyyy123456",
    "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/0123456bbbbbbb0123456bbbbbbb0123456/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/0123456bbbbbbb0123456bbbbbbb0123456/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 On. 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/0123456bbbbbbb0123456bbbbbbb0123456/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/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
abcdefg1234567",
  "RoutingControlState": "Off"}, \
  {"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/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 Route 53 ARC

Temas

- [Creación de componentes del control de enrutamiento de Route 53 ARC](#)
- [Visualización y actualización de los estados de control de enrutamiento en Route 53 ARC](#)
- [Crear reglas de seguridad para el control de rutas](#)

- [Support multicuenta para clústeres en Route 53 ARC](#)

Creación de componentes del control de enrutamiento de Route 53 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 del controlador de recuperación de aplicaciones de Amazon Route 53.

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 compartido de recursos mediante AWS Resource Access Manager, de modo que un clúster pueda alojar controles de enrutamiento y otros recursos ARC de Route 53 que sean propiedad de varios Cuentas de AWS. Para obtener información sobre el uso compartido de recursos en Route 53 ARC, [Support multicuenta para clústeres en Route 53 ARC](#). Para obtener información sobre los precios, consulte los [precios de Amazon Route 53 Application Recovery Controller](#) 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](#).

En estas secciones se incluyen los pasos para crear los componentes para el control de enrutamiento en la consola de Route 53 ARC. Para obtener información sobre el uso de las operaciones de la API de configuración de control de recuperación con Route 53 ARC, consulte la [Operaciones de la API de control de enrutamiento](#).

Creación de un clúster en Route 53 ARC

Debe crear un clúster para alojar los controles de enrutamiento y los paneles de control en Route 53 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.

Pasos para crear un clúster

1. Abra la consola ARC de Route 53 en <https://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 de Route 53 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 que tenga 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 de Route 53 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.

Creación de una comprobación de estado de control de enrutamiento de Route 53 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, simplemente actualice el estado del control de enrutamiento asociado para redirigir el tráfico en el controlador de recuperación de aplicaciones de Amazon Route 53 y establecerlo en On o 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 de Route 53 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 Route 53 ARC conmute correctamente el tráfico 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 de Route 53 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 de Route 53, consulte [Ejemplos del uso de las operaciones de la API de control de enrutamiento ARC de Route 53 con AWS CLI](#).

Creación de un panel de control en Route 53 ARC

El panel de control del controlador de recuperación de aplicaciones de Amazon Route 53 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, Route 53 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.

En esta sección se incluyen los pasos para crear un panel de control en la consola de Route 53 ARC. Para obtener información sobre el uso de las operaciones de la API de configuración de control de recuperación con Route 53 ARC, consulte [Operaciones de la API de control de enrutamiento](#).

Creación de un panel de control

1. Abra la consola ARC de Route 53 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 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 Route 53 ARC

En esta sección se describe cómo ver y actualizar los estados del control de enrutamiento en el controlador de recuperación de aplicaciones de Amazon Route 53. 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 a veces, son zonas de disponibilidad que incluyen sus recursos. Si el estado de un control de enrutamiento es On, 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 un estado de control de enrutamiento en la consola de Route 53 ARC o mediante la API ARC de Route 53. Le recomendamos que actualice los estados del control de enrutamiento mediante la API. En primer lugar, Route 53 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 de Route 53 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 de Route 53 ARC (recomendado)

Le recomendamos que utilice las operaciones de la API de Amazon Route 53 Application Recovery Controller 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 de Route 53 con uno de AWS los SDK. 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.

Route 53 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. Route 53 ARC garantiza que siempre pueda acceder al menos a tres de los cinco puntos de conexión regionales del clúster 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 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 Route 53 ARC para obtener y actualizar los estados de control de enrutamiento y trabajar con puntos de conexión regionales del clúster. Para 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 el controlador de recuperación de aplicaciones mediante AWS SDK](#).
- Para obtener información sobre cómo usar el AWS CLI para obtener y actualizar los estados del 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 ningún proceso para elegir y rotar los puntos de conexión del clúster en la consola, como se puede hacer con la API del controlador de recuperación de aplicaciones de Amazon Route 53. Además, la consola no tiene una alta disponibilidad, mientras que el plano de datos de Route 53 ARC ofrece una fiabilidad extrema. Por estos motivos, recomendamos que utilice la API de Route 53 ARC para obtener y actualizar los estados de control de enrutamiento de las operaciones de producción.

Para obtener más recomendaciones sobre el uso de Route 53 ARC para la conmutación por error, consulte [Mejores prácticas para el control de enrutamiento en Route 53 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 de Route 53 en <https://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. Abra la consola de Amazon Route 53 en <https://console.aws.amazon.com/route53/home>.
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 contar con 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 Route 53 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, al cambiar uno o un conjunto de estados de control de enrutamiento, Route 53 ARC exige que se cumplan los criterios que estableció al configurar la regla, o de lo contrario, no se 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 de Route 53 con AWS CLI](#).

Para obtener información detallada sobre las propiedades de operación de la API de reglas de aserción, consulte [AssertionRule](#) la Guía de referencia de la API de control de enrutamiento para Amazon Route 53 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 de Route 53 con AWS CLI](#).

Para obtener información detallada sobre las propiedades de operación de la API de la regla de bloqueo, consulte [GatingRule](#) la Guía de referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53.

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 de Route 53 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 recuperación y control de enrutamiento con el controlador de recuperación de aplicaciones Amazon Route 53, consulte [Operaciones de la API de control de enrutamiento](#).

Creación de una regla de seguridad

1. Abra la consola ARC de Route 53 en <https://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 [AssertionRule](#) funcionamiento en la Guía de referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53. Para obtener más información sobre cómo especificar una regla de bloqueo, consulte la información proporcionada sobre la [GatingRule](#) operación en la Guía de

referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53.

8. Seleccione Crear.

Modificación o eliminación de una regla de seguridad en la consola

En los pasos de esta sección se explica cómo modificar o eliminar una regla de seguridad en la consola de Route 53 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 operaciones de API con Amazon Route 53 Application Recovery Controller, consulte [Operaciones de la API de control de enrutamiento](#).

Eliminación de una regla de seguridad

1. Abra la consola ARC de Route 53 en <https://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 de ARN separados por comas 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 los ARN de reglas de seguridad a la lista de reglas que desee anular en el comando update, separados por comas, hasta que el comando update se complete correctamente.

Para obtener más información sobre el uso de la `SafetyRulesToOverride` propiedad con la API y los SDK, 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/0123456bbbbbbb0123456bbbbbbb0123456/  
routingcontrol/abcdefg1234567 \  
  --routing-control-state On \  
  --safety-rules-to-override "arn:aws:route53-recovery-  
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/safetyrule/  
yyyyyyy8888888" \  
  "arn:aws:route53-recovery-  
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/safetyrule/  
qqqqqq7777777" \  
  --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Support multicuenta para clústeres en Route 53 ARC

El controlador de recuperación de aplicaciones Amazon Route 53 se integra AWS Resource Access Manager para permitir el uso compartido de recursos. AWS RAM es un servicio que le permite compartir recursos con otras Cuentas de AWS o a través de ellas AWS Organizations. En Route 53 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 Route 53 ARC, puede utilizar un clúster para alojar los paneles de control y los controles de enrutamiento que pertenecen a varias personas diferentes Cuentas de AWS. Si opta por compartir un clúster, las demás personas Cuentas de AWS que especifique pueden usar 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 (OU) 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 de ejecución del clúster a diferentes equipos para aumentar al máximo los beneficios de Route 53 ARC con un costo menor (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 Route 53 ARC, especialmente si tiene una gran cantidad de aplicaciones distribuidas en varias cuentas y equipos de operaciones.

Para empezar a compartir entre cuentas en Route 53 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. Luego, los participantes pueden crear recursos, como paneles de control y controles de enrutamiento, en el clúster mediante AWS Management Console o ejecutando las operaciones de la API ARC de Route 53 con los AWS SDK AWS Command Line Interface o.

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 el tuyo 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

Al compartir un clúster de su propiedad, los participantes que especifique para compartir el clúster pueden crear y alojar sus propios recursos de Route 53 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 los AWS Command Line Interface AWS SDK.

Si formas parte de una organización AWS Organizations y el uso compartido dentro de ella está activado, los participantes de tu 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 que te pertenezca mediante la AWS RAM consola o mediante las operaciones de la AWS RAM API con los AWS CLI SDK.

Para compartir un clúster de tu propiedad mediante la consola AWS RAM

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](#).

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. Puedes hacerlo mediante la AWS RAM consola o mediante operaciones de AWS RAM API con los AWS CLI SDK.

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 recursos compartidos a través de la consola de Route 53 ARC y AWS CLI.

En general, para obtener más información sobre los recursos que has compartido o que se han compartido contigo, consulta 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 en las operaciones de la API ARC de Route 53 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, consulte el estado de uso compartido del clúster.

Para identificar si un clúster de tu propiedad está compartido mediante el AWS CLI

Utilice el comando [get-resource-policy](#): 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 otras 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 API de control de enrutamiento ARC de Route 53](#) mediante los AWS SDK AWS Command Line Interface o.

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 Route 53 ARC se le facturan los costos 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 Route 53 Application Recovery Controller](#) y desplácese hacia abajo hasta el controlador de recuperación de aplicaciones de Amazon Route 53.

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 lo 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, consulte [Cuotas para el control de enrutamiento](#).

Registro y supervisión para el control de enrutamiento en Amazon Route 53 Application Recovery Controller

Puede usarlo AWS CloudTrail para monitorear el control de enrutamiento en Amazon Route 53 Application Recovery Controller, para analizar patrones y ayudar a solucionar problemas.

Temas

- [Registro de llamadas a la API ARC de Route 53 mediante AWS CloudTrail](#)

Registro de llamadas a la API ARC de Route 53 mediante AWS CloudTrail

El controlador de recuperación de aplicaciones Amazon Route 53 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 Route 53 ARC. CloudTrail captura todas las llamadas a la API para Route 53 ARC como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de Route 53 ARC y las llamadas de código a las operaciones de la API de Route 53 ARC.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Route 53 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 Route 53 ARC, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

Información sobre Route 53 ARC en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce actividad en Route 53 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 los eventos en su territorio Cuenta de AWS, incluidos los eventos de Route 53 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 ARC de Route 53 se registran CloudTrail y documentan en la Guía de [referencia de la API de preparación para el controlador de recuperación de aplicaciones Amazon Route 53](#), la Guía de [referencia de la API de configuración de control de recuperación para el controlador de recuperación de aplicaciones Amazon Route 53](#) y la [Guía de referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53](#). 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 lo 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 [CloudTrail UserIdentity](#).

Visualización de eventos de Route 53 ARC en el historial de eventos

CloudTrail permite ver los eventos recientes en el historial de eventos. Para ver los eventos de solicitudes de API de Route 53 ARC, debe elegir Oeste de EE. UU. (Oregón) en el selector de regiones de la parte superior de la consola. Para obtener más información, consulte [Uso del historial de CloudTrail eventos](#) en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de archivos de registro de Route 53 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 boto3/2.0.0dev7",
  "requestParameters": {
    "RoutingControlName": "XYZRoutingControl3",
    "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/routingcontrol/
abcdefg1234567"
  },
  "responseElements": {
    "RoutingControl": {
      "ControlPanelArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456",
      "Name": "XYZRoutingControl3",
      "Status": "DEPLOYED",
      "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbbb0123456/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

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para

utilizar recursos de Route 53 ARC. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Contenido

- [Cómo funciona el control de enrutamiento de Amazon Route 53 Application Recovery Controller con IAM](#)
- [Ejemplos de políticas basadas en identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)
- [AWS políticas administradas para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)

Cómo funciona el control de enrutamiento de Amazon Route 53 Application Recovery Controller con IAM

Antes de usar IAM para administrar el acceso al control de enrutamiento en Amazon Route 53 Application Recovery Controller, 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 Route 53 Application Recovery Controller

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
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí

Característica de IAM	Soporte de control de enrutamiento
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 identidades de Route 53 ARC

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 adjunto. Para 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 de Route 53 para el control de enrutamiento, consulte. [Ejemplos de políticas basadas en identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)

Políticas basadas en recursos dentro del control de enrutamiento

Compatibilidad con las políticas basadas en recursos	No
--	----

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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

Admite acciones de política	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 las acciones ARC de Route 53 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 de política en Route 53 ARC para el control de enrutamiento utilizan los siguientes prefijos antes de la acción, según 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 ARC basadas en la identidad de Route 53 para el control de enrutamiento, consulte. [Ejemplos de políticas basadas en identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)

Recursos de políticas para Route 53 ARC

Admite 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 puede 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 \(ARN\)](#). Puede 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, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

En la Referencia de autorización de servicio, puede ver la siguiente información relacionada con Route 53 ARC:

Para ver una lista de tipos de recursos y sus ARN, y las acciones que puede especificar con el ARN de cada recurso, consulte los siguientes temas en la Referencia de autorizaciones de servicio:

- [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 de Route 53 para el control de enrutamiento, consulte. [Ejemplos de políticas basadas en identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)

Claves de condición de la política para Route 53 ARC

Admite 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 puede 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. Puede crear expresiones condicionales que utilicen [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 puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte [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 ARC de Route 53 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 ARN, 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 de Route 53 para el control de enrutamiento, consulte [Ejemplos de políticas basadas en identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)

Listas de control de acceso (ACL) en Route 53 ARC

Admite las ACL

No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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 Route 53 ARC

Admite 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 [¿Qué es 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 de Route 53 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 Route 53 ARC

Compatible con el uso de credenciales temporales	Sí
--	----

Algunos 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 más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) 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 más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos de entidades principales entre servicios de Route 53 ARC

Admite Forward access sessions (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 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](#)

Servicio de roles de Route 53 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.

Roles vinculados a servicios de Route 53 ARC

Compatible con roles vinculados al servicio	Sí
---	----

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 identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Route 53 ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la 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 puede añadir las políticas de IAM a roles y los usuarios pueden 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](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Route 53 ARC, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición del controlador de recuperación de aplicación de Amazon Route 53 ARC](#) en la Referencia de autorizaciones de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Ejemplo: acceso a la consola Route 53 ARC para el control de enrutamiento](#)
- [Ejemplos: acciones de la API ARC de Route 53 para la configuración del control de enrutamiento](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Route 53 ARC de la 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, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) 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, consulte [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, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice 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 [Política de validación de Analizador de acceso de IAM](#) en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

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

Ejemplo: acceso a la consola Route 53 ARC para el control de enrutamiento

Para acceder a la consola del controlador de recuperación de aplicación de Amazon Route 53, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver

detalles sobre los recursos ARC de Route 53 en su 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 conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite 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 usando la consola ARC de Route 53 cuando solo se permite el acceso a operaciones de API específicas, adjunte también una política `ReadOnly` y AWS administrada para Route 53 ARC a las entidades. Para obtener más información, consulte la [página de políticas administradas de Route 53 ARC](#) o [Añadir permisos a un usuario](#) en la Guía del usuario de IAM.

Para dar a los usuarios acceso total para usar las funciones de control de enrutamiento ARC de Route 53 a través de la consola, adjunte al usuario una política como la siguiente para otorgarle todos los permisos para configurar los recursos y las operaciones del control de enrutamiento ARC de Route 53:

```
{
  "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 de Route 53 para la configuración del control de enrutamiento

Para garantizar que un usuario pueda usar las acciones de la API ARC de Route 53 para trabajar con la configuración de control de enrutamiento ARC de Route 53, adjunte una política que corresponda a las operaciones de 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 ARC de Route 53 con la API del plano de datos del clúster de recuperación, por ejemplo, actualizar los estados del control de enrutamiento para que se produzca una conmutación por error durante un desastre, puede adjuntar a su usuario de IAM una política de IAM de Route 53 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 Route 53 Application Recovery Controller

Una política AWS administrada es una política independiente creada y administrada por 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 por 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 de control de recuperación en Route 53 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:GetHealthCheck,route53:CreateHealthCheck,route53:DeleteHealthCheck, yroute53:ChangeTagsForResource.

Para ver los permisos de esta política, consulte [AmazonRoute53 RecoveryControlConfigFullAccess](#) en la Referencia de políticas AWS gestionadas.

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 concede acceso de solo lectura a las acciones para trabajar con la configuración de control de recuperación en Route 53 ARC. Estos usuarios no pueden crear, actualizar ni eliminar recursos de control de recuperación.

Para ver los permisos de esta política, consulte [AmazonRoute53 RecoveryControlConfigReadOnlyAccess](#) en la Referencia de políticas AWS gestionadas.

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 Route 53 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 [AmazonRoute53 RecoveryClusterFullAccess](#) en la Referencia de políticas AWS gestionadas.

AWS política gestionada: AmazonRoute 53 RecoveryClusterReadOnlyAccess

Puede adjuntar `AmazonRoute53RecoveryClusterReadOnlyAccess` a sus entidades de IAM. Esta política concede acceso de solo lectura al plano de datos del clúster en Route 53 ARC. Estos usuarios pueden recuperar los estados de control de enrutamiento, pero no pueden actualizarlos.

Para ver los permisos de esta política, consulte [AmazonRoute53 RecoveryClusterReadOnlyAccess](#) en la Referencia de políticas AWS gestionadas.

Actualizaciones de las políticas AWS administradas para el control de enrutamiento

Para obtener detalles sobre las actualizaciones de las políticas AWS administradas para el control de enrutamiento en Route 53 ARC desde que este servicio comenzó a rastrear estos cambios, consulte [Actualizaciones de las políticas AWS administradas para Amazon Route 53 Application Recovery Controller](#). Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la [página de historial de documentos](#) de Route 53 ARC.

Cuotas para el control de enrutamiento

El control de enrutamiento de Amazon Route 53 Application Recovery Controller está sujeto a las siguientes cuotas (anteriormente denominadas límites).

Entidad	Cuota
Número de clústeres por cuenta	2
Número de paneles de control por clúster	50

Entidad	Cuota
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 UpdateRoutingControlStates de operación	10
Número de llamadas a la API mutantes a un punto final del clúster, por segundo	3

Comprobación de disponibilidad del controlador de recuperación de aplicaciones de Amazon Route 53

Con la verificación de disponibilidad en Amazon Route 53 Application Recovery Controller, puede obtener información sobre si sus aplicaciones y recursos están preparados para la recuperación. Después de modelar AWS la aplicación en Route 53 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 la aplicación en Route 53 ARC para configurar la estructura que permita que funcionen las comprobaciones de preparación, mediante la creación de

un grupo de recuperación y celdas que describan la aplicación. Luego, puede seguir los pasos para agregar comprobaciones de preparación y alcances de preparación para que Route 53 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 Route 53 Application Recovery Controller?

Una verificación de disponibilidad en Route 53 ARC audita continuamente (a intervalos de un minuto) para detectar desajustes 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 el caso de las cuotas, cuando Route 53 ARC detecta una discrepancia con una comprobación de 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 el estado de preparación de los recursos de un grupo de recuperación (su aplicación) o de celdas individuales (réplicas, que son regiones o zonas de disponibilidad (AZ)).

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 Route 53 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 agregar comprobaciones de preparación, puede supervisar el estado de preparación de varias maneras: con EventBridge, en las acciones de la AWS Management Console API ARC de Route 53 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. Use la [función de autorización entre cuentas](#) de Route 53 ARC para facilitar la configuración y el monitoreo de los recursos distribuidos desde una sola AWS cuenta.

Supervise las réplicas de las aplicaciones con comprobaciones de disponibilidad

Route 53 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 verificación 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. Route 53 ARC inspecciona continuamente (una vez por minuto) su aplicación para garantizar que la capacidad aprovisionada coincida con todas las zonas o regiones de disponibilidad.

La capacidad que inspecciona Route 53 ARC incluye, por ejemplo, el recuento de instancias de Amazon EC2, 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, Route 53 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 preparación para el ARC de Route 53 no están muy disponibles, 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 preparación 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 del control de disponibilidad en Route 53 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

Route 53 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. Route 53 ARC inspecciona continuamente (una vez por minuto) su aplicación para garantizar que la capacidad aprovisionada coincida con todas las zonas o regiones de disponibilidad. La capacidad que inspecciona Route 53 ARC incluye, por ejemplo, el recuento de instancias de Amazon EC2, 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, Route 53 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 preparación para el ARC de Route 53 no están muy disponibles, 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 preparación 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 `NotReady`, creando reglas en ella EventBridge. Para obtener más información, consulte [Uso del control de disponibilidad](#)

en [Route 53 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 preparación del ARC de Route 53 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. Route 53 ARC incluye un grupo de reglas para cada tipo de recurso que admite. Por ejemplo, Route 53 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 Route 53 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` o `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 todas las 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, Route 53 ARC da un paso más en cuanto a las cuotas. Si una comprobación de disponibilidad detecta una discrepancia entre las celdas en cuanto a las cuotas de servicio (el valor máximo para la creación y las operaciones de los recursos) de cualquier recurso compatible, Route 53 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.

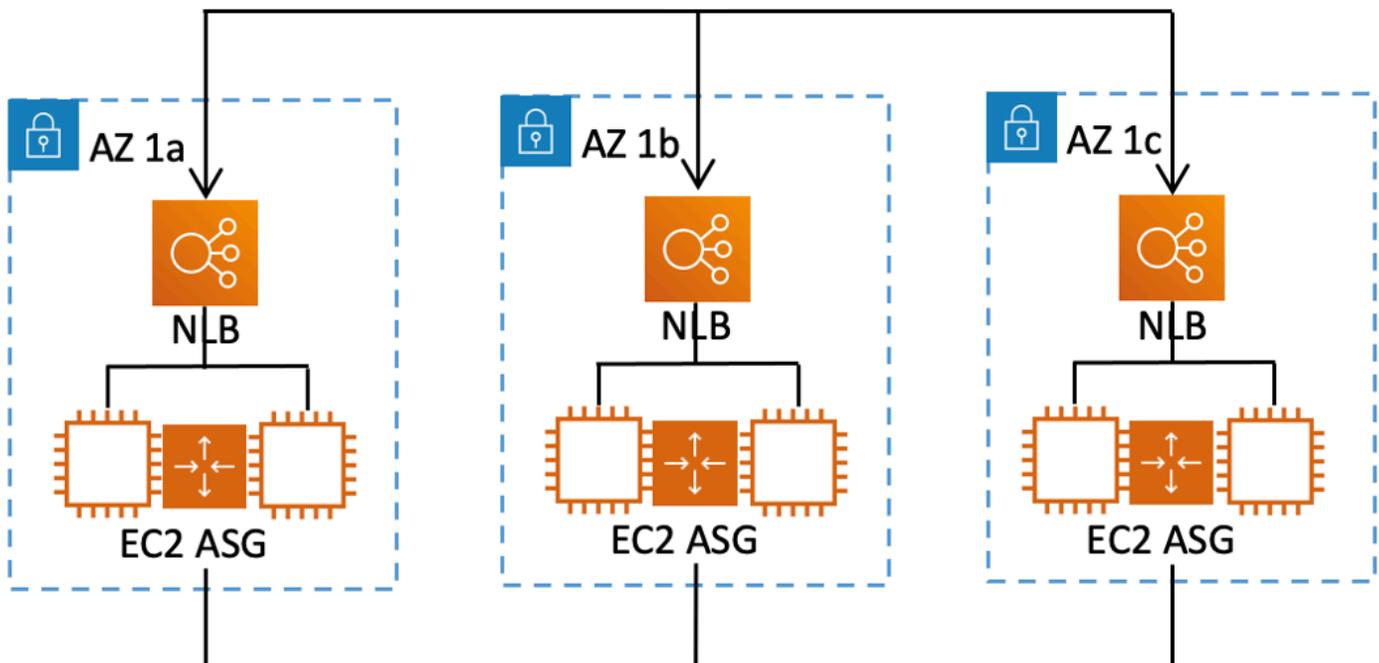
También puedes configurar una EventBridge notificación de Amazon para las comprobaciones de disponibilidad, por ejemplo, cuando el estado de una comprobación de preparación cambie aNOT READY. Luego, cuando se detecta una discrepancia en la configuración, le EventBridge envía una notificación para que 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 del control de disponibilidad en Route 53 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. Puede crear conjuntos de recursos (por separado o mientras 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 Route 53 ARC, de modo que pueda 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 Route 53 ARC mostrar el estado correcto READY o de NOT READY preparación para las comprobaciones resumidas de preparación de los grupos de recuperación y las comprobaciones resumidas de preparación a nivel de celda. A menos que establezca los alcances de preparación, Route 53 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 preparación de los recursos de destino de DNS en Route 53 ARC, puede auditar la preparación de la arquitectura y la 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, Route 53 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.

Route 53 ARC detecta automáticamente el número y el alcance de las celdas (que representan réplicas o unidades de contención de fallas) de su aplicación y si las celdas están agrupadas en silos por zona de disponibilidad o por región. Luego, Route 53 ARC identifica y proporciona información sobre los recursos de la aplicación en las celdas, para determinar si están correctamente aislados 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 Route 53 ARC](#).

Comprobaciones de preparación y escenarios de recuperación ante desastres

Las comprobaciones de preparación para el ARC de Route 53 le permiten saber si sus aplicaciones y recursos están preparados para la recuperación, ya que le ayudan a garantizar que sus aplicaciones estén 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 para el Route 53 ARC se realizan en una sola región de AWS, el oeste de EE. UU. (Oregón), y durante una interrupción o un desastre, la información de verificación de preparación 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 preparados

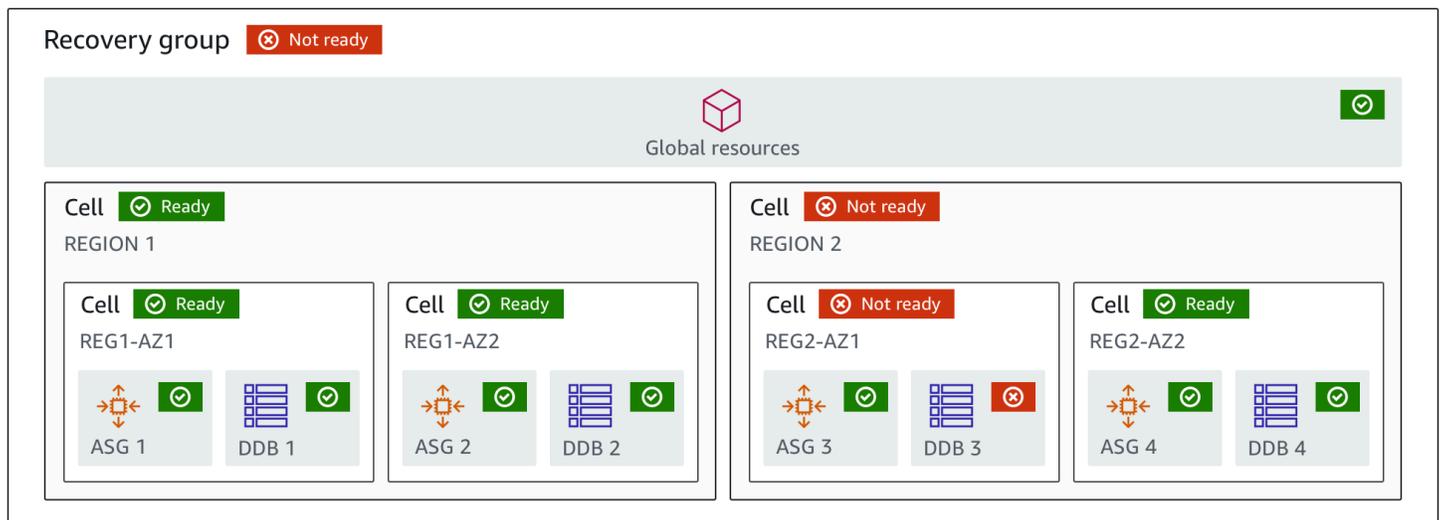
Para obtener información detallada sobre el soporte regional y los puntos de enlace de servicio para Amazon Route 53 Application Recovery Controller, consulte los [puntos de enlace y las cuotas de Amazon Route 53 Application Recovery Controller](#) en la Referencia general de Amazon Web Services.

Note

La comprobación de disponibilidad del controlador de recuperación de aplicaciones Amazon Route 53 es una función global. Sin embargo, los recursos de comprobación 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 los AWS CLI comandos ARC de Regional Route 53, por ejemplo, al crear recursos como conjuntos de recursos y comprobaciones de preparación.

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 preparación de Route 53 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, como las AZ 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 que se replica en us-east-1a y us-east-1b, donde us-east-1b es el entorno de conmutación por error, puede representar esta aplicación en Route 53 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

Cuando crea componentes para las comprobaciones de disponibilidad en Route 53 ARC, 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 Route 53 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 Route 53 ARC para los recursos de destino de 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 los AWS recursos o los recursos de destino del DNS, que abarcan 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. Route 53 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 Route 53 ARC realiza en relación con un conjunto de recursos de un conjunto de recursos. Route 53 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 Route 53 ARC los recursos.

Verificación de preparación

Una comprobación de preparación monitorea un conjunto de recursos de la aplicación, como un conjunto de instancias de Amazon Aurora, para el que Route 53 ARC audita la comprobación de 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 Auto Scaling de Amazon EC2 en dos zonas

de disponibilidad, puede crear una comprobación de preparación para un conjunto de recursos con dos ARN de recursos, uno para cada grupo de Auto Scaling. Luego, para asegurarse de que cada grupo tenga la misma escala, Route 53 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). Para un recurso que sea un recurso global para Route 53 ARC, establezca el alcance de preparación en el nivel de grupo de recuperación o de recurso global. Por ejemplo, una comprobación de estado de Route 53 es un recurso global en Route 53 ARC porque no es específica de una región o zona de disponibilidad.

Planos de datos y control para comprobar la disponibilidad

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 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 Route 53 Application Recovery Controller

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 añade.

Puede etiquetar los siguientes recursos en la comprobación de disponibilidad en Route 53 ARC:

- Conjuntos de recursos
- Comprobador de preparación de

El etiquetado en Route 53 ARC solo está disponible a través de la API, por ejemplo, mediante. AWS CLI

Los siguientes son ejemplos de cómo etiquetar en la verificación 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 [TagResource](#) de referencia de la API de preparación para la recuperación de aplicaciones Amazon Route 53 Application Recovery Controller.

Precios para comprobar la disponibilidad en Route 53 ARC

Con el Controlador de recuperación de aplicaciones de Amazon Route 53, solo paga por lo que configura para usarlo en el servicio. Para la verificación de disponibilidad, usted paga un costo por hora por cada verificación de disponibilidad que configure.

Para obtener información detallada sobre los precios de Route 53 ARC y ejemplos de precios, consulte los [precios de Amazon Route 53 Application Recovery Controller](#) y desplácese hacia abajo hasta Amazon Route 53 Application Recovery Controller.

Configure un proceso de recuperación flexible para su aplicación

Para usar Amazon Route 53 Application Recovery Controller con AWS aplicaciones que se encuentran en varias AWS regiones, hay pautas que debe seguir para configurar sus aplicaciones de manera 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 Route 53 ARC proporciona 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 de Route 53 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 de zona en el controlador de recuperación de aplicaciones de Amazon Route 53](#).

Para obtener más información sobre cómo empezar a utilizar configuraciones de conmutación por error resilientes, consulte [Introducción a la recuperación multirregional en Amazon Route 53 Application Recovery Controller](#)

Mejores prácticas para comprobar la preparación en Route 53 ARC

Recomendamos seguir las siguientes prácticas recomendadas para comprobar la disponibilidad en Amazon Route 53 Application Recovery Controller.

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 aplicación), 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 del control de disponibilidad en Route 53 ARC con Amazon EventBridge](#).

Operaciones de la API de verificación de disponibilidad

En la siguiente tabla se enumeran las operaciones de Route 53 ARC que puede utilizar para prepararse para la recuperación (comprobación de 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 preparación para ARC de Route 53 con AWS CLI](#).

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Creación de una celda	Consulte Creación, actualización y eliminación de grupos	Consulte CreateCell .

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
	de recuperación en Route 53 ARC	
Consigue un móvil	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Consulte GetCell .
Eliminar una celda	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Consulte DeleteCell .
Actualizar una celda	N/A	Consulte UpdateCell
Listar las celdas de una cuenta	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Consulte ListCells .
Creación de un grupo de recuperación	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Ver CreateRecoverygrupo
Crea un grupo de recuperación	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Ver GetRecoverygrupo
Actualizar un grupo de recuperación	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Ver UpdateRecoverygrupo

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Eliminación de un grupo de recuperación	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Ver DeleteRecoverygrupo
Descripción de grupos de recuperación	Consulte Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC	Ver ListRecoverygrupos
Creación de un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver CreateResourceconjunto
Obtenga un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver GetResourceconjunto
Actualización de un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver UpdateResourceconjunto
Eliminar un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver DeleteResourceconjunto
Enumeración de conjuntos de recursos	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver ListResourceconjuntos
Cree una comprobación de disponibilidad	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Consulte CreateReadinessVerificar

Acción	Uso de la consola de Route 53 ARC	Uso de la API de Route 53 ARC
Obtenga una verificación de preparación	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver GetReadinesscheque
Actualice una verificación de preparación	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver UpdateReadinesscheque
Elimine una comprobación de disponibilidad	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver DeleteReadinesscheque
Lista de verificación de preparación	Consulte Creación y actualización de comprobaciones de preparación en Route 53 ARC	Ver ListReadinesscheques
Enumere las reglas de preparación	Consulte Descripciones de las reglas de preparación en Route 53 ARC	Consulte ListRules .
Compruebe el estado de una verificación de disponibilidad completa	Consulte Supervisión del estado de preparación en Route 53 ARC	Consulte GetReadinessCheckStatus
Compruebe el estado de un recurso	Consulte Supervisión del estado de preparación en Route 53 ARC	Ver GetReadinessCheckResourceestado
Compruebe el estado de una celda	Consulte Supervisión del estado de preparación en Route 53 ARC	Consulte GetCellReadinessSummary
Compruebe el estado de un grupo de recuperación	Consulte Supervisión del estado de preparación en Route 53 ARC	Ver GetRecoveryGroupReadinessresumen

Ejemplos del uso de las operaciones de la API de verificación de preparación para ARC de Route 53 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 Route 53 Application Recovery Controller 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 la preparación en las auditorías ARC de Route 53 para detectar discrepancias en los recursos de las réplicas de sus aplicaciones. Para configurar las comprobaciones de preparación de la aplicación, debe configurar (o modelar) los recursos de la aplicación en celdas ARC de Route 53 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 ejemplo sencillo en el que tenemos la aplicación Simple-Service que actualmente se ejecuta en la región del Este de EE. UU. (Norte de Virginia) (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 Route 53 ARC representan los límites de los errores (como las regiones o zonas 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

Route 53 ARC es un servicio global que admite varios puntos de conexión 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 Route 53 ARC.

Por ejemplo, para crear recursos como grupos de recuperación o comprobaciones de disponibilidad.

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 Route 53 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 Route 53 ARC, un grupo de recursos que 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 la aplicación Simple-Service es realmente muy sencilla 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 los recursos de la aplicación Simple-Service.

```
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 la aplicación Simple-Service en Route 53 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 Route 53 ARC, utilice `list-rules` o consulte [Descripciones de las reglas de preparación en Route 53 ARC](#). Route 53 ARC tiene un conjunto específico de reglas que se ejecutan para cada tipo de recurso; por el momento, no se pueden personalizar.

4a. Cree una verificación de preparación 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"  
    }  
  ]  
}
```

Trabajar con grupos de recuperación y comprobaciones 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.

Creación, actualización y eliminación de grupos de recuperación en Route 53 ARC

Un grupo de recuperación representa su aplicación en Amazon Route 53 Application Recovery Controller. 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 (ARN) 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 Route 53 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, agregue las comprobaciones de preparación de Route 53 ARC para los recursos de su aplicación, de modo que Route 53 ARC pueda ayudar a 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 de Route 53 ARC. Para obtener información sobre el uso de operaciones de la API de preparación para la recuperación con Amazon Route 53 Application Recovery Controller, consulte [Operaciones de la API de verificación de disponibilidad](#).

Para crear un grupo de recuperación

1. Abra la consola ARC de Route 53 en <https://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

En los pasos de esta sección se explica cómo actualizar y eliminar un grupo de recuperación y cómo eliminar una celda de la consola ARC de Route 53. Para obtener información sobre el uso de operaciones de la API de preparación para la recuperación con Amazon Route 53 Application Recovery Controller, 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 de Route 53 en <https://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 Route 53 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 de Route 53. Para obtener información sobre el uso de operaciones de la API de preparación para la recuperación con Amazon Route 53 Application Recovery Controller, 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 de Route 53 en <https://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 recursos de Amazon (ARN) 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 Route 53 ARC espera para cada tipo de recurso, consulte [Tipos de recursos y formatos de ARN en Route 53 ARC](#).

7. Si lo desea, consulte las reglas de preparación que se utilizarán cuando Route 53 ARC compruebe el tipo de recurso que incluyó en esta verificación de disponibilidad. A continuación, elija Next.
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 al elegir aquí los ámbitos de preparación, Route 53 ARC no puede devolver información resumida sobre la preparación del grupo o las células de recuperación.

9. Elija 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 de Route 53 en <https://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. En los pasos de esta sección se explica cómo crear o editar un conjunto de recursos en la consola de Route 53 ARC. Para obtener información sobre el uso de operaciones de la API de preparación para la recuperación con Amazon Route 53 Application Recovery Controller, 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/home>.
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 de Route 53 en <https://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 siguientes:
 - 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.

Supervisión del estado de preparación en Route 53 ARC

Puede ver si su aplicación está lista en Amazon Route 53 Application Recovery Controller 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) de 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 CLI de Route 53 ARC.

Notificación del estado de preparación

Puede usar Amazon EventBridge para configurar reglas basadas en eventos para monitorear los recursos ARC de Route 53 y notificarle los cambios en el estado de preparación. Para obtener más información, consulte [Uso del control de disponibilidad en Route 53 ARC con Amazon EventBridge](#).

Monitorear el estado de preparación en la consola de Route 53 ARC

El siguiente procedimiento describe cómo supervisar la preparación para la recuperación en el AWS Management Console

1. Abra la consola ARC de Route 53 en <https://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 Route 53 ARC

Si ya tiene una aplicación, Amazon Route 53 Application Recovery Controller puede evaluar la arquitectura de la aplicación y las políticas de enrutamiento a fin de ofrecer recomendaciones para modificar el diseño a fin de mejorar la resiliencia de recuperación de la aplicación. Después de crear

un grupo de recuperación en Route 53 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, Route 53 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, Route 53 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 de Route 53 en <https://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 Route 53 ARC pueda proporcionar 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 Route 53 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. Route 53 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.

Creación de autorizaciones entre cuentas en Route 53 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 Route 53 Application Recovery Controller, puede utilizar la autorización multicuenta.

La autorización entre cuentas en Route 53 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 de Route 53 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). Route 53 ARC puede permitirle 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 AWS cuentas:

- 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 entre cuentas en cada cuenta adicional que tenga AWS recursos que desee agregar y monitorear en Route 53 ARC.

Note

Route 53 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 Route 53 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 descripciones de las reglas de preparación y los tipos de recursos admitidos, así como el formato de los nombres de recursos de Amazon (ARN) que se utilizan para los conjuntos de recursos.

Descripciones de las reglas de preparación en Route 53 ARC

En esta sección se enumeran las descripciones de las reglas de preparación para todos los tipos de recursos compatibles con Amazon Route 53 Application Recovery Controller. Para ver una lista de los tipos de recursos compatibles con Route 53 ARC, consulte [Tipos de recursos y formatos de ARN en Route 53 ARC](#).

También puede ver las descripciones de las reglas de preparación en la consola de Route 53 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 [ListRules](#) operación.

Temas

- [Reglas de preparación en Route 53 ARC](#)
- [Ver las reglas de preparación en la consola](#)

Reglas de preparación en Route 53 ARC

En esta sección se muestra el conjunto de reglas de preparación para cada tipo de recurso que admite Route 53 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 cómo funciona una regla en el contexto de una verificación de preparación y otros detalles sobre cómo Route 53 ARC establece el estado de preparación, consulte [Cómo las reglas de preparación determinan el estado de preparación](#).

Reglas de preparación

Route 53 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 caché del registro de recursos (TTL) y de que los TTL 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 de EC2.
- **ElbV1AnyInstancesHealthy:** Inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen al menos una instancia de EC2 en buen estado.
- **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 todos los EBS volúmenes para asegurarse de que tienen el mismo valor de cifrado (ACTIVADO o DESACTIVADO).
- **EbsVolumeEncryptionDefault:** inspecciona todos los EBS volúmenes para asegurarse de que tienen el mismo valor de cifrado de forma predeterminada (ACTIVADO o DESACTIVADO).

- `EbsVolumelops`: Inspecciona todos los EBS volúmenes para garantizar que tengan las mismas operaciones de entrada/salida por segundo (IOPS).
- `EbsVolumeKmsKeyId`: inspecciona todos los EBS volúmenes para asegurarse de que tienen el mismo identificador de AWS KMS clave predeterminado.
- `EbsVolumeMultiAttach`: inspecciona todos los EBS volúmenes para asegurarse de que tienen el mismo valor para la conexión múltiple (ACTIVADA o DESACTIVADA).
- `EbsVolumeQuotas`: Inspecciona todos los EBS volúmenes para asegurarse de que se ajustan a las cuotas (límites) establecidas por Service Quotas.
- `EbsVolumeSize`: inspecciona todos los EBS volúmenes para asegurarse de que tienen el mismo tamaño legible.
- `EbsVolumeState`: inspecciona todos los EBS volúmenes para asegurarse de que tienen el mismo estado de volumen.
- `EbsVolumeType`: inspecciona todos los 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 EC2 en buen estado.
- `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 instancia de Amazon EC2.
- `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 ARN de certificados de autorización de clientes.
- `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 VPC

- `VpcCidrBlock`: Inspecciona todas las VPC para asegurarse de que todas tienen el mismo valor para el tamaño de la red de bloques CIDR.
- `VpcCidrBlocksSameProtocolVersion`: inspecciona todas las VPC que tienen los mismos bloques de 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 de todas las VPC para asegurarse de que todas tienen bloques de CIDR en un mismo estado. `ASSOCIATED`
- `Vpclpv6CidrBlocksStateInAssociationSets`: Inspecciona todos los conjuntos de asociaciones de bloques de CIDR de todas las VPC para asegurarse de que todas tienen bloques de CIDR con el mismo número de direcciones.
- `VpcCidrBlocksInAssociationSets`: Inspecciona todos los conjuntos de asociaciones de bloques CIDR de todas las VPC para asegurarse de que todas tienen el mismo tamaño.
- `Vpclpv6CidrBlocksInAssociationSets`: inspecciona todos los conjuntos de asociaciones de bloques CIDR de IPv6 para todas las VPC para asegurarse de que tienen el mismo tamaño.
- `VpcState`: inspecciona cada VPC para asegurarse de que se encuentra en `AVAILABLE` un estado.
- `VpcInstanceTenancy`: Inspecciona todas las VPC para asegurarse de que todas tienen el mismo valor. `Instance Tenancy`

- `VpclsDefault`: Inspecciona todos los VPC 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 de Route 53 en <https://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 Route 53 ARC

Al crear un conjunto de recursos en Amazon Route 53 Application Recovery Controller, se especifica el tipo de recurso que se va a incluir en el conjunto y los nombres de los recursos de Amazon (ARN) de cada uno de los recursos que se van a incluir. Route 53 ARC espera un formato de ARN específico para cada tipo de recurso. En esta sección se enumeran los tipos de recursos compatibles con Route 53 ARC y los formatos de ARN asociados a cada uno de ellos.

El formato específico depende del recurso. Cuando proporcione un ARN, reemplace el texto en *cursiva* por la información específica del recurso.

Note

Tenga en cuenta que el formato de ARN que Route 53 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 de servicio](#) no incluyan el Cuenta de AWS ID u otra información que el ARC de Route 53 necesita para admitir las funciones del servicio ARC de Route 53.

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, consulte [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/LoadBalancerName`

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 Nombres de recursos de Amazon \(ARN\) 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:123456789012345567890

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, consulte [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-123456789acdefgh`

Para obtener más información, consulte [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 los ARN de la zona alojada, tal y como se especifica aquí. El ID de cuenta es obligatorio para que Route 53 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 Route 53 Application Recovery Controller

Puede utilizar Amazon y Amazon CloudWatch EventBridge para supervisar la verificación de disponibilidad en Amazon Route 53 Application Recovery Controller, a fin de analizar patrones y ayudar a solucionar problemas. AWS CloudTrail

Note

Debe ver CloudWatch las métricas y los registros de Route 53 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 Route 53 ARC](#)
- [Registrar las llamadas a la API de verificación de disponibilidad mediante AWS CloudTrail](#)
- [Uso del control de disponibilidad en Route 53 ARC con Amazon EventBridge](#)

Uso de Amazon CloudWatch con verificación de disponibilidad en Route 53 ARC

El controlador de recuperación de aplicaciones Amazon Route 53 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 Route 53 ARC](#)
- [Estadísticas de Route 53 ARC](#)
- [Ver CloudWatch las métricas en Route 53 ARC](#)

Métricas de Route 53 ARC

El espacio de nombres de AWS/Route53RecoveryReadiness incluye las siguientes métricas.

Métrica	Descripción
ReadinessChecks	<p>Representa la cantidad de comprobaciones de preparación procesadas por Route 53 ARC. La métrica se puede dimensionar según sus estados, que se indican a continuación.</p> <p>Unidad: Count.</p> <p>Criterios del informe: hay un valor distinto de cero.</p> <p>Estadísticas: la única estadística útil es Sum.</p> <p>Dimensiones</p> <ul style="list-style-type: none"> • READY • NOT_READY • NOT_AUTHORIZED

Métrica	Descripción
	<ul style="list-style-type: none"> UNKNOWN
Resources	<p>Representa la cantidad de recursos procesados por Route 53 ARC, que se pueden dimensionar según su identificador de recursos, según lo define la API.</p> <p>Unidad: Count.</p> <p>Criterios del informe: hay un valor distinto de cero.</p> <p>Estadísticas: la única estadística útil es Sum.</p> <p>Dimensiones</p> <ul style="list-style-type: none"> ResourceSetType : Estos son los tipos de recursos, filtrados por la cantidad de recursos por tipo determinado evaluados por Route 53 ARC <p>Por ejemplo: AWS::CloudWatch::Alarm</p>

Estadísticas de Route 53 ARC

CloudWatch proporciona estadísticas basadas en los puntos de datos métricos publicados por Route 53 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 la cantidad de comprobaciones de preparación evaluadas por Route 53 ARC.
- Vea la cantidad total de recursos para un tipo de conjunto de recursos determinado evaluado por Route 53 ARC.

Ver CloudWatch las métricas en Route 53 ARC

Puede ver las CloudWatch métricas de Route 53 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 Route 53 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`.

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

Utilice el siguiente [get-metric-statistics](#) comando 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 Route 53 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

El controlador de recuperación de aplicaciones Amazon Route 53 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 Route 53 ARC. CloudTrail captura todas las llamadas a la API para Route 53 ARC como

eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de Route 53 ARC y las llamadas de código a las operaciones de la API de Route 53 ARC.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Route 53 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 Route 53 ARC, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

Información sobre Route 53 ARC en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce actividad en Route 53 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 los eventos en su territorio Cuenta de AWS, incluidos los eventos de Route 53 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 ARC de Route 53 se registran CloudTrail y documentan en la Guía de [referencia de la API de preparación para el controlador de recuperación de aplicaciones Amazon Route 53](#), la Guía de [referencia de la API de configuración de control de recuperación para el controlador](#)

de recuperación de aplicaciones Amazon Route 53 y la [Guía de referencia de la API de control de enrutamiento para el controlador de recuperación de aplicaciones Amazon Route 53](#). 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 lo 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 [CloudTrail UserIdentity](#).

Visualización de eventos de Route 53 ARC en el historial de eventos

CloudTrail permite ver los eventos recientes en el historial de eventos. Para ver los eventos de solicitudes de API de Route 53 ARC, debe elegir Oeste de EE. UU. (Oregón) en el selector de regiones de la parte superior de la consola. Para obtener más información, consulte [Uso del historial de CloudTrail eventos](#) en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de archivos de registro de Route 53 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": "ARO33L3W36EXAMPLE",
    "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 del control de disponibilidad en Route 53 ARC con Amazon EventBridge

Con Amazon EventBridge, puede configurar reglas basadas en eventos que supervisen sus recursos de comprobación de disponibilidad en Amazon Route 53 Application Recovery Controller y, a continuación, iniciar acciones específicas que utilicen otros AWS servicios. Por ejemplo, puedes establecer una regla para enviar 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

Route 53 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 su grado de preparación, cree 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 de Route 53:

- 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 ARC de Route 53 específicos que le interesen, defina patrones específicos de eventos que EventBridge pueda usar para detectar los eventos. 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 Route 53 ARC hasta casi EventBridge en tiempo real 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 verificación de preparación con EventBridge

Con EventBridge, puede crear reglas que definan las acciones que se deben tomar cuando Route 53 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. Abra 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. Elija Create rule.
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, 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 Route 53 ARC.

Los siguientes patrones de eventos proporcionan ejemplos que puede utilizar EventBridge para la capacidad de comprobación de preparación en Route 53 ARC.

- Seleccione todos los eventos de la verificación de preparación para Route 53 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 ARC de Route 53 para un cambio de 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"
    }
  }
}
```

```
}
```

A continuación se muestra un ejemplo de evento de Route 53 ARC para un cambio del estado de preparación de celda:

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

A continuación se muestra un ejemplo de evento de Route 53 ARC para un cambio de estado de comprobación de preparación:

```
{
  "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 la CloudWatch PutResource API de políticas.](#) A continuación, puede usar el comando CLI [describe-resource-policies](#) para comprobar que la política se aplicó correctamente.

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

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 CloudWatch como objetivo.

5. Elija un grupo de CloudWatch registros en el menú desplegable.

Identity and Access Management para comprobar la disponibilidad

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Route 53 ARC. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Contenido

- [Cómo funciona la verificación de disponibilidad en ServiceLong; con IAM](#)
- [Ejemplos de políticas basadas en la identidad para comprobar la disponibilidad en Amazon Route 53 Application Recovery Controller](#)
- [Uso de un rol vinculado al servicio para comprobar la preparación en Route 53 ARC](#)
- [AWS políticas administradas para la verificación de disponibilidad en Amazon Route 53 Application Recovery Controller](#)

Cómo funciona la verificación de disponibilidad en ServiceLong; con IAM

Antes de utilizar IAM para administrar el acceso a Route 53 ARC, conozca qué características de IAM se pueden utilizar con Route 53 ARC.

Antes de usar IAM para administrar el acceso a la verificación de preparación en Amazon Route 53 Application Recovery Controller, conozca qué funciones de IAM están disponibles para usar con la verificación de preparación.

Funciones de IAM que puede utilizar con la comprobación de disponibilidad en Amazon Route 53 Application Recovery Controller

Característica de IAM	Soporte de verificación de disponibilidad
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí

Característica de IAM	Soporte de verificación de disponibilidad
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
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 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 adjunto. Para 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 basadas en identidad de Route 53 ARC, consulte [Ejemplos de políticas basadas en identidad en Amazon Route 53 Application Recovery Controller](#).

Políticas basadas en los recursos incluidas en el control de disponibilidad

Compatibilidad con las políticas basadas en recursos	No
--	----

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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

Admite acciones de política	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 las acciones ARC de Route 53 para comprobar la disponibilidad, consulte [Acciones definidas por Amazon Route 53 Recovery Readiness](#) en la Referencia de autorización de servicio.

Las acciones políticas en Route 53 ARC para comprobar la preparación 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 ARC basadas en la identidad de Route 53 para comprobar la preparación, consulte. [Ejemplos de políticas basadas en la identidad para comprobar la disponibilidad en Amazon Route 53 Application Recovery Controller](#)

Recursos de políticas para la verificación de la preparación

Admite 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 puede 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 \(ARN\)](#). Puede 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, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de las acciones ARC de Route 53 para el cambio zonal, consulte [Acciones definidas por Amazon Route 53 Recovery Readiness](#).

Para ver ejemplos de políticas ARC basadas en la identidad de Route 53 para comprobar la preparación, consulte. [Ejemplos de políticas basadas en la identidad para comprobar la disponibilidad en Amazon Route 53 Application Recovery Controller](#)

Condiciones de la política: claves para la verificación de disponibilidad

Admite 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 puede 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. Puede crear expresiones condicionales que utilicen [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 puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte [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 acciones ARC de Route 53 para comprobar la preparación, consulte [Claves de estado 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 ARC basadas en la identidad de Route 53 para comprobar la preparación, consulte. [Ejemplos de políticas basadas en la identidad para comprobar la disponibilidad en Amazon Route 53 Application Recovery Controller](#)

Comprobación de la disponibilidad de las listas de control de acceso (ACL)

Admite las ACL

No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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

Admite 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 [¿Qué es 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

Compatible con el uso de credenciales temporales	Sí
--	----

Algunos 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 más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) 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 más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos principales entre servicios para comprobar si están listos

Admite Forward access sessions (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

Compatible con roles vinculados al servicio	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 acerca de cómo crear o administrar roles vinculados a servicios de Route 53 ARC, consulte [Uso de un rol vinculado al servicio para comprobar la preparación en Route 53 ARC](#).

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte [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 disponibilidad en Amazon Route 53 Application Recovery Controller

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Route 53 ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la 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 puede añadir las políticas de IAM a roles y los usuarios pueden 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](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Route 53 ARC, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición del controlador de recuperación de aplicación de Amazon Route 53 ARC](#) en la Referencia de autorizaciones de servicio.

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 identidades determinan si alguien puede crear, acceder o eliminar los recursos de Route 53 ARC de la 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, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) 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, consulte [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, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice 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 [Política de validación de Analizador de acceso de IAM](#) en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [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 del controlador de recuperación de aplicación de Amazon Route 53, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de Route 53 en su 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 conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite 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 verificación de disponibilidad cuando solo se permita el acceso a determinadas operaciones de la API, adjunte también a las entidades una política ReadOnly y AWS gestionada de verificación 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 la función vinculada al servicio que está asociada a la comprobación de disponibilidad en Route 53 ARC. Para obtener más información, consulte [Uso de un rol vinculado al servicio para comprobar la preparación en Route 53 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 ARC de Route 53 para trabajar con el plano de control de la comprobación de preparación del ARC de Route 53 (por ejemplo, para crear grupos de recuperación, conjuntos de recursos y comprobaciones de preparación), 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 la función vinculada al servicio que está asociada a la comprobación de disponibilidad en Route 53 ARC. Para obtener más información, consulte [Uso de un rol vinculado al servicio para comprobar la preparación en Route 53 ARC](#).

Para trabajar con las operaciones de la API para comprobar la disponibilidad, 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: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 Route 53 ARC

El controlador de recuperación de aplicaciones Amazon Route 53 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 de (en este caso, Route 53 ARC). Route 53 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 a servicios simplifican la configuración de Route 53 ARC porque ya no tendrá que añadir manualmente los permisos necesarios. Route 53 ARC determina los permisos de sus roles vinculados a servicios y a menos que se hayan definido de otra manera, solo Route 53 ARC puede asumir su roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Route 53 ARC, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Yes (Sí) en la columna Service-Linked Role (Rol vinculado a servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Route 53 ARC tiene los siguientes roles vinculados a servicios, que se describen en este capítulo:

- Route 53 ARC usa el rol vinculado al servicio denominado Route53 RecoveryReadinessServiceRolePolicy para acceder a los recursos y las configuraciones y comprobar la preparación.
- Route 53 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

Route 53 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 `RecoveryReadinessServiceRolePolicy` vinculado al servicio de Route53 para Route 53 ARC

No es necesario crear manualmente el rol vinculado al servicio de Route53.

`RecoveryReadinessServiceRolePolicy` Cuando crea la primera verificación de disponibilidad o autorización entre cuentas en la AWS Management Console, la o la AWS API AWS CLI, Route 53 ARC crea la función vinculada al servicio para usted.

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. Cuando se crea la primera verificación de disponibilidad o autorización entre cuentas, Route 53 ARC vuelve a crear el rol vinculado al servicio.

Edición del rol `RecoveryReadinessServiceRolePolicy` vinculado al servicio de Route53 para Route 53 ARC

Route 53 ARC no le permite editar el rol vinculado al `RecoveryReadinessServiceRolePolicy` servicio de Route53. 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 `RecoveryReadinessServiceRolePolicy` vinculado al servicio de Route53 para Route 53 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 monitoree 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 [Comprobación de disponibilidad del controlador de recuperación de aplicaciones de Amazon Route 53](#). Para obtener más información sobre autorizaciones entre cuentas, consulte [Creación de autorizaciones entre cuentas en Route 53 ARC](#).

Note

Si el servicio Route 53 ARC está utilizando el rol cuando intenta eliminar los recursos, la eliminación del rol de servicio podría producir un error. En tal caso, espere unos minutos e intente eliminar de nuevo el rol.

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la o la AWS API para eliminar la función AWS CLI vinculada al servicio de Route53. `RecoveryReadinessServiceRolePolicy` 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 de Route 53 para comprobar la preparación

Para ver las actualizaciones de las políticas AWS administradas para las funciones vinculadas al servicio de Route 53 ARC, consulte la [tabla de actualizaciones de políticas AWS administradas](#) de Route 53 ARC. También puede suscribirse a alertas RSS automáticas en la [página del historial de documentos](#) ARC de Route 53.

AWS políticas administradas para la verificación de disponibilidad en Amazon Route 53 Application Recovery Controller

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 por AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: Route53 RecoveryReadinessServiceRolePolicy

No puede asociar Route53RecoveryReadinessServiceRolePolicy a sus entidades IAM. Esta política está adjuntada a un rol vinculado a un servicio que permite a Amazon Route 53 acceder a servicios y recursos de que utiliza o administra. Para obtener más información, consulte [Uso de un rol vinculado al servicio para comprobar la preparación en Route 53 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 preparación) en Route 53 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 [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 concede acceso de solo lectura a las acciones para trabajar con la preparación para la recuperación en Route 53 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 [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 administradas para comprobar la disponibilidad en Route 53 ARC desde que este servicio comenzó a rastrear estos cambios, consulte [Actualizaciones de las políticas AWS administradas para Amazon Route 53 Application Recovery Controller](#). Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la [página de historial de documentos](#) de Route 53 ARC.

Cuotas para comprobar la disponibilidad

La comprobación de disponibilidad en Amazon Route 53 Application Recovery Controller 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
Número de conjuntos de recursos por cuenta	200
Número de comprobaciones de disponibilidad por cuenta	200
Número de autorizaciones de entre las cuentas	100

Ejemplos de código para Application Recovery Controller mediante AWS SDK

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 funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Para obtener una lista completa de 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.

Ejemplos de código

- [Acciones para el controlador de recuperación de aplicaciones mediante AWS SDK](#)
 - [Úselo GetRoutingControlState con un AWS SDK o CLI](#)
 - [Úselo UpdateRoutingControlState con un AWS SDK o CLI](#)

Acciones para el controlador de recuperación de aplicaciones mediante AWS SDK

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de Application Recovery Controller con los AWS SDK. Estos fragmentos llaman a la API del controlador de recuperación de aplicaciones y son fragmentos de código de programas más grandes que deben ejecutarse en contexto. 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

- [Úselo GetRoutingControlState con un AWS SDK o CLI](#)
- [Úselo UpdateRoutingControlState con un AWS SDK o CLI](#)

Úselo `GetRoutingControlState` con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `GetRoutingControlState`.

Java

SDK para Java 2.x

Note

Hay más información 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 [GetRoutingControlState](#) la 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 [GetRoutingControlState](#) la AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de 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.

Úselo **UpdateRoutingControlState** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `UpdateRoutingControlState`.

Java

SDK para Java 2.x

Note

Hay más información 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 [UpdateRoutingControlState](#) la Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

Note

Hay más información al respecto en 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 [UpdateRoutingControlState](#) la AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de 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 el controlador de recuperación de aplicaciones de Amazon Route 53

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 Route 53 Application Recovery Controller, consulte [AWS Servicios incluidos en el ámbito por programa de conformidad AWS](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Route 53 ARC. En los siguientes temas, se le mostrará cómo configurar Route 53 ARC para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que lo ayudan a monitorear y proteger sus recursos ARC de Route 53.

Temas

- [Protección de datos en el controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Identity and Access Management para el Controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Registro y monitorización del controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Validación de conformidad para el controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Resistencia en el controlador de recuperación de aplicaciones de Amazon Route 53](#)
- [Seguridad de la infraestructura del controlador de recuperación de aplicaciones de Amazon Route 53](#)

Protección de datos en el controlador de recuperación de aplicaciones de Amazon Route 53

El [modelo de](#) se aplica a protección de datos en Amazon Route 53 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. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS 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
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice 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 140-2 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, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

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 Route 53 ARC u otro Servicios de AWS

mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos 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 de Route 53 ARC se escriben en un volumen de Amazon EBS como respaldo. Route 53 ARC usa el cifrado predeterminado de Amazon EBS mientras los datos están en reposo.

Cifrado en tránsito

Las solicitudes y respuestas de los clientes (para la configuración de Route 53 ARC, las consultas sobre el estado de preparación, las actualizaciones del estado de las celdas, etc.) se cifran durante el transporte por todo el servicio mediante TLS.

Identity and Access Management para el Controlador de recuperación de aplicaciones de Amazon Route 53

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 estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Route 53 ARC. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Route 53 ARC.

Usuario de servicio: si utiliza el servicio de Route 53 ARC para realizar el trabajo, el administrador le proporciona las credenciales y los permisos necesarios. A medida que utilice más características de Route 53 ARC para realizar su trabajo, es posible que necesite permisos adicionales. Entender

cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Route 53 ARC, consulte .

Administrador de servicio: si está a cargo de los recursos de Route 53 ARC en su empresa, probablemente tenga acceso completo a Route 53 ARC. Su trabajo consiste en determinar a qué características y recursos de Route 53 ARC deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador 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 Route 53 ARC, consulte [Cómo funcionan las capacidades del controlador de recuperación de aplicaciones Amazon Route 53 con IAM](#).

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Route 53 ARC. Para consultar ejemplos de políticas basadas en identidades de Route 53 ARC que puede utilizar en IAM, consulte [Ejemplos de políticas basadas en identidad en Amazon Route 53 Application Recovery Controller](#).

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 (Centro de identidades de IAM), 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 administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo 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 cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar las solicitudes de la AWS 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 [Uso de la autenticación multifactor \(MFA\) en AWS](#) 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 utilice 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, consulte [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 utilice 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, consulte [¿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 puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo 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 permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) 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 determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console [cambiando](#) de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) 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 para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del usuario de IAM. Si utiliza 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, consulte [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, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común 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 ellas AWS, se te considera director. 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:** puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla 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 a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2](#) en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) 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 utilice 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 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. 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 (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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 que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte [Información general de 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). Puede 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 (SCP):** las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). 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 habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus 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 acerca de Organizations y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del usuario de AWS Organizations .
- **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 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 del controlador de recuperación de aplicaciones Amazon Route 53 con IAM

Para obtener información sobre cómo funciona cada función de Amazon Route 53 Application Recovery Controller 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](#)

Ejemplos de políticas basadas en identidad en Amazon Route 53 Application Recovery Controller

Para ver ejemplos de políticas basadas en la identidad para cada capacidad de Amazon Route 53 Application Recovery Controller, consulte los siguientes temas en los AWS Identity and Access Management capítulos de cada capacidad:

- [Ejemplos de políticas basadas en la identidad para el cambio automático zonal](#)
- [Ejemplos de políticas basadas en la identidad para el cambio zonal en Amazon Route 53 Application Recovery Controller](#)
- [Ejemplos de políticas basadas en identidad para el control de enrutamiento en Amazon Route 53 Application Recovery Controller](#)
- [Ejemplos de políticas basadas en la identidad para comprobar la disponibilidad en Amazon Route 53 Application Recovery Controller](#)

AWS políticas administradas para Amazon Route 53 Application Recovery Controller

Para obtener información sobre las políticas AWS administradas para las capacidades de Amazon Route 53 Application Recovery Controller con políticas administradas, incluida una política administrada para un rol vinculado a un servicio, consulte los siguientes temas:

- [Políticas administradas para el cambio automático zonal](#)
- [Políticas gestionadas para el control de enrutamiento](#)
- [Políticas gestionadas para comprobar la preparación](#)

Actualizaciones de las políticas AWS administradas para Amazon Route 53 Application Recovery Controller

Vea los detalles sobre las actualizaciones de las políticas AWS administradas para las capacidades de Route 53 ARC desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbese a la fuente RSS en la [página de historial de documentos](#) de Route 53 ARC.

Cambio	Descripción	Fecha
AWSServiceRoleForPercPracticePolicy — Nueva política	<p>Route 53 ARC crea un nuevo rol vinculado para cambios automáticos y ejecuciones de práctica.</p> <p>Route 53 ARC usa los permisos habilitados por la función 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.</p> <p>Para obtener más información sobre el nuevo rol vinculado a servicios, consulte Permisos de rol vinculados al servicio para AWSServiceRoleForZonalAutoshiftPracticeRun.</p>	30 de noviembre de 2023
AmazonRoute53 — Política actualizada RecoveryControlConfigRead OnlyAccess	Añade permisos para <code>GetResourcePolicy</code> , a fin de permitir la devolución de detalles sobre las políticas	18 de octubre de 2023

Cambio	Descripción	Fecha
	de AWS Resource Access Manager recursos para los recursos compartidos.	
<p>Política de Route53: RecoveryReadiness ServiceRole política actualizada</p>	<p>Route 53 ARC agregó nuevos permisos para consultar información sobre las instancias de Amazon EC2.</p> <p>Route 53 ARC utiliza los siguientes permisos para admitir el sondeo de las instancias de Amazon EC2, ejecutar comprobaciones de preparación y determinar el estado de preparación de las instancias.</p> <p><code>ec2:DescribeVpnGateways</code></p> <p><code>ec2:DescribeCustomerGateways</code></p>	17 de febrero de 2023

Cambio	Descripción	Fecha
Política de Route53 RecoveryReadiness ServiceRole : política actualizada	<p>Route 53 ARC incorporó un nuevo permiso para consultar información sobre las funciones de Lambda.</p> <p>Route 53 ARC usa el siguiente permiso para consultar información sobre las funciones de Lambda a fin de ejecutar comprobaciones de preparación y determinar el estado de preparación de las funciones.</p> <p><code>lambda:ListProvisionedConcurrencyConfigs</code></p>	31 de agosto de 2022
AmazonRoute53 RecoveryControl ConfigFull Access : 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 RecoveryControl ConfigFull Access : 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 RecoveryCluster ReadOnly Access : política actualizada	Route 53 ARC agregó un nuevo permiso, <code>route53-recovery-cluster:ListRoutingControls</code> , para permitir enumerar los ARN de control de enrutamiento con alta disponibilidad.	15 de marzo de 2022

Cambio	Descripción	Fecha
AmazonRoute53 RecoveryControl ConfigRead OnlyAccess — Política actualizada	Route 53 ARC agregó un nuevo permiso <code>route53-recovery-control-config:ListTagsForResource</code> , para permitir incluir etiquetas para un recurso.	20 de diciembre de 2021
Política de Route53: RecoveryReadiness ServiceRole política actualizada	<p>Route 53 ARC agregó un nuevo permiso para consultar información sobre Amazon API Gateway.</p> <p>Route 53 ARC usa el permiso <code>apigateway:GET</code> , para consultar información sobre API Gateway a fin de ejecutar comprobaciones de preparación y determinar el estado de preparación.</p>	28 de octubre de 2021

Cambio	Descripción	Fecha
<p>AmazonRoute53 RecoveryReadiness ReadOnly Access: se agregaron nuevos permisos</p>	<p>Route 53 ARC agregó dos permisos nuevos a AmazonRoute53 RecoveryReadiness ReadOnly Access:</p> <p>Route 53 ARC utiliza <code>route53-recovery-readiness:GetArchitectureRecommendations</code> y <code>route53-recovery-readiness:GetCellReadinessSummary</code> permite el acceso de solo lectura a estas acciones para trabajar con la preparación para la recuperación.</p>	<p>15 de octubre de 2021</p>

Cambio	Descripción	Fecha
<p>Política de Route53: RecoveryReadiness ServiceRole política actualizada</p>	<p>Route 53 ARC agregó nuevos permisos para consultar información sobre las funciones de Lambda.</p> <p>Route 53 ARC usa los siguientes permisos para consultar información sobre las funciones de Lambda para ejecutar comprobaciones de disponibilidad y determinar el estado de preparación de esas funciones.</p> <p>lambda:GetFunction Concurrency</p> <p>lambda:GetFunction Configuration</p> <p>lambda:GetProvisionedConcurrencyConfig</p> <p>lambda:ListAliases</p> <p>lambda:ListVersionsByFunction</p> <p>lambda:ListEventSourceMappings</p> <p>lambda:ListFunctions</p>	<p>8 de octubre de 2021</p>

Cambio	Descripción	Fecha
Política de Route53: se agregaron RecoveryReadiness ServiceRole nuevas políticas administradas	Route 53 ARC agregó las siguientes políticas administradas nuevas: AmazonRoute53 RecoveryReadiness FullAccess AmazonRoute53 RecoveryReadiness ReadOnly Acceso AmazonRoute53 RecoveryCluster FullAccess AmazonRoute53 RecoveryCluster ReadOnly Acceso AmazonRoute5.3 RecoveryControl ConfigFull Acceso AmazonRoute53 RecoveryControl ConfigRead OnlyAccess	18 de agosto de 2021
Route 53 ARC comenzó el seguimiento de los cambios	Route 53 ARC comenzó a rastrear los cambios en sus políticas AWS administradas.	27 de julio de 2021

Solucionar problemas de identidad y acceso a la controladora de recuperación de aplicaciones de Amazon Route 53

Utilice la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Amazon Route 53 Application Recovery Controller e IAM.

Temas

- [No tengo autorización para realizar una acción en Route 53 ARC](#)
- [No estoy autorizado a realizar lo siguiente: PassRole](#)

- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos ARC de Route 53](#)

No tengo autorización para realizar una acción en Route 53 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 recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Route 53 ARC.

Algunos Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Route 53 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 administrador. AWS El administrador 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 ARC de Route 53

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 admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Route 53 admite estas características, consulte [Cómo funcionan las capacidades del controlador de recuperación de aplicaciones Amazon Route 53 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 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, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

Registro y monitorización del controlador de recuperación de aplicaciones de Amazon Route 53

La supervisión es una parte importante del mantenimiento de la disponibilidad y el rendimiento de Amazon Route 53 Application Recovery Controller y sus AWS soluciones. Debe recopilar datos de monitoreo de todas las partes de su AWS solución para poder depurar más fácilmente una falla

multipunto en caso de que se produzca. AWS proporciona varias herramientas para monitorear los recursos y la actividad de Route 53 ARC y responder a posibles incidentes, por ejemplo, AWS CloudTrail y Amazon CloudWatch.

Para obtener información sobre la supervisión de cada capacidad de Route 53 ARC, consulte los siguientes temas:

- [Registro y monitoreo del cambio zonal](#)
- [Registro y supervisión del cambio automático zonal](#)
- [Registro y supervisión para el control de enrutamiento](#)
- [Registro y supervisión para comprobar la disponibilidad](#)

Validación de conformidad para el controlador de recuperación de aplicaciones de Amazon Route 53

Los auditores externos evalúan la seguridad y la conformidad de Amazon Route 53 Application Recovery Controller como parte de varios programas de AWS conformidad. Esto incluye SOC, PCI, HIPAA y otros.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de conformidad específicos, consulte [Servicios de AWS Alcance por programa](#) 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:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de [arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

Note

No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la [Referencia de servicios compatibles con HIPAA](#).

- [AWS Recursos 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](#)— Este 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.

Resistencia en el controlador de recuperación de aplicaciones de Amazon Route 53

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, Route 53 ARC ofrece varias funciones para respaldar sus necesidades de respaldo y resiliencia de datos.

Seguridad de la infraestructura del controlador de recuperación de aplicaciones de Amazon Route 53

Como servicio gestionado, Amazon Route 53 Application Recovery Controller 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.

Utiliza las llamadas a la API AWS publicadas para acceder a Route 53 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 de seguridad de IAM principal. También puede 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 Route 53 Application Recovery Controller

Las siguientes entradas describen cambios importantes realizados en la documentación del Controlador de recuperación de aplicaciones de Amazon Route 53.

- Versión: más actualizada
- Última actualización de la documentación: 30 de abril de 2024

Cambio	Descripción	Fecha
Reorganización del documento por cada capacidad	<p>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 Route 53 ARC: cambio zonal y cambio automático zonal para la recuperación en zonas de disponibilidad múltiples, y control de enrutamiento y verificación de preparación para la recuperación en varias regiones.</p> <p>Para obtener más información, consulte Qué es Amazon Route 53 Application Recovery Controller.</p>	30 de abril de 2024
Añade la capacidad de cambio automático de zona	Agrega una nueva capacidad en Route 53 ARC, en la que	30 de noviembre de 2023

Cambio	Descripción	Fecha
	<p>usted autoriza AWS a desviar el tráfico de recursos de una aplicación desde una zona de disponibilidad, en su nombre, para ayudar a reducir el tiempo de recuperación durante los eventos.</p> <p>Para obtener más información, consulte Cambio automático de zona en el controlador de recuperación de aplicaciones de Amazon Route 53.</p>	
<p>Añade un nuevo rol vinculado a un servicio</p>	<p>Añade una nueva función vinculada al servicio AWSServiceRoleForZonalAutoshiftPracticeRun, para las prácticas de cambio automático zonales.</p> <p>Para obtener más información, consulte Permisos de roles vinculados a un servicio para. AWSServiceRoleForZonalAutoshiftPracticeRun</p>	<p>30 de noviembre de 2023</p>

Cambio	Descripción	Fecha
Se agrega soporte entre cuentas para los clústeres	<p>Añade compatibilidad con varias cuentas para los clústeres de Route 53 ARC AWS Resource Access Manager, de modo que puede utilizar un clúster de forma fácil y segura para alojar paneles de control y controles de enrutamiento propiedad de varias AWS cuentas diferentes.</p> <p>Para obtener más información, consulte Support cross-account for clusters in Route 53 ARC.</p>	18 de octubre de 2023
Actualiza una política administrada	<p>Actualiza la política AmazonRoute53RecoveryControlConfigReadOnly administrada para añadir permisos y permitir GetResourcePolicy la devolución de detalles sobre las políticas de AWS Resource Access Manager recursos para los recursos compartidos.</p> <p>Para obtener más información, consulte Políticas administradas de AWS.</p>	19 de septiembre de 2023

Cambio	Descripción	Fecha
Actualización del rol vinculado al servicio	<p>Se han añadido nuevos permisos (<code>ec2:DescribeVpnGateways</code> y <code>ec2:DescribeCustomerGateways</code>) al rol vinculado a un servicio para Route 53 ARC para admitir el sondeo de instancias de Amazon EC2.</p> <p>Para obtener más información, consulte Uso de roles vinculados a servicios para Route 53 ARC.</p>	17 de febrero de 2023
Versión de GA para el cambio zonal	<p>Es compatible con la versión GA del cambio zonal para Route 53 ARC, que incluye el control de acceso basado en atributos (ABAC) para los recursos gestionados que están registrados en Route 53 ARC para el cambio zonal.</p> <p>Para obtener más información, consulte Control de acceso basado en atributos (ABAC) con Route 53 ARC.</p>	10 de enero de 2023

Cambio	Descripción	Fecha
Se agregó un nuevo cambio zonal Multi-AZ	<p>Se agregó contenido que describe un nuevo servicio en Route 53 ARC, 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.</p> <p>Para obtener más información, consulte Cambio de zona en Route 53 ARC.</p>	28 de noviembre de 2022
Actualización del rol vinculado al servicio	<p>Se ha añadido un nuevo permiso (<code>lambda:ListProvisionedConcurrencyConfigs</code>) al rol vinculado a un servicio para Route 53 ARC para consultar información sobre las funciones de Lambda.</p> <p>Para obtener más información, consulte Uso de roles vinculados a servicios para Route 53 ARC.</p>	31 de agosto de 2022

Cambio	Descripción	Fecha
Se ha actualizado la política administrada	<p>Se actualizó la política AmazonRoute53RecoveryControlConfigFullAccess administrada para eliminar los permisos de Amazon Route 53 e incluirlos como opcionales.</p> <p>Para obtener más información, consulte AWS políticas gestionadas de Amazon Route 53 Application Recovery Controller.</p>	26 de mayo de 2022
Se ha actualizado la política administrada	<p>Se actualizó la política AmazonRoute53RecoveryControlConfigFullAccess administrada para incluir los permisos de Amazon Route 53 necesarios.</p> <p>Para obtener más información, consulte AWS políticas gestionadas de Amazon Route 53 Application Recovery Controller.</p>	15 de abril de 2022

Cambio	Descripción	Fecha
Se agregó un ejemplo de CLI para la nueva API de controles de enrutamiento de listas	<p>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 de Route 53 ARC.</p> <p>Para obtener más información, consulte Listar y actualizar los controles y estados de enrutamiento.</p>	31 de marzo de 2022
Se ha agregado compatibilidad con las normas de seguridad	<p>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.</p> <p>Para obtener más información, consulte Anular las normas de seguridad para redirigir el tráfico.</p>	2 de marzo de 2022

Cambio	Descripción	Fecha
Se agregó soporte de etiquetado adicional	<p>Se agregó soporte para etiquetar recursos adicionales en Route 53 ARC, incluidos clústeres, paneles de control, controles de enrutamiento y reglas de seguridad.</p> <p>Para obtener más información, consulte la Etiquetado en Amazon Route 53 Application Recovery Controller.</p>	20 de diciembre de 2021
Se ha actualizado la política administrada	<p>Se ha actualizado AmazonRoute53RecoveryControllerConfigReadOnly la política de administración para agregar permiso para enumerar las etiquetas de un recurso.</p> <p>Para obtener más información, consulte AWS políticas gestionadas de Amazon Route 53 Application Recovery Controller</p>	20 de diciembre de 2021

Cambio	Descripción	Fecha
Se agregó soporte para alertas en tiempo real con EventBridge	<p>Se agregó compatibilidad con EventBridge, lo que significa que ahora puede agregar reglas para recibir alertas y actuar en caso de cambios de estado de verificación de preparación para el ARC de Route 53, por ejemplo, cuando un estado cambia de LISTO a NO LISTO.</p> <p>Para obtener más información, consulte Uso de Route 53 ARC con Amazon EventBridge.</p>	20 de diciembre de 2021
Se agregaron ejemplos de códigos de estado de control de enrutamiento	<p>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 actualizar los estados del control de enrutamiento.</p> <p>Para obtener más información, consulte Ejemplos de API de Amazon Route 53 Application Recovery Controller.</p>	16 de noviembre de 2021

Cambio	Descripción	Fecha
Ha agregado una política nueva que concede permisos de solo lectura	<p>Ha añadido dos nuevos permisos a la política AmazonRoute53RecoveryReadinessReadOnlyAccess : route53-recovery-readiness:GetArchitectureRecommendations y route53-recovery-readiness:GetCellReadinessSummary .</p> <p>Para obtener más información, consulte AWS políticas gestionadas de Amazon Route 53 Application Recovery Controller.</p>	9 de noviembre de 2021
Ha añadido compatibilidad con el tipo de recurso Amazon API Gateway	<p>Se agregó un nuevo tipo de recurso, Amazon API Gateway, y se actualizaron los permisos de los roles vinculados al servicio de Route 53 ARC para que Route 53 ARC pueda auditar API Gateway con comprobaciones de disponibilidad.</p> <p>Para obtener más información, consulte Reglas de preparación y tipos de recursos compatibles y Uso de funciones vinculadas a servicios para Route 53 ARC.</p>	28 de octubre de 2021

Cambio	Descripción	Fecha
Se agregó soporte para el tipo de recurso de funciones Lambda	<p>Se agregó un nuevo tipo de recurso, las funciones de Lambda, y se actualizaron los permisos de los roles vinculados al servicio de Route 53 ARC para que Route 53 ARC pueda auditar las funciones de Lambda con comprobaciones de disponibilidad.</p> <p>Para obtener más información, consulte Reglas de preparación y tipos de recursos compatibles y Uso de funciones vinculadas a servicios para Route 53 ARC.</p>	8 de octubre de 2021
Se agregaron enlaces CloudFormation y plantillas de Terraform	<p>Se agregaron enlaces a plantillas Terraform descargables AWS CloudFormation y de Hashicorp para ayudarle a empezar rápidamente a utilizar Route 53 Arc. Para obtener más información, consulte Preparación para la recuperación con una nueva aplicación.</p>	13 de septiembre de 2021

Cambio	Descripción	Fecha
Nuevas políticas administradas añadidas	<p>Se agregaron las siguientes políticas AWS administradas para Route 53 ARC:</p> <p>AmazonRoute53RecoveryReadinessFullAccess AmazonRoute53RecoveryReadinessReadOnlyAccess AmazonRoute53RecoveryClusterFullAccess AmazonRoute53RecoveryClusterReadOnlyAccess AmazonRoute53RecoveryControlConfigFullAccess AmazonRoute53RecoveryControlConfigReadOnlyAccess</p> <p>Para obtener más información, consulte AWS políticas gestionadas de Amazon Route 53 Application Recovery Controller.</p>	18 de agosto de 2021

Cambio	Descripción	Fecha
Comenzó a rastrear las políticas AWS administradas para Amazon Route 53 Application Recovery Controller	<p>Se realizará un seguimiento de las actualizaciones de las políticas administradas a partir de la fecha de lanzamiento inicial.</p> <p>Para obtener más información, consulte AWS políticas gestionadas de Amazon Route 53 Application Recovery Controller.</p>	27 de julio de 2021
Publicación inicial del controlador de recuperación de aplicaciones Amazon Route 53.	<p>Route 53 ARC mejora la disponibilidad de las aplicaciones al coordinar centralmente las conmutaciones por error dentro de una AWS región o entre varias regiones. Route 53 ARC proporciona comprobaciones de preparación para garantizar que sus aplicaciones estén escaladas para gestionar el tráfico de conmutación por error y configuradas para evitar las fallas. También proporciona un control de enrutamiento extremadamente confiable para que pueda recuperar las aplicaciones redirigiendo el tráfico, por ejemplo, entre zonas o regiones de disponibilidad. Para obtener más información, consulte Qué es Route 53 ARC.</p>	27 de julio de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.