AWS Well-Architected Framework

Pilar de fiabilidad

Principios para diseñar, operar y evolucionar cargas de trabajo confiables en la nube.

- ALTA DISPONIBILIDAD
- RESILIENCIA
- RECUPERACIÓN
- OPERACIONES CONFIABLES

Amazon Web Services

Diseño original de portada

© 2026 Amazon Web Services, Inc. and/or its affiliates.

Pilar de fiabilidad: AWS Well-Architected Framework

Copyright © 2026 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

Resumen e introducción ... 1
Introducción ... 1
Fiabilidad ... 3
Modelo de responsabilidad compartida para la resiliencia ... 3
Principios de diseño ... 7
Definiciones ... 8
La resiliencia y los componentes de la fiabilidad ... 8
Disponibilidad ... 9
Objetivos de recuperación de desastres (DR) ... 13
Comprensión de las necesidades de disponibilidad ... 15
Principios básicos ... 17
Administración de cuotas de servicio y restricciones ... 17
REL01-BP01 Conocimiento de las cuotas y restricciones del servicio ... 18
REL01-BP02 Administración de cuotas de servicio en cuentas y regiones ... 24
REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura ... 28
REL01-BP04 Supervisión y administración de cuotas ... 32
REL01-BP05 Automatización de la administración de cuotas ... 36
REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error ... 39
Planificación de la topología de la red ... 43
REL02-BP01 Uso de conectividad de red de alta disponibilidad para los puntos de conexión públicos de la carga de trabajo ... 44
REL02-BP02 Aprovisionamiento de conectividad redundante entre las redes privadas en la nube y los entornos en las instalaciones ... 49
REL02-BP03 Garantía de que la asignación de subredes IP tenga en cuenta la expansión y la disponibilidad ... 52
REL02-BP04 Preferencia de topologías radiales (“hub-and-spoke”) frente a una conexión en malla de varios a varios ... 55
REL02-BP05 Aplicación de intervalos de direcciones IP privadas que no se superponen en todos los espacios de direcciones privadas en los que están conectados ... 59
Arquitectura de la carga de trabajo ... 62
Diseño de la arquitectura de servicio de su carga de trabajo ... 62
REL03-BP01 Elección de cómo segmentar su carga de trabajo ... 63

REL03-BP02 Desarrollo de servicios centrados en funcionalidades y dominios empresariales específicos ... 67
REL03-BP03 Disposición de contratos de servicio por cada API ... 71
Diseño de las interacciones en un sistema distribuido para evitar los errores ... 75
REL04-BP01 Identificación del tipo de sistemas distribuidos de los que depende ... 75
REL04-BP02 Implementación de dependencias con acoplamiento débil ... 81
REL04-BP03 Trabajo constante ... 85
REL04-BP04 Cómo hacer idempotentes las operaciones de mutación ... 86
Diseño de interacciones en un sistema distribuido para mitigar o tolerar errores ... 92
REL05-BP01 Implementación de una degradación estable para transformar las dependencias estrictas en flexibles ... 93
REL05-BP02 Limitación de las solicitudes ... 97
REL05-BP03 Control y limitación de las llamadas de reintento ... 101
REL05-BP04 Respuesta rápida a los errores y limitación de las colas ... 104
REL05-BP05 Definición de los tiempos de espera del cliente ... 108
REL05-BP06 Creación de sistemas sin estado cuando sea posible ... 112
REL05-BP07 Implementación de recursos de emergencia ... 114
Administración de cambios ... 117
Supervisión de los recursos de la carga de trabajo ... 117
REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación) ... 118
REL06-BP02 Definición y cálculo de métricas (agregación) ... 122
REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real) ... 127
REL06-BP04 Automatización de las respuestas (procesamiento y alarmas en tiempo real) . 131
REL06-BP05 Análisis de registros ... 134
REL06-BP06 Revisiones frecuentes ... 136
REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema ... 139
Diseño de su carga de trabajo para adaptarla a los cambios en la demanda ... 143
REL07-BP01 Uso de la automatización al obtener o escalar recursos ... 143
REL07-BP02 Obtención de recursos tras detectar un impedimento en una carga de trabajo ... 146
REL07-BP03 Obtención de recursos tras detectar que se necesitan más recursos para una carga de trabajo ... 148
REL07-BP04 Pruebas en su carga de trabajo ... 152
Implementación de cambios ... 154

REL08-BP01 Uso de manuales de procedimientos para actividades estándar como la implementación ... 155
REL08-BP02 Integración de las pruebas funcionales como parte de la implementación ... 157
REL08-BP03 Integración de las pruebas de resiliencia como parte de la implementación ... 160
REL08-BP04 Implementación mediante una infraestructura inmutable ... 163
REL08-BP05 Implementación de cambios con automatización ... 168
Administración de errores ... 171
Copia de seguridad de los datos ... 172
REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes ... 172
REL09-BP02 Protección y cifrado de copias de seguridad ... 176
REL09-BP03 Copias de seguridad automáticas de los datos ... 180
REL09-BP04 Recuperación periódica de los datos para verificar la integridad de la copia de seguridad y los procesos ... 183
Uso del aislamiento de errores para proteger su carga de trabajo ... 187
REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones ... 188
REL10-BP02 Automatización de la recuperación de los componentes restringidos a una sola ubicación ... 197
REL10-BP03 Uso de arquitecturas herméticas para limitar el alcance del impacto ... 199
Diseño de la carga de trabajo para que tolere los errores de los componentes ... 204
REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores ... 204
REL11-BP02 Conmutación por error a recursos en buen estado ... 208
REL11-BP03 Automatización de la reparación en todas las capas ... 212
REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación ... 216
REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal ... 221
REL11-BP06 Envío de notificaciones cuando los eventos afecten a la disponibilidad ... 225
REL11-BP07 Diseño de su producto para cumplir objetivos de disponibilidad y acuerdos de nivel de servicio (SLA) de tiempo de actividad ... 228
Pruebas de fiabilidad ... 231
REL12-BP01 Uso de manuales de estrategias para investigar los errores ... 231
REL12-BP02 Análisis después del incidente ... 233
REL12-BP03 Requisitos de escalado y rendimiento de las pruebas ... 236
REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos ... 241

REL12-BP05 Planificación periódica de días de juego 252
Planificación de la recuperación de desastres (DR) 255
REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos 256
REL13-BP02 Uso de estrategias de recuperación definidas para cumplir los objetivos de recuperación 261
REL13-BP03 Prueba de la implementación de recuperación de desastres para validarla 276
REL13-BP04 Administración de la desviación de la configuración en el sitio o región de DR 278
REL13-BP05 Automatización de la recuperación 281
Conclusión 286
Colaboradores 287
Documentación adicional 288
Revisiones del documento 289
Avisos 296
Glosario de AWS 297

Pilar de fiabilidad: Marco de AWS Well-Architected

Fecha de publicación: 6 de noviembre de 2024 (Revisiones del documento)

Este documento se centra en el pilar de fiabilidad del Marco de AWS Well-Architected. Proporciona una guía para ayudar a los clientes a aplicar las prácticas recomendadas a la hora de diseñar, entregar y mantener los entornos de Amazon Web Services (AWS).

Introducción

El Marco de AWS Well-Architected le ayuda a comprender las ventajas y desventajas de las decisiones que toma al crear cargas de trabajo en AWS. El uso del marco le permitirá conocer las prácticas recomendadas de arquitectura para diseñar y operar cargas de trabajo en la nube que sean fiables, seguras, eficientes, rentables y sostenibles. Proporciona una forma de medir sus arquitecturas de forma constante en función de las prácticas recomendadas y de identificar áreas de mejora. Creemos que contar con cargas de trabajo bien diseñadas aumenta en gran medida la probabilidad de éxito empresarial.

El Marco de AWS Well-Architected se basa en seis pilares:

- Excelencia operativa
- Seguridad
- Fiabilidad
- Eficacia del rendimiento
- Optimización de costes
- Sostenibilidad

El presente documento se centra en el pilar de fiabilidad y cómo aplicarlo a sus soluciones. Lograr la fiabilidad puede ser un reto en los entornos tradicionales en las instalaciones debido a factores de puntos únicos de errores, la falta de automatización y la falta de elasticidad. Al adoptar las prácticas de este documento, creará arquitecturas con fundamentos sólidos, una arquitectura resiliente, una administración de cambios consistente y procesos de recuperación de errores comprobados.

Este documento está destinado a aquellos que ocupan puestos en tecnología, como los directores de tecnología (CTO), arquitectos, desarrolladores y miembros del equipo de operaciones. Después de leer este documento, comprenderá mejor las prácticas recomendadas y estrategias de AWS

que puede utilizar cuando diseñe arquitecturas en la nube para lograr que sean fiables. El presente documento incluye detalles de implementación de alto nivel y patrones de arquitectura, así como referencias a recursos adicionales.

Fiabilidad

El pilar de fiabilidad abarca la capacidad de una carga de trabajo para llevar a cabo su función prevista de forma correcta y coherente cuando se espera que lo haga. Esto incluye la capacidad de utilizar y probar la carga de trabajo a lo largo de todo su ciclo de vida. En este documento se incluye orientación de prácticas recomendadas para la implementación de cargas de trabajo fiables en AWS.

Temas

- Modelo de responsabilidad compartida para la resiliencia
- Principios de diseño
- Definiciones
- Comprensión de las necesidades de disponibilidad

Modelo de responsabilidad compartida para la resiliencia

La resiliencia es una responsabilidad compartida entre AWS y el cliente. Es importante que entienda cómo la recuperación de desastres (DR) y la disponibilidad, como parte de la resiliencia, operan bajo este modelo compartido.

AWS Responsabilidad de : resiliencia de la nube

AWS es responsable de la resiliencia de la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la Nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan servicios de la Nube de AWS. AWS hace todos los esfuerzos razonables desde el punto de vista comercial para que estos servicios de la Nube de AWS estén disponibles, lo que garantiza que la disponibilidad del servicio cumpla o supere los acuerdos de nivel de servicio (SLA) de AWS.

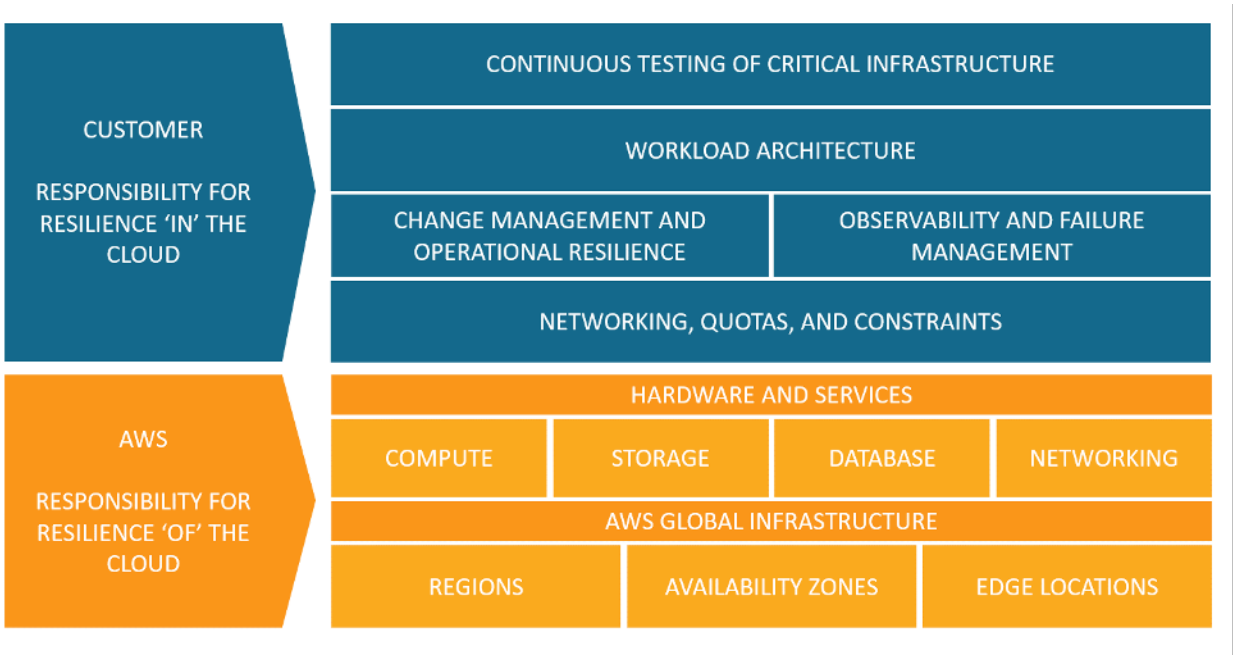
La infraestructura en la nube global de AWS está diseñada para permitir a los clientes crear arquitecturas de cargas de trabajo altamente resilientes. Cada Región de AWS está totalmente aislada y se compone de múltiples zonas de disponibilidad, que son particiones físicamente aisladas de la infraestructura. Las zonas de disponibilidad aíslan errores que podrían afectar la resiliencia de la carga de trabajo y les impide repercutir en otras zonas en la región. Al mismo tiempo, todas las AZ de una Región de AWS están interconectadas con ancho de banda alto y redes de baja latencia, y utilizan fibra metropolitana dedicada y totalmente redundante, lo que ofrece una conexión de red de baja latencia y alto rendimiento entre las zonas. Todo el tráfico entre las zonas está cifrado. El

rendimiento de la red es suficiente para llevar a cabo la replicación sincrónica entre zonas. Cuando una aplicación está particionada en varias AZ, las empresas estarán mejor aisladas y contarán con mayor protección frente a problemas como interrupciones de alimentación eléctrica, tormentas eléctricas, tornados, huracanes, etc.

Responsabilidad del cliente: resiliencia en la nube

Su responsabilidad vendrá determinada por los servicios de Nube de AWS que elija. Esto determina la cantidad de trabajo de configuración que debe llevar a cabo como parte de sus responsabilidades de resiliencia. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) exige que el cliente lleve a cabo todas las tareas necesarias de configuración y administración de la resiliencia. Los clientes que implementan instancias de Amazon EC2 son responsables de implementar las instancias de Amazon EC2 en varias ubicaciones (como las zonas de disponibilidad de AWS), implementar la autorreparación mediante servicios como el escalado automático y utilizar las prácticas recomendadas de arquitectura de carga de trabajo resiliente para las aplicaciones instaladas en las instancias. En el caso de los servicios administrados, como Amazon S3 y Amazon DynamoDB, AWS se encarga de gestionar la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de conexión para guardar y recuperar información. El cliente es responsable de administrar la resiliencia de sus datos, incluidas las estrategias de copia de seguridad, control de versiones y replicación.

La implementación de la carga de trabajo en varias zonas de disponibilidad de una Región de AWS forma parte de una estrategia de alta disponibilidad diseñada para proteger las cargas de trabajo al aislar los problemas en una zona de disponibilidad, que utiliza la redundancia de las demás zonas de disponibilidad para seguir atendiendo las solicitudes. Una arquitectura de varias zonas de disponibilidad también forma parte de una estrategia de DR diseñada para que las cargas de trabajo estén mejor aisladas y protegidas de problemas como interrupciones de alimentación eléctrica, tormentas eléctricas, tornados, terremotos, etc. Las estrategias de DR también pueden hacer uso de varias Regiones de AWS. Por ejemplo, en una configuración activa-pasiva, el servicio para la carga de trabajo pasa de su región activa a su región de DR si la región activa ya no puede atender solicitudes.



Responsabilidad de los clientes y en cuanto a la resiliencia dentro y fuera de la nube AWS.

Puede utilizar los servicios de AWS para lograr sus objetivos de resiliencia. Como cliente, es responsable de la administración de los siguientes aspectos de su sistema para lograr la resiliencia en la nube. Para obtener más información sobre cada servicio en particular, consulte la documentación de AWS.

Redes, cuotas y limitaciones

- Las prácticas recomendadas para esta área del modelo de responsabilidad compartida se describen en detalle en Principios básicos.
- Planifique su arquitectura con el espacio suficiente para escalarla y comprenda las cuotas de servicio y las limitaciones de los servicios que incluya, en función de los aumentos de carga esperados en las solicitudes, cuando proceda.
- Diseñe la topología de red para que sea de alta disponibilidad, redundante y escalable.

Administración de cambios y resiliencia operativa

- Administración de cambios incluye cómo introducir y administrar los cambios en su entorno. La implementación de cambios requiere crear y mantener actualizados los manuales de procedimientos y estrategias de implementación para su aplicación e infraestructura.

- Una estrategia flexible para supervisar los recursos de la carga de trabajo considera todos los componentes, incluidas las métricas técnicas y empresariales, las notificaciones, la automatización y el análisis.
- Las cargas de trabajo en la nube deben adaptarse a los cambios en la demanda al reducir horizontalmente en respuesta a las deficiencias o fluctuaciones del uso.

Observabilidad y administración de errores

- Es necesario observar los fallos mediante la supervisión para automatizar la reparación, de modo que sus cargas de trabajo puedan soportar los fallos de los componentes.
- La administración de errores requiere hacer copias de seguridad de los datos, aplicar las prácticas recomendadas para permitir que la carga de trabajo resista los fallos de los componentes y planificar la recuperación de desastres.

Arquitectura de la carga de trabajo

- La arquitectura de la carga de trabajo incluye la forma de diseñar los servicios en torno a los dominios empresariales, aplicar el diseño de sistemas distribuidos y de SOA para evitar fallos e incorporar capacidades como la limitación, los reintentos, la gestión de colas, los tiempos de espera y las palancas de emergencia.
- Confíe en las soluciones de AWS probadas, la Amazon Builders' Library y los patrones sin servidor para alinearse con las prácticas recomendadas y poner en marcha las implementaciones.
- Utilice la mejora continua para descomponer su sistema en servicios distribuidos para escalar e innovar con más rapidez. Utilice la orientación sobre microservicios de AWS y las opciones de servicios administrados para simplificar y acelerar su capacidad de introducir cambios e innovar.

Pruebas continuas de infraestructura crucial

- Prueba de fiabilidad implica hacer pruebas a nivel funcional, de rendimiento y de caos, así como adoptar prácticas de análisis de incidentes y prácticas propias del día de juego para adquirir experiencia en la resolución de problemas que no se comprenden bien.
- Tanto para las aplicaciones en la nube como para las híbridas, saber cómo se comporta su aplicación cuando surgen problemas o se caen los componentes le permite recuperarse de las interrupciones de forma rápida y fiable.

- Cree y documente experimentos repetibles para comprender cómo se comporta su sistema cuando las cosas no funcionan como se esperaba. Estas pruebas demostrarán la eficacia de su capacidad de recuperación general y proporcionarán un bucle de retroalimentación para sus procedimientos operativos antes de enfrentarse a escenarios de error reales.

Principios de diseño

En la nube, hay algunos principios que pueden contribuir a aumentar la fiabilidad. Téngalos presentes cuando hablemos de las prácticas recomendadas:

- Recuperación automática de un error: al supervisar una carga de trabajo de indicadores clave de rendimiento (KPI), se puede ejecutar la automatización cuando se supera un umbral. Estos KPI deben ser una medida del valor de negocio, no de los aspectos técnicos del funcionamiento del servicio. De este modo, se permite la notificación y el seguimiento automático de los errores, así como los procesos de recuperación automatizada que pueden solucionar o corregir el error. Con una automatización más sofisticada, es posible anticipar y solucionar errores antes de que sucedan.
- Prueba de los procedimientos de recuperación: en un entorno en las instalaciones, a menudo se hacen pruebas para ver si una carga de trabajo funciona en una situación concreta. Normalmente, las pruebas no se usan para comprobar estrategias de recuperación. En la nube, puede probar los errores de la carga de trabajo y validar los procedimientos de recuperación. Puede usar la automatización para simular diferentes errores o recrear escenarios que anteriormente han producido algún error. Esto expone vías de error que puede probar y arreglar antes de que se produzca una situación de error real, lo que reduce el riesgo.
- Escalado horizontal para aumentar la disponibilidad agregada de la carga de trabajo: reemplace un gran recurso por varios recursos pequeños para reducir el efecto de un solo error en toda la carga de trabajo. Distribuya las solicitudes a través de varios recursos más pequeños para garantizar que no compartan el mismo error.
- No más conjeturas sobre la capacidad: un factor común de error de los sistemas en las instalaciones es la saturación de recursos, cuando las demandas que se hacen a una carga de trabajo superan su capacidad (este es a menudo el objetivo de los ataques de denegación de servicio). En la nube, se puede supervisar la demanda y el uso de la carga de trabajo, además de automatizar la incorporación o eliminación de recursos de forma automatizada para mantener un nivel óptimo y satisfacer la demanda sin tener un aprovisionamiento excesivo o insuficiente. Aún hay límites, pero algunas cuotas se pueden controlar, mientras que otras se pueden administrar (consulte Manage Service Quotas and Constraints).

- Administración de los cambios mediante la automatización: los cambios que se apliquen a la infraestructura deben hacerse mediante la automatización. Entre los cambios que se deben administrar se encuentran los de la automatización, de los que, posteriormente, se puede hacer un seguimiento y una revisión.

Definiciones

En este documento técnico se trata la fiabilidad en la nube y se describen las prácticas recomendadas para estas cuatro áreas:

- Principios básicos
- Arquitectura de la carga de trabajo
- Administración de cambios
- Administración de errores

Para lograr la fiabilidad hay que empezar por los cimientos: un entorno en el que las cuotas de servicio y la topología de la red se adapten a la carga de trabajo. La arquitectura de la carga de trabajo del sistema distribuido debe estar diseñada para prevenir y mitigar los errores. La carga de trabajo debe gestionar los cambios en la demanda o los requisitos, y debe estar diseñada para detectar errores y repararse automáticamente.

Temas

- La resiliencia y los componentes de la fiabilidad
- Disponibilidad
- Objetivos de recuperación de desastres (DR)

La resiliencia y los componentes de la fiabilidad

La fiabilidad de una carga de trabajo en la nube depende de varios factores, el principal de los cuales es la resiliencia:

- La resiliencia es la capacidad de una carga de trabajo para recuperarse de interrupciones en la infraestructura o el servicio, para incorporar dinámicamente recursos computacionales que satisfagan la demanda y para mitigar las interrupciones, como errores de configuración o problemas de red temporales.

Los otros factores que influyen en la fiabilidad de la carga de trabajo son:

- Excelencia operativa, que incluye la automatización de los cambios, el uso de manuales de estrategias para responder a los errores y las revisiones de disponibilidad operativa (ORR) para confirmar que las aplicaciones estén listas para las operaciones de producción.
- La seguridad, que incluye la prevención de daños a los datos o a la infraestructura por parte de infractores, lo que afectaría a la disponibilidad. Por ejemplo, cifrar las copias de seguridad para garantizar la seguridad de los datos.
- Eficiencia del rendimiento, que incluye el diseño para obtener las máximas tasas de solicitudes y minimizar las latencias para su carga de trabajo.
- Optimización de costos, que incluye compensaciones tales como si se debe gastar más en instancias de EC2 para lograr la estabilidad estática o confiar en el escalado automático cuando se necesita más capacidad.

La resiliencia es el objetivo principal de este documento técnico.

Los otros cuatro aspectos también son importantes y están cubiertos por sus respectivos pilares del Marco de AWS Well-Architected. En muchas de estas prácticas recomendadas también se tratan esos aspectos de la fiabilidad, pero el enfoque se centra en la resiliencia.

Disponibilidad

La disponibilidad (también conocida como disponibilidad del servicio) es una métrica de uso común para medir cuantitativamente la resiliencia, así como un objetivo de resiliencia.

- La disponibilidad es el porcentaje de tiempo que una carga de trabajo está dispondisponibilidad es el porcentaje de tiempo que una carga de trabajo está disponible para utilizarse.

Que esté disponible para su uso significa que cumple satisfactoriamente la función acordada cuando es necesario.

Este porcentaje se calcula en periodos de tiempo, por ejemplo, mensual, anual o trienal. Al aplicar la interpretación más estricta posible, la disponibilidad se reduce siempre que la aplicación no funciona con normalidad, ya sea con interrupciones programadas o no programadas. Definimos la disponibilidad de la siguiente manera:

$$Availability = \frac{Available\ for\ Use\ Time}{Total\ Time}$$

- La disponibilidad es un porcentaje de tiempo de actividad (como el 99,9 %) durante un periodo de actividad (normalmente un mes o un año)
- La denominación común se refiere únicamente al “número de nueves” (por ejemplo, “cinco nueves” se traduce en una disponibilidad del 99,999 %).
- Algunos clientes optan por excluir el tiempo de inactividad del servicio programado (por ejemplo, el mantenimiento previsto) del tiempo total en la formula. Sin embargo, esto no es aconsejable, ya que es probable que sus usuarios quieran utilizar su servicio durante esas horas.

A continuación, se presenta una tabla con los objetivos comunes de diseño de disponibilidad de aplicaciones y la duración máxima en el que de las interrupciones se pueden producir en un año sin dejar de cumplir el objetivo. En la tabla figuran ejemplos de los tipos de aplicaciones que se suelen ver en cada nivel de disponibilidad. A lo largo del documento, trataremos estos valores.

Disponibilidad	Falta de disponibilidad máxima (por año)	Categorías de aplicación
99%	3 días 15 horas	Procesamiento en lotes, extracción de datos, transfere ncia y trabajos de carga
99,9%	8 horas 45 minutos	Herramientas internas como la administración del conocimie nto o el seguimiento de proyectos
99,95 %	4 horas 22 minutos	Comercio en línea, punto de venta
99,99%	52 minutos	Cargas de trabajo de entrega y transmisión de video

Disponibilidad	Falta de disponibilidad máxima (por año)	Categorías de aplicación
99,999 %	5 minutos	Cargas de trabajo de transacciones en cajeros automáticos y telecomunicaciones

Medición de la disponibilidad en función de las solicitudes. Para su servicio, puede ser más fácil contar las solicitudes correctas y erróneas en lugar del “tiempo disponible para su uso”. En este caso, se puede utilizar el siguiente cálculo:

$$Availability = \frac{Successful\ Responses}{Valid\ Requests}$$

Suele medirse por periodos de uno o cinco minutos. Se puede calcular un porcentaje de tiempo de actividad mensual (medición de la disponibilidad en función del tiempo) a partir de la media de estos periodos. Si no se recibe ninguna solicitud en un periodo determinado, se cuenta con el 100 % disponible para ese tiempo.

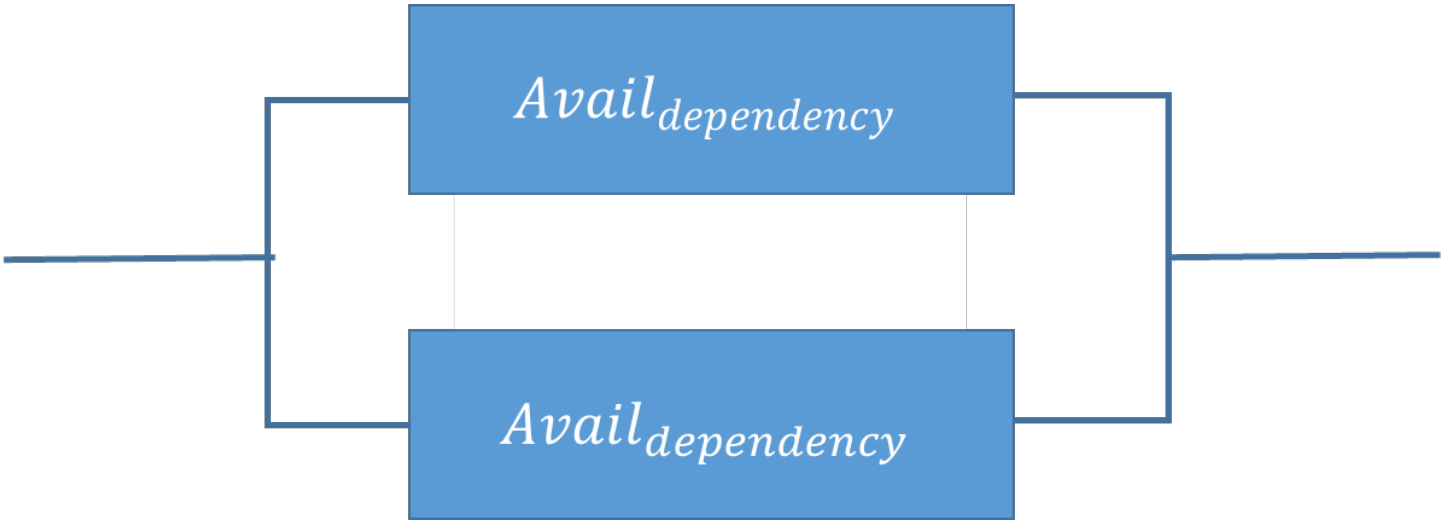
Cálculo de la disponibilidad con gran dependencia. Muchos sistemas dependen de otros, por lo que la interrupción de un sistema dependiente se interpreta directamente como una interrupción en el sistema de invocación. Esto se contrapone a una dependencia flexible, en la que un error del sistema dependiente se compensa en la aplicación. Cuando se producen las dependencias estrictas, la invocación de la disponibilidad del sistema es el producto de las disponibilidades de los sistemas dependientes. Por ejemplo, si se tiene un sistema diseñado para una disponibilidad del 99,99 % que tenga una dependencia estricta de otros dos sistemas independientes que están diseñados para una disponibilidad del 99,99 % cada uno, la carga de trabajo puede teóricamente lograr una disponibilidad del 99,97 %:

$Avail_{invok} \times Avail_{dep1} \times Avail_{dep2} = Avail_{workload}$

99,99 % × 99,99 % × 99,99 % = 99,97 %

Por lo tanto, es importante entender sus dependencias y sus objetivos de diseño de disponibilidad al hacer los cálculos.

Cálculo de la disponibilidad con componentes redundantes. Cuando un sistema implica el uso de componentes independientes y redundantes (por ejemplo, recursos redundantes en diferentes zonas de disponibilidad), la disponibilidad teórica se calcula como el 100 % menos el producto de las tasas de error de los componentes. Por ejemplo, si un sistema utiliza dos componentes independientes, cada uno con una disponibilidad del 99,9 %, la disponibilidad efectiva de esta dependencia es 99,9999 %:



$Avail_{effective} = Avail_{MAX} - ((100\% - Avail_{dependency}) \times (100\% - Avail_{dependency}))$

99,9999 % = 100 % − (0,1 % × 0,1 %)

Cálculo abreviado: si la disponibilidad de todos los componentes del cálculo consiste únicamente en el dígito nueve, puede sumar el número de nueves dígitos para obtener la respuesta. En el ejemplo anterior, dos componentes redundantes e independientes con una disponibilidad de tres nueves dan como resultado seis nueves.

Cálculo de la disponibilidad de las dependencias. Algunas dependencias proporcionan orientación sobre su disponibilidad, por ejemplo, los objetivos de diseño de disponibilidad de muchos servicios de AWS. Pero en los casos en los que no está disponible (por ejemplo, un componente en el que el fabricante no publica la información sobre la disponibilidad), una forma sencilla de estimarla es determinar el tiempo medio entre errores (MTBF) y el tiempo medio de recuperación (MTTR). Se puede estimar la disponibilidad:

$$Avail_{EST} = \frac{MTBF}{MTBF + MTTR}$$

Por ejemplo, si el MTBF es de 150 días y el MTTR es de 1 hora, la disponibilidad estimada será del 99,97 %.

Para obtener más información, consulte Availability and Beyond: Understanding and improving the resilience of distributed systems on AWS, que puede ayudarle a calcular su disponibilidad.

Costos de disponibilidad. El diseño de aplicaciones para niveles más altos de disponibilidad suele aumentar los costos, por lo que es conveniente identificar las verdaderas necesidades de disponibilidad antes de iniciar el diseño de la aplicación. Los altos niveles de disponibilidad exigen requisitos más estrictos para el ensayo y la validación en situaciones de error exhaustivas. Requieren la automatización para la recuperación de todo tipo de errores y necesitan que todos los aspectos de las operaciones del sistema se desarrollen y prueben de forma similar con los mismos estándares. Por ejemplo, el aumento o la disminución de la capacidad, la implementación o restauración de software actualizado o cambios en la configuración, o la migración de los datos del sistema se deben efectuar hasta alcanzar el objetivo de disponibilidad deseado. Al sumar los costos de desarrollo de software con niveles de disponibilidad muy elevados, la innovación se ve afectada por la necesidad de avanzar más lentamente en la implementación de los sistemas. Por lo tanto, la orientación debe ser minuciosa al aplicar las normas y considerar el objetivo de disponibilidad adecuado para todo el ciclo de vida del sistema.

La selección de dependencias es otra forma con la que aumentan los costos en los sistemas que funcionan con objetivos de diseño de mayor disponibilidad. En estos objetivos superiores, el conjunto de programas o servicios que se pueden elegir como dependencias disminuye en función de cuáles de estos servicios han tenido las inversiones más importantes que hemos descrito anteriormente. A medida que aumenta el objetivo de diseño de la disponibilidad, es habitual encontrar menos servicios de uso múltiple (como una base de datos relacional) y más servicios de uso específico. Esto se debe a que los servicios de uso específico son más fáciles de evaluar, probar y automatizar, además de que muestran menos posibilidades de interacciones inesperadas con funcionalidades incluidas, pero sin utilizar.

Objetivos de recuperación de desastres (DR)

Además de los objetivos de disponibilidad, su estrategia de resiliencia debe incluir también objetivos de recuperación de desastres (DR) basados en estrategias para recuperar la carga de trabajo en caso de que se produzca un desastre. La recuperación de desastres se centra en objetivos de recuperación puntuales en respuesta a catástrofes naturales, errores técnicos a gran escala o amenazas humanas como ataques o errores. Es distinto de la disponibilidad, que mide la resiliencia

media durante un periodo de tiempo en respuesta a los errores de los componentes, los picos de carga o los errores de software.

Objetivo de tiempo de recuperación (RTO) definido por la organización. El RTO es la máxima demora aceptable entre la interrupción del servicio y el restablecimiento del servicio. Este valor determina el período de tiempo que se considera aceptable cuando el servicio no está disponible.

Objetivo de punto de recuperación (RPO) definido por la organización. El RPO es la cantidad máxima de tiempo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

La relación entre el RPO (objetivo de punto de recuperación), el RTO (objetivo de tiempo de recuperación) y el evento del desastre.

El RTO es similar al MTTR (tiempo medio de recuperación) en el sentido de que ambos miden el tiempo transcurrido entre el inicio de una interrupción y la recuperación de la carga de trabajo. Sin embargo, el MTTR es un valor medio que se aplica a varios eventos que afectan a la disponibilidad durante un periodo de tiempo, mientras que el RTO es un valor objetivo, o el valor máximo permitido, para un solo evento que afecta a la disponibilidad.

Comprensión de las necesidades de disponibilidad

Es común pensar inicialmente en la disponibilidad de una aplicación como un solo objetivo para la aplicación en su totalidad. Sin embargo, al analizarlo más detenidamente, con frecuencia encontramos que ciertos aspectos de una aplicación o servicio tienen requisitos de disponibilidad diferentes. Por ejemplo, algunos sistemas podrían dar prioridad a la capacidad de recibir y almacenar nuevos datos antes que a la de recuperar datos ya existentes. Otros sistemas dan prioridad a las operaciones en tiempo real sobre las operaciones que cambian la configuración o el entorno de un sistema. Los servicios pueden tener requisitos de disponibilidad muy elevados durante ciertas horas del día, pero pueden tolerar periodos mucho más largos de interrupción fuera de esas horas. Estas son algunas de las formas en que se puede separar una sola aplicación en las unidades funcionales y evaluar los requisitos de disponibilidad de cada una de ellas. El beneficio de hacerlo consiste en centrar los esfuerzos (y los gastos) en la disponibilidad de acuerdo con las necesidades específicas, en lugar de diseñar todo el sistema según los requisitos de mayor exigencia.

Recomendación
Evalúe de forma crítica los aspectos exclusivos de sus aplicaciones y, según corresponda, determine los objetivos de diseño de la disponibilidad y de la recuperación de desastres para reflejar las necesidades de su empresa.

En AWS, normalmente dividimos los servicios en el “plano de datos” y el “plano de control”. El plano de datos se encarga de entregar el servicio en tiempo real mientras que el plano de control se utiliza para configurar el entorno. Por ejemplo, las instancias de Amazon EC2, las bases de datos de Amazon RDS y las operaciones de escritura de tablas de Amazon DynamoDB son operaciones de plano de datos. Por el contrario, el lanzamiento de nuevas instancias de EC2 o bases de datos RDS o agregar o cambiar los metadatos de las tablas en DynamoDB se consideran operaciones de plano de control. Si bien los altos niveles de disponibilidad son importantes para todas estas capacidades, los planos de datos suelen tener objetivos de diseño de disponibilidad más altos que los planos de control. Por lo tanto, las cargas de trabajo con requisitos de alta disponibilidad deben evitar la dependencia en tiempo de ejecución de las operaciones de plano de control.

Muchos clientes de AWS adoptan un enfoque similar para evaluar de forma crítica sus aplicaciones e identificar los subcomponentes con diferentes necesidades de disponibilidad. Los objetivos de diseño de la disponibilidad se adaptan a los diferentes aspectos y se llevan a cabo los debidos estudios de ingeniería del sistema. AWS cuenta con gran experiencia en aplicaciones de ingeniería

con un intervalo de objetivos de diseño de disponibilidad, incluidos servicios con una disponibilidad del 99,999 % o mayor. AWS Los arquitectos de soluciones (SA) pueden ayudarle a crear el diseño adecuado para lograr sus objetivos de disponibilidad. Involucrar a AWS en la fase inicial de su proceso de diseño aumenta nuestra capacidad para ayudarle a cumplir sus objetivos de disponibilidad. La planificación de la disponibilidad no solo se hace antes de lanzar la carga de trabajo. También se hace continuamente para perfeccionar su diseño a medida que se adquiere experiencia operativa, se aprende de los eventos reales y se toleran errores de diferentes tipos. De esta forma, podrá aplicar el esfuerzo de trabajo adecuado para mejorar su aplicación.

Las necesidades de disponibilidad que se requieren para una carga de trabajo deben estar alineadas con la necesidad empresarial y la criticidad. Al definir primero el marco de criticidad empresarial con RTO, RPO y disponibilidad definidos, podrá evaluar cada carga de trabajo. Este enfoque requiere que los implicados en la implementación de la carga de trabajo conozcan el marco y el impacto que su carga de trabajo tiene en las necesidades empresariales.

Principios básicos

Los requisitos fundamentales son aquellos cuyo ámbito va más allá de una única carga de trabajo o proyecto. Antes de diseñar la arquitectura de cualquier sistema, los requisitos básicos que afectan a la fiabilidad deberían estar aplicados. Por ejemplo, es preciso que haya suficiente ancho de banda de la red en el centro de datos.

En un entorno en las instalaciones, estos requisitos pueden alargar los plazos por las dependencias y, por lo tanto, se tienen que incorporar durante la planificación inicial. En AWS, sin embargo, la mayor parte de estos requisitos básicos están incorporados o pueden ser abordados según corresponda. La nube está diseñada para que sea, en esencia, ilimitada, por lo que la responsabilidad de ofrecer suficiente capacidad de computación y red recae en AWS. Esto permite que pueda cambiar la asignación y el tamaño de los recursos bajo demanda.

En las siguientes secciones se explican las prácticas recomendadas que se centran en estas consideraciones de fiabilidad.

Temas

- Administración de cuotas de servicio y restricciones
- Planificación de la topología de la red

Administración de cuotas de servicio y restricciones

Para las arquitecturas de carga de trabajo basadas en la nube, existen cuotas de servicio (que también se denominan límites de servicio). Estas cuotas existen para evitar el aprovisionamiento accidental de más recursos de los que se necesitan y para limitar las tasas de solicitudes en las operaciones de la API a fin de proteger los servicios contra el abuso. También hay limitaciones de recursos, por ejemplo, la velocidad a la que se pueden introducir bits por un cable de fibra óptica o la cantidad de almacenamiento en un disco físico.

Si usa aplicaciones de AWS Marketplace, debe comprender las limitaciones de esas aplicaciones. Si usa servicios web o software de terceros como servicio, también debe conocer dichos límites.

Prácticas recomendadas

- REL01-BP01 Conocimiento de las cuotas y restricciones del servicio
- REL01-BP02 Administración de cuotas de servicio en cuentas y regiones

- REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura
- REL01-BP04 Supervisión y administración de cuotas
- REL01-BP05 Automatización de la administración de cuotas
- REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error

REL01-BP01 Conocimiento de las cuotas y restricciones del servicio

Conozca las cuotas predeterminadas y administre las solicitudes de aumento de cuota para su arquitectura de carga de trabajo. Sepa qué restricciones de recursos en la nube, como el disco o la red, pueden causar impacto.

Resultado deseado: los clientes pueden evitar la degradación o la interrupción de sus Cuentas de AWS mediante la implementación de las directrices adecuadas para supervisar las métricas clave, las revisiones de la infraestructura y los pasos de corrección de la automatización para comprobar que no se alcancen las cuotas ni las restricciones de los servicios que puedan provocar un deterioro o interrupción de los mismos.

Patrones comunes de uso no recomendados:

- Implementar una carga de trabajo sin conocer las cuotas estrictas o flexibles y sus límites para los servicios utilizados.
- Implementar una carga de trabajo de reemplazo sin analizar ni volver a configurar las cuotas necesarias o sin contactar previamente con el servicio de asistencia.
- Suponer que los servicios en la nube no tienen límites y que los servicios pueden utilizarse sin tener en cuenta tarifas, límites, recuentos o cantidades.
- Suponer que las cuotas se incrementarán automáticamente.
- Desconocer el proceso y la cronología de las solicitudes de cuotas.
- Suponer que la cuota de servicio predeterminada en la nube es la misma para todos los servicios en diferentes regiones.
- Suponer que se pueden incumplir las restricciones del servicio y que los sistemas se escalarán automáticamente o agregarán un aumento del límite más allá de las restricciones del recurso.
- No probar la aplicación en picos de tráfico para estresar el uso de sus recursos.
- Aprovisionar el recurso sin analizar el tamaño de recurso requerido.

- Sobreaprovisionar la capacidad mediante la elección de tipos de recursos que van mucho más allá de las necesidades reales o de los picos previstos.
- No evaluar las necesidades de capacidad para nuevos niveles de tráfico antes de que se produzca un nuevo evento con un cliente o de implementar una nueva tecnología.

Beneficios de establecer esta práctica recomendada: la supervisión y la administración automatizada de las cuotas de servicio y las limitaciones de recursos pueden reducir los fallos de forma proactiva. Los cambios en los patrones de tráfico para el servicio de un cliente pueden provocar una interrupción o un deterioro si no se siguen las prácticas recomendadas. Con la supervisión y la administración de estos valores en todas las regiones y en todas las cuentas, las aplicaciones pueden tener una mayor resiliencia ante acontecimientos adversos o imprevistos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Service Quotas es un servicio de AWS que le ayuda a administrar sus cuotas de más de 250 servicios de AWS desde una sola ubicación. Además de consultar los valores de las cuotas, también puede solicitar y hacer un seguimiento de los aumentos de las cuotas desde la consola de Service Quotas o mediante el AWS SDK. AWS Trusted Advisor ofrece una comprobación de las cuotas que muestra su uso y las cuotas para ciertos aspectos de algunos servicios. Las cuotas de servicio predeterminadas por servicio también se encuentran en la documentación de AWS de cada servicio correspondiente (por ejemplo, consulte Cuotas de Amazon VPC).

Algunos límites de servicio, como los límites de velocidad en las API limitadas, se establecen en Amazon API Gateway mediante la configuración de un plan de uso. Algunos límites que se establecen como configuración en sus servicios respectivos incluyen las IOPS aprovisionadas, el almacenamiento asignado en Amazon RDS y las asignaciones de volumen de Amazon EBS. Amazon Elastic Compute Cloud tiene su propio panel de límites de servicio que puede ayudarle a administrar su instancia, Amazon Elastic Block Store y los límites de direcciones IP elásticas. Si tiene un caso de uso en el que las cuotas de servicio repercuten en el rendimiento de su aplicación y no se ajustan a sus necesidades, contacte con Soporte para ver si existen mitigaciones.

Las cuotas de servicio pueden ser específicas de una región o también pueden tener carácter global. El uso de un servicio de AWS que alcance su cuota no actuará del modo previsto en un uso normal y puede provocar la interrupción o el deterioro del servicio. Por ejemplo, una cuota de servicio limita el número de instancias de Amazon EC2 de DL utilizadas en una región. Ese límite se puede alcanzar durante un evento de escalado de tráfico mediante grupos de escalado automático (ASG).

Las cuotas de servicio de cada cuenta deben evaluarse periódicamente para determinar cuáles podrían ser los límites de servicio adecuados para esa cuenta. Estas cuotas de servicio existen como barreras de protección operativas para evitar aprovisionar por accidente más recursos de los necesarios. También sirven para limitar las tasas de solicitudes en las operaciones de API para proteger los servicios del abuso.

Las restricciones de servicio son diferentes de las cuotas de servicio. Las restricciones de servicio representan los límites de un recurso concreto, tal y como los define ese tipo de recurso. Pueden ser la capacidad de almacenamiento (por ejemplo, gp2 tiene un límite de tamaño de 1 GB - 16 TB) o el rendimiento del disco. Es esencial que las restricciones de un tipo de recurso se diseñen y evalúen constantemente para detectar un uso que pueda alcanzar su límite. Si se alcanza una restricción de forma inesperada, las aplicaciones o servicios de la cuenta pueden deteriorarse o interrumpirse.

Si existe un caso de uso en el que las cuotas de servicio repercuten en el rendimiento de una aplicación y no pueden ajustarse a las necesidades requeridas, contacte con Soporte para ver si existen mitigaciones. Para obtener más información sobre el ajuste de las cuotas fijas, consulte REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura.

Hay una serie de servicios y herramientas de AWS con las que se puede supervisar y administrar Service Quotas. El servicio y las herramientas se deben utilizar para proporcionar comprobaciones automatizadas o manuales de los niveles de cuota.

- AWS Trusted Advisor ofrece una comprobación de cuotas de servicio que muestra su uso y las cuotas para ciertos aspectos de algunos servicios. Puede ayudar a identificar los servicios que están cerca de la cuota.
- Consola de administración de AWS proporciona métodos para mostrar los valores de las cuotas de los servicios, administrar, solicitar nuevas cuotas, supervisar el estado de las solicitudes de cuotas y mostrar el historial de cuotas.
- AWS CLI y los CDK ofrecen métodos programáticos para administrar y supervisar automáticamente los niveles de cuota de servicio y el uso.

Pasos para la implementación

Para Service Quotas:

- Revise AWS Service Quotas.
- Para conocer sus cuotas de servicio existentes, determine los servicios (como Analizador de acceso de IAM) que se utilizan. Hay aproximadamente 250 servicios de AWS controlados por

cuotas de servicio. A continuación, determine el nombre específico de la cuota de servicio que se podría utilizar en cada cuenta y región. Hay aproximadamente 3000 nombres de cuotas de servicio por región.

- Amplíe este análisis de cuotas con AWS Config para encontrar todos los recursos de AWS que utiliza en suCuentas de AWS.
- Utilice los datos de AWS CloudFormation para determinar los recursos de AWS que utiliza. Observe los recursos que se crearon en la Consola de administración de AWS o con el comando `list-stack-resources` de la AWS CLI. También puede ver los recursos configurados para implementarlos en la propia plantilla.
- Consulte el código de implementación para determinar todos los servicios que necesita su carga de trabajo.
- Determine las cuotas de servicio que se aplican. Use la información accesible mediante programación de Trusted Advisor y Service Quotas.
- Establezca un método de supervisión automatizado (consulte REL01-BP02 Administración de cuotas de servicio en cuentas y regiones y REL01-BP04 Supervisión y administración de cuotas) para alertar e informar si las cuotas de servicios están cerca o han alcanzado su límite.
- Establezca un método automatizado y programático para comprobar si se ha modificado una cuota de servicio en una región, pero no en otras regiones de la misma cuenta (consulte REL01-BP02 Administración de cuotas de servicio en cuentas y regiones y REL01-BP04 Supervisión y administración de cuotas).
- Automatice el análisis de los registros y las métricas de las aplicaciones para determinar si existen errores de cuotas o restricciones de servicio. Si se producen estos errores, envíe alertas al sistema de supervisión.
- Establezca procedimientos de ingeniería para calcular el cambio requerido en la cuota (consulte REL01-BP05 Automatización de la administración de cuotas) una vez que se haya identificado que se requieren cuotas más altas para servicios específicos.
- Cree un flujo de trabajo de aprovisionamiento y aprobación para solicitar cambios en la cuota de servicio. Debería incluir un flujo de trabajo de excepciones en caso de denegación de la solicitud o de aprobación parcial.
- Cree un método de ingeniería para efectuar una revisión de las cuotas de servicio previa al aprovisionamiento y el uso de nuevos servicios de AWS antes de implementarlos en entornos de producción o de carga (por ejemplo, una cuenta de pruebas de carga).

Para las restricciones de servicio:

- Establezca métodos de supervisión y medición para alertar de la lectura de los recursos próximos a sus restricciones. Use CloudWatch de manera correspondiente para las métricas o la supervisión de registros.
- Establezca umbrales de alerta para cada recurso con una restricción significativa para la aplicación o el sistema.
- Cree procedimientos de administración de flujos de trabajo e infraestructuras para cambiar el tipo de recurso si la restricción está próxima a su uso. Como práctica recomendada, este flujo de trabajo debe incluir pruebas de carga para verificar que el nuevo tipo sea el tipo de recurso correcto con las nuevas restricciones.
- Migre el recurso identificado al nuevo tipo de recurso recomendado, mediante los procedimientos y los procesos existentes.

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP02 Administración de cuotas de servicio en cuentas y regiones
- REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura
- REL01-BP04 Supervisión y administración de cuotas
- REL01-BP05 Automatización de la administración de cuotas
- REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error
- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP03 Automatización de la reparación en todas las capas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Documentos relacionados:

- AWS Well-Architected Framework’s Reliability Pillar: Availability
- AWS Service Quotas (conocido anteriormente como límites del servicio)
- AWS Trusted Advisor Best Practice Checks (consulte la sección Service Limits)

- Monitor de cuotas para AWS en respuestas de AWS
- Cuotas de servicio de Amazon EC
- What is Service Quotas?
- How to Request Quota Increase
- Service endpoints and quotas
- Guía del usuario de Service Quotas
- Monitor de cuotas para AWS
- AWS Fault Isolation Boundaries
- Disponibilidad con redundancia
- AWS para datos
- ¿Qué es la integración continua?
- ¿Qué es la entrega continua?
- Socio de APN: socios que pueden ayudar con la administración de la configuración
- Managing the account lifecycle in account-per-tenant SaaS environments on AWS
- Managing and monitoring API throttling in your workloads
- View AWS Trusted Advisor recommendations at scale with AWS Organizations
- Automating Service Limit Increases and Enterprise Support with AWS Control Tower

Videos relacionados:

- AWS Live re:Inforce 2019 - Service Quotas
- View and Manage Quotas for AWS Services Using Service Quotas
- AWS IAM Quotas Demo

Herramientas relacionadas:

- Revisor de Amazon CodeGuru
- AWS CodeDeploy
- AWS CloudTrail
- Amazon CloudWatch
- Amazon EventBridge

- Amazon DevOps Guru
- AWS Config
- AWS Trusted Advisor
- AWS CDK
- AWS Systems Manager
- AWS Marketplace

REL01-BP02 Administración de cuotas de servicio en cuentas y regiones

Si utiliza múltiples cuentas o regiones, solicite las cuotas pertinentes en todos los entornos en los que se ejecutan sus cargas de trabajo de producción.

Resultado deseado: los servicios y las aplicaciones no deberían verse afectados por el agotamiento de la cuota de servicio de las configuraciones que abarquen cuentas o regiones o que tengan diseños de resiliencia que utilicen la conmutación por error de zona, región o cuenta.

Patrones comunes de uso no recomendados:

- Permitir que aumente el uso de recursos en una región aislada sin ningún mecanismo para mantener la capacidad en las demás.
- Configurar manualmente todas las cuotas de forma independiente en regiones aisladas.
- No considerar el efecto de las arquitecturas de resiliencia (activa o pasiva) en las futuras necesidades de cuota durante un deterioro de la región no principal.
- No evaluar las cuotas periódicamente ni hacer los cambios necesarios en cada región y cuenta donde se ejecuta la carga de trabajo.
- No utilizar las plantillas de solicitud de cuotas para solicitar aumentos en varias regiones y cuentas.
- No actualizar las cuotas de servicio por pensar erróneamente que el aumento de las cuotas tiene implicaciones de costo, como las solicitudes de reserva de computación.

Beneficios de establecer esta práctica recomendada: comprobar que puede gestionar la carga actual en regiones o cuentas secundarias en caso de que los servicios regionales dejen de estar disponibles. Esto puede reducir el número de errores o los niveles de deterioro que se producen durante la pérdida de una región.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

El seguimiento de las cuotas de servicio se lleva a cabo por cuenta. A no ser que se especifique lo contrario, cada cuota es específica de una Región de AWS. Además de los entornos de producción, administre también las cuotas en todos los entornos que no sean de producción aplicables, de modo que las pruebas y el desarrollo no se vean limitados. El mantenimiento de un elevado nivel de resiliencia requiere que las cuotas de servicio se evalúen continuamente (ya sea de forma automatizada o manual).

Dado que cada vez hay más cargas de trabajo en todas las regiones debido a la implementación de diseños que utilizan enfoques Activo/Activo, Activo/Pasivo (caliente), Activo/Pasivo (frío) y Activo/Pasivo (luz piloto), es esencial comprender los niveles de cuota de todas las regiones y cuentas. Los patrones de tráfico anteriores no siempre son un buen indicador de si la cuota de servicio está configurada correctamente.

Igualmente importante es el hecho de que el límite de nombres de cuota de servicio no es siempre el mismo para todas las regiones. En una región, el valor podría ser cinco, y en otra, diez. La administración de estas cuotas debe abarcar los mismos servicios, cuentas y regiones para proporcionar una resiliencia coherente bajo carga.

Concilie todas las diferencias de cuota de servicio entre las distintas regiones (región activa o región pasiva) y cree procesos para conciliar continuamente estas diferencias. Los planes de prueba de las conmutaciones por error pasivas de las regiones en muy pocas ocasiones se escalan a la capacidad activa máxima, lo que significa que los ejercicios del día de juego o de mesa pueden no encontrar diferencias en las cuotas de servicio entre las regiones y tampoco mantener los límites correctos.

Es muy importante hacer un seguimiento y evaluar la variación de las cuotas de servicio, es decir, la condición en la que se modifican los límites de las cuotas de servicio para una cuota determinada en una región y no en todas las regiones. Debe considerarse la posibilidad de cambiar la cuota en las regiones con tráfico o con posibilidad de tener tráfico.

- Seleccione las cuentas y regiones que correspondan según sus requisitos de servicio, latencia, normativos y de recuperación de desastres (DR).
- Identifique las cuotas de servicio en todas las cuentas, regiones y zonas de disponibilidad pertinentes. Los límites se determinan por cuenta y región. Estos valores deben compararse para detectar diferencias.

Pasos para la implementación

- Revise los valores de Service Quotas que podrían haber superado el nivel de riesgo de uso. AWS Trusted Advisor proporciona alertas si superan los umbrales del 80 % y el 90 %.
- Revise los valores de las cuotas de servicio en cualquier región pasiva (en un diseño Activo/Pasivo). Verifique que la carga se ejecutará correctamente en las regiones secundarias si se produce un error en la región principal.
- Automatice la evaluación de si se ha producido alguna desviación de la cuota de servicio entre regiones de la misma cuenta y actúe en consecuencia para modificar los límites.
- Si las unidades organizativas (UO) del cliente están estructuradas de la forma admitida, las plantillas de cuotas de servicio se deberán actualizar para reflejar los cambios en las cuotas que deban aplicarse a varias regiones y cuentas.
  - Cree una plantilla y asocie regiones al cambio de cuota.
  - Revise todas las plantillas de cuota de servicio existentes por si fuera necesario hacer algún cambio (región, límites y cuentas).

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP01 Conocimiento de las cuotas y restricciones del servicio
- REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura
- REL01-BP04 Supervisión y administración de cuotas
- REL01-BP05 Automatización de la administración de cuotas
- REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error
- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP03 Automatización de la reparación en todas las capas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Documentos relacionados:

- AWS Well-Architected Framework’s Reliability Pillar: Availability

- AWS Service Quotas (conocido anteriormente como límites del servicio)
- AWS Trusted Advisor Best Practice Checks (consulte la sección Service Limits)
- Monitor de cuotas para AWS en respuestas de AWS
- Cuotas de servicio de Amazon EC
- What is Service Quotas?
- How to Request Quota Increase
- Service endpoints and quotas
- Guía del usuario de Service Quotas
- Monitor de cuotas para AWS
- AWS Fault Isolation Boundaries
- Disponibilidad con redundancia
- AWS para datos
- ¿Qué es la integración continua?
- ¿Qué es la entrega continua?
- Socio de APN: socios que pueden ayudar con la administración de la configuración
- Managing the account lifecycle in account-per-tenant SaaS environments on AWS
- Managing and monitoring API throttling in your workloads
- View AWS Trusted Advisor recommendations at scale with AWS Organizations
- Automating Service Limit Increases and Enterprise Support with AWS Control Tower

Videos relacionados:

- AWS Live re:Inforce 2019 - Service Quotas
- View and Manage Quotas for AWS Services Using Service Quotas
- AWS IAM Quotas Demo

Servicios relacionados:

- Revisor de Amazon CodeGuru
- AWS CodeDeploy
- AWS CloudTrail

- Amazon CloudWatch
- Amazon EventBridge
- Amazon DevOps Guru
- AWS Config
- AWS Trusted Advisor
- AWS CDK
- AWS Systems Manager
- AWS Marketplace

REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura

Conozca las cuotas de servicio inalterables, las restricciones de servicio y los límites de recursos físicos. Diseñe arquitecturas para aplicaciones y servicios que eviten que estos límites afecten a la fiabilidad.

Algunos ejemplos son el ancho de banda de la red, el tamaño de la carga útil de la invocación de funciones sin servidor, la tasa de ráfagas de aceleración para una puerta de enlace de API y las conexiones simultáneas de usuarios a una base de datos.

Resultado deseado: la aplicación o el servicio funciona según lo esperado en condiciones de tráfico normal y alto. Se han diseñado para funcionar dentro de las limitaciones fijadas para ese recurso o cuotas de servicio.

Patrones comunes de uso no recomendados:

- Elegir un diseño que utilice el recurso de un servicio, sin saber que existen restricciones que provocarán que este diseño produzca un error en el escalado.
- Efectuar una evaluación comparativa que no es realista y que alcanzará las cuotas fijas del servicio durante la evaluación. Por ejemplo, ejecutar pruebas con un límite de ráfagas, pero durante un periodo prolongado.
- Elegir un diseño que no pueda escalarse ni modificarse si se van a superar las cuotas de servicio fijas. Por ejemplo, un tamaño de carga útil de SQS de 256 KB.
- No se diseña ni se implementa la observabilidad para supervisar y avisar sobre umbrales de cuotas de servicio que podrían estar en riesgo durante eventos de alto tráfico.

Beneficios de establecer esta práctica recomendada: comprobar que la aplicación se ejecute en todos los niveles de carga de servicios proyectados sin interrupciones ni deterioro.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

A diferencia de las cuotas de servicio o recursos flexibles que pueden sustituirse por unidades de mayor capacidad, las cuotas fijas de los servicios de AWS no pueden modificarse. Esto significa que todos estos tipos de servicios de AWS deben evaluarse para detectar posibles límites estrictos de capacidad cuando se utilizan en el diseño de una aplicación.

Los límites estrictos se muestran en la consola de Service Quotas. Si las columnas muestran `ADJUSTABLE = No`, el servicio tiene un límite estricto. Los límites estrictos también se muestran en algunas páginas de configuración de recursos. Por ejemplo, Lambda tiene límites estrictos específicos que no se pueden ajustar.

Por ejemplo, cuando se diseña una aplicación python para que se ejecute en una función de Lambda, es necesario evaluar la aplicación para determinar si existe alguna posibilidad de que Lambda se ejecute durante más de 15 minutos. Si el código puede ejecutarse durante más tiempo de este límite de cuota de servicio, deben considerarse tecnologías o diseños alternativos. Si se alcanza el límite después de la implementación en producción, la aplicación sufrirá degradación e interrupciones hasta que pueda remediarse. A diferencia de las cuotas flexibles, no existe ningún método para cambiar estos límites, ni siquiera en caso de eventos de emergencia de gravedad 1.

Una vez que la aplicación se ha implementado en un entorno de pruebas, se deben utilizar estrategias para averiguar si se puede alcanzar algún límite estricto. Las pruebas de estrés, las pruebas de carga y las pruebas de caos deben formar parte del plan de pruebas de introducción.

Pasos para la implementación

- Revise la lista completa de servicios de AWS que podrían utilizarse en la fase de diseño de la aplicación.
- Revise los límites de cuotas flexibles y estrictos para todos estos servicios. No todos los límites se muestran en la consola de Service Quotas. Algunos servicios describen estos límites en ubicaciones alternativas.
- Al diseñar su aplicación, revise los impulsores empresariales y tecnológicos de la carga de trabajo, como los resultados empresariales, el caso de uso, los sistemas dependientes, los objetivos de disponibilidad y los objetos de recuperación de desastres. Permita que sus impulsores

empresariales y tecnológicos guíen el proceso para identificar el sistema distribuido adecuado para su carga de trabajo.

- Analice la carga de servicio en todas las regiones y cuentas. Muchos límites estrictos se basan en la región para los servicios. Sin embargo, algunos límites se basan en las cuentas.
- Analice el uso de recursos de las arquitecturas de resistencia durante un error zonal y un error regional. En la progresión de los diseños multirregionales que utilizan enfoques activo/activo, activo/pasivo: en caliente, activo/pasivo: en frío y activo/pasivo: luz piloto, estos casos de error provocarán un mayor uso. Esto crea un caso de uso potencial para alcanzar límites estrictos.

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP01 Conocimiento de las cuotas y restricciones del servicio
- REL01-BP02 Administración de cuotas de servicio en cuentas y regiones
- REL01-BP04 Supervisión y administración de cuotas
- REL01-BP05 Automatización de la administración de cuotas
- REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error
- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP03 Automatización de la reparación en todas las capas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Documentos relacionados:

- AWS Well-Architected Framework’s Reliability Pillar: Availability
- AWS Service Quotas (conocido anteriormente como límites del servicio)
- AWS Trusted Advisor Best Practice Checks (consulte la sección Service Limits)
- Monitor de cuotas para AWS en respuestas de AWS
- Cuotas de servicio de Amazon EC
- What is Service Quotas?

- How to Request Quota Increase
- Service endpoints and quotas
- Guía del usuario de Service Quotas
- Monitor de cuotas para AWS
- AWS Fault Isolation Boundaries
- Disponibilidad con redundancia
- AWS para datos
- Qué es la integración continua?
- Qué es la entrega continua?
- Socio de APN: socios que pueden ayudar con la administración de la configuración
- Managing the account lifecycle in account-per-tenant SaaS environments on AWS
- Managing and monitoring API throttling in your workloads
- View AWS Trusted Advisor recommendations at scale with AWS Organizations
- Automating Service Limit Increases and Enterprise Support with AWS Control Tower
- Actions, resources, and condition keys for Service Quotas

Videos relacionados:

- AWS Live re:Inforce 2019 - Service Quotas
- View and Manage Quotas for AWS Services Using Service Quotas
- AWS IAM Quotas Demo
- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small

Herramientas relacionadas:

- AWS CodeDeploy
- AWS CloudTrail
- Amazon CloudWatch
- Amazon EventBridge
- Amazon DevOps Guru

- AWS Config
- AWS Trusted Advisor
- AWS CDK
- AWS Systems Manager
- AWS Marketplace

REL01-BP04 Supervisión y administración de cuotas

Evalúe el uso potencial y aumente las cuotas pertinentemente, lo que permitirá un crecimiento planificado del uso.

Resultado deseado: se implementaron sistemas activos y automatizados que administran y supervisan. Estas soluciones operativas garantizan que los umbrales de uso de las cuotas estén a punto de alcanzarse. Esto se solucionaría de forma proactiva mediante cambios solicitados en las cuotas.

Patrones comunes de uso no recomendados:

- No configurar la supervisión para comprobar el umbral de cuota de servicio.
- No configurar la supervisión de los límites estrictos, aunque esos valores no puedan modificarse.
- Suponer que el tiempo necesario para solicitar y asegurar un cambio de cuota flexible es inmediato o de corta duración.
- Configurar alarmas de aproximación para cuotas de servicio sin contar con ningún proceso para responder a una alerta.
- Configurar alarmas solo para servicios compatibles con AWS Service Quotas y no supervisar ningún otro servicio de AWS.
- No considerar la administración de cuotas para diseños de resiliencia multirregional, como los métodos activo/activo, activo/pasivo: en caliente, activo/pasivo: en frío y activo/pasivo: luz piloto.
- No evaluar las diferencias de cuota entre regiones.
- No evaluar las necesidades de cada región para una solicitud específica de aumento de cuota.
- No utilizar plantillas para la gestión de cuotas en varias regiones.

Beneficios de establecer esta práctica recomendada: el seguimiento automático de AWS Service Quotas y la supervisión del uso en función de dichas cuotas le permitirá comprobar cuándo se

acerca al límite de una cuota. También puede utilizar estos datos de supervisión para ayudar a limitar cualquier degradación debida al agotamiento de cuotas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Para los servicios admitidos, puede supervisar las cuotas por medio de la configuración de varios servicios diferentes que pueden evaluar y enviar alertas o alarmas. Esto puede ayudar a supervisar el uso y alertarle de que se aproxima a las cuotas. Estas alarmas se pueden invocar desde AWS Config, funciones de Lambda, Amazon CloudWatch o AWS Trusted Advisor. También puede usar filtros de métricas en Registros de CloudWatch para buscar y extraer patrones en registros de modo que pueda determinar si el uso se aproxima a los umbrales de las cuotas.

Pasos para la implementación

Para la supervisión:

- Capture el consumo de recursos actual (por ejemplo, buckets o instancias). Utilice las operaciones de la API de servicio, como la API `DescribeInstances` de Amazon EC2, para recopilar el consumo actual de recursos.
- Capture las cuotas actuales que son esenciales y aplicables a los servicios que utilizan lo siguiente:
  - Service Quotas de AWS
  - AWS Trusted Advisor
  - Documentación de AWS
  - Páginas específicas de los servicios de AWS
  - AWS Command Line Interface (AWS CLI)
  - Kit de desarrollo de la nube de AWS (AWS CDK)
- Utilice AWS Service Quotas, un servicio de AWS que le ayuda a administrar sus cuotas de más de 250 servicios de AWS desde una sola ubicación.
- Utilice los límites de servicio de Trusted Advisor para supervisar sus límites de servicio actuales en diversos umbrales.
- Utilice el historial de cuotas de servicio (consola o AWS CLI) para comprobar los aumentos regionales.
- Compare los cambios de cuota de servicio en cada región y cada cuenta para crear equivalencias, si es necesario.

Para la administración:

- Automatizada: configure una regla personalizada de AWS Config para analizar las cuotas de servicio en todas las regiones y comparar las diferencias.
- Automatizada: configure una función de Lambda programada para analizar las cuotas de servicio en todas las regiones y comparar las diferencias.
- Manual: analice la cuota de servicios a través de la AWS CLI, la API o la consola de AWS para analizar las cuotas de servicio en todas las regiones y comparar las diferencias. Informe de las diferencias.
- Si se identifican diferencias en las cuotas entre las regiones, solicite un cambio de cuota, si es necesario.
- Revise el resultado de todas las solicitudes.

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP01 Conocimiento de las cuotas y restricciones del servicio
- REL01-BP02 Administración de cuotas de servicio en cuentas y regiones
- REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura
- REL01-BP05 Automatización de la administración de cuotas
- REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error
- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP03 Automatización de la reparación en todas las capas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Documentos relacionados:

- AWS Well-Architected Framework’s Reliability Pillar: Availability
- AWS Service Quotas (conocido anteriormente como límites del servicio)

- AWS Trusted Advisor Best Practice Checks (consulte la sección Service Limits)
- Monitor de cuotas para AWS en respuestas de AWS
- Cuotas de servicio de Amazon EC2
- What is Service Quotas?
- How to Request Quota Increase
- Service endpoints and quotas
- Guía del usuario de Service Quotas
- Monitor de cuotas para AWS
- AWS Fault Isolation Boundaries
- Disponibilidad con redundancia
- AWS para datos
- ¿Qué es la integración continua?
- ¿Qué es la entrega continua?
- Socio de APN: socios que pueden ayudar con la administración de la configuración
- Managing the account lifecycle in account-per-tenant SaaS environments on AWS
- Managing and monitoring API throttling in your workloads
- View AWS Trusted Advisor recommendations at scale with AWS Organizations
- Automating Service Limit Increases and Enterprise Support with AWS Control Tower
- Actions, resources, and condition keys for Service Quotas

Videos relacionados:

- AWS Live re:Inforce 2019 - Service Quotas
- View and Manage Quotas for AWS Services Using Service Quotas
- AWS IAM Quotas Demo
- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small

Herramientas relacionadas:

- AWS CodeDeploy

- AWS CloudTrail
- Amazon CloudWatch
- Amazon EventBridge
- Amazon DevOps Guru
- AWS Config
- AWS Trusted Advisor
- AWS CDK
- AWS Systems Manager
- AWS Marketplace

REL01-BP05 Automatización de la administración de cuotas

Las cuotas de servicio, que también se denominan límites en el servicio de AWS, establecen los valores máximos de recursos para la Cuenta de AWS. Cada servicio de AWS define un conjunto de cuotas y sus valores predeterminados. Para proporcionar a su carga de trabajo acceso a todos los recursos que necesita, tal vez deba aumentar los valores de las cuotas de servicio.

El aumento del consumo de recursos de AWS por parte de la carga de trabajo puede poner en peligro la estabilidad de la carga de trabajo y afectar a la experiencia del usuario si se superan las cuotas. Implemente herramientas que lo avisen cuando su carga de trabajo se acerque a los límites y considere la posibilidad de crear solicitudes de aumento de cuota automáticamente.

Resultado deseado: las cuotas están configuradas adecuadamente para las cargas de trabajo que se ejecutan en cada región de Cuenta de AWS.

Patrones comunes de uso no recomendados:

- No tiene en cuenta las cuotas ni las ajusta de forma adecuada para cumplir con los requisitos de carga de trabajo.
- Realiza un seguimiento de las cuotas y el uso mediante métodos que pueden quedar obsoletos, como hojas de cálculo.
- Los límites de servicio solo se actualizan de forma periódica.
- Su organización carece de procesos operativos para revisar las cuotas existentes y solicitar aumentos de las cuotas de servicio cuando sea necesario.

Beneficios de establecer esta práctica recomendada:

- Mayor resiliencia de la carga de trabajo: evita los errores causados por superar las cuotas de recursos de AWS.
- Recuperación ante desastres simplificada: puede reutilizar los mecanismos automatizados de gestión de cuotas creados en la región principal durante la configuración de recuperación ante desastres en otra Región de AWS.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Consulte las cuotas actuales y realice un seguimiento del consumo continuo de cuotas a través de mecanismos como la consola de AWS Service Quotas, AWS Command Line Interface (AWS CLI) y los SDK de AWS. También puede integrar las bases de datos de gestión de la configuración (CMDB) y los sistemas de gestión de servicios de TI (ITSM) con las API de cuota de servicio de AWS.

Genere alertas automatizadas si el uso de la cuota alcanza los umbrales definidos y defina un proceso para enviar las solicitudes de aumento de cuota cuando reciba alertas. Si la carga de trabajo subyacente es fundamental para su empresa, puede automatizar las solicitudes de aumento de cuota, pero extreme las precauciones al realizar las pruebas de automatización para evitar el riesgo de que se tomen medidas descontroladas, como un ciclo de retroalimentación sobre el crecimiento.

Los aumentos de cuota más pequeños suelen aprobarse automáticamente. Es posible que el soporte técnico de AWS deba procesar manualmente las solicitudes de cuotas más altas, y su revisión y procesamiento pueden tardar más tiempo. Disponga de más tiempo para procesar varias solicitudes o solicitudes de grandes aumentos.

Pasos para la implementación

- Implemente un monitoreo automatizado de las cuotas de servicio y emita alertas si el aumento del uso de los recursos de su carga de trabajo se acerca a los límites de su cuota. Por ejemplo, el Supervisor de cuotas para AWS puede proporcionar un monitoreo automatizado de las cuotas de servicio. Esta herramienta se integra con AWS Organizations y se implementa mediante CloudFormation StackSets para que las nuevas cuentas se monitoreen automáticamente al crearlas.
- Utilice características como las plantillas de solicitud de Service Quotas o AWS Control Tower para simplificar la configuración de Service Quotas para cuentas nuevas.

- Cree paneles de control del uso actual de sus cuotas de servicio en todas las regiones de Cuentas de AWS y consúltelos según sea necesario para no superar sus cuotas. El panel organizativo de Trusted Advisor (TAO), que forma parte de los paneles de inteligencia en la nube, puede ayudarlo a empezar rápidamente con dicho panel.
- Lleve un seguimiento de las solicitudes de aumento de límites de servicio. Con Consolidated Insights from Multiple Accounts (CIMA) puede ver las solicitudes de toda su organización.
- Pruebe la generación de alertas y cualquier automatización de solicitudes de aumento de cuotas estableciendo umbrales de cuota más bajos en las cuentas que no son de producción. No realice estas pruebas en una cuenta de producción.

Recursos

Prácticas recomendadas relacionadas:

- OPS10-BP07 Automatización de las respuestas a eventos

Documentos relacionados:

- Socio de APN: socios que pueden ayudar con la administración de la configuración
- AWS Marketplace: productos de CMDB que ayudan a hacer un seguimiento de los límites
- AWS Service Quotas (conocido anteriormente como límites del servicio)
- AWS Trusted Advisor Best Practice Checks (consulte la sección Service Limits)
- Monitor de cuotas para AWS. Solución de AWS
- What is Service Quotas?
- ¿Qué son las plantillas de solicitud de Service Quotas?

Videos relacionados:

- AWS Live re:Inforce 2019 - Service Quotas
- Automating Service Limit Increases and Enterprise Support with AWS Control Tower

Herramientas relacionadas:

- Monitor de cuotas para AWS

REL01-BP06 Garantía de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error

En este artículo se explica cómo mantener el espacio entre la cuota de recursos y su uso, y cómo puede beneficiar a su organización. Cuando termine de usar un recurso, es posible que la cuota de uso siga teniendo en cuenta ese recurso. Esto puede provocar un fallo del recurso o que sea inaccesible. Para prevenir el fallo del recurso, compruebe que sus cuotas cubran el solapamiento de los recursos inaccesibles y sus sustitutos. A la hora de calcular esta brecha, tenga en cuenta casos de uso tales como los errores de red, los errores de la zona de disponibilidad o los errores regionales.

Resultado deseado: los errores pequeños o grandes en los recursos o en su accesibilidad pueden cubrirse dentro de los umbrales de servicio actuales. En la planificación de recursos se tienen en cuenta los errores de zona, de red o, incluso, regionales.

Patrones comunes de uso no recomendados:

- Se establecen cuotas de servicio sobre la base de las necesidades actuales sin tener en cuenta los casos de conmutación por error.
- No se tienen en cuenta los principios de estabilidad estática al calcular la cuota máxima de un servicio.
- No se tiene en cuenta el potencial de recursos inaccesibles al calcular la cuota total necesaria para cada región.
- No se tienen en cuenta los límites de aislamiento de errores del servicio de AWS para algunos servicios y sus posibles patrones de uso anómalos.

Beneficios de establecer esta práctica recomendada: cuando los eventos de interrupción del servicio afecten a la disponibilidad de las aplicaciones, utilice la nube para implementar estrategias que le permitan recuperarse de estos eventos. Un ejemplo de estrategia es crear recursos adicionales para reemplazar los recursos inaccesibles y adaptarse a las condiciones de conmutación por error sin agotar el límite de servicio.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Al evaluar el límite de cuota, considere los casos de conmutación por error que podrían producirse debido a algún deterioro. Considere los siguientes casos de conmutación por error.

- Una VPC interrumpida o inaccesible.
- Una subred inaccesible.
- Una zona de disponibilidad degradada que afecta a la accesibilidad de los recursos.
- Rutas de red o puntos de entrada y salida bloqueados o modificados.
- Una región degradada que afecta a la accesibilidad de los recursos.
- Un subconjunto de recursos afectados por un fallo en una región o zona de disponibilidad.

La decisión de utilizar la conmutación por error es única para cada situación, ya que el efecto empresarial puede variar drásticamente. Planifique la capacidad de los recursos en la ubicación de conmutación por error y las cuotas de los recursos antes de decidir llevar a cabo la conmutación por error de una aplicación o un servicio.

Tenga en cuenta los picos de actividad superiores a los normales al revisar las cuotas de cada servicio. Estos picos pueden estar relacionados con recursos que son inaccesibles a causa de la red o los permisos, pero que siguen activos. Los recursos activos no finalizados cuentan para el límite de cuota de servicio.

Pasos para la implementación

- Deje espacio entre la cuota de servicio y el uso máximo para permitir la conmutación por error o una pérdida de accesibilidad.
- Determine sus cuotas de servicio. Tenga en cuenta los patrones de implementación típicos, los requisitos de disponibilidad y el crecimiento del consumo.
- Solicite aumentos de la cuota si fuera necesario. Prevea un tiempo de espera para la solicitud de aumento de cuota.
- Determine sus requisitos de fiabilidad (también conocidos como número de nueves).
- Comprenda los posibles escenarios de error, como la pérdida de un componente, una zona de disponibilidad o una región.
- Establezca su metodología de implementación (por ejemplo, canario, azul/verde, rojo/negro o continua).
- Incluya un búfer adecuado en el límite de cuota actual. Un ejemplo de búfer podría ser del 15 %.
- Incluya cálculos de estabilidad estática (zonal y regional) cuando proceda.
- Planifique el crecimiento del consumo y supervise sus tendencias de consumo.

- Considere la repercusión de la estabilidad estática para las cargas de trabajo más críticas. Evalúe los recursos conforme a un sistema estáticamente estable en todas las regiones y zonas de disponibilidad.
- Considere el uso de reservas de capacidad bajo demanda para programar la capacidad antes de que se produzca una conmutación por error. Es una estrategia útil para implementar las programaciones comerciales críticas a fin de reducir los riesgos potenciales de obtener la cantidad y el tipo correctos de recursos durante la conmutación por error.

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP01 Conocimiento de las cuotas y restricciones del servicio
- REL01-BP02 Administración de cuotas de servicio en cuentas y regiones
- REL01-BP03 Adaptación de las cuotas de servicio fijas y las restricciones a través de la arquitectura
- REL01-BP04 Supervisión y administración de cuotas
- REL01-BP05 Automatización de la administración de cuotas
- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP03 Automatización de la reparación en todas las capas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Documentos relacionados:

- AWS Well-Architected Framework’s Reliability Pillar: Availability
- AWS Service Quotas (conocido anteriormente como límites del servicio)
- AWS Trusted Advisor Best Practice Checks (consulte la sección Service Limits)
- Monitor de cuotas para AWS en respuestas de AWS
- Cuotas de servicio de Amazon EC2
- What is Service Quotas?
- How to Request Quota Increase

- Service endpoints and quotas
- Guía del usuario de Service Quotas
- Monitor de cuotas para AWS
- AWS Fault Isolation Boundaries
- Disponibilidad con redundancia
- AWS para datos
- ¿Qué es la integración continua?
- ¿Qué es la entrega continua?
- Socio de APN: socios que pueden ayudar con la administración de la configuración
- Managing the account lifecycle in account-per-tenant SaaS environments on AWS
- Managing and monitoring API throttling in your workloads
- View AWS Trusted Advisor recommendations at scale with AWS Organizations
- Automating Service Limit Increases and Enterprise Support with AWS Control Tower
- Actions, resources, and condition keys for Service Quotas

Videos relacionados:

- AWS Live re:Inforce 2019 - Service Quotas
- View and Manage Quotas for AWS Services Using Service Quotas
- AWS IAM Quotas Demo
- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small

Herramientas relacionadas:

- AWS CodeDeploy
- AWS CloudTrail
- Amazon CloudWatch
- Amazon EventBridge
- Amazon DevOps Guru
- AWS Config
- AWS Trusted Advisor

- AWS CDK
- AWS Systems Manager
- AWS Marketplace

Planificación de la topología de la red

Las cargas de trabajo suelen existir en varios entornos. Estos incluyen varios entornos de nube (tanto de acceso público como privados) y, posiblemente, la infraestructura de su centro de datos existente. Los planes deben incluir consideraciones, como la conectividad dentro de los sistemas y entre ellos, la administración de las direcciones IP públicas, la administración de las direcciones IP privadas y la resolución de nombres de dominio.

Si diseña sistemas que utilicen redes basadas en direcciones IP, debe planificar la topología y el direccionamiento de la red para anticiparse a posibles errores y para acomodar el crecimiento futuro y la integración con otros sistemas y sus redes.

Amazon Virtual Private Cloud (Amazon VPC) permite aprovisionar una sección privada y aislada de la nube de AWS donde podrá lanzar recursos de AWS en una red virtual.

Prácticas recomendadas

- REL02-BP01 Uso de conectividad de red de alta disponibilidad para los puntos de conexión públicos de la carga de trabajo
- REL02-BP02 Aprovisionamiento de conectividad redundante entre las redes privadas en la nube y los entornos en las instalaciones
- REL02-BP03 Garantía de que la asignación de subredes IP tenga en cuenta la expansión y la disponibilidad
- REL02-BP04 Preferencia de topologías radiales (“hub-and-spoke”) frente a una conexión en malla de varios a varios
- REL02-BP05 Aplicación de intervalos de direcciones IP privadas que no se superponen en todos los espacios de direcciones privadas en los que están conectados

REL02-BP01 Uso de conectividad de red de alta disponibilidad para los puntos de conexión públicos de la carga de trabajo

La creación de una conectividad de red de alta disponibilidad para los puntos de conexión públicos de las cargas de trabajo puede ayudarle a reducir el tiempo de inactividad debido a la pérdida de conectividad y mejorar la disponibilidad y el SLA de su carga de trabajo. Para conseguirlo, use DNS, redes de entrega de contenido (CDN), puertas de enlace de API, un equilibrador de carga o proxies inversos altamente disponibles.

Resultado deseado: es fundamental planificar, construir y poner en funcionamiento una conectividad de red de alta disponibilidad para sus puntos de conexión públicos. Si la carga de trabajo resulta inaccesible debido a una pérdida de conectividad, incluso si la carga de trabajo está en funcionamiento y disponible, los clientes verán su sistema como caído. Al combinar una conectividad de red de alta disponibilidad y resistente para los puntos de conexión públicos de la carga de trabajo, junto con una arquitectura resistente para la propia carga de trabajo, puede proporcionar la mejor disponibilidad y nivel de servicio posibles a sus clientes.

AWS Global Accelerator, Amazon CloudFront, Amazon API Gateway, las URL de funciones de AWS Lambda, las API de AWS AppSync y Elastic Load Balancing (ELB) ofrecen puntos de conexión públicos de alta disponibilidad. Amazon Route 53 proporciona un servicio de DNS de alta disponibilidad para la resolución de nombres de dominio a fin de comprobar que las direcciones de los puntos de conexión públicos se puedan resolver.

También puede evaluar las aplicaciones de software de AWS Marketplace que proporcionen equilibrio de carga o uso de proxies.

Patrones comunes de uso no recomendados:

- Diseñar una carga de trabajo de alta disponibilidad sin planificar el DNS y la conectividad de red para alta disponibilidad.
- Usar direcciones de internet públicas en instancias o contenedores individuales y administrar la conectividad a ellas a con DNS.
- Usar direcciones IP en lugar de nombres de dominio para localizar los servicios.
- No hacer pruebas de escenarios en que se pierda la conectividad con sus puntos de conexión públicos.
- No analizar las necesidades de rendimiento de la red y los patrones de distribución.

- No hacer pruebas ni planificar escenarios en los que la conectividad de la red de internet a sus puntos de conexión públicos de la carga de trabajo puede ser interrumpida.
- Proporcionar contenido (como páginas web, activos estáticos o archivos multimedia) a una gran área geográfica y no usar una red de entrega de contenido.
- No planificar en caso de que se produzcan ataques de denegación de servicio distribuido (DDoS). Los ataques DDoS corren el riesgo de cerrar el tráfico legítimo y reducir la disponibilidad para sus usuarios.

Beneficios de establecer esta práctica recomendada: diseñar una conectividad de red flexible y de alta disponibilidad garantiza que su carga de trabajo sea accesible y esté disponible para los usuarios.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

El enrutamiento del tráfico es el núcleo de la creación de una conectividad de red de alta disponibilidad para sus puntos de conexión públicos. Para verificar que el tráfico puede llegar a los puntos de conexión, el DNS debe ser capaz de resolver los nombres de dominio en sus direcciones IP correspondientes. Use un sistema de nombres de dominio (DNS) escalable y de alta disponibilidad, como Amazon Route 53, para administrar los registros de DNS de su dominio. También puede utilizar las comprobaciones de estado proporcionadas por Amazon Route 53. Las comprobaciones de estado verifican que la aplicación sea accesible, esté disponible y funcione; se pueden configurar de manera que imiten el comportamiento de su usuario, como la solicitud de una página web o una URL concreta. En caso de error, Amazon Route 53 responde a las solicitudes de resolución de DNS y dirige el tráfico únicamente a los puntos de conexión en buen estado. También puede plantearse el uso de las capacidades de DNS geográfico y enrutamiento basado en la latencia que ofrece Amazon Route 53.

Para comprobar que la carga de trabajo sea de alta disponibilidad, use Elastic Load Balancing (ELB). Amazon Route 53 se puede utilizar para dirigir el tráfico a ELB, que distribuye el tráfico a las instancias de computación de destino. También puede utilizar Amazon API Gateway junto con AWS Lambda para una solución sin servidor. Los clientes también pueden ejecutar cargas de trabajo en varias Regiones de AWS. Con un patrón activo/activo de varios sitios, la carga de trabajo puede atender el tráfico de varias regiones. Con un patrón activo/pasivo de varios sitios, la carga de trabajo atiende el tráfico de la región activa, mientras que los datos se replican en la región secundaria y se activan en caso de que se produzca un error en la región principal. Las comprobaciones de estado

de Route 53 se pueden utilizar para controlar la conmutación por error de DNS desde cualquier punto de conexión de una región principal a un punto de conexión de una región secundaria, lo que permite comprobar que los usuarios tengan acceso a la carga de trabajo y que esta esté disponible para ellos.

Amazon CloudFront proporciona una API sencilla para distribuir contenido con baja latencia y altas velocidades de transferencia de datos, ya que atiende las solicitudes mediante una red de ubicaciones periféricas en todo el mundo. Las redes de entrega de contenido (CDN) atienden a los clientes al proporcionarles contenido ubicado o almacenado en caché en una ubicación cercana al usuario. Esto también mejora la disponibilidad de la aplicación, ya que la carga de contenido se traslada de los servidores a las ubicaciones periféricas de CloudFront. Las ubicaciones periféricas y las cachés periféricas regionales mantienen copias en caché de su contenido cerca de sus usuarios, lo que permite una recuperación rápida y aumenta la accesibilidad y la disponibilidad de su carga de trabajo.

Para cargas de trabajo con usuarios distribuidos geográficamente, AWS Global Accelerator ayuda a mejorar la disponibilidad y el rendimiento de las aplicaciones. AWS Global Accelerator proporciona direcciones IP estáticas anycast que sirven como punto de entrada fijo a su aplicación alojada en una o más Regiones de AWS. Esto permite que el tráfico entre en la red global de AWS lo más cerca posible de sus usuarios, lo que mejora la accesibilidad y disponibilidad de su carga de trabajo. AWS Global Accelerator también supervisa el estado de los puntos de conexión de su aplicación mediante comprobaciones de estado de TCP, HTTP y HTTPS. Cualquier cambio en el estado o la configuración de sus puntos de conexión permite el redireccionamiento del tráfico de usuario a puntos de conexión en buen estado que ofrezcan el mejor rendimiento y disponibilidad a los usuarios. Además, AWS Global Accelerator cuenta con un diseño de aislamiento de errores que utiliza dos direcciones IPv4 estáticas atendidas por zonas de red independientes que aumentan la disponibilidad de las aplicaciones.

Para ayudar a proteger a los clientes de los ataques DDoS, AWS proporciona AWS Shield Standard. Shield Estándar se activa automáticamente y protege de los ataques comunes a la infraestructura (capas 3 y 4), como las inundaciones SYN/UDP y los ataques de reflexión, para respaldar la alta disponibilidad de sus aplicaciones en AWS. Para obtener protecciones adicionales contra ataques más sofisticados y grandes (como inundaciones UDP) y ataques de agotamiento de estado (como inundaciones de TCP SYN), y para ayudar a proteger sus aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Route 53, puede considerar el uso de AWS Shield Advanced. Para la protección contra ataques en la capa de aplicación como HTTP POST o inundaciones GET, utilice AWS WAF. AWS WAF puede utilizar condiciones de direcciones IP, encabezados HTTP, cuerpos HTTP,

cadenas de URI, inyección de código SQL y scripting entre sitios para determinar si se debe bloquear o permitir una solicitud.

Pasos para la implementación

1. Configuración de un DNS de alta disponibilidad: Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Route 53 conecta las solicitudes de los usuarios con las aplicaciones de Internet que se ejecutan en AWS o en las instalaciones. Para obtener más información, consulte Configuring Amazon Route 53 as your DNS service.
2. Configuración de comprobaciones de estado: cuando utilice Route 53, verifique que solo se puedan resolver los destinos en buen estado. Comience por la creación de comprobaciones de estado de Amazon Route 53 y la configuración de la conmutación por error de DNS. Es importante tener en cuenta los siguientes aspectos a la hora de configurar las comprobaciones de estado:
   a. How Amazon Route 53 determines whether a health check is healthy
   b. Creating, updating, and deleting health checks
   c. Monitoring health check status and getting notifications
   d. Best practices for Amazon Route 53 DNS
3. Conecte su servicio de DNS a los puntos de conexión.
   a. Cuando utilice Elastic Load Balancing como objetivo para el tráfico, cree un registro de alias con Amazon Route 53 que apunte al punto de conexión regional del equilibrador de carga. Durante la creación del registro de alias, establezca la opción de evaluación de estado del destino en Sí.
   b. Utilice Route 53 para dirigir el tráfico a API Gateway para las cargas de trabajo sin servidor o API privadas.
4. Decida la red de entrega de contenido.
   a. Para entregar contenido con ubicaciones periféricas más cercanas al usuario, antes debe entender cómo entrega contenido CloudFront.
   b. Comience con una distribución sencilla de CloudFront. CloudFront sabrá entonces desde dónde desea que se entregue el contenido, así como los detalles sobre cómo hacer el seguimiento y administrar la entrega de contenido. Es importante comprender y tener en cuenta los siguientes aspectos al configurar la distribución de CloudFront:
      i. Cómo funciona el almacenamiento en caché con ubicaciones periférica de CloudFront
      ii. Incremento de la proporción de solicitudes que se atienden directamente desde las cachés de CloudFront (tasa de aciertos de caché)

   iii. Uso de Origin Shield de Amazon CloudFront

   iv. Optimización de alta disponibilidad con conmutación por error de origen de CloudFront

5. Configuración de la protección de la capa de aplicación: AWS WAF le ayuda a protegerse contra ataques web y bots habituales que pueden afectar a la disponibilidad, comprometer la seguridad o consumir demasiados recursos. Para obtener una comprensión más profunda, consulte How AWS WAF works y, cuándo lo tenga todo listo para implementar protecciones contra las inundaciones HTTP, POST y GET de la capa de aplicaciones, consulte Getting started with AWS WAF. También puede usar AWS WAF con CloudFront. Consulte la documentación sobre cómo funciona AWS WAF con las características de Amazon CloudFront.
6. Configuración de protección DDoS adicional: de forma predeterminada, todos los clientes de AWS reciben protección frente a los ataques DDoS más habituales y frecuentes de la capa de red y transporte dirigidos a su sitio web o aplicación con AWS Shield Standard y sin ningún cargo adicional. Para obtener una protección adicional de las aplicaciones con acceso a Internet que se ejecutan en Amazon EC2, Elastic Load Balancing, Amazon CloudFront, AWS Global Accelerator y Amazon Route 53, puede considerar AWS Shield Advanced y ver ejemplos de arquitecturas resistentes a DDoS. Para proteger su carga de trabajo y sus puntos de conexión públicos de los ataques DDoS, consulte Getting started with AWS Shield Advanced.

Recursos

Prácticas recomendadas relacionadas:

- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación
- REL11-BP06 Envío de notificaciones cuando los eventos afecten a la disponibilidad

Documentos relacionados:

- Socio de APN: socios que pueden ayudarle a planificar sus redes
- AWS Marketplace para la infraestructura de red
- Qué es AWS Global Accelerator?
- ¿Qué es Amazon CloudFront?
- What is Amazon Route 53?
- Qué es Elastic Load Balancing?

- Network Connectivity capability - Establishing Your Cloud Foundations
- ¿Qué es Amazon API Gateway?
- What are AWS WAF, AWS Shield, and AWS Firewall Manager?
- What is Amazon Application Recovery Controller?
- Configuración de las comprobaciones de estado personalizadas para la conmutación por error de DNS

Videos relacionados:

- AWS re:Invent 2022 - Improve performance and availability with AWS Global Accelerator
- AWS re:Invent 2020: Global traffic management with Amazon Route 53
- AWS re:Invent 2022 - Operating highly available Multi-AZ applications
- AWS re:Invent 2022 - Dive deep on AWS networking infrastructure
- AWS re:Invent 2022 - Building resilient networks

Ejemplos relacionados:

- Disaster Recovery with Amazon Application Recovery Controller (ARC)
- AWS Global Accelerator Workshop

REL02-BP02 Aprovisionamiento de conectividad redundante entre las redes privadas en la nube y los entornos en las instalaciones

Implemente la redundancia en las conexiones entre redes privadas en la nube y entornos en las instalaciones para lograr la resiliencia de la conectividad. Esto se puede lograr mediante la implementación de dos o más enlaces y rutas de tráfico, lo que permite mantener la conectividad en el caso de que se produzcan errores en la red.

Patrones comunes de uso no recomendados:

- Depende de una única conexión de red, lo que crea un único punto de error.
- Utiliza únicamente un túnel de VPN o varios túneles que terminan en la misma zona de disponibilidad.
- Confía en un único proveedor de servicios de Internet (ISP) para la conectividad de VPN, lo que puede provocar un fallo total de la conexión durante las interrupciones del ISP.

- No implementar protocolos de enrutamiento dinámico como BGP, que son fundamentales para redirigir el tráfico durante las interrupciones de la red.
- Ignora las limitaciones de ancho de banda de los túneles de VPN y sobrestima sus capacidades de copia de seguridad.

Beneficios de establecer esta práctica recomendada: al implementar la conectividad redundante entre el entorno en la nube y su entorno corporativo o en las instalaciones, puede garantizar que los servicios dependientes entre los dos entornos se puedan comunicar con fiabilidad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Al utilizar AWS Direct Connect para conectar la red en las instalaciones a AWS, puede lograr la máxima resiliencia de la red (SLA del 99,99 %) mediante el uso de conexiones independientes que terminan en distintos dispositivos en más de una ubicación en las instalaciones y en más de una ubicación de AWS Direct Connect. Esta topología ofrece resiliencia frente a los errores de los dispositivos, los problemas de conectividad y las interrupciones totales de la conexión producidas en la ubicación. Como alternativa, puede lograr una alta resiliencia (SLA del 99,9 %) mediante el uso de dos conexiones individuales a varias ubicaciones (cada ubicación en las instalaciones conectada a una única ubicación de Direct Connect). Este enfoque protege frente a las interrupciones de conectividad provocadas por cortes en la fibra o errores en los dispositivos y ayuda a mitigar los fallos totales de la conexión producidos en la ubicación. El Kit de herramientas de resiliencia de Direct Connect puede ayudarle a diseñar su topología de AWS Direct Connect.

También puede plantearse la posibilidad de utilizar AWS Site-to-Site VPN que finaliza en una AWS Direct Connect como una opción de conexión alternativa y rentable en el caso de que surjan problemas con la conexión principal de AWS Transit Gateway. Esta configuración permite el enrutamiento de múltiples rutas de igual costo (ECMP) a través de varios túneles de VPN, lo que permite un rendimiento de hasta 50 Gbps, aunque cada túnel de VPN tenga un límite de 1,25 Gbps. Sin embargo, es importante tener en cuenta que AWS Direct Connect sigue siendo la opción más eficaz para reducir al mínimo las interrupciones producidas en la red y proporcionar una conectividad estable.

Al utilizar VPN a través de Internet para conectar el entorno de nube al centro de datos en las instalaciones, configure dos túneles de VPN como parte de una única conexión de Site-to-Site VPN. Cada túnel debe terminar en una zona de disponibilidad diferente para lograr una alta disponibilidad y usar hardware redundante con el fin de evitar errores en los dispositivos en las

instalaciones. Asimismo, tenga en cuenta la posibilidad de establecer varias conexiones a Internet de varios proveedores de servicios de Internet (ISP) en su ubicación en las instalaciones para evitar una interrupción total de la conectividad de la VPN debido a una única interrupción del ISP. La selección de ISP con enrutamientos e infraestructuras diversos, especialmente aquellos con rutas físicas independientes a los puntos de conexión de AWS, proporciona una alta disponibilidad de la conectividad.

Además de la redundancia física con varias conexiones de AWS Direct Connect y varios túneles de VPN (o una combinación de ambos), también es fundamental implementar el enrutamiento dinámico del protocolo de puerta de enlace fronteriza (BGP). El BGP dinámico permite redirigir automáticamente el tráfico de una ruta a otra en función de las condiciones de la red en tiempo real y las políticas configuradas. Este comportamiento dinámico es especialmente beneficioso para mantener la disponibilidad de la red y la continuidad del servicio en caso de que se produzcan errores de enlace o en la red. Selecciona rápidamente rutas alternativas, lo que mejora la resiliencia y la fiabilidad de la red.

Pasos para la implementación

- Establezca una conectividad de alta disponibilidad entre AWS y el entorno en las instalaciones.
  - Use varias conexiones de AWS Direct Connect o túneles de VPN entre redes privadas implementadas por separado.
  - Use varias ubicaciones de Direct Connect para contar con alta disponibilidad.
  - Si utiliza varias Regiones de AWS, cree redundancia en al menos dos de ellas.
- Use AWS Transit Gateway, cuando sea posible, para finalizar su conexión VPN.
- Evalúe los dispositivos de AWS Marketplace para finalizar las VPN o ampliar su SD-WAN a AWS. Si utiliza dispositivos de AWS Marketplace, implemente instancias redundantes para obtener alta disponibilidad en diferentes zonas de disponibilidad.
- Proporcione una conexión redundante al entorno en las instalaciones.
  - Es posible que necesite conexiones redundantes a varias Regiones de AWS para cubrir sus necesidades de disponibilidad.
  - Use el Kit de herramientas de resiliencia de Direct Connect para comenzar.

Recursos

Documentos relacionados:

- Recomendaciones sobre resiliencia de AWS Direct Connect
- Using Redundant Site-to-Site VPN Connections to Provide Failover
- Routing policies and BGP communities
- Active/Active and Active/Passive Configurations in AWS Direct Connect
- Socio de APN: socios que pueden ayudarle a planificar sus redes
- AWS Marketplace para la infraestructura de red
- Documento técnico sobre las opciones de conectividad a la nube virtual privada de Amazon
- Creación de una infraestructura de red de AWS multiVPC escalable y segura
- Using redundant Site-to-Site VPN connections to provide failover
- Using the Direct Connect Resiliency Toolkit to get started
- Puntos de conexión de VPC y servicios de punto de conexión de VPC (AWS PrivateLink)
- Qué es Amazon VPC?
- What is a transit gateway?
- Qué es AWS Site-to-Site VPN?
- Uso de puertas de enlace de Direct Connect

Videos relacionados:

- AWS re:Invent 2018: Advanced VPC Design and New Capabilities for Amazon VPC
- AWS re:Invent 2019: AWS Transit Gateway reference architectures for many VPCs

REL02-BP03 Garantía de que la asignación de subredes IP tenga en cuenta la expansión y la disponibilidad

Los intervalos de direcciones IP de Amazon VPC deben ser lo suficientemente amplios como para dar cabida a los requisitos de las cargas de trabajo, como la posible expansión futura y la asignación de direcciones IP a las subredes de las zonas de disponibilidad. Esto incluye equilibradores de carga, instancias de EC2 y aplicaciones basadas en contenedores.

Cuando planifica la topología de su red, el primer paso es definir el espacio de la dirección IP. Se deben asignar rangos de direcciones IP privadas para cada VPC (según las directrices de la RFC 1918). Facilite los siguientes requisitos como parte de este proceso:

- Permita los espacios de direcciones IP para más de una VPC por región.
- En una VPC, deje espacio para varias subredes para poder cubrir varias zonas de disponibilidad.
- Considere la posibilidad de dejar siempre un espacio de bloque de CIDR sin usar en una VPC para posibles expansiones futuras.
- Asegúrese de que haya espacio de direcciones IP suficiente como para satisfacer las necesidades de flotas transitorias de instancias de Amazon EC2 que podría usar, como flotas de spot para el machine learning, clústeres de Amazon EMR o clústeres de Amazon Redshift. Se debe prestar una atención similar a los clústeres de Kubernetes, como Amazon Elastic Kubernetes Service (Amazon EKS), ya que a cada pod de Kubernetes se le asigna una dirección enrutable desde el bloque de CIDR de la VPC de forma predeterminada.
- Tenga en cuenta que las primeras cuatro direcciones IP y la última dirección IP de cada bloque CIDR de subred están reservadas y no están disponibles para que las use.
- Tenga en cuenta que el bloque de CIDR de la VPC inicial asignado a su VPC no debe cambiar ni eliminarse, pero puede agregar bloques de CIDR que no se solapen a la VPC. Los CIDR IPv4 de subred no se pueden cambiar; sin embargo, los CIDR IPv6 sí.
- El bloque de CIDR de VPC más grande posible es un /16 y el más pequeño es un /28.
- Tenga en cuenta otras redes conectadas (VPC, en las instalaciones u otros proveedores de nube) y asegúrese de que el espacio de direcciones IP no se superponga. Para obtener más información, consulte REL02-BP05 Aplicación de intervalos de direcciones IP privadas que no se superponen en todos los espacios de direcciones privadas en los que están conectados.

Resultado deseado: una subred IP escalable puede ayudarle a adaptarse al crecimiento futuro y evitar desperdicios innecesarios.

Patrones comunes de uso no recomendados:

- No tener en cuenta el crecimiento futuro, lo que hace que los bloques de CIDR sean demasiado pequeños y se tengan que reconfigurar, lo que puede provocar tiempos de inactividad a su vez.
- Calcular incorrectamente cuántas direcciones IP puede usar un equilibrador de carga elástico.
- Implementar muchos equilibradores de carga de tráfico intenso en las mismas subredes
- Usar mecanismos de escalado automatizados sin supervisar el consumo de direcciones IP.
- Definir rangos de CIDR excesivamente grandes que superen con creces las expectativas de crecimiento futuro, lo que puede generar dificultades para conectarse con otras redes con rangos de direcciones superpuestos.

Beneficios de establecer esta práctica recomendada: de esta forma, se asegurará de dar cabida al crecimiento de sus cargas de trabajo y seguir proporcionando disponibilidad al escalar verticalmente.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Planificar su red para que se adapte al crecimiento, el cumplimiento normativo y la integración con otros. El crecimiento se puede subestimar, la conformidad normativa puede variar y las adquisiciones y conexiones de redes privadas pueden ser difíciles de llevar a cabo sin una planificación adecuada.

- Seleccione las regiones y Cuentas de AWS que correspondan según sus requisitos normativos y de servicio, latencia y recuperación de desastres (DR).
- Identifique sus necesidades para implementaciones regionales de VPC.
- Identifique el tamaño de las VPC.
  - Determine si va a implementar la conectividad de varias VPC.
    - What Is a Transit Gateway?
    - Single Region Multi-VPC Connectivity
  - Determine si necesita redes divididas conforme a los requisitos normativos.
  - Cree VPC con bloques de CIDR del tamaño adecuado para adaptarse a sus necesidades actuales y futuras.
    - Si desconoce sus proyecciones de crecimiento, es posible que desee optar por bloques de CIDR más grandes para no tener que volver a configurarlos en el futuro
  - Considere la posibilidad de utilizar las direcciones IPv6 para las subredes como parte de una VPC de doble pila. IPv6 es ideal en subredes privadas que contengan flotas de instancias o contenedores efímeros que, de otro modo, requerirían un gran número de direcciones IPv4.

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- REL02-BP05 Aplicación de intervalos de direcciones IP privadas que no se superponen en todos los espacios de direcciones privadas en los que están conectados

Documentos relacionados:

- Socio de APN: socios que pueden ayudarle a planificar sus redes

- AWS Marketplace para la infraestructura de red
- Documento técnico sobre las opciones de conectividad a la nube virtual privada de Amazon
- Conectividad a la red de varios centros de datos HA
- Single Region Multi-VPC Connectivity
- Qué es Amazon VPC?
- IPv6 en AWS
- IPv6 on reference architectures
- Amazon Elastic Kubernetes Service launches IPv6 support
- Recommendations for your VPC - Classic Load Balancers
- Subredes de zona de disponibilidad - Equilibrador de carga de aplicación
- Zonas de disponibilidad - Equilibradores de carga de red

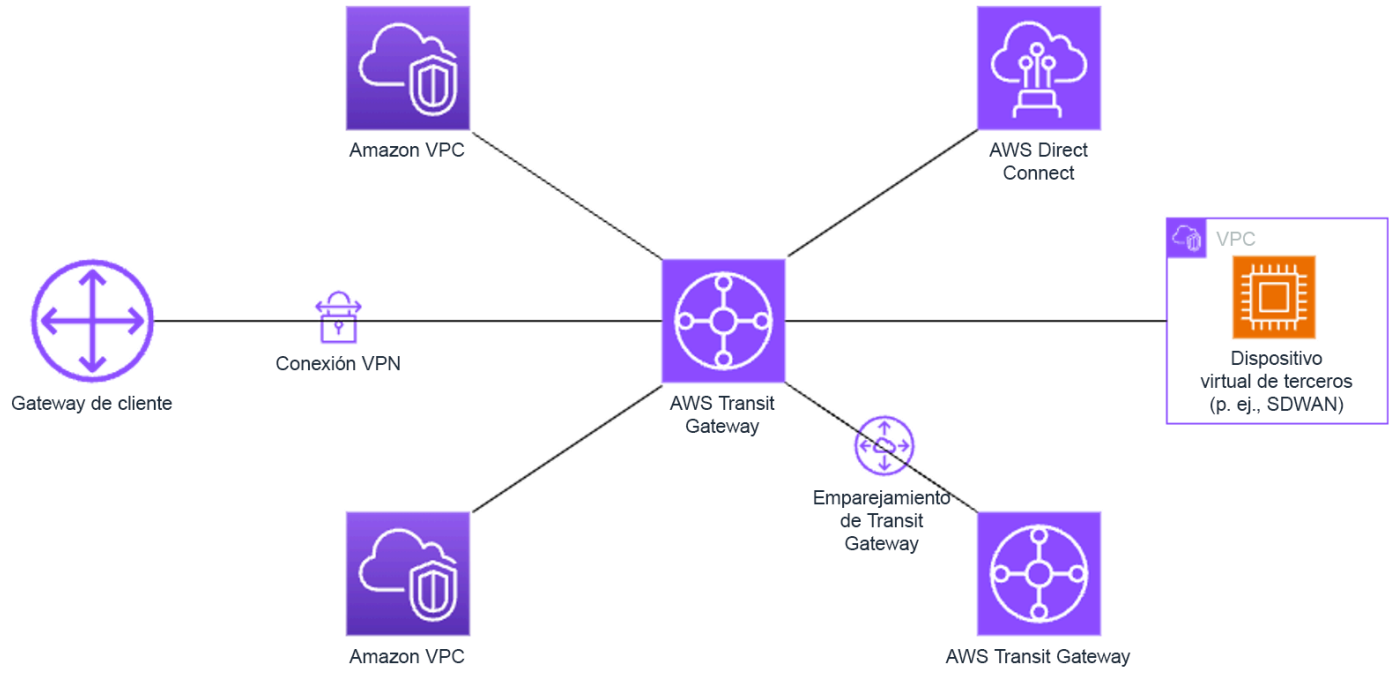
Videos relacionados:

- AWS re:Invent 2018: Advanced VPC Design and New Capabilities for Amazon VPC (NET303)
- AWS re:Invent 2019: AWS Transit Gateway reference architectures for many VPCs (NET406-R1)
- AWS re:Invent 2023: AWS Ready for what's next? Designing networks for growth and flexibility (NET310)

REL02-BP04 Preferencia de topologías radiales (“hub-and-spoke”) frente a una conexión en malla de varios a varios

Al conectar varias redes privadas, como nubes privadas virtuales (VPC) y redes en las instalaciones, opte por una topología radial (“hub-and-spoke”) en lugar de una en malla. A diferencia de las topologías en malla, en las que cada red se conecta directamente a las demás y aumenta la complejidad y la sobrecarga de administración, la arquitectura radial (“hub-and-spoke”) centraliza las conexiones a través de un único hub. Esta centralización simplifica la estructura de la red y mejora su operatividad, escalabilidad y control.

AWS Transit Gateway es un servicio administrado, escalable y de alta disponibilidad diseñado para la construcción de redes radiales (“hub-and-spoke”) en AWS. Sirve como centro de la red que proporciona una segmentación de la red, un enrutamiento centralizado y una conexión simplificada a los entornos en las instalaciones y en la nube. La siguiente figura muestra cómo puede utilizar AWS Transit Gateway para crear su topología radial (“hub-and-spoke”).



Resultado deseado: ha conectado las nubes privadas virtuales (VPC) y las redes en las instalaciones a través de un concentrador central. Las conexiones de emparejamiento se configuran a través del hub, que actúa como un enrutador en la nube altamente escalable. El enrutamiento se simplifica porque no es necesario trabajar con relaciones de interconexión complejas. El tráfico entre redes está cifrado y tiene la capacidad de aislar las redes.

Patrones comunes de uso no recomendados:

- Crea reglas de interconexión de redes complejas.
- Proporciona rutas entre redes que no deberían comunicarse entre sí (por ejemplo, cargas de trabajo independientes que no tienen interdependencias).
- La gobernanza de la instancia central es ineficaz.

Beneficios de establecer esta práctica recomendada: a medida que aumenta la cantidad de redes conectadas, la administración y la expansión de la conectividad en malla se vuelven cada vez más desafiantes. Una arquitectura de malla presenta desafíos adicionales, como componentes de infraestructura adicionales, requisitos de configuración y cuestiones de implementación. La malla también introduce una sobrecarga adicional para administrar y monitorear el plano de datos y los componentes del plano de control. Debe pensar en cómo proporcionar una alta disponibilidad de la

arquitectura de malla, cómo monitorear el estado y el rendimiento de la malla y cómo gestionar las actualizaciones de los componentes de la malla.

Por otro lado, un modelo radial establece un enrutamiento de tráfico centralizado en varias redes. Simplifica la estrategia de administración y monitoreo del plano de datos y los componentes del plano de control.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Cree una cuenta de servicios de red si no hay ninguna. Coloque el hub en la cuenta de servicios de red de la organización. Este enfoque permite que los ingenieros de redes administren el hub de forma centralizada.

El hub del modelo radial funciona como un enrutador virtual del flujo de tráfico entre las nubes privadas virtuales (VPC) y las redes en las instalaciones. Esta estrategia reduce la complejidad de la red y facilita la resolución de problemas de red.

Tenga en cuenta el diseño de su red, incluidas las VPC, AWS Direct Connect y las conexiones VPN de sitio a sitio que desee interconectar.

Plantéese utilizar una subred independiente para cada archivo asociado a la VPC de la puerta de enlace de tránsito. En cada subred, utilice un CIDR pequeño, (por ejemplo /28), a fin de tener más espacio de direcciones para los recursos de computación. Además, cree una única ACL de red y asóciela a todas las subredes relacionadas con el hub. Mantenga abierta la ACL de red tanto en las direcciones de entrada como de salida.

Diseñe e implemente sus tablas de enrutamiento de manera que las rutas se establezcan solo entre redes que deban comunicarse. Omita rutas entre redes que no deberían comunicarse entre sí (por ejemplo, cargas de trabajo independientes que no tienen interdependencias).

Pasos para la implementación

1. Planifique su red. Determine qué redes desea conectar y compruebe que no compartan rangos de CIDR superpuestos.
2. Cree una AWS Transit Gateway y asocie sus VPC.
3. Si es necesario, cree conexiones VPN o puertas de enlace de Direct Connect y asócielas a la instancia de Transit Gateway.

4. Defina cómo se dirige el tráfico entre las VPC conectadas y otras conexiones mediante la configuración de las tablas de enrutamiento de Transit Gateway.
5. Utilice Amazon CloudWatch para supervisar y ajustar las configuraciones según sea necesario para optimizar el rendimiento y los costos.

Recursos

Prácticas recomendadas relacionadas:

- REL02-BP03 Garantía de que la asignación de subredes IP tenga en cuenta la expansión y la disponibilidad
- REL02-BP05 Aplicación de intervalos de direcciones IP privadas que no se superponen en todos los espacios de direcciones privadas en los que están conectados

Documentos relacionados:

- What Is a Transit Gateway?
- Prácticas recomendadas de diseño de una puerta de enlace de tránsito
- Creación de una infraestructura de red de AWS multiVPC escalable y segura
- Building a global network using AWS Transit Gateway Inter-Region peering
- Opciones de conectividad de Amazon Virtual Private Cloud
- Socio de APN: socios que pueden ayudarle a planificar sus redes
- AWS Marketplace para la infraestructura de red

Videos relacionados:

- AWS re:Invent 2023 - AWS networking foundations
- AWS re:Invent 2023 - Advanced VPC designs and new capabilities

Talleres relacionados:

- AWS Transit Gateway Workshop

REL02-BP05 Aplicación de intervalos de direcciones IP privadas que no se superponen en todos los espacios de direcciones privadas en los que están conectados

Los intervalos de direcciones IP de cada VPC no deben superponerse si se emparejan o conectan mediante Transit Gateway o VPN. Evite conflictos de direcciones IP entre una VPC y los entornos en las instalaciones o con otros proveedores de servicios en la nube que utilice. También debe tener una forma de asignar intervalos de direcciones IP privadas cuando sea necesario. Un sistema Administrador de direcciones IP (IPAM) puede ayudar en esta automatización.

Resultado deseado:

- No hay conflictos de intervalo de direcciones IP entre VPC, entornos en las instalaciones u otros proveedores de servicios en la nube.
- La administración adecuada de las direcciones IP permite escalar de forma más sencilla la infraestructura de red para adaptarse al crecimiento y los cambios en los requisitos de la red.

Patrones comunes de uso no recomendados:

- Usar el mismo intervalo de direcciones IP en la VPC que en el entorno en las instalaciones, en la red corporativa o en otros proveedores de servicios en la nube
- No controlar los intervalos de direcciones IP de las VPC usadas para implementar sus cargas de trabajo.
- Confiar en los procesos manuales de administración de direcciones IP, como, por ejemplo, las hojas de cálculo.
- Sobredimensionar o infradimensionar bloques de CIDR, lo que provoca un derroche en el uso de direcciones IP o un espacio insuficiente para las direcciones de la carga de trabajo.

Beneficios de establecer esta práctica recomendada: la planificación activa de la red garantizará que no tenga varias instancias de la misma dirección IP en las redes interconectadas. Con esto evitará que se produzcan problemas de enrutamiento en las partes de la carga de trabajo que usan las diferentes aplicaciones.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Utilice un IPAM, como el Administrador de direcciones IP de Amazon VPC, para supervisar y administrar el uso del CIDR. En AWS Marketplace, también hay disponibles varios IPAM. Evalúe su potencial de uso en AWS, agregue intervalos de CIDR a las VPC existentes y cree VPC para permitir un crecimiento planificado del uso.

Pasos para la implementación

- Capture el consumo actual de CIDR (por ejemplo, VPC y subredes).
  - Use operaciones de la API de servicio para recopilar el consumo actual de CIDR.
  - Utilice el Administrador de direcciones IP de Amazon VPC para detectar recursos.
- Registre el uso actual de la subred.
  - Use operaciones de la API de servicio para recopilar las subredes por VPC en cada región.
  - Utilice el Administrador de direcciones IP de Amazon VPC para detectar recursos.
- Registre el uso actual.
- Determine si creó intervalos de direcciones IP superpuestos.
- Calcule la capacidad de reserva.
- Identifique los intervalos de direcciones IP superpuestos. Puede migrar a un nuevo intervalo de direcciones o considerar la posibilidad de utilizar técnicas como una puerta de enlace NAT privada o AWS PrivateLink si necesita conectar los intervalos superpuestos.

Recursos

Prácticas recomendadas relacionadas:

- Protección de redes

Documentos relacionados:

- Socio de APN: socios que pueden ayudarle a planificar sus redes
- AWS Marketplace para la infraestructura de red
- Documento técnico sobre las opciones de conectividad a la nube virtual privada de Amazon
- Conectividad a la red de varios centros de datos HA
- Connecting Networks with Overlapping IP Ranges

- Qué es Amazon VPC?
- ¿Qué es IPAM?

Videos relacionados:

- AWS re:Invent 2023 - Advanced VPC designs and new capabilities
- AWS re:Invent 2019: AWS Transit Gateway reference architectures for many VPCs
- AWS re:Invent 2023 - Ready for what's next? Designing networks for growth and flexibility
- AWS re:Invent 2021 - {New Launch} Manage your IP addresses at scale on AWS

Arquitectura de la carga de trabajo

Una carga de trabajo fiable comienza por tomar decisiones de diseño anticipadas tanto para el software como para la infraestructura. Sus elecciones respecto a la arquitectura afectarán al comportamiento de su carga de trabajo en los seis pilares de Well-Architected. Para la fiabilidad, debe seguir patrones específicos.

En las siguientes secciones se explican las prácticas recomendadas que se pueden utilizar con estos patrones para garantizar la fiabilidad.

Temas

- Diseño de la arquitectura de servicio de su carga de trabajo
- Diseño de las interacciones en un sistema distribuido para evitar los errores
- Diseño de interacciones en un sistema distribuido para mitigar o tolerar errores

Diseño de la arquitectura de servicio de su carga de trabajo

Desarrolle cargas de trabajo escalables y fiables mediante una arquitectura orientada a servicios (SOA) o una arquitectura de microservicios. La arquitectura orientada a servicios (SOA) es hacer que los componentes de software se puedan reutilizar mediante interfaces de servicio. La arquitectura de microservicios va más allá, para hacer que los componentes sean más pequeños y sencillos.

Las interfaces de arquitectura orientada a servicios (SOA) utilizan estándares de comunicación comunes para que puedan incorporarse rápidamente a las nuevas cargas de trabajo. La SOA sustituyó a la práctica de crear arquitecturas monolíticas, que consistían en unidades indivisibles e interdependientes.

En AWS, siempre hemos utilizado SOA, pero ahora hemos optado por crear nuestros sistemas mediante microservicios. Si bien los microservicios tienen varias cualidades atractivas, el beneficio más importante para la disponibilidad es que estos son más pequeños y sencillos. Permiten diferenciar la disponibilidad requerida de diferentes servicios y, por lo tanto, centrar las inversiones más específicamente en los microservicios que tienen mayores necesidades de disponibilidad. Por ejemplo, para entregar páginas de información de productos en Amazon.com (“páginas de detalles”), se invocan cientos de microservicios para crear porciones discretas de la página. Si bien hay algunos servicios que deben estar disponibles para proporcionar el precio y los detalles del producto, la gran mayoría del contenido de la página puede simplemente excluirse si el servicio no está disponible.

Incluso las fotos y las reseñas no son necesarias para proporcionar una experiencia en la que un cliente pueda comprar un producto.

Prácticas recomendadas

- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL03-BP02 Desarrollo de servicios centrados en funcionalidades y dominios empresariales específicos
- REL03-BP03 Disposición de contratos de servicio por cada API

REL03-BP01 Elección de cómo segmentar su carga de trabajo

La segmentación de la carga de trabajo es importante a la hora de determinar los requisitos de resiliencia de su aplicación. La arquitectura monolítica debe evitarse siempre que sea posible. En su lugar, considere detenidamente qué componentes de la aplicación pueden dividirse en microservicios. Según los requisitos de su aplicación, esto puede terminar siendo una combinación de una arquitectura orientada a servicios (SOA) con microservicios cuando sea posible. Las cargas de trabajo que son capaces de no tener estado son más capaces de implementarse como microservicios.

Resultado deseado: las cargas de trabajo se deben admitir, ser escalables y tener el acoplamiento más débil que sea posible.

A la hora de elegir cómo segmentar la carga de trabajo, hay que sopesar las ventajas frente a las complejidades. Lo que puede ser adecuado para un nuevo producto encaminado a su primer lanzamiento es diferente a lo que necesita una carga de trabajo creada para escalarse desde el principio. Al refactorizar un monolito existente, tendrá que considerar en qué medida soportará la aplicación una descomposición hacia la falta de estado. Dividir los servicios en partes más pequeñas permite que equipos pequeños y bien definidos los desarrollen y administren. No obstante, los servicios más pequeños pueden introducir complejidades que incluyen un aumento de la latencia, una depuración más compleja y un mayor lastre operativo.

Patrones comunes de uso no recomendados:

- La Estrella de la muerte de microservicios es una situación en la que los componentes atómicos son tan interdependientes que el error de uno de ellos provoca un error mucho mayor, lo que hace que los componentes sean tan rígidos y frágiles como un monolito.

Beneficios de establecer esta práctica:

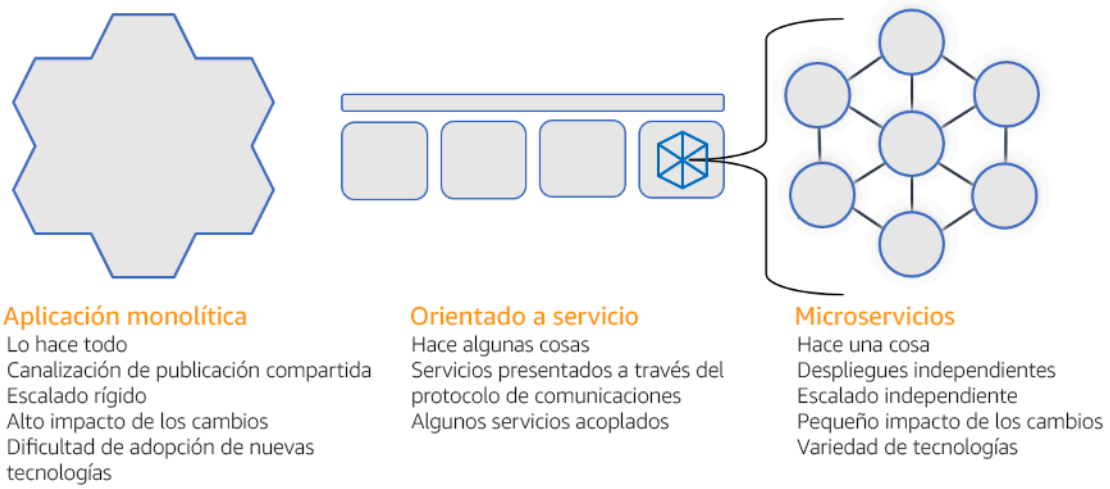
- Los segmentos más específicos conducen a una mayor agilidad, flexibilidad organizativa y escalabilidad.
- Reducción del impacto de las interrupciones del servicio.
- Los componentes de la aplicación pueden tener diferentes requisitos de disponibilidad, que pueden soportarse mediante una segmentación más atómica.
- Responsabilidades bien definidas para los equipos que apoyan la carga de trabajo.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Seleccione el tipo de arquitectura en función de cómo va a segmentar su carga de trabajo. Seleccione una SOA o una arquitectura de microservicios (o, en algunos casos raros, una arquitectura monolítica). Incluso si decide empezar con una arquitectura monolítica, debe asegurarse de que sea modular y de que pueda evolucionar hacia SOA o microservicios de forma definitiva, a medida que su producto escala con la adopción por parte de los usuarios. La SOA y los microservicios ofrecen respectivamente una segmentación más pequeña, lo que resulta preferible como arquitectura moderna escalable y fiable, pero existen compensaciones a tener en cuenta, especialmente al implementar una arquitectura de microservicios.

Una compensación principal es que se dispone de una arquitectura de computación distribuida que puede dificultar el cumplimiento de los requisitos de latencia del usuario y existe una complejidad adicional en la depuración y el rastreo de las interacciones del usuario. Puede utilizar AWS X-Ray para ayudarle a resolver este problema. Otro efecto que hay que tener en cuenta es el aumento de la complejidad operativa a medida que aumenta el número de aplicaciones que se administran, lo que requiere la implementación de componentes con varias independencias.



Arquitecturas monolíticas, orientadas al servicio y de microservicios

Pasos para la implementación

- Determine la arquitectura adecuada para refactorizar o desarrollar su aplicación. La SOA y los microservicios ofrecen respectivamente una segmentación más pequeña, lo que resulta preferible como arquitectura moderna escalable y fiable. La SOA puede ofrecer un término intermedio ideal para conseguir una segmentación más pequeña y, a la vez, evitar algunas de las complejidades de los microservicios. Para obtener más información, consulte Microservice Trade-Offs.
- Si su carga de trabajo lo admite y su organización puede permitírselo, debería usar una arquitectura de microservicios para conseguir la mejor agilidad y fiabilidad. Para obtener más información, consulte Implementing Microservices on AWS.
- Considere la posibilidad de seguir el patrón del higo estrangulador para refactorizar un monolito en componentes más pequeños. Esto implica reemplazar gradualmente componentes específicos de la aplicación por nuevas aplicaciones y servicios. AWS Migration Hub Refactor Spaces actúa como punto de partida para la refactorización incremental. Para obtener más información, consulte Seamlessly migrate on-premises legacy workloads using a strangler pattern.
- La implementación de microservicios puede necesitar de un mecanismo de detección de servicios que permita que estos servicios distribuidos se comuniquen entre sí. AWS App Mesh se puede utilizar con arquitecturas orientadas a los servicios para proporcionar una detección y un acceso fiables a estos. AWS Cloud Map también se puede utilizar para la detección dinámica de servicios basada en DNS.
- Si va a migrar de un entorno monolítico a SOA, Amazon MQ puede ayudarle a cerrar la brecha, en calidad de bus de servicio, a la hora de rediseñar aplicaciones heredadas en la nube.

- Para los monolitos existentes con una única base de datos compartida, elija cómo reorganizar los datos en segmentos más pequeños. Puede ser por unidad de negocio, patrón de acceso o estructura de datos. En este punto del proceso de refactorización, debe elegir entre una base de datos de tipo relacional o no relacional (NoSQL). Para obtener más información, consulte From SQL to NoSQL.

Nivel de esfuerzo para el plan de implementación: alto

Recursos

Prácticas recomendadas relacionadas:

- REL03-BP02 Desarrollo de servicios centrados en funcionalidades y dominios empresariales específicos

Documentos relacionados:

- Amazon API Gateway: Configuring a REST API Using OpenAPI
- ¿Qué es la arquitectura orientada a servicios (SOA)?
- Bounded Context (a central pattern in Domain-Driven Design)
- Implementing Microservices on AWS
- Microservice Trade-Offs
- Microservices - a definition of this new architectural term
- Microservicios en AWS
- Qué es AWS App Mesh?

Ejemplos relacionados:

- Iterative App Modernization Workshop

Videos relacionados:

- Delivering Excellence with Microservices on AWS

REL03-BP02 Desarrollo de servicios centrados en funcionalidades y dominios empresariales específicos

La arquitectura orientada a servicios (SOA) define servicios con funciones bien delineadas y determinadas por necesidades empresariales. Los microservicios utilizan modelos de dominio y contextos delimitados para trazar los límites de los servicios en los límites del contexto empresarial. Centrarse en los dominios y las funcionalidades empresariales ayuda a los equipos a definir requisitos de fiabilidad independientes para sus servicios. Los contextos delimitados aíslan y encapsulan la lógica empresarial, lo que permite a los equipos mejorar la forma en que gestionan los errores.

Resultado deseado: los ingenieros y las partes interesadas de la empresa definen conjuntamente los contextos delimitados y los utilizan para diseñar sistemas como servicios que cumplan funciones empresariales específicas. Estos equipos utilizan prácticas establecidas, como las tormentas de eventos, para definir los requisitos. Las nuevas aplicaciones se diseñan como límites bien definidos de servicios y con acoplamiento débil. Los monolitos existentes se descomponen en contextos delimitados y los diseños de sistemas avanzan hacia arquitecturas SOA o de microservicios. Cuando los monolitos se refactorizan, se aplican enfoques establecidos, como contextos burbuja y patrones de descomposición de monolitos.

Los servicios orientados al dominio se ejecutan como uno o más procesos que no comparten el estado. Responden de forma independiente a las fluctuaciones de la demanda y gestionan los escenarios de error en función de los requisitos específicos del dominio.

Patrones comunes de uso no recomendados:

- Se forman equipos en torno a dominios técnicos específicos, como la interfaz de usuario y la experiencia de usuario, el middleware o la base de datos, en lugar de formarse en torno a dominios empresariales específicos.
- Las aplicaciones abarcan las responsabilidades del dominio. Los servicios que abarcan contextos delimitados pueden ser más difíciles de mantener, exigen más pruebas y requieren la participación de equipos de varios dominios en las actualizaciones del software.
- Las dependencias de dominio, como las bibliotecas de entidades de dominio, se comparten entre los servicios, de modo que los cambios en un dominio de servicio requieren cambios en otros dominios de servicio

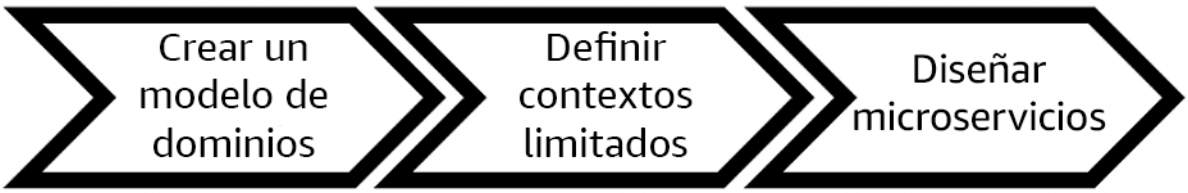
- Los contratos de servicio y la lógica empresarial no expresan las entidades en un lenguaje de dominio común y coherente, lo que genera capas de traducción que complican los sistemas e incrementan los esfuerzos de depuración.

Beneficios de establecer esta práctica recomendada: las aplicaciones se diseñan como servicios independientes delimitados por dominios empresariales y utilizan un lenguaje empresarial común. Los servicios se pueden probar e implementar de forma independiente. Los servicios cumplen los requisitos de resiliencia específicos del dominio implementado.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

El enfoque de decisiones impulsadas por dominio (DDD) es el enfoque fundamental para diseñar y crear software en torno a los dominios empresariales. Resulta útil trabajar con un marco existente a la hora de crear servicios centrados en dominios empresariales. Si trabaja con aplicaciones monolíticas existentes, puede utilizar patrones de descomposición que ofrecen técnicas establecidas para modernizar las aplicaciones y convertirlas en servicios.



Diseño basado en el dominio

Pasos para la implementación

- Los equipos pueden organizar talleres de tormentas de eventos para identificar rápidamente eventos, comandos, agregados y dominios en un formato de notas adhesivas más ligero.
- Cuando las entidades y funciones del dominio se formen en un contexto de dominio, puede dividir el dominio en servicios mediante un contexto delimitado, en el que se agrupan las entidades que comparten características y atributos similares. Si el modelo está dividido en contextos, tendrá una plantilla para limitar los microservicios.
  - Por ejemplo, las entidades del sitio web de Amazon.com podrían incluir el empaquetado, la entrega, la programación, el precio, el descuento y la divisa.

  - El empaquetado, la entrega y la programación se agrupan en el contexto del envío, mientras que el precio, el descuento y la divisa se agrupan en el contexto de los precios.
- La descomposición de los monolitos en microservicios describe los patrones para refactorizar los microservicios. El uso de patrones de descomposición por capacidad empresarial, subdominio o transacción se ajusta bien a los enfoques basados en dominios.
- Técnicas tácticas como el contexto burbuja, que permiten introducir DDD en aplicaciones existentes o heredadas sin necesidad de reescrituras iniciales ni confirmaciones completas de las DDD. En un enfoque con contexto burbuja, se establece un pequeño contexto delimitado mediante una capa de asignación y coordinación de servicios (capa anticorrupción), que protege el modelo de dominio recién definido de influencias externas.

Después de que los equipos analicen el dominio y definan las entidades y los contratos de servicio, podrán utilizar los servicios de AWS para implementar su diseño basado en dominio como servicios basados en la nube.

- Para comenzar el desarrollo, defina pruebas en las que se utilicen las reglas empresariales de su dominio. El desarrollo basado en pruebas (TDD) y el desarrollo basado en comportamiento (BDD) ayudan a los equipos a mantener los servicios centrados en resolver problemas empresariales.
- Seleccione los servicios de AWS que mejor se adapten a los requisitos del dominio empresarial y a la arquitectura de microservicios:
  - AWS sin servidor permite a su equipo centrarse en una lógica de dominio específica en lugar de administrar servidores e infraestructuras.
  - Los contenedores en AWS simplifican la administración de su infraestructura para que pueda centrarse en los requisitos de su dominio.
  - Las bases de datos personalizadas le ayudan a adaptar los requisitos de su dominio al tipo de base de datos más adecuado.
- La creación de arquitecturas hexagonales en AWS describe un marco para integrar la lógica empresarial en los servicios que funcionan de manera inversa desde un dominio empresarial para cumplir los requisitos funcionales y, a continuación, asociar los adaptadores de integración. Los patrones que separan los detalles de la interfaz de la lógica empresarial con los servicios de AWS ayudan a los equipos a centrarse en la funcionalidad del dominio y a mejorar la calidad del software.

Recursos

Prácticas recomendadas relacionadas:

- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL03-BP03 Disposición de contratos de servicio por cada API

Documentos relacionados:

- Microservicios de AWS
- Implementing Microservices on AWS
- How to break a Monolith into Microservices
- Getting Started with DDD when Surrounded by Legacy Systems
- Domain-Driven Design: Tackling Complexity in the Heart of Software
- Building hexagonal architectures on AWS
- Decomposing monoliths into microservices
- Event Storming
- Messages Between Bounded Contexts
- Microservices
- Desarrollo guiado por pruebas
- Desarrollo guiado por comportamiento

Ejemplos relacionados:

- Designing Cloud Native Microservices on AWS (from DDD/EventStormingWorkshop)

Herramientas relacionadas:

- Bases de datos en la nube de Nube de AWS
- Sin servidor en AWS
- Contenedores en AWS

REL03-BP03 Disposición de contratos de servicio por cada API

Los contratos de servicio son acuerdos documentados entre los productores y los consumidores de las API que se encuentran en una definición de API legible por máquina. Una estrategia de control de versiones permite a los clientes seguir usando la API existente y migrar sus aplicaciones a la nueva API cuando estén listas. La implementación del productor puede efectuarse en cualquier momento, siempre y cuando se cumpla el contrato. Los equipos del servicio pueden usar la pila tecnológica que prefieran para cumplir el contrato de la API.

Resultado deseado: las aplicaciones creadas con arquitecturas orientadas a servicios o de microservicios pueden funcionar de forma independiente y, al mismo tiempo, tener integrada una dependencia de la versión en tiempo de ejecución. Los cambios implementados en un consumidor o productor de API no interrumpen la estabilidad del sistema general cuando ambas partes utilizan el mismo contrato de API. Los componentes que se comunican a través de las API de servicio pueden llevar a cabo lanzamientos funcionales independientes, actualizar las dependencias en tiempo de ejecución o efectuar conmutaciones por error a un sitio de recuperación de desastres (DR) con poco o ningún impacto entre sí. Además, los servicios discretos pueden escalarse de forma independiente y absorber la demanda de recursos sin que sea necesario que otros servicios se escalen al unísono.

Patrones comunes de uso no recomendados:

- Crear API de servicio sin esquemas estrictamente asignados. Como consecuencia, las API no se pueden usar para generar enlaces de API y las cargas útiles no se pueden validar mediante programación.
- No adoptar una estrategia de control de versiones, lo que obliga a los usuarios de la API a actualizarla y lanzarla; de lo contrario, fallará cuando los contratos de servicio evolucionen.
- Mensajes de error que filtran detalles de la implementación del servicio subyacente en lugar de describir los errores de integración en el contexto y el lenguaje del dominio.
- No utilizar contratos de API para desarrollar casos de prueba ni simulaciones de implementaciones de API para probar de forma independiente los componentes del servicio.

Beneficios de establecer esta práctica recomendada: los sistemas distribuidos que constan de componentes que se comunican a través de contratos de servicio de API pueden mejorar la fiabilidad. Los desarrolladores pueden detectar posibles problemas al principio del proceso de desarrollo mediante la comprobación de tipos durante la compilación para comprobar que las solicitudes y las respuestas cumplan el contrato de la API y que los campos obligatorios estén

presentes. Los contratos de la API proporcionan una interfaz clara y autodocumentada para las API y mejoran la interoperabilidad entre diferentes sistemas y lenguajes de programación.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Una vez que hayan identificado los dominios empresariales y determinado la segmentación de la carga de trabajo, podrá desarrollar las API de sus servicios. Primero, defina contratos de servicio legibles por máquina para las API y, a continuación, implemente una estrategia de control de versiones de API. Cuando lo tenga todo preparado para integrar servicios a través de protocolos comunes, como REST, GraphQL o eventos asíncronos, podrá incorporar servicios de AWS a su arquitectura para integrar sus componentes con contratos de API estrictamente asignados.

Servicios de AWS para contratos de API de servicios

Incorpore servicios de AWS como Amazon API Gateway, AWS AppSync y Amazon EventBridge a su arquitectura para utilizar los contratos de servicios de API en su aplicación. Amazon API Gateway le ayuda a integrarse directamente con servicios de AWS nativos y otros servicios web. API Gateway admite el control de versiones y la especificación de OpenAPI. AWS AppSync es un punto de conexión de GraphQL administrado que se configura mediante la definición de un esquema de GraphQL para definir una interfaz de servicio para consultas, mutaciones y suscripciones. Amazon EventBridge utiliza esquemas de eventos para definir eventos y generar enlaces de código para sus eventos.

Pasos para la implementación

- Primero, defina un contrato para su API. En un contrato, se expresan las capacidades de una API y se definen objetos y campos de datos estrictamente asignados para la entrada y la salida de la API.
- Cuando configure las API en API Gateway, puede importar y exportar las especificaciones de OpenAPI para sus puntos de conexión.
  - La importación de una definición de OpenAPI simplifica la creación de su API y se puede integrar con la infraestructura de AWS, como herramientas de código (por ejemplo, AWS Serverless Application Model y Kit de desarrollo de la nube de AWS (AWS CDK)).
  - La exportación de una definición de API simplifica la integración con las herramientas de prueba de API y proporciona a los consumidores de servicios una especificación de la integración.

- Puede definir y administrar las API de GraphQL con AWS AppSync mediante la definición de un archivo de esquema de GraphQL para generar su interfaz de contrato y simplificar la interacción con modelos de REST complejos, múltiples tablas de bases de datos o servicios heredados.
- Los proyectos de AWS Amplify que están integrados con AWS AppSync generan archivos de consulta de JavaScript estrictamente asignados para usarlos en su aplicación, así como una biblioteca de clientes de AWS AppSync GraphQL para tablas de Amazon DynamoDB.
- Cuando se consumen eventos de servicio de Amazon EventBridge, los eventos se ajustan a esquemas que ya existen en el registro de esquemas o que se definen con la especificación de OpenAPI. Si tiene un esquema definido en el registro, también puede generar enlaces de clientes desde el contrato de esquema para integrar el código con los eventos.
- Amplíe la API o lleve a cabo un control de versiones. Ampliar una API es la opción más sencilla cuando se agregan campos que se pueden configurar con campos opcionales o valores predeterminados para los campos obligatorios.
  - Los contratos basados en JSON para protocolos como REST y GraphQL pueden ser una buena opción para la ampliación del contrato.
  - Los contratos basados en XML para protocolos como SOAP deben probarse con los consumidores de servicios para determinar la viabilidad de la ampliación del contrato.
- Al llevar a cabo el control de versiones de una API, considere la posibilidad de implementar un control de versiones por proxy en el que se utilice una fachada para admitir las versiones, de modo que la lógica se pueda mantener en una única base de código.
  - Con API Gateway, puede usar asignaciones de solicitud y respuesta para simplificar la absorción de los cambios en los contratos mediante el establecimiento de una fachada que proporcione valores predeterminados para los campos nuevos o para quitar los campos eliminados de una solicitud o respuesta. Con este enfoque, el servicio subyacente puede mantener una única base de código.

Recursos

Prácticas recomendadas relacionadas:

- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL03-BP02 Desarrollo de servicios centrados en funcionalidades y dominios empresariales específicos
- REL04-BP02 Implementación de dependencias con acoplamiento débil
- REL05-BP03 Control y limitación de las llamadas de reintento

- REL05-BP05 Definición de los tiempos de espera del cliente

Documentos relacionados:

- ¿Qué es una interfaz de programación de aplicaciones (API)?
- Implementing Microservices on AWS
- Microservice Trade-Offs
- Microservices - a definition of this new architectural term
- Microservicios en AWS
- Working with API Gateway extensions to OpenAPI
- OpenAPI-Specification
- GraphQL: Schemas and Types
- Amazon EventBridge code bindings

Ejemplos relacionados:

- Amazon API Gateway: Configuring a REST API Using OpenAPI
- Amazon API Gateway to Amazon DynamoDB CRUD application using OpenAPI
- Modern application integration patterns in a serverless age: API Gateway Service Integration
- Implementing header-based API Gateway versioning with Amazon CloudFront
- AWS AppSync: Building a client application

Videos relacionados:

- Using OpenAPI in AWS SAM to manage API Gateway

Herramientas relacionadas:

- Amazon API Gateway
- AWS AppSync
- Amazon EventBridge

Diseño de las interacciones en un sistema distribuido para evitar los errores

Los sistemas distribuidos se basan en las redes de comunicaciones para interconectar componentes, como servidores o servicios. Su carga de trabajo debe funcionar de manera fiable a pesar de la pérdida de datos o la latencia en estas redes. Los componentes del sistema distribuido deben funcionar de manera que no afecten negativamente a otros componentes o a la carga de trabajo. Estas prácticas recomendadas previenen los fallos y mejoran el tiempo medio entre errores (MTBD).

Prácticas recomendadas

- REL04-BP01 Identificación del tipo de sistemas distribuidos de los que depende
- REL04-BP02 Implementación de dependencias con acoplamiento débil
- REL04-BP03 Trabajo constante
- REL04-BP04 Cómo hacer idempotentes las operaciones de mutación

REL04-BP01 Identificación del tipo de sistemas distribuidos de los que depende

Los sistemas distribuidos pueden ser síncronos, asíncronos o por lotes. Los sistemas síncronos deben procesar las solicitudes lo más rápido posible y comunicarse entre sí mediante llamadas síncronas de solicitud y respuesta mediante protocolos HTTP/S, REST o de llamada a procedimiento remoto (RPC). Los sistemas asíncronos se comunican entre sí mediante el intercambio de datos de forma asíncrona a través de un servicio intermediario sin acoplar sistemas individuales. Los sistemas por lotes reciben un gran volumen de datos de entrada, ejecutan procesos de datos automatizados sin intervención humana y generan datos de salida.

Resultado deseado: diseñe una carga de trabajo que interactúe eficazmente con las dependencias síncronas, asíncronas y por lotes.

Patrones comunes de uso no recomendados:

- La carga de trabajo espera indefinidamente una respuesta de sus dependencias, lo que podría provocar que se agote el tiempo de espera de los clientes de la carga de trabajo sin saber si su solicitud se ha recibido.
- La carga de trabajo utiliza una cadena de sistemas dependientes que se llaman entre sí de forma síncrona. Para ello, cada sistema debe estar disponible y procesar correctamente una

solicitud para que toda la cadena pueda tener éxito, lo que se traduce en un comportamiento y una disponibilidad general potencialmente frágiles.

- La carga de trabajo se comunica con sus dependencias de forma asíncrona y se basa en la entrega garantizada de mensajes exactamente una vez, aunque aún es posible que se reciban mensajes duplicados.
- La carga de trabajo no utiliza herramientas adecuadas de programación por lotes y permite la ejecución simultánea del mismo trabajo por lotes.

Beneficios de establecer esta práctica recomendada: es habitual que una carga de trabajo determinada implemente uno o más estilos de comunicación entre los sistemas síncronos, asíncronos o por lotes. Esta práctica recomendada le ayuda a identificar las diferentes ventajas y desventajas asociadas a cada estilo de comunicación para que su carga de trabajo pueda tolerar las interrupciones en cualquiera de sus dependencias.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las siguientes secciones contienen una guía de implementación general y específica para cada tipo de dependencia.

General guidance

- Asegúrese de que los objetivos de nivel de servicio (SLO) de rendimiento y fiabilidad que ofrecen sus dependencias cumplan los requisitos de rendimiento y fiabilidad de su carga de trabajo.
- Utilice los servicios de observabilidad de AWS para supervisar los tiempos de respuesta y las tasas de error y asegurarse de que su dependencia presta el servicio a los niveles que necesita su carga de trabajo.
- Identifique los posibles desafíos a los que puede enfrentarse su carga de trabajo al comunicarse con sus dependencias. Los sistemas distribuidos se enfrentan a una amplia gama de desafíos que pueden aumentar la complejidad de la arquitectura, la carga operativa y el costo. Entre los desafíos comunes, se incluyen la latencia, las interrupciones de la red, la pérdida de datos, el escalado y el retardo en la replicación de datos.
- Implemente un sistema sólido de gestión y registro de errores para ayudarle a solucionar problemas cuando su dependencia experimente problemas.

Dependencia síncrona

En las comunicaciones síncronas, la carga de trabajo envía una solicitud a su dependencia y bloquea la operación en espera de una respuesta. Cuando la dependencia recibe la solicitud, intenta gestionarla lo antes posible y envía una respuesta a su carga de trabajo. Un problema importante de la comunicación síncrona es que provoca un acoplamiento temporal, por lo que la carga de trabajo y sus dependencias deben estar disponibles al mismo tiempo. Cuando la carga de trabajo necesite comunicarse de forma síncrona con sus dependencias, tenga en cuenta lo siguiente:

- La carga de trabajo no debe depender de varias dependencias síncronas para llevar a cabo una sola función. Esta cadena de dependencias aumenta la fragilidad general, porque todas las dependencias de la ruta deben estar disponibles para que la solicitud se complete correctamente.
- Cuando una dependencia no esté en buen estado o no esté disponible, determine sus estrategias de gestión de errores y reintentos. Evite utilizar un comportamiento bimodal. El comportamiento bimodal se produce cuando la carga de trabajo presenta un comportamiento diferente en los modos normal y de error. Para obtener más información sobre el comportamiento bimodal, consulte REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal.
- Tenga en cuenta que responder rápido a los errores es mejor que hacer esperar a la carga de trabajo. Por ejemplo, la Guía para desarrolladores de AWS Lambda describe cómo gestionar los reintentos y los errores al invocar funciones de Lambda.
- Establezca tiempos de espera cuando la carga de trabajo llame a su dependencia. Esta técnica evita esperar demasiado o indefinidamente una respuesta. Para un análisis útil sobre este tema, consulte Tuning AWS Java SDK HTTP request settings for latency-aware Amazon DynamoDB applications.
- Minimice la cantidad de llamadas que se hacen desde la carga de trabajo a su dependencia para atender una sola solicitud. Si hay una conversación demasiado intensa entre ellos, aumenta el acoplamiento y la latencia.

Dependencia asíncrona

Para desvincular temporalmente la carga de trabajo de su dependencia, deben comunicarse de forma asíncrona. Con un enfoque asíncrono, la carga de trabajo puede continuar con cualquier otro procesamiento sin tener que esperar a que su dependencia o cadena de dependencias envíe una respuesta.

Cuando la carga de trabajo necesite comunicarse de forma asíncrona con su dependencia, tenga en cuenta lo siguiente:

- Determine si va a utilizar la mensajería o la transmisión de eventos en función de su caso de uso y sus requisitos. La mensajería permite que la carga de trabajo se comunique con su dependencia mediante el envío y la recepción de mensajes a través de un agente de mensajes. La transmisión de eventos permite que su carga de trabajo y su dependencia utilicen un servicio de transmisión para publicar y suscribirse a eventos. Estas transmisiones se distribuyen como flujos continuos de datos, que deben procesarse lo antes posible.

- La mensajería y la transmisión de eventos gestionan los mensajes de manera diferente, por lo que debe decidir si compensan en función de lo siguiente:
  - Prioridad de mensajes: los agentes de mensajes pueden procesar los mensajes de alta prioridad antes que los de prioridad normal. En la transmisión de eventos, todos los mensajes tienen la misma prioridad.
  - Consumo de mensajes: los agentes de mensajes se aseguran de que los consumidores reciban el mensaje. Los consumidores de la transmisión de eventos deben llevar un registro del último mensaje que leyeron.
  - Orden de los mensajes: con la mensajería, no se garantiza la recepción de los mensajes en el orden exacto en que se envíen, a menos que se utilice el enfoque de “el primero en entrar es el primero en salir” (FIFO). La transmisión de eventos siempre mantiene el orden en que se produjeron los datos.
  - Eliminación de mensajes: en el caso de la mensajería, el consumidor debe eliminar el mensaje después de procesarlo. El servicio de transmisión de eventos agrega el mensaje a una transmisión y permanece allí hasta que venza el periodo de retención. Esta política de eliminación hace que la transmisión de eventos sea adecuada para volver a reproducir mensajes.
- Defina la forma en que la carga de trabajo sabe cuándo su dependencia ha terminado el trabajo. Por ejemplo, cuando la carga de trabajo invoca una función de Lambda de forma asíncrona, Lambda pone la solicitud en una cola y devuelve una respuesta de operación correcta sin información adicional. Cuando finalice el procesamiento, la función de Lambda puede enviar el resultado a un destino, que se puede configurar con base en el éxito o el error.
- Aumente la carga de trabajo para gestionar los mensajes duplicados mediante la idempotencia. La idempotencia significa que los resultados de la carga de trabajo no cambian aunque esta se genere más de una vez para el mismo mensaje. Es importante señalar que los servicios de mensajería o transmisión volverán a entregar un mensaje si se produce un error en la red o si no se ha recibido un acuse de recibo.

- Si la carga de trabajo no recibe una respuesta de su dependencia, debe volver a enviar la solicitud. Considere la posibilidad de limitar el número de reintentos para conservar los recursos de CPU, memoria y red de la carga de trabajo para gestionar otras solicitudes. La documentación de AWS Lambda muestra cómo gestionar los errores en la invocación asíncrona.
- Utilice las herramientas de observabilidad, depuración y rastreo adecuadas para administrar y utilizar la comunicación asíncrona de la carga de trabajo con su dependencia. Puede utilizar Amazon CloudWatch para supervisar los servicios de mensajería y transmisión de eventos. También puede instrumentar su carga de trabajo con AWS X-Ray para obtener información rápidamente que le permita solucionar problemas.

Dependencia por lotes

Los sistemas por lotes toman los datos de entrada, inician una serie de trabajos para procesarlos y producen algunos datos de salida, sin intervención manual. Según el tamaño de los datos, los trabajos pueden durar desde unos minutos hasta, en algunos casos, varios días. Cuando la carga de trabajo se comunique con su dependencia por lotes, tenga en cuenta lo siguiente:

- Defina el intervalo de tiempo en el que la carga de trabajo debe ejecutar el trabajo por lotes. La carga de trabajo puede configurar un patrón de recurrencia para invocar un sistema por lotes como, por ejemplo, cada hora o al final de cada mes.
- Determine la ubicación de la entrada de datos y la salida de los datos procesados. Elija un servicio de almacenamiento, como Amazon Simple Storage Service (Amazon S3), Amazon Elastic File System (Amazon EFS) y Amazon FSx para Lustre, que permita que su carga de trabajo lea y escriba archivos a escala.
- Si su carga de trabajo necesita invocar varios trabajos por lotes, puede utilizar AWS Step Functions para simplificar la orquestación de los trabajos por lotes que se ejecutan en AWS o en las instalaciones. Este proyecto de ejemplo demuestra la orquestación de trabajos por lotes mediante Step Functions, AWS Batch y Lambda.
- Supervise los trabajos por lotes para detectar anomalías, como que un trabajo tarde más de lo debido en completarse. Puede utilizar herramientas como Información de contenedores de CloudWatch para supervisar entornos y trabajos de AWS Batch. En este caso, su carga de trabajo impediría el inicio del siguiente trabajo e informaría al personal correspondiente de la excepción.

Recursos

Documentos relacionados:

- Operaciones de Nube de AWS: supervisión y observabilidad
- Amazon Builders' Library: los desafíos de los sistemas distribuidos
- REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal
- Guía para desarrolladores de AWS Lambda: control de errores y reintentos automáticos en AWS Lambda
- Tuning AWS Java SDK HTTP request settings for latency-aware Amazon DynamoDB applications
- Mensajería de AWS
- ¿Qué son los datos de streaming?
- Guía para desarrolladores de AWS Lambda: invocación asíncrona
- Preguntas frecuentes sobre Amazon Simple Queue Service: colas FIFO
- Amazon Kinesis Data Streams Developer Guide: Handling Duplicate Records
- Amazon Simple Queue Service Developer Guide: Available CloudWatch metrics for Amazon SQS
- Amazon Kinesis Data Streams Developer Guide: Monitoring the Amazon Kinesis Data Streams Service with Amazon CloudWatch
- AWS X-Ray Developer Guide: AWS X-Ray concepts
- Ejemplos de AWS en GitHub: aplicación de AWS Step Functions Complex Orchestrator
- AWS Batch User Guide: AWS Batch CloudWatch Container Insights

Videos relacionados:

- AWS Summit SF 2022 - Full-stack observability and application monitoring with AWS (COP310)

Herramientas relacionadas:

- Amazon CloudWatch
- Registros de Amazon CloudWatch
- AWS X-Ray
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic File System (Amazon EFS)
- Amazon FSx para Lustre
- AWS Step Functions
- AWS Batch

REL04-BP02 Implementación de dependencias con acoplamiento débil

Las dependencias, como los sistemas de colas, los sistemas de transmisión, los flujos de trabajo y los equilibradores de carga, tienen un acoplamiento débil. El acoplamiento débil ayuda a aislar el comportamiento de un componente de otros componentes que dependen de él, lo que aumenta la resiliencia y la agilidad.

El desacoplamiento de las dependencias, como los sistemas de colas, los sistemas de transmisión y los flujos de trabajo, ayuda a minimizar el impacto de los cambios o los errores en un sistema. Esta separación aísla el comportamiento de un componente para que no afecte a otros que dependan de él, lo que mejora la resiliencia y la agilidad.

En sistemas de acoplamiento ajustado, los cambios en un componente pueden requerir cambios en otros componentes que dependan de él, lo que reduce el rendimiento de todos los componentes. El acoplamiento débil elimina esta dependencia, de forma que los componentes dependientes solo necesitan conocer la interfaz publicada y con control de versiones. La implementación de un acoplamiento débil entre las dependencias aísla un error en una de ellas para que no afecte a otra.

El acoplamiento débil permite modificar el código o agregar características a un componente y, al mismo tiempo, minimizar el riesgo para otros componentes que dependan de él. También permite una resiliencia granular de los componentes, lo que permite escalar horizontalmente o incluso cambiar la implementación subyacente de la dependencia.

Para mejorar aún más la resiliencia mediante el acoplamiento débil, haga que las interacciones entre componentes sean asincrónicas siempre que sea posible. Este modelo es adecuado para cualquier interacción que no necesite una respuesta inmediata y en la que baste con el reconocimiento de que una solicitud se ha registrado. Consta de un componente que genera eventos y de otro que los consume. Ambos componentes no se integran mediante una interacción directa de punto a punto, sino que normalmente emplean una capa de almacenamiento duradera intermedia, como una cola de Amazon SQS o una plataforma de restringa de datos como Amazon Kinesis o AWS Step Functions.

Figura 4: Las dependencias, como los sistemas de colas y los balanceadores de carga, tienen un acoplamiento débil

Las colas de Amazon SQS y AWS Step Functions son solo dos formas de agregar una capa intermedia para el acoplamiento débil. Las arquitecturas basadas en eventos también se pueden crear en la Nube de AWS con Amazon EventBridge, que puede separar a los clientes (productores

de eventos) de los servicios de los que dependen (consumidores de eventos). Amazon Simple Notification Service (Amazon SNS) es una solución eficaz para cuando sean necesarios mensajes de alto rendimiento, de tipo push y de varios a varios. Con el uso de temas de Amazon SNS, los sistemas de su publicador pueden repartir mensajes por una gran cantidad de puntos de conexión de suscriptores para procesarlos en paralelo.

Aunque las colas ofrecen varias ventajas, en la mayoría de sistemas en tiempo real estricto, las solicitudes que superan un umbral temporal (que suele ser de segundos) se consideran obsoletas (el cliente ha desistido y ya no espera una respuesta), por lo que no se procesan. De esta manera, se pueden procesar las solicitudes más recientes (y probablemente aún válidas) en su lugar.

Resultado deseado: la implementación de dependencias con un acoplamiento débil permite minimizar la superficie de posibles errores a nivel del componente, lo que ayuda a diagnosticar y resolver problemas. También simplifica los ciclos de desarrollo, lo que permite a los equipos implementar cambios a nivel modular sin que eso afecte al rendimiento de otros componentes que dependan de él. Este enfoque ofrece la capacidad de escalar horizontalmente a nivel de componente en función de los recursos que sean necesarios, así como de utilizar un componente que contribuye a ahorrar costos.

Patrones comunes de uso no recomendados:

- Implementar una carga de trabajo monolítica.
- Invocar directamente las API entre capas de la carga de trabajo sin la capacidad de conmutar por error ni procesar de manera asíncrona la solicitud.
- Utilizar un acoplamiento ajustado con datos compartidos. Los sistemas de acoplamiento débil no deben compartir datos a través de bases de datos compartidas u otras formas de almacenamiento de datos de acoplamiento ajustado, que pueden reintroducir el acoplamiento ajustado y dificultar la escalabilidad.
- Ignorar la contrapresión. La carga de trabajo debe tener la capacidad de ralentizar o detener los datos entrantes cuando un componente no pueda procesarlos al mismo ritmo.

Beneficios de establecer esta práctica recomendada: el acoplamiento débil ayuda a aislar el comportamiento de un componente de otros que dependen de él, lo que aumenta la resiliencia y la agilidad. Un error en un componente está aislado de los demás componentes.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Implemente dependencias con acoplamiento débil. Existen varias soluciones que permiten crear aplicaciones con un acoplamiento débil. Entre ellas, se incluyen servicios para implementar colas totalmente administradas, flujos de trabajo automatizados, reacción a eventos y API, entre otras, que pueden ayudar a aislar el comportamiento de los componentes de otros componentes y, por lo tanto, aumentar la resiliencia y la agilidad.

- Creación de arquitecturas basadas en eventos: Amazon EventBridge le ayuda a crear arquitecturas impulsadas por eventos distribuidas y acopladas de forma débil.
- Implementación de colas en sistemas distribuidos: puede utilizar Amazon Simple Queue Service (Amazon SQS) para integrar y desacoplar sistemas distribuidos.
- Colocación en contenedores de los componentes como microservicios: los microservicios permiten a los equipos crear aplicaciones compuestas por pequeños componentes independientes que se comunican a través de API bien definidas. Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS) le pueden ayudar a comenzar con el uso de contenedores.
- Administración de los flujos de trabajo con Step Functions: Step Functions le ayuda a coordinar varios servicios de AWS en flujos de trabajo flexibles.
- Uso de las arquitecturas de mensajería de publicación y suscripción (pub/sub): Amazon Simple Notification Service (Amazon SNS) proporciona la entrega de mensajes de los publicadores a los suscriptores (también conocidos como productores y consumidores).

Pasos para la implementación

- Los componentes de una arquitectura basada en eventos se inician mediante eventos. Los eventos son acciones que ocurren en un sistema, como cuando un usuario agrega un artículo a una cesta. Cuando una acción se lleva a cabo correctamente, se genera un evento que activa el siguiente componente del sistema.
  - Building Event-driven Applications with Amazon EventBridge
  - AWS re:Invent 2022 - Designing Event-Driven Integrations using Amazon EventBridge
- Los sistemas de mensajería distribuida tienen tres partes principales que deben implementarse para una arquitectura basada en colas. Incluyen los componentes del sistema distribuido, la cola que se usa para el desacoplamiento (distribuida en servidores de Amazon SQS servers) y los mensajes de la cola. Un sistema típico tiene productores que inician el mensaje en la cola y el

consumidor que recibe el mensaje de la cola. La cola almacena los mensajes en varios servidores de Amazon SQS para garantizar la redundancia.

  - Basic Amazon SQS architecture
  - Send Messages Between Distributed Applications with Amazon Simple Queue Service
- Los microservicios, cuando se utilizan bien, facilitan el mantenimiento y aumentan la escalabilidad, ya que los componentes de acoplamiento débil los administran equipos independientes. También permiten aislar los comportamientos en un solo componente en caso de que se hagan cambios.
  - Implementing Microservices on AWS
  - Let's Architect! Architecting microservices with containers
- Con AWS Step Functions, puede crear aplicaciones distribuidas, automatizar procesos y orquestar microservicios, entre otras cosas. La orquestación de varios componentes en un flujo de trabajo automatizado le permite desacoplar las dependencias de su aplicación.
  - Cree un flujo de trabajo sin servidor con y AWS Step FunctionsAWS Lambda
  - Introducción a AWS Step Functions

Recursos

Documentos relacionados:

- Amazon EC2: Ensuring Idempotency
- Amazon Builders' Library: Desafíos de los sistemas distribuidos
- Amazon Builders' Library: Reliability, constant work, and a good cup of coffee
- Qué es Amazon EventBridge?
- What Is Amazon Simple Queue Service?
- Break up with your monolith
- Orchestrate Queue-based Microservices with AWS Step Functions and Amazon SQS
- Basic Amazon SQS architecture
- Queue-Based Architecture

Videos relacionados:

- AWS New York Summit 2019: Intro to Event-driven Architectures and Amazon EventBridge (MAD205)

- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small ARC337 (includes loose coupling, constant work, static stability)
- AWS re:Invent 2019: Moving to event-driven architectures (SVS308)
- AWS re:Invent 2019: Scalable serverless event-driven applications using Amazon SQS and Lambda
- AWS re:Invent 2022 - Designing event-driven integrations using Amazon EventBridge
- AWS re:Invent 2017: Elastic Load Balancing Deep Dive and Best Practices

REL04-BP03 Trabajo constante

Los sistemas pueden producir error cuando hay cambios rápidos grandes en la carga. Por ejemplo, si la carga de trabajo está llevando a cabo una comprobación de estado que supervisa el estado de miles de servidores, debería enviar siempre una carga del mismo tamaño (una instantánea completa del estado actual). Si no hay errores en ningún servidor, o hay errores en todos ellos, el sistema de comprobación de estado estará haciendo un trabajo constante sin rápidos cambios de gran tamaño.

Por ejemplo, si el sistema de comprobación de estado supervisa 100 000 servidores, la carga contenida en él es nominal con un porcentaje de errores del servidor normalmente bajo. Sin embargo, si un evento importante deja a la mitad de esos servidores en mal estado, el sistema de comprobación de estado se sobrecargaría al intentar actualizar los sistemas de notificación y comunicar el estado a sus clientes. Por ello, el sistema de comprobación de estado debería enviar cada vez la instantánea completa del estado actual. 100 000 estados de servidor, cada uno representado por un bit, solo constituiría una carga de 12,5 KB. Si no hay errores en ningún servidor, o hay errores en todos ellos, el sistema de comprobación de estado estará haciendo un trabajo constante y los cambios rápidos de gran tamaño no pondrán en peligro la estabilidad del sistema. En realidad, así es como Amazon Route 53 gestiona las comprobaciones de estado de los puntos de conexión (como las direcciones IP) para determinar cómo se enruta a los usuarios finales.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: bajo

Guía para la implementación

- Trabaje constantemente para que los sistemas no tengan errores cuando haya cambios grandes y rápidos en la carga.
- Implemente dependencias con acoplamiento débil. Las dependencias, como los sistemas de colas, los sistemas de transmisión, los flujos de trabajo y los equilibradores de carga, tienen un

acoplamiento débil. El acoplamiento débil ayuda a aislar el comportamiento de un componente de otros componentes que dependen de él, lo que aumenta la resiliencia y la agilidad.

- Amazon Builders' Library: Reliability, constant work, and a good cup of coffee
- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small ARC337 (includes constant work)
  - En el ejemplo de una sistema de comprobación de estado que supervisa 100 000 servidores, diseñe las cargas de trabajo de forma que los tamaños de la carga útil sean iguales independientemente del número de éxitos o fracasos.

Recursos

Documentos relacionados:

- Amazon EC2: Ensuring Idempotency
- Amazon Builders' Library: Desafíos de los sistemas distribuidos
- Amazon Builders' Library: Reliability, constant work, and a good cup of coffee

Videos relacionados:

- AWS New York Summit 2019: Intro to Event-driven Architectures and Amazon EventBridge (MAD205)
- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small ARC337 (includes constant work)
- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small ARC337 (includes loose coupling, constant work, static stability)
- AWS re:Invent 2019: Moving to event-driven architectures (SVS308)

REL04-BP04 Cómo hacer idempotentes las operaciones de mutación

Un servicio idempotente promete que cada solicitud se procesará una y solo una vez, de tal forma que hacer varias solicitudes idénticas tiene el mismo efecto que hacer una sola solicitud. De este modo, un cliente lo tiene más fácil para implementar los reintentos sin la preocupación de que una solicitud se procese varias veces por error. Para ello, los clientes pueden emitir solicitudes de API con un token de idempotencia, que se utiliza siempre que se repite la solicitud. Una API de servicio

idempotente usa el token para devolver una respuesta idéntica a la que se devolvió por primera vez cuando se completó la solicitud, incluso aunque haya cambiado el estado subyacente del sistema.

En un sistema distribuido, es relativamente fácil llevar a cabo una acción una vez como máximo (el cliente solo hace una solicitud) o al menos una vez (sigue haciendo la solicitud hasta que el cliente obtiene una confirmación del éxito). Es más difícil garantizar que una acción se realice exactamente una vez, de modo que hacer varias solicitudes idénticas tenga el mismo efecto que llevar a cabo una sola solicitud. Con el uso de tokens de idempotencia en las API, los servicios pueden recibir una solicitud de migración una o más veces sin necesidad de crear registros duplicados ni efectos secundarios.

Resultado deseado: un enfoque coherente, bien documentado y ampliamente adoptado para garantizar la idempotencia de todos los componentes y servicios.

Patrones comunes de uso no recomendados:

- Aplica la idempotencia de forma indiscriminada, incluso cuando no es necesaria.
- Introduce una lógica demasiado compleja para implementar la idempotencia.
- Usa las marcas de tiempo como claves para la idempotencia. Esto puede provocar imprecisiones debido al sesgo de reloj o a que varios clientes utilicen las mismas marcas de tiempo para aplicar los cambios.
- Almacena cargas útiles completas para la idempotencia. Con este enfoque, se guardan las cargas útiles de datos completas de cada solicitud y se sobrescriben en cada nueva solicitud. Esto puede reducir el rendimiento y afectar a la escalabilidad.
- Genera claves de forma incoherente en todos los servicios. Sin claves coherentes, es posible que los servicios no reconozcan las solicitudes duplicadas, lo que se traduce en resultados imprevistos.

Beneficios de establecer esta práctica recomendada:

- Mayor escalabilidad: el sistema puede gestionar los reintentos y las solicitudes duplicadas sin tener que realizar una lógica adicional o una compleja gestión del estado.
- Fiabilidad mejorada: la idempotencia ayuda a los servicios a gestionar varias solicitudes idénticas de manera coherente, lo que reduce el riesgo de efectos secundarios no deseados o registros duplicados. Esto es especialmente importante en los sistemas distribuidos, donde se producen fallos de red y reintentos con frecuencia.

- Mejora de la coherencia de datos: dado que la misma solicitud produce la misma respuesta, la idempotencia ayuda a mantener la coherencia de datos en todos los sistemas distribuidos. Esto es esencial para mantener la integridad de las transacciones y las operaciones.
- Gestión de errores: los tokens de idempotencia simplifican la gestión de errores. Si un cliente no recibe una respuesta debido a un problema, puede reenviar la solicitud de forma segura con el mismo token de idempotencia.
- Transparencia operativa: la idempotencia permite una mejor supervisión y registro. Los servicios pueden registrar las solicitudes con sus tokens de idempotencia, lo que facilita el rastreo y la depuración de los problemas.
- Contrato de API simplificado: puede simplificar el contrato entre los sistemas del cliente y del servidor y reducir la preocupación por posibles errores en el procesamiento de los datos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

En un sistema distribuido, es relativamente fácil llevar a cabo una acción una vez como máximo (el cliente solo hace una solicitud) o al menos una vez (sigue haciendo la solicitud hasta que el cliente obtiene una confirmación del funcionamiento correcto). Sin embargo, es difícil implementar un comportamiento que se dé una sola vez. Para lograrlo, sus clientes deben generar y proporcionar un token de idempotencia para cada solicitud.

Mediante el uso de fichas de idempotencia, un servicio puede distinguir entre solicitudes nuevas y solicitudes repetidas. Cuando un servicio recibe una solicitud con un token de idempotencia, comprueba si el token ya se ha utilizado. Si se ha utilizado el token, el servicio recupera y devuelve la respuesta almacenada. Si el token es nuevo, el servicio procesa la solicitud, almacena la respuesta junto con el token y, a continuación, devuelve la respuesta. Este mecanismo hace que todas las respuestas sean idempotentes, lo que mejora la fiabilidad y la coherencia del sistema distribuido.

La idempotencia también es un comportamiento importante de las arquitecturas basadas en eventos. Estas arquitecturas suelen estar respaldadas por una cola de mensajes como Amazon SQS, Amazon MQ, Amazon Kinesis Streams o Amazon Managed Streaming para Apache Kafka (MSK). En algunas circunstancias, un mensaje que se ha publicado solo una vez puede entregarse accidentalmente más de una vez. Cuando un publicador genera e incluye símbolos de idempotencia en los mensajes, solicita que al procesar cualquier mensaje duplicado recibido no se repita ninguna acción para el mismo mensaje. Los consumidores deben llevar un registro de cada token recibido e ignorar los mensajes que contengan tokens duplicados.

Los servicios y los consumidores también deberían transferir el token de idempotencia recibido a cualquier servicio posterior al que este llame. Todos los servicios posteriores de la cadena de procesamiento son igualmente responsables de garantizar que la idempotencia se implemente para evitar el efecto secundario de procesar un mensaje más de una vez.

Pasos para la implementación

1. Identifique las operaciones idempotentes

   Determine qué operaciones requieren idempotencia. Por lo general, incluyen los métodos HTTP POST, PUT y DELETE y las operaciones de inserción, actualización o eliminación de bases de datos. Las operaciones que no cambian de estado, como las consultas de solo lectura, no suelen requerir idempotencia, a menos que tengan efectos secundarios.

2. Use identificadores únicos

   Incluye un token único en cada solicitud de operación idempotente que envíe el remitente, ya sea directamente en la solicitud o como parte de sus metadatos (por ejemplo, un encabezado HTTP). Esto permite al receptor reconocer y gestionar las solicitudes u operaciones duplicadas. Los identificadores que se utilizan habitualmente para los tokens incluyen los identificadores únicos universales (UUID) y los identificadores únicos clasificables por K (KSUID).

3. Rastree y gestione el estado

   Mantenga el estado de cada operación o solicitud de su carga de trabajo. Esto se puede lograr almacenando el token de idempotencia y el estado correspondiente (como pendiente, completado o fallido) en una base de datos, caché u otro almacén persistente. Esta información de estado permite a la carga de trabajo identificar y gestionar las solicitudes u operaciones duplicadas.

   Mantenga la coherencia y la atomicidad mediante el uso de los mecanismos de control de simultaneidad adecuados, si es necesario, como bloqueos, transacciones o controles de simultaneidad optimistas. Esto incluye el proceso de registrar el token idempotente y ejecutar todas las operaciones de mutación asociadas con la atención de la solicitud. Esto ayuda a prevenir las condiciones de carrera y verifica que las operaciones idempotentes se ejecuten correctamente.

   Elimine periódicamente los tokens de idempotencia antiguos del almacén de datos para gestionar el almacenamiento y el rendimiento. Si su sistema de almacenamiento lo admite, plantéese utilizar marcas de tiempo de caducidad para los datos (conocidas como tiempo de vida o valores TTL). La probabilidad de que se reutilicen los tokens de idempotencia disminuye con el tiempo.

Las opciones de almacenamiento de AWS más comunes que se suelen utilizar para almacenar los tokens de idempotencia y el estado relacionado incluyen:

- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL que proporciona un rendimiento de baja latencia y alta disponibilidad, lo que lo hace ideal para el almacenamiento de datos relacionados con la idempotencia. El modelo de datos de documentos y valores clave de DynamoDB permite almacenar y recuperar de forma eficiente los símbolos de idempotencia y la información de estado asociada. DynamoDB también puede hacer que los tokens de idempotencia caduquen automáticamente si la aplicación establece un valor TTL al insertarlos.
- Amazon ElastiCache: ElastiCache puede almacenar tokens de idempotencia con alto rendimiento, baja latencia y bajo coste. Tanto ElastiCache (Redis) como ElastiCache (Memcached) también pueden hacer que los tokens de idempotencia caduquen automáticamente si la aplicación establece un valor TTL al insertarlos.
- Amazon Relational Database Service (RDS): puede utilizar Amazon RDS para almacenar los tokens de idempotencia y la información de estado relacionada, especialmente si su aplicación ya utiliza una base de datos relacional para otros fines.
- Amazon Simple Storage Service (S3): Amazon S3 es un servicio de almacenamiento de objetos duradero y altamente escalable que se puede utilizar para almacenar tokens de idempotencia y metadatos relacionados. Las capacidades de control de versiones de S3 pueden resultar particularmente útiles para mantener el estado de las operaciones idempotentes. La elección del servicio de almacenamiento suele depender de factores como el volumen de datos relacionados con la idempotencia, las características de rendimiento requeridas, la necesidad de durabilidad y disponibilidad y la forma en que el mecanismo de idempotencia se integra en la arquitectura de la carga de trabajo general.

4. Implemente operaciones idempotentes

   Diseñe sus componentes de API y de carga de trabajo para que sean idempotentes. Incorpore controles de idempotencia en los componentes de su carga de trabajo. Antes de procesar una solicitud o realizar una operación, compruebe si el identificador único ya se ha procesado. Si es así, devuelva el resultado anterior en lugar de volver a ejecutar la operación. Por ejemplo, si un cliente envía una solicitud para crear un usuario, compruebe si ya existe un usuario con el mismo identificador único. Si el usuario existe, debería devolver la información del usuario existente en lugar de crear una nueva. Del mismo modo, si un consumidor de la cola recibe un mensaje con un token de idempotencia duplicado, debe ignorar el mensaje.

Cree conjuntos de pruebas integrales que validen la idempotencia de las solicitudes. Deben cubrir una amplia gama de escenarios, como las solicitudes correctas, las fallidas y las duplicadas.

Si su carga de trabajo aprovecha las funciones de AWS Lambda, puede usar Powertools para AWS Lambda. Powertools para AWS Lambda es un kit de herramientas para desarrolladores para implementar prácticas recomendadas sin servidor y aumentar la velocidad de los desarrolladores cuando trabaja con funciones de AWS Lambda. En concreto, proporciona una utilidad para convertir las funciones de Lambda en operaciones idempotentes que se pueden volver a intentar de forma segura.

5. Comunique la idempotencia con claridad

   Documente su API y los componentes de la carga de trabajo para comunicar claramente la naturaleza idempotente de las operaciones. Esto ayuda a los clientes a entender el comportamiento esperado y cómo interactuar con su carga de trabajo de forma fiable.

6. Monitoree y audite:

   Implemente mecanismos de supervisión y auditoría para detectar cualquier problema relacionado con la idempotencia de las respuestas, como las variaciones inesperadas de las respuestas o el exceso de gestión de solicitudes duplicadas. Esto puede ayudarlo a detectar e investigar cualquier problema o comportamiento inesperado en su carga de trabajo.

Recursos

Prácticas recomendadas relacionadas:

- REL05-BP03 Control y limitación de las llamadas de reintento
- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)
- REL08-BP02 Integración de las pruebas funcionales como parte de la implementación

Documentos relacionados:

- Amazon Builders' Library: Making retries safe with idempotent APIs
- Amazon Builders' Library: Desafíos de los sistemas distribuidos
- Amazon Builders' Library: Reliability, constant work, and a good cup of coffee

- Amazon Elastic Container Service: Ensuring idempotency
- ¿Cómo puedo hacer que mi función de Lambda sea idempotente?
- Ensuring idempotency in Amazon EC2 API requests

Videos relacionados:

- Building Distributed Applications with Event-driven Architecture. Charlas técnicas en línea de AWS
- AWS re:Invent 2023 - Building next-generation applications with event-driven architecture
- AWS re:Invent 2023 - Advanced integration patterns & trade-offs for loosely coupled systems
- AWS re:Invent 2023 - Advanced event-driven patterns with Amazon EventBridge
- AWS re:Invent 2018 - Close Loops and Opening Minds: How to Take Control of Systems, Big and Small ARC337 (includes loose coupling, constant work, static stability)
- AWS re:Invent 2019 - Moving to event-driven architectures (SVS308)

Herramientas relacionadas:

- Idempotencia con AWS Lambda Powertools (Java)
- Idempotencia con AWS Lambda Powertools (Python)
- Página de GitHub de AWS Lambda Powertools

Diseño de interacciones en un sistema distribuido para mitigar o tolerar errores

Los sistemas distribuidos dependen de las redes de comunicaciones para interconectar componentes, como servidores o servicios. Su carga de trabajo debe funcionar de manera fiable aunque se pierdan datos o haya latencia en estas redes. Los componentes del sistema distribuido deben funcionar de manera que no afecten negativamente a otros componentes o a la carga de trabajo. Estas prácticas recomendadas permiten que las cargas de trabajo toleren el estrés o los errores, se recuperen más rápidamente de ellos y mitiguen el impacto de dichos errores. El resultado es un tiempo medio de recuperación (MTTR) mejor.

Estas prácticas recomendadas previenen los fallos y mejoran el tiempo medio entre errores (MTBD).

Prácticas recomendadas

- REL05-BP01 Implementación de una degradación estable para transformar las dependencias estrictas en flexibles
- REL05-BP02 Limitación de las solicitudes
- REL05-BP03 Control y limitación de las llamadas de reintento
- REL05-BP04 Respuesta rápida a los errores y limitación de las colas
- REL05-BP05 Definición de los tiempos de espera del cliente
- REL05-BP06 Creación de sistemas sin estado cuando sea posible
- REL05-BP07 Implementación de recursos de emergencia

REL05-BP01 Implementación de una degradación estable para transformar las dependencias estrictas en flexibles

Los componentes de la aplicación deben seguir desempeñando su función principal incluso si las dependencias dejan de estar disponibles. Es posible que proporcionen datos ligeramente obsoletos, datos alternativos o incluso ningún dato. Esto garantiza que los errores localizados solo impidan lo mínimo del funcionamiento general del sistema y, al mismo tiempo, se obtenga el valor empresarial central.

Resultado deseado: cuando las dependencias de un componente no están en buen estado, el propio componente puede seguir funcionando, aunque con capacidad mermada. Los modos de errores de los componentes deben considerarse parte del funcionamiento normal. Los flujos de trabajo deben diseñarse de tal manera que dichos errores no produzcan un fallo total o, al menos, lleven a estados predecibles y recuperables.

Patrones comunes de uso no recomendados:

- No identificar la funcionalidad empresarial principal necesaria. No probar que los componentes funcionen, incluso durante los errores de dependencia.
- No proporcionar datos en caso de error o cuando solo una de las múltiples dependencias no está disponible y aún se pueden devolver resultados parciales.
- Crear un estado incoherente cuando una transacción falla parcialmente.
- No tener una forma alternativa de acceder a un almacén de parámetros central.
- Invalidar o vaciar un estado local como resultado de un fallo de actualización sin tener en cuenta las consecuencias.

Beneficios de establecer esta práctica recomendada: la degradación gradual mejora la disponibilidad del sistema en su conjunto y mantiene la funcionalidad de las funciones más importantes incluso cuando hay errores.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

La implementación de una degradación gradual ayuda a minimizar el impacto de los errores de dependencia en la función de los componentes. Lo ideal sería que un componente detectara los errores de dependencia y siguiese funcionando de una forma que afectara lo menos posible a otros componentes o clientes.

Diseñar una arquitectura que permita una degradación gradual implica considerar los posibles modos de errores durante el diseño de las dependencias. Para cada modo de error, disponga de una forma de ofrecer la mayoría o, al menos la funcionalidad más crítica del componente, a las personas que llaman o a los clientes. Estos factores pueden convertirse en requisitos adicionales que se pueden probar y verificar. Lo ideal es que un componente pueda desempeñar su función principal de manera aceptable incluso cuando falla una o varias dependencias.

Se trata tanto de una cuestión empresarial como técnica. Todos los requisitos empresariales son importantes y deben cumplirse si es posible. Sin embargo, es lógico preguntarse qué debe suceder cuando no se puedan cumplir todos. Se puede diseñar un sistema para que esté disponible y sea coherente, pero en circunstancias en las que haya que eliminar un requisito, ¿cuál es más importante? En el caso del procesamiento de pagos, puede ser la coherencia. En una aplicación en tiempo real, puede ser la disponibilidad. En el caso de un sitio web orientado al cliente, la respuesta dependería de las expectativas del cliente.

Lo que esto significa depende de los requisitos del componente y de lo que deba considerarse su función principal. Por ejemplo:

- Un sitio web de comercio electrónico podría mostrar en su página de inicio los datos de varios sistemas diferentes, como las recomendaciones personalizadas, los productos mejor clasificados y el estado de los pedidos de los clientes. Cuando un sistema anterior falla, sigue siendo lógico mostrar todo lo demás en lugar de mostrar una página de error al cliente.
- Un componente que lleva a cabo escrituras por lotes puede seguir procesando un lote si se produce un error en una de las operaciones individuales. Implementar un mecanismo de reintento debería ser sencillo. Para hacerlo, se puede devolver a la persona que llama información sobre

qué operaciones se han hecho correctamente, cuáles han fallado y por qué han fallado, o colocar las solicitudes que han fallado en una cola de mensajes fallidos para implementar reintentos asíncronos. También se debe registrar la información sobre las operaciones que han fallado.

- Un sistema que procese las transacciones debe verificar que se ejecuten todas o ninguna de las actualizaciones individuales. En el caso de las transacciones distribuidas, se puede usar el patrón Saga para revertir operaciones anteriores en caso de que falle una operación posterior de la misma transacción. En este caso, la función principal es mantener la coherencia.
- Los sistemas en los que el tiempo es crítico deberían contar con la capacidad de gestionar de manera oportuna las dependencias que no respondan. En estos casos, se puede utilizar el patrón del disyuntor. Cuando se agota el tiempo de espera de las respuestas de una dependencia, el sistema puede cambiar a un estado cerrado en el que no se hacen llamadas adicionales.
- Una aplicación puede leer parámetros de un almacén de parámetros. Puede resultar útil crear imágenes de contenedores con un conjunto predeterminado de parámetros y utilizarlos en caso de que ese almacén de parámetros no esté disponible.

Tenga en cuenta que las soluciones que se adopten en caso de fallo de un componente deben probarse y ser significativamente más sencillas que la solución principal. En general, se debe evitar el uso de estrategias alternativas.

Pasos para la implementación

Identifique las dependencias externas e internas. Considere qué tipos de errores pueden producirse en ellas. Piense en formas de minimizar el impacto negativo en los sistemas anteriores y posteriores y en los clientes durante esos errores.

A continuación, tenemos una lista de dependencias y la descripción de cómo degradar correctamente cuando fallan:

1. Errores parciales de dependencias: un componente puede hacer varias solicitudes a los sistemas posteriores, ya sean varias solicitudes a un sistema o una sola solicitud destinada a varios sistemas. En función del contexto empresarial, es posible que haya diferentes formas apropiadas de gestionar este problema (para obtener más información, consulte los ejemplos anteriores en la Guía de implementación).
2. Un sistema descendente no puede procesar las solicitudes debido a la alta carga: si las solicitudes a un sistema descendente fallan constantemente, no tiene sentido volver a intentarlo. Esto puede suponer una carga adicional para un sistema ya sobrecargado y dificultar la recuperación. Aquí se puede utilizar el patrón de disyuntor, que supervisa las llamadas que fallaron al enviarlas a un

sistema posterior. Si falla un gran número de llamadas, dejará de enviar más solicitudes al sistema posterior y solo permitirá ocasionalmente el paso de las llamadas para comprobar si el sistema posterior vuelve a estar disponible.

3. Un almacén de parámetros no está disponible: para transformar un almacén de parámetros, se puede utilizar el almacenamiento en caché de dependencia flexible o los valores predeterminados en buen estado que se incluyen en las imágenes de contenedores o máquinas. Tenga en cuenta que estos valores predeterminados deben mantenerse actualizados e incluirse en los conjuntos de pruebas.
4. Un servicio de supervisión u otra dependencia no funcional no está disponible: si un componente no puede enviar registros, métricas o rastros de forma intermitente a un servicio de monitorización central, suele ser mejor seguir ejecutando las funciones empresariales como de costumbre. No registrar ni subir métricas de forma silenciosa durante mucho tiempo no suele ser aceptable. Además, algunos casos de uso pueden requerir entradas de auditoría completas para satisfacer los requisitos de cumplimiento.
5. Es posible que una instancia principal de una base de datos relacional no esté disponible: Amazon Relational Database Service, como casi todas las bases de datos relacionales, solo puede tener una instancia de escritura principal. Esto crea un único punto de error para las cargas de trabajo de escritura y dificulta el escalamiento. Este problema se puede mitigar parcialmente mediante el uso de una configuración Multi-AZ para lograr alta disponibilidad o de Amazon Aurora sin servidor para mejorar el escalado. Cuando los requisitos de disponibilidad son muy altos, podría ser conveniente no utilizar en absoluto el escritor principal. Para consultas de solo lectura, se pueden utilizar réplicas de lectura, que proporcionan redundancia y capacidad de escalado horizontal, no solo vertical. Las escrituras se pueden almacenar en búfer, por ejemplo, en una cola de Amazon Simple Queue Service, de modo que las solicitudes de escritura de los clientes puedan seguir aceptándose incluso si la principal no está disponible temporalmente.

Recursos

Documentos relacionados:

- Amazon API Gateway: Throttle API Requests for Better Throughput
- CircuitBreaker (summarizes Circuit Breaker from “Release It!” book)
- Error Retries and Exponential Backoff in AWS
- Michael Nygard “Release It! Design and Deploy Production-Ready Software”
- Amazon Builders' Library: Evitar los planes alternativos en los sistemas distribuidos

- Amazon Builders' Library: Cómo evitar demoras de colas insuperables
- Amazon Builders' Library: Desafíos y estrategias del almacenamiento en caché
- Amazon Builders' Library: Tiempos de espera, reintentos y retardo con fluctuación

Videos relacionados:

- Retry, backoff, and jitter: AWS re:Invent 2019: Introducing The Amazon Builders' Library (DOP328)

REL05-BP02 Limitación de las solicitudes

Limite las solicitudes para mitigar el agotamiento de los recursos debido a aumentos inesperados de la demanda. Las solicitudes por debajo de los índices de limitación se procesan, pero las que superan el límite definido se rechazan y se envía un mensaje que indica que la solicitud no se ha procesado a causa de la limitación.

Resultado deseado: la limitación de las solicitudes mitiga los grandes picos de volumen, ya sea debido a un aumento repentino del tráfico de clientes, a ataques por desbordamiento o a tormentas de reintentos, lo que permite que las cargas de trabajo sigan procesando de manera normal el volumen de solicitudes admitido.

Patrones comunes de uso no recomendados:

- Las limitaciones de puntos de conexión de la API no se implementan o se mantienen en los valores predeterminados sin tener en cuenta los volúmenes esperados.
- Los puntos de conexión de la API no se someten a pruebas de carga ni se prueban las limitaciones.
- Los índices de solicitudes se limitan sin tener en cuenta el tamaño o la complejidad de las solicitudes.
- Los índices o el tamaño máximos de las solicitudes se prueban, pero por separado.
- Los recursos no se aprovisionan con los mismos límites establecidos en las pruebas.
- No se han configurado ni considerado planes de uso para los consumidores de API de aplicación a aplicación (A2A).
- Los consumidores de cola que escalan horizontalmente no tienen configurado un valor máximo de simultaneidad.
- No se ha implementado la limitación de índices por dirección IP.

Beneficios de establecer esta práctica recomendada: las cargas de trabajo que establecen límites pueden funcionar con normalidad y procesar correctamente la carga de solicitudes aceptada en caso de que se produzcan picos de volumen inesperados. Los picos repentinos o sostenidos de solicitudes a las API y las colas se limitan y no agotan los recursos de procesamiento de solicitudes. Hay límites de índices que limitan a solicitantes individuales para que un gran volumen de tráfico desde una sola dirección IP o un único consumidor de API no agote los recursos y afecte a otros consumidores.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Los servicios deben diseñarse para procesar una capacidad de solicitudes conocida; esta capacidad se puede establecer mediante pruebas de carga. Si los índices de llegada de solicitudes superan los límites, se emite la respuesta correspondiente que indica que la solicitud no se ha procesado a causa de las limitaciones. Esto permite al consumidor gestionar el error y volver a intentarlo más tarde.

Cuando su servicio requiera la implementación de limitaciones, considere la posibilidad de implementar el algoritmo del bucket de tokens, en el que un token se refiere a una solicitud. Los tokens se recargan a un índice de limitación por segundo y se vacían de forma asíncrona a un ritmo de un token por solicitud.

El algoritmo del bucket de tokens.

Amazon API Gateway implementa el algoritmo del bucket de tokens de acuerdo con los límites de la cuenta y la región, y se puede configurar por cliente con planes de uso. Además, Amazon Simple Queue Service (Amazon SQS) y Amazon Kinesis pueden almacenar las solicitudes en búfer para

reducir la tasa de solicitudes y permitir tasas de limitación más altas para las solicitudes que se pueden atender. Por último, puede implementar una limitación de velocidad con AWS WAF para limitar los consumidores de API específicos que generan una carga inusualmente alta.

Pasos para la implementación

Puede configurar API Gateway con límites de limitación para sus API y devolver errores `429 Too Many Requests` cuando se superen los límites. Puede utilizar AWS WAF con sus puntos de conexión de AWS AppSync y API Gateway para habilitar la limitación de índices por dirección IP. Además, si su sistema tolera el procesamiento asíncrono, puede colocar los mensajes en una cola o secuencia para acelerar las respuestas a los clientes del servicio, lo que le permite ampliar los índices de limitación más altos.

Con el procesamiento asíncrono, cuando haya configurado Amazon SQS como origen de eventos de AWS Lambda, podrá configurar la máxima simultaneidad para evitar que las altas tasas de eventos consuman la cuota de ejecución simultánea de la cuenta disponible necesaria para otros servicios de su carga de trabajo o cuenta.

Si bien API Gateway proporciona una implementación administrada del bucket de tokens, en los casos en que no pueda usar API Gateway, puede utilizar las implementaciones de código abierto específicas de cada lenguaje (consulte los ejemplos relacionados en Recursos) del bucket de tokens para sus servicios.

- Comprenda y configure los límites de limitación de API Gateway en la cuenta por región, API por etapa y clave de API por nivel de plan de uso.
- Aplique reglas de limitación de tasas de AWS WAF a API Gateway y a los puntos de conexión de AWS AppSync para protegerse contra las inundaciones y bloquear las IP maliciosas. Las reglas de limitación de índices también se pueden configurar en las claves de API de AWS AppSync para los consumidores de A2A.
- Analice si necesita un control de limitación superior a la limitación de índices para las API de AWS AppSync y, de ser así, configure una API Gateway enfrente de su punto de conexión de AWS AppSync.
- Cuando las colas de Amazon SQS se configuran como activadores para los consumidores de colas de Lambda, defina la simultaneidad máxima en un valor que procese lo suficiente como para cumplir sus objetivos de nivel de servicio, pero que no consuma los límites de simultaneidad que afecten a otras funciones de Lambda. Considere la posibilidad de configurar la simultaneidad reservada en otras funciones de Lambda de la misma cuenta y región cuando consuma colas con Lambda.

- Utilice API Gateway con integraciones de servicios nativos para Amazon SQS o Kinesis para almacenar en búfer las solicitudes.
- Si no puede utilizar API Gateway, consulte las bibliotecas específicas del lenguaje para implementar el algoritmo del bucket de tokens para su carga de trabajo. Consulte la sección de ejemplos e investigue por su cuenta para encontrar una biblioteca adecuada.
- Pruebe los límites que tiene pensado establecer o que va a permitir que se aumenten, y documente los límites probados.
- No aumente los límites por encima de lo que establezca en las pruebas. Cuando aumente un límite, antes de aplicar ese aumento, compruebe que los recursos aprovisionados sean equivalentes o superiores a los de las situaciones de prueba.

Recursos

Prácticas recomendadas relacionadas:

- REL04-BP03 Trabajo constante
- REL05-BP03 Control y limitación de las llamadas de reintento

Documentos relacionados:

- Amazon API Gateway: Throttle API Requests for Better Throughput
- AWS WAF: Rate-based rule statement
- Introducing maximum concurrency of AWS Lambda when using Amazon SQS as an event source
- AWS Lambda: Maximum Concurrency

Ejemplos relacionados:

- The three most important AWS WAF rate-based rules
- Java Bucket4j
- Python token-bucket
- Node token-bucket
- .NET System Threading Rate Limiting

Videos relacionados:

- Implementing GraphQL API security best practices with AWS AppSync

Herramientas relacionadas:

- Amazon API Gateway
- AWS AppSync
- Amazon SQS
- Amazon Kinesis
- AWS WAF
- Sala de espera virtual en AWS

REL05-BP03 Control y limitación de las llamadas de reintento

Utilice un retroceso exponencial para reintentar las solicitudes a intervalos progresivamente más largos entre cada reintento. Introduzca una fluctuación entre reintentos para aleatorizar los intervalos de reintentos. Limite el número máximo de reintentos.

Resultado deseado: entre los componentes típicos de un sistema de software distribuido se incluyen servidores, equilibradores de carga, bases de datos y servidores DNS. Durante el funcionamiento normal, estos componentes pueden responder a las solicitudes con errores temporales o limitados, y también con errores que serían persistentes independientemente de los reintentos. Cuando los clientes hacen solicitudes a los servicios, esas solicitudes consumen recursos, como memoria, subprocesos, conexiones, puertos o cualquier otro recurso limitado. Controlar y limitar los reintentos es una estrategia para liberar y minimizar el consumo de recursos, de modo que los componentes del sistema sometidos a presión no se sobrecarguen.

Cuando se agota el tiempo de espera de las solicitudes del cliente o se reciben respuestas de error, deben determinar si deben volver a intentarlo o no. Si lo vuelven a intentar, lo hacen con un retroceso exponencial con fluctuaciones y un valor de reintento máximo. Como resultado, los servicios y procesos de backend tienen menos carga y más tiempo para recuperarse automáticamente, lo que se traduce en una recuperación más rápida y una tramitación satisfactoria de las solicitudes.

Patrones comunes de uso no recomendados:

- Implementar los reintentos sin agregar valores de retroceso exponencial, fluctuación y reintentos máximos. El retroceso y la fluctuación ayudan a evitar picos de tráfico artificiales debidos a reintentos coordinados involuntariamente a intervalos comunes.

- Implementar reintentos sin probar sus efectos o asumir que los reintentos ya están integrados en un SDK sin probar los escenarios de reintento.
- No entender los códigos de error publicados de las dependencias, lo que lleva a volver a intentar todos los errores, incluidos los que tienen una causa clara que indica una falta de permisos, un error de configuración u otro problema que es de esperar que no se pueda resolver sin una intervención manual.
- No utilizar prácticas de observabilidad, como supervisión y alertas en caso de errores de servicio repetidos, para conocer problemas subyacentes y poder solucionarlos.
- Desarrollar mecanismos de reintento personalizados cuando son suficientes las capacidades de reintento integradas o de terceros.
- Reintentar en varias capas de la pila de aplicaciones de una forma que se acumulen, lo que consume aún más recursos en una tormenta de reintentos. Asegúrese de entender cómo afectan estos errores a las dependencias en las que se basa y, a continuación, implemente los reintentos en un solo nivel.
- Reintentar llamadas de servicio que no son idempotentes, lo que provoca efectos secundarios inesperados, como resultados duplicados.

Beneficios de establecer esta práctica recomendada: los reintentos ayudan a los clientes a obtener los resultados deseados cuando las solicitudes fallan, pero también consumen más tiempo del servidor para obtener las respuestas satisfactorias que desean. Cuando los errores son poco frecuentes o transitorios, los reintentos funcionan bien. Cuando los errores se deben a una sobrecarga de recursos, los reintentos pueden empeorar las cosas. Agregar un retroceso exponencial con fluctuaciones para los reintentos de los clientes permite que los servidores se recuperen cuando los errores se deben a una sobrecarga de recursos. La fluctuación evita que haya picos de solicitudes y el retroceso disminuye el escalamiento de la carga provocado por la adición de reintentos a la carga normal de solicitudes. Por último, es importante configurar un número de reintentos máximo o un tiempo transcurrido máximo para evitar que se acumulen tareas pendientes que generen errores metaestables.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Controle y limite las llamadas de reintento. Use el retroceso exponencial para los reintentos tras intervalos cada vez más largos. Introduzca una fluctuación para aleatorizar los intervalos de reintento y limite el número máximo de reintentos.

Algunos AWS SDK implementan los reintentos y el retroceso exponencial de forma predeterminada. Utilice estas implementaciones de AWS integradas cuando corresponda en su carga de trabajo. Implemente una lógica similar en su carga de trabajo cuando llame a servicios que sean idempotentes y en los que los reintentos mejoren la disponibilidad de sus clientes. Decida cuáles son los tiempos de espera y cuándo dejar de reintentar según su caso de uso. Cree y ejecute situaciones de prueba para esos casos de uso de reintentos.

Pasos para la implementación

- Determine la capa óptima de la pila de aplicaciones para implementar los reintentos de los servicios de los que depende su aplicación.
- Tenga en cuenta que los SDK existentes implementan estrategias de reintento probadas con retroceso exponencial y fluctuaciones para el lenguaje que elija, y dé preferencia a estas estrategias en lugar de escribir sus propias implementaciones de reintentos.
- Verifique que los servicios sean idempotentes antes de implementar los reintentos. Una vez implementados, asegúrese de que se prueben y se utilicen regularmente en producción.
- Al llamar a las API del servicio de AWS, utilice los AWS SDK y AWS CLI y comprenda las opciones de configuración de reintentos. Determine si los valores predeterminados funcionan para su caso de uso, pruébelos y ajústelos según sea necesario.

Recursos

Prácticas recomendadas relacionadas:

- REL04-BP04 Cómo hacer idempotentes las operaciones de mutación
- REL05-BP02 Limitación de las solicitudes
- REL05-BP04 Respuesta rápida a los errores y limitación de las colas
- REL05-BP05 Definición de los tiempos de espera del cliente
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores

Documentos relacionados:

- Error Retries and Exponential Backoff in AWS
- Amazon Builders' Library: Tiempos de espera, reintentos y retardo con fluctuación
- Exponential Backoff and Jitter

- Making retries safe with idempotent APIs

Ejemplos relacionados:

- Spring Retry
- Resilience4j Retry

Videos relacionados:

- Retry, backoff, and jitter: AWS re:Invent 2019: Introducing The Amazon Builders' Library (DOP328)

Herramientas relacionadas:

- AWS SDKs and Tools: Retry behavior
- AWS Command Line Interface: Reintentos de AWS CLI

REL05-BP04 Respuesta rápida a los errores y limitación de las colas

Cuando un servicio no pueda responder correctamente a una solicitud, responda rápido a los errores. Esto permite que se liberen los recursos asociados a una solicitud y que un servicio se recupere cuando se le agotan los recursos. La respuesta rápida a los errores es un patrón de diseño de software bien establecido que se puede utilizar para conseguir cargas de trabajo enormemente fiables en la nube. Las colas también son un patrón de integración empresarial bien establecido que puede suavizar la carga y permitir a los clientes liberar recursos cuando se pueda tolerar el procesamiento asíncrono. Cuando un servicio puede responder correctamente en condiciones normales, pero falla cuando el índice de solicitudes es demasiado alto, utilice una cola para almacenar en búfer las solicitudes. Sin embargo, no permita que se acumulen largas colas de tareas pendientes, ya que eso podría hacer que se procesaran solicitudes obsoletas a las que un cliente ya ha renunciado.

Resultado deseado: cuando los sistemas sufren contención de recursos, tiempos de espera, excepciones o errores grises que hacen que los objetivos de nivel de servicio sean inalcanzables, las estrategias de respuesta rápida a los errores permiten recuperar el sistema más rápido. Los sistemas que deben absorber los picos de tráfico y pueden adaptarse al procesamiento asíncrono pueden mejorar la fiabilidad al permitir a los clientes liberar rápidamente las solicitudes mediante el uso de colas para almacenar en búfer las solicitudes a los servicios de backend. Cuando las solicitudes a

las colas se almacenan en búfer, se implementan estrategias de administración de colas para evitar retrasos insuperables.

Patrones comunes de uso no recomendados:

- Implementar colas de mensajes, pero no configurar colas de mensajes fallidos (DLQ) ni alarmas en los volúmenes de DLQ para detectar cuándo está fallando un sistema.
- No medir la antigüedad de los mensajes de una cola, que es una medida de la latencia para saber cuándo los usuarios de la cola sufren retrasos o producen errores que dan lugar a reintentos.
- No borrar los mensajes pendientes de una cola cuando no sirve de nada procesar esos mensajes si la empresa ya no necesita hacerlo.
- Configurar colas de primero en entrar/primero en salir (FIFO) cuando las colas de último en entrar, primero en salir (LIFO) responderían mejor a las necesidades de los clientes, por ejemplo, cuando no se requieren pedidos estrictos y el procesamiento pendiente retrasa todas las solicitudes nuevas y urgentes, lo que hace que se infrinjan los niveles de servicio de todos los clientes.
- Exponer las colas internas a los clientes en lugar de exponer las API que administran la entrada de trabajo y colocan las solicitudes en colas internas.
- Combinar demasiados tipos de solicitudes de trabajo en una sola cola puede agravar las condiciones de las tareas pendientes al distribuir la demanda de recursos entre los tipos de solicitudes.
- Procesar solicitudes complejas y simples en la misma cola, a pesar de necesitar diferentes niveles de supervisión, tiempos de espera y asignaciones de recursos.
- No validar las entradas ni utilizar afirmaciones para implementar mecanismos de respuesta rápida a los errores en el software que envíen las excepciones a componentes de nivel superior que puedan gestionar los errores con facilidad.
- No eliminar los recursos que fallan del enrutamiento de solicitudes, especialmente cuando los errores grises emiten tanto éxitos como errores debido a bloqueos y reinicios, errores de dependencia intermitentes, una reducción de la capacidad o la pérdida de paquetes de red.

Beneficios de establecer esta práctica recomendada: los sistemas que responden rápido a los errores son más fáciles de depurar y corregir y, a menudo, revelan problemas de codificación y configuración antes de que las versiones se publiquen en producción. Los sistemas que incorporan estrategias de puesta en cola eficaces tienen una mayor resiliencia y fiabilidad a los picos de tráfico y a las condiciones de errores intermitentes del sistema.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las estrategias de respuesta rápida a los errores pueden codificarse en soluciones de software y también configurarse en la infraestructura. Además de la respuesta rápida a los errores, las colas son una técnica arquitectónica sencilla, pero potente, para desacoplar los componentes del sistema sin problemas de carga. Amazon CloudWatch proporciona capacidades para supervisar los errores y alertar en caso de que existan. Una vez que se sabe que un sistema está fallando, se pueden invocar estrategias de mitigación, como el alejamiento de los recursos deteriorados. Cuando los sistemas implementan colas con Amazon SQS y otras tecnologías de cola para facilitar la carga, deben considerar cómo administrar los atrasos en las colas, así como los errores en el consumo de mensajes.

Pasos para la implementación

- Implemente afirmaciones programáticas o métricas específicas en su software y utilícelas para alertar explícitamente sobre problemas del sistema. Amazon CloudWatch le ayuda a crear métricas y alarmas basadas en el patrón de registro de la aplicación y la instrumentación del SDK.
- Utilice métricas y alarmas de CloudWatch para alejarse de los recursos deteriorados que aumentan la latencia del procesamiento o que no procesan las solicitudes de forma reiterada.
- Utilice el procesamiento asíncrono diseñando API que acepten solicitudes y las anexen a las colas internas mediante Amazon SQS y, a continuación, respondan al cliente que produce los mensajes con un mensaje de éxito, de modo que el cliente pueda liberar recursos y continuar con otras tareas mientras los consumidores de la cola del backend procesan las solicitudes.
- Para medir y supervisar la latencia de procesamiento de las colas, genere una métrica de CloudWatch cada vez que se retire un mensaje de una cola mediante la comparación en ese momento con la marca de tiempo del mensaje.
- Cuando los errores impidan procesar correctamente los mensajes o los picos de tráfico en los volúmenes que no se pueden procesar dentro de los acuerdos de nivel de servicio, aparte el tráfico antiguo o excesivo y colóquelo en una cola secundaria. Esto permite procesar de forma prioritaria los trabajos nuevos y dejar los antiguos para cuando haya capacidad disponible. Esta técnica es una aproximación al procesamiento LIFO y permite que el sistema procese normalmente todos los trabajos nuevos.
- Utilice colas de mensajes fallidos o redireccione las colas para sacar de la lista de espera los mensajes que no se puedan procesar y colocarlos en una ubicación que pueda investigarse y resolverse más adelante

- Vuelva a intentarlo o, cuando sea tolerable, elimine los mensajes antiguos. Para ello, compárelos en ese momento con la marca de tiempo del mensaje y descarte los mensajes que ya no sean pertinentes para el cliente que los ha solicitado.

Recursos

Prácticas recomendadas relacionadas:

- REL04-BP02 Implementación de dependencias con acoplamiento débil
- REL05-BP02 Limitación de las solicitudes
- REL05-BP03 Control y limitación de las llamadas de reintento
- REL06-BP02 Definición y cálculo de métricas (agregación)
- REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema

Documentos relacionados:

- Cómo evitar demoras de colas insuperables
- Fail Fast
- ¿Cómo puedo evitar que se acumulen mensajes en mi cola de Amazon SQS?
- Elastic Load Balancing: Zonal Shift
- Amazon Application Recovery Controller: Routing control for traffic failover

Ejemplos relacionados:

- Enterprise Integration Patterns: Dead Letter Channel

Videos relacionados:

- AWS re:Invent 2022 - Operating highly available Multi-AZ applications

Herramientas relacionadas:

- Amazon SQS
- Amazon MQ
- AWS IoT Core

- Amazon CloudWatch

REL05-BP05 Definición de los tiempos de espera del cliente

Defina tiempos de espera adecuados para las conexiones y las solicitudes, verifíquelos sistemáticamente y no use los valores predeterminados, ya que no tienen en cuenta las características específicas de la carga de trabajo.

Resultado deseado: en los tiempos de espera de los clientes, se debe tener en cuenta el costo para el cliente, el servidor y la carga de trabajo asociados a la espera de las solicitudes que tardan un tiempo anormal en completarse. Dado que no es posible conocer la causa exacta de ningún tiempo de espera, los clientes deben utilizar el conocimiento de los servicios para fijar expectativas sobre las causas probables y los tiempos de espera adecuados

El tiempo de espera de las conexiones del cliente se agota en función de los valores configurados. Cuando el tiempo de espera se agota, los clientes toman la decisión de dar marcha atrás y volver a intentarlo o abrir un disyuntor. Estos patrones evitan que se emitan solicitudes que puedan agravar una condición de error subyacente.

Patrones comunes de uso no recomendados:

- No estar al tanto de los tiempos de espera del sistema o de los tiempos de espera predeterminados.
- No estar al tanto del tiempo normal de finalización de las solicitudes.
- No conocer las posibles causas por las que las solicitudes tardan un tiempo anormalmente largo en completarse ni los costos para el rendimiento del cliente, el servicio o la carga de trabajo asociados a la espera a que se completen.
- No conocer la probabilidad de que la red deteriorada haga que una solicitud falle solo una vez que se haya agotado el tiempo de espera, ni de los costos que supone para el rendimiento del cliente y la carga de trabajo no utilizar un tiempo de espera más corto.
- No probar escenarios de tiempo de espera tanto para las conexiones como para las solicitudes.
- Definir tiempos de espera demasiado altos, lo que puede provocar tiempos de espera prolongados y aumentar el uso de los recursos.
- Definir tiempos de espera demasiado bajos, lo que provoca errores artificiales.
- Pasar por alto los patrones para solucionar los errores de tiempo de espera de las llamadas remotas, como disyuntores y reintentos.

- No considerar la posibilidad de supervisar los índices de errores de las llamadas de servicio, los objetivos de nivel de servicio referentes a la latencia y los valores atípicos de latencia. Estas métricas pueden proporcionar información sobre tiempos de espera agresivos o permisivos

Beneficios de establecer esta práctica recomendada: los tiempos de espera de las llamadas remotas están configurados y los sistemas están diseñados para gestionar los tiempos de espera correctamente, de modo que los recursos se conserven cuando las llamadas remotas responden con una lentitud anormal y los clientes del servicio gestionan correctamente los errores de tiempo de espera.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Defina un tiempo de espera de conexión y un tiempo de espera de solicitud en cualquier llamada de dependencia del servicio y, normalmente, en todas las llamadas de los procesos. Muchos marcos integran capacidades de tiempo de espera, pero tenga cuidado, ya que algunos tienen valores predeterminados que son infinitos o superiores a lo aceptable para sus objetivos de servicio. Un valor demasiado alto reduce la utilidad del tiempo de espera porque se siguen consumiendo recursos mientras el cliente espera a que transcurra el tiempo de espera. Un valor demasiado bajo puede generar un aumento del tráfico en el backend y un aumento de la latencia debido a que las solicitudes hacen demasiados reintentos. En algunos casos, esto puede producir una interrupción completa si se reintentan todas las solicitudes.

Tenga en cuenta lo siguiente al determinar las estrategias de tiempo de espera:

- Las solicitudes pueden tardar más de lo normal en procesarse debido a su contenido, a deficiencias en un servicio de destino o a un error en la partición de la red.
- Las solicitudes con contenido anormalmente caro podrían consumir recursos innecesarios del servidor y del cliente. En este caso, si se agota el tiempo de espera de estas solicitudes y no se vuelven a intentar, se pueden conservar los recursos. Los servicios también deberían protegerse del contenido anormalmente caro con restricciones y tiempos de espera del lado del servidor.
- Se puede agotar el tiempo de espera y volver a intentar las solicitudes que tarden un tiempo anormalmente largo debido a una interrupción del servicio. Se deben tener en cuenta los costos del servicio de la solicitud y el reintento, pero si la causa es una deficiencia localizada, es probable que el reintento no sea caro y reduzca el consumo de recursos del cliente. El tiempo de espera también puede liberar recursos del servidor según la naturaleza de la deficiencia.

- Se puede agotar el tiempo de espera y volver a intentar las solicitudes que tarden mucho en completarse porque la red no ha podido entregar la solicitud o la respuesta. Como la solicitud o la respuesta no se han entregado, el resultado habría sido un error independientemente del tiempo de espera. En este caso, el tiempo de espera no liberará los recursos del servidor, pero sí liberará los recursos del cliente y mejorará el rendimiento de la carga de trabajo.

Aproveche patrones de diseño bien establecidos, como los reintentos y los disyuntores, para gestionar los tiempos de espera correctamente y ofrecer enfoques de respuesta rápida a los errores. AWS Los SDK y AWS CLI permiten configurar los tiempos de espera de conexión y solicitud y los reintentos con retrocesos y fluctuaciones exponenciales. Las funciones de AWS Lambda permiten configurar los tiempos de espera y, con AWS Step Functions, se pueden crear disyuntores con poco código que aprovechen las integraciones predefinidas con servicios de AWS y SDK. AWS App Mesh Envoy incluye capacidades de tiempo de espera y de disyuntor.

Pasos para la implementación

- Configure tiempos de espera en las llamadas de servicio remotas y aproveche las características integradas de tiempo de espera del lenguaje o las bibliotecas de tiempo de espera de código abierto.
- Cuando su carga de trabajo haga llamadas con un AWS SDK, consulte la documentación para ver la configuración del tiempo de espera específica de cada lenguaje.
  - Python
  - PHP
  - .NET
  - Ruby
  - Java
  - Go
  - Node.js
  - C++
- Cuando utilice AWS SDK o comandos de la AWS CLI en su carga de trabajo, defina los valores predeterminados de tiempo de espera mediante la configuración de los valores predeterminados de configuración de AWS para `connectTimeoutInMillis` y `tlsNegotiationTimeoutInMillis`.
- Aplique las opciones de línea de comandos `cli-connect-timeout` y `cli-read-timeout` para controlar comandos únicos de la AWS CLI para los servicios de AWS.

- Supervise las llamadas de servicio remotas para comprobar si hay tiempos de espera y configure alarmas en caso de errores persistentes para poder gestionar los escenarios de error de forma proactiva.
- Implemente métricas de CloudWatch y la detección de anomalías de CloudWatch en los índices de error de las llamadas, los objetivos de nivel de servicio en lo que se refiere a la latencia y los valores atípicos de latencia para proporcionar información sobre la administración de tiempos de espera demasiado agresivos o permisivos.
- Configure los tiempos de espera en las funciones de Lambda.
- Los clientes de API Gateway deben implementar sus propios reintentos al gestionar los tiempos de espera. API Gateway admite un tiempo de espera de integración de 50 milisegundos a 29 segundos para las integraciones posteriores y no lo vuelve a intentar cuando la integración solicita el tiempo de espera.
- Implemente el patrón de disyuntor para que no se hagan llamadas remotas cuando se agote el tiempo de espera. Abra el circuito para evitar llamadas fallidas y ciérrelo cuando las llamadas respondan con normalidad.
- Para las cargas de trabajo basadas en contenedores, consulte las funciones de App Mesh Envoy para aprovechar los tiempos de espera y los disyuntores integrados.
- Utilice AWS Step Functions para crear disyuntores de poco código para las llamadas de servicio remotas, especialmente cuando se utilizan AWS SDK nativos e integraciones de Step Functions compatibles para simplificar la carga de trabajo.

Recursos

Prácticas recomendadas relacionadas:

- REL05-BP03 Control y limitación de las llamadas de reintento
- REL05-BP04 Respuesta rápida a los errores y limitación de las colas
- REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema

Documentos relacionados:

- AWS SDK: Retries and Timeouts
- Amazon Builders' Library: Tiempos de espera, reintentos y retardo con fluctuación
- Cuotas de Amazon API Gateway y notas importantes
- AWS Command Line Interface: Command line options

- AWS SDK for Java 2.x: Configure API Timeouts
- AWS Botocore using the config object and Config Reference
- AWS SDK para .NET: Retries and Timeouts
- AWS Lambda: Configuración de funciones de Lambda

Ejemplos relacionados:

- Using the circuit breaker pattern with AWS Step Functions and Amazon DynamoDB
- Martin Fowler: CircuitBreaker

Herramientas relacionadas:

- AWS SDK
- AWS Lambda
- Amazon SQS
- AWS Step Functions
- AWS Command Line Interface

REL05-BP06 Creación de sistemas sin estado cuando sea posible

Los sistemas deben o bien no requerir estado o bien descargar el estado, de forma que entre solicitudes de clientes distintos no haya dependencia en los datos almacenados localmente en disco y en memoria. Esto permite reemplazar los servidores a voluntad sin que la disponibilidad resulte afectada.

Cuando los usuarios o los servicios interactúan con una aplicación, suelen llevar a cabo una serie de interacciones que constituyen una sesión. Una sesión es un dato único para los usuarios que persiste entre las solicitudes mientras utilizan la aplicación. Una aplicación sin estado es aquella que no necesita conocer las interacciones anteriores y no almacena la información de la sesión.

Una vez se ha diseñado para no tener estado, puede utilizar servicios de computación sin servidor, como AWS Lambda o AWS Fargate.

Además del reemplazo del servidor, otro beneficio de las aplicaciones sin estado es que pueden escalar horizontalmente porque cualquiera de los recursos de computación disponibles (como las instancias de EC2 y las funciones de AWS Lambda) puede dar servicio a cualquier solicitud.

Beneficios de establecer esta práctica recomendada: los sistemas que se han diseñado para no tener estado se adaptan mejor al escalado horizontal, lo que permite agregar o eliminar capacidad en función de la fluctuación del tráfico y la demanda. También son intrínsecamente resistentes a los errores y proporcionan flexibilidad y agilidad en el desarrollo de aplicaciones.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Cree aplicaciones sin estado. Las aplicaciones sin estado permiten el escalado horizontal y toleran el error de un nodo individual. Analice y comprenda los componentes de la aplicación que mantienen el estado dentro de la arquitectura. Esto le ayuda a evaluar el posible impacto de la transición a un diseño sin estado. Una arquitectura sin estado desacopla los datos del usuario y descarga los datos de la sesión. Esto proporciona la flexibilidad para escalar cada componente de forma independiente para cumplir con las diferentes demandas de carga de trabajo y optimizar el uso de los recursos.

Pasos para la implementación

- Identifique y comprenda los componentes con estado de la aplicación.
- Para desacoplar los datos, separe y administre los datos de usuario de la lógica principal de la aplicación.
  - Amazon Cognito puede desacoplar los datos de usuario del código de la aplicación mediante características, tales como grupos de identidades, grupos de usuarios y Amazon Cognito Sync.
  - Para usar AWS Secrets Manager a fin de desacoplar los datos de usuario, almacene los secretos en una ubicación segura y centralizada. Esto significa que el código de la aplicación no necesita almacenar secretos, lo que la hace más segura.
  - Plantéese utilizar Amazon S3 para almacenar datos no estructurados y de gran volumen, como imágenes y documentos. La aplicación puede recuperar estos datos cuando sea necesario, lo que elimina la necesidad de almacenarlos en la memoria.
  - Utilice Amazon DynamoDB para almacenar información, como, por ejemplo, perfiles de usuario. La aplicación puede consultar estos datos prácticamente en tiempo real.
- Descargue los datos de la sesión en una base de datos, caché o archivos externos.
  - Amazon ElastiCache, Amazon DynamoDB, Amazon Elastic File System (Amazon EFS) y Amazon MemoryDB son ejemplos de servicios de AWS que puede usar para descargar datos de sesión.
- Diseñe una arquitectura sin estado después de identificar qué datos de estado y de usuario deben conservarse con la solución de almacenamiento que elija.

Recursos

Prácticas recomendadas relacionadas:

- REL11-BP03 Automatización de la reparación en todas las capas

Documentos relacionados:

- Amazon Builders' Library: Evitar los planes alternativos en los sistemas distribuidos
- Amazon Builders' Library: Cómo evitar demoras de colas insuperables
- Amazon Builders' Library: Desafíos y estrategias del almacenamiento en caché
- Prácticas recomendadas para el nivel web sin estado en AWS

REL05-BP07 Implementación de recursos de emergencia

Los recursos de emergencia son procesos rápidos que pueden mitigar el impacto en la disponibilidad de la carga de trabajo.

Los recursos de emergencia desactivan, limitan o cambian el comportamiento de componentes o dependencias mediante mecanismos conocidos y probados. Esto puede aliviar las deficiencias de la carga de trabajo causadas por el agotamiento de los recursos debido a los aumentos inesperados de la demanda y reducir el impacto de los fallos en los componentes no críticos de la carga de trabajo.

Resultado deseado: al implementar recursos de emergencia, puede establecer procesos que se sabe que son buenos para mantener la disponibilidad de los componentes críticos de su carga de trabajo. La carga de trabajo debe degradarse de forma estable y seguir llevando a cabo sus funciones críticas para la empresa durante la activación de un recurso de emergencia. Para obtener más información sobre la degradación estable, consulte REL05-BP01 Implementación de una degradación estable para transformar las dependencias estrictas en flexibles.

Patrones comunes de uso no recomendados:

- El fallo de las dependencias no críticas repercute en la disponibilidad de su carga de trabajo principal.
- No probar o verificar el comportamiento de los componentes críticos durante el deterioro de los componentes no críticos.
- No definir criterios claros y deterministas para la activación o desactivación de un recurso de emergencia.

Beneficios de establecer esta práctica recomendada: la implementación de recursos de emergencia puede mejorar la disponibilidad de los componentes críticos de su carga de trabajo al proporcionar a sus solucionadores procesos establecidos para responder a picos inesperados de demanda o fallos de dependencias no críticas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

- Identifique los componentes críticos de su carga de trabajo.
- Diseñe y cree los componentes críticos de su carga de trabajo para que resistan los fallos de los componentes no críticos.
- Haga pruebas para validar el comportamiento de sus componentes críticos durante el fallo de los componentes no críticos.
- Defina y supervise las métricas o los factores desencadenantes relevantes para iniciar los procedimientos de recursos de emergencia.
- Defina los procedimientos (manuales o automáticos) que componen el recurso de emergencia.

Pasos para la implementación

- Identifique los componentes críticos para la empresa en su carga de trabajo.
  - Cada componente técnico de su carga de trabajo debe asignarse a su función empresarial relevante y clasificarse como crítico o no crítico. Para ver ejemplos de funciones críticas y no críticas de Amazon, consulte Any Day Can Be Prime Day: How Amazon.com Search Uses Chaos Engineering to Handle Over 84K Requests Per Second.
  - Se trata de una decisión tanto técnica como empresarial, y varía según la organización y la carga de trabajo.
- Diseñe y cree los componentes críticos de su carga de trabajo para que resistan los fallos de los componentes no críticos.
  - Durante el análisis de dependencias, tenga en cuenta todos los modos de fallo potenciales y verifique que sus mecanismos de recursos de emergencia proporcionan la funcionalidad crítica a los componentes descendentes.
- Haga pruebas para validar el comportamiento de sus componentes críticos durante la activación de sus recursos de emergencia.
  - Evite el comportamiento bimodal. Para obtener más información, consulte REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal.

- Defina, supervise y alerte sobre las métricas relevantes para iniciar el procedimiento del recurso de emergencia.
  - Encontrar las métricas adecuadas para supervisar depende de su carga de trabajo. Algunos ejemplos de métricas son la latencia o el número de solicitudes fallidas a una dependencia.
- Defina los procedimientos manuales o automáticos que componen el recurso de emergencia.
  - Esto puede incluir mecanismos como el desbordamiento de carga, la limitación de solicitudes o la implementación de una degradación estable.

Recursos

Prácticas recomendadas relacionadas:

- REL05-BP01 Implementación de una degradación estable para transformar las dependencias estrictas en flexibles
- REL05-BP02 Limitación de las solicitudes
- REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal

Documentos relacionados:

- Automatización de implementaciones seguras y sin intervención
- Any Day Can Be Prime Day: How Amazon.com Search Uses Chaos Engineering to Handle Over 84K Requests Per Second

Videos relacionados:

- AWS re:Invent 2020: Reliability, consistency, and confidence through immutability

Administración de cambios

Se deben prever y ajustar los cambios en la carga de trabajo o el entorno para lograr un funcionamiento fiable de la carga de trabajo. Los cambios incluyen aquellos impuestos a la carga de trabajo, como los picos de demanda, además de los inherentes a ella, como las implementaciones de características o los parches de seguridad.

En las siguientes secciones, se explican las prácticas recomendadas para la administración de cambios.

Temas

- Supervisión de los recursos de la carga de trabajo
- Diseño de su carga de trabajo para adaptarla a los cambios en la demanda
- Implementación de cambios

Supervisión de los recursos de la carga de trabajo

Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión permite que su carga de trabajo reconozca cuándo se cruzan umbrales de bajo rendimiento o se producen errores, para que pueda recuperarse de los errores de forma automática una vez recibida una respuesta.

La supervisión es vital para garantizar el cumplimiento de los requisitos de disponibilidad. La supervisión debe detectar los errores de manera efectiva. El peor modo de error es el “silencioso”, en el que la funcionalidad ya no sirve, pero no hay forma de detectarlo, excepto indirectamente. Los clientes se dan cuenta antes que usted. Poder alertar cuando tiene problemas es una de las principales razones por las que debe supervisar. Las alertas deben estar desacopladas del sistema en la medida de lo posible. Si la interrupción del servicio elimina la posibilidad de generar alertas, habrá un periodo de interrupción más largo.

En AWS, instrumentamos nuestras aplicaciones en múltiples niveles. Registramos la latencia, las tasas de error y la disponibilidad de cada solicitud, de todas las dependencias y de las operaciones clave dentro del proceso. También registramos métricas de operación exitosa. Esto permite ver los problemas inminentes antes de que sucedan. No solo tenemos en cuenta la latencia media. Nos

centramos aún más en los valores atípicos de latencia, como los percentiles 99,9 y 99,99. Esto se debe a que, si una de cada 1000 o 10 000 solicitudes es lenta, la experiencia sigue siendo mala. Si el promedio es aceptable, pero una de cada 100 solicitudes causa una latencia extrema, cuando el tráfico crezca, eventualmente se convertirá en un problema.

La supervisión en AWS consta de cinco fases distintas:

1. Generación: supervisión de todos los componentes de la carga de trabajo
2. Agregación: definición y cálculo de métricas
3. Procesamiento y alarmas en tiempo real: envío de notificaciones y automatización de respuestas
4. Almacenamiento y análisis

Prácticas recomendadas

- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL06-BP02 Definición y cálculo de métricas (agregación)
- REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)
- REL06-BP04 Automatización de las respuestas (procesamiento y alarmas en tiempo real)
- REL06-BP05 Análisis de registros
- REL06-BP06 Revisiones frecuentes
- REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema

REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)

Supervise los componentes de la carga de trabajo con Amazon CloudWatch o herramientas de terceros. Supervise los servicios de AWS con el panel de AWS Health.

Debe supervisar todos los componentes de su carga de trabajo, incluidos los niveles del frontend, la lógica empresarial y el almacenamiento. Defina métricas claves, describa cómo extraerlas de los registros (si fuera necesario) y establezca umbrales para desencadenar los eventos de alarma correspondientes. Asegúrese de que las métricas sean pertinentes para los indicadores clave de rendimiento (KPI) de su carga de trabajo, y utilice métricas y registros para identificar signos de advertencia tempranos de degradación del servicio. Por ejemplo, una métrica relacionada con los resultados empresariales como el número de pedidos procesado satisfactoriamente por minuto, puede indicar problemas con la carga de trabajo más rápido que una métrica técnica, como el uso de

la CPU. Utilice el panel de AWS Health para obtener una vista personalizada sobre el rendimiento y la disponibilidad de los servicios de AWS subyacentes a sus recursos de AWS.

La supervisión en la nube ofrece nuevas oportunidades. La mayoría de proveedores en la nube han desarrollado enlaces personalizables y pueden proporcionar conocimientos para ayudarle a supervisar varias capas de su carga de trabajo. Los servicios de AWS como Amazon CloudWatch aplican algoritmos estadísticos y de machine learning para analizar continuamente las métricas de los sistemas y aplicaciones, determinar las bases de referencia normales y hacer aflorar anomalías con una intervención mínima del usuario. Los algoritmos de detección de anomalías dan cuenta de la estacionalidad y los cambios de tendencia de las métricas.

AWS pone a disposición una gran cantidad de información de supervisión y registro para el consumo que se puede usar para definir métricas específicas de la carga de trabajo, procesos de cambio en la demanda y adoptar técnicas de machine learning independientemente de los conocimientos sobre ML.

Además, puede supervisar todos sus puntos de conexión externos para asegurarse de que sean independientes de su implementación base. Esta supervisión activa se puede llevar a cabo con transacciones sintéticas (a las que a veces se denomina canarios de usuario, y que no deben confundirse con las implementaciones canario), que ejecutan periódicamente varias tareas comunes que se ajustan a las acciones que hacen los clientes de la carga de trabajo. Mantenga una duración breve para estas tareas y asegúrese de no sobrecargar sus cargas de trabajo durante las pruebas. Amazon CloudWatch Synthetics le permite crear canarios sintéticos para supervisar sus puntos de conexión y API. También puede combinar los nodos de cliente del canario sintético con la consola de AWS X-Ray para detectar qué canarios sintéticos están teniendo problemas de errores, fallos o limitaciones para el periodo de tiempo seleccionado.

Resultado deseado:

Recopila y usa métricas esenciales de todos los componentes de la carga de trabajo para garantizar la fiabilidad de la carga de trabajo y una experiencia de usuario óptima. Detectar que una carga de trabajo no está logrando resultados empresariales le permite declarar rápidamente un desastre y recuperarse de un incidente.

Patrones comunes de uso no recomendados:

- Supervisar solamente las interfaces externas con su carga de trabajo.
- No generar métricas específicas de una carga de trabajo y basarse solamente en las métricas que proporcionan los servicios de AWS que usa su carga de trabajo.

- Usar exclusivamente métricas técnicas en su carga de trabajo y no supervisar las métricas relacionadas con KPI no técnicos a los que contribuye la carga de trabajo.
- Confiar en el tráfico de producción y las comprobaciones de estado sencillas para supervisar y evaluar el estado de las cargas de trabajo.

Beneficios de establecer esta práctica recomendada: la supervisión de todos los niveles de la carga de trabajo le permite prever y resolver los problemas rápidamente en los componentes de la carga de trabajo.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

1. Active el registro cuando esté disponible. La supervisión de los datos debe obtenerse a partir de todos los componentes de las cargas de trabajo. Active métodos de registro adicionales, como los registros de acceso de S3, y permita que su carga de trabajo registre datos específicos de la carga de trabajo. Recopile métricas para los promedios de CPU, E/S de red y E/S de disco de servicios como Amazon ECS, Amazon EKS, Amazon EC2, Elastic Load Balancing, AWS Auto Scaling y Amazon EMR. Consulte Servicios de AWS que publican métricas de CloudWatch para consultar una lista de servicios de AWS que publican métricas en CloudWatch.
2. Revise todas las métricas predeterminadas y explore las carencias en cuanto a recopilación de datos. Todos los servicios generan métricas predeterminadas. La recopilación de métricas predeterminadas le permite comprender mejor las dependencias entre los componentes de la carga de trabajo, y cómo la fiabilidad y el rendimiento de los componentes afectan a la carga de trabajo. También puede crear y publicar sus propias métricas en CloudWatch mediante la AWS CLI o una API.
3. Evalúe todas las métricas para decidir sobre cuáles alertar en cada servicio de AWS en su carga de trabajo. Puede decidir seleccionar un subconjunto de métricas que tenga un impacto importante en la fiabilidad de la carga de trabajo. Al centrarse en las métricas y umbrales críticos, podrá refinar el número de alertas de emergencia y contribuir a reducir al mínimo los falsos positivos.
4. Defina las alertas y los procesos de recuperación para su carga de trabajo una vez que se active la alerta. La definición de alertas le permite notificar, escalar y seguir los pasos necesarios rápidamente para recuperarse de un incidente y cumplir el objetivo de tiempo de recuperación (RTO) prescrito. Puede usar alarmas de Amazon CloudWatch para invocar flujos de trabajo automatizados e iniciar procedimientos de recuperación basados en los umbrales definidos.

5. Explore el uso de transacciones sintéticas para recopilar datos relevantes sobre el estado de las cargas de trabajo. La supervisión sintética sigue las mismas rutas y lleva a cabo las mismas acciones que un cliente, lo que le permite verificar continuamente su experiencia de usuario incluso si no tiene tráfico de cliente en sus cargas de trabajo. Al usar transacciones sintéticas, puede detectar los problemas antes de que lo hagan los clientes.

Recursos

Prácticas recomendadas relacionadas:

- REL11-BP03 Automatización de la reparación en todas las capas

Documentos relacionados:

- Getting started with your AWS Health Dashboard – Your account health
- Servicios de AWS que publican métricas de CloudWatch
- Access Logs for Your Network Load Balancer
- Access logs for your application load balancer
- Uso de Registros de Amazon CloudWatch con AWS Lambda
- Registro de acceso al servidor de Simple Storage Service (Amazon S
- Enable Access Logs for Your Classic Load Balancer
- Exporting log data to Amazon S3
- Instalación del agente de CloudWatch en una instancia de Amazon EC2
- Publicar métricas personalizadas
- Uso de paneles de Amazon CloudWatch
- Uso de métricas de Amazon CloudWatch
- Uso de canarios (Amazon CloudWatch Synthetics)
- What are Amazon CloudWatch Logs?

Guías del usuario:

- Creating a trail
- Supervisión de memoria y métricas del disco para las instancias de Linux de Amazon EC2
- Uso de Registros de CloudWatch con instancias de contenedor
- registros de flujo de VPC

- What is Amazon DevOps Guru?
- Qué es AWS X-Ray?

Blogs relacionados:

- Debugging with Amazon CloudWatch Synthetics and AWS X-Ray

Ejemplos relacionados:

- Amazon Builders' Library: Instrumentación de los sistemas distribuidos para obtener visibilidad operativa
- Observability workshop

REL06-BP02 Definición y cálculo de métricas (agregación)

Recopile métricas y registros de los componentes de su carga de trabajo y calcule las métricas agregadas relevantes a partir de ellos. Estas métricas proporcionan una observabilidad amplia y profunda de su carga de trabajo y pueden mejorar significativamente su posición de resiliencia.

La observabilidad es algo más que recopilar métricas de los componentes de la carga de trabajo a fin de poder verlas y alertar sobre ellas. Se trata de obtener una visión de conjunto de cómo se comporta la carga de trabajo. Esta información de comportamiento proviene de todos los componentes de sus cargas de trabajo, que incluyen los servicios en la nube de los que dependen, los registros bien elaborados y las métricas. Estos datos le permiten supervisar el comportamiento de la carga de trabajo en su conjunto, así como comprender la interacción de cada componente con cada unidad de trabajo con un nivel de detalle preciso.

Resultado deseado:

- Recopila registros de los componentes de su carga de trabajo y las dependencias de los servicios de AWS y los publica en una ubicación central donde se puede acceder a ellos y procesarlos fácilmente.
- Sus registros contienen marcas de tiempo precisas y de alta fidelidad.
- Sus registros contienen información relevante sobre el contexto de procesamiento, como un identificador de rastreo, un identificador de usuario o de cuenta y una dirección IP remota.
- Crea métricas agregadas a partir de sus registros, que representan el comportamiento de su carga de trabajo desde una perspectiva de alto nivel.

- Puede consultar sus registros agregados para obtener información detallada y relevante sobre su carga de trabajo e identificar problemas reales y potenciales.

Patrones comunes de uso no recomendados:

- No recopila registros ni métricas relevantes de las instancias de computación en las que se ejecutan sus cargas de trabajo ni de los servicios en la nube que utilizan.
- Pasa por alto la recopilación de registros y métricas relacionados con los indicadores clave de rendimiento (KPI) de su empresa.
- Analiza la telemetría relacionada con la carga de trabajo de forma aislada, sin agregación ni correlación.
- Permite que las métricas y los registros caduquen demasiado rápido, lo que dificulta el análisis de tendencias y la identificación de problemas recurrentes.

Ventajas de establecer estas prácticas recomendadas: puede detectar más anomalías y correlacionar eventos y métricas entre los distintos componentes de su carga de trabajo. Puede crear información estratégica a partir de los componentes de su carga de trabajo en función de la información contenida en los registros que, por lo general, no está disponible únicamente en las métricas. Puede determinar las causas de los errores con mayor rapidez consultando sus registros a escala.

Nivel de exposición al riesgo si no se establecen estas prácticas recomendadas: alto

Guía para la implementación

Identifique las fuentes de datos de telemetría que son relevantes para sus cargas de trabajo y sus componentes. Estos datos provienen no solo de los componentes que publican métricas, como el sistema operativo (SO), y los tiempos de ejecución de las aplicaciones, como Java, sino también de los registros de aplicaciones y servicios en la nube. Por ejemplo, los servidores web suelen registrar cada solicitud con información detallada, como la marca de tiempo, la latencia del procesamiento, el ID de usuario, la dirección IP remota, la ruta y la cadena de consulta. El nivel de detalle de estos registros lo ayuda a realizar consultas detalladas y a generar métricas que de otro modo no estarían disponibles.

Recopile las métricas y los registros mediante las herramientas y los procesos adecuados. Un agente, como el Agente de Amazon CloudWatch, puede recopilar los registros generados por las aplicaciones que se ejecutan en una instancia de Amazon EC2 y publicarlos en un servicio

de almacenamiento central, como Registros de Amazon CloudWatch. Los servicios de cómputo gestionados por AWS, como AWS Lambda y Amazon Elastic Container Service, publican automáticamente los registros en CloudWatch Logs. Habilite la recopilación de registros para los servicios de almacenamiento y procesamiento de AWS que utilizan sus cargas de trabajo, como Amazon CloudFront, Amazon S3, Elastic Load Balancing y Amazon API Gateway.

Mejore sus datos de telemetría con dimensiones que lo ayuden a ver los patrones de comportamiento con mayor claridad y a aislar los problemas correlacionados en grupos de componentes relacionados. Una vez agregados, puede observar el comportamiento de los componentes con un nivel de detalle más preciso, detectar los fallos correlacionados y tomar las medidas correctivas adecuadas. Algunos ejemplos de dimensiones útiles son la zona de disponibilidad, el ID de instancia de EC2 y la tarea de contenedor o ID de pod.

Una vez recopiladas las métricas y los registros, puede escribir consultas y generar métricas agregadas a partir de ellas que proporcionen información útil sobre el comportamiento normal y anómalo. Por ejemplo, puede utilizar Información de registros de Amazon CloudWatch para obtener métricas personalizadas de los registros de las aplicaciones, Información de métricas de Amazon CloudWatch para consultar las métricas a escala, Información de contenedores de Amazon CloudWatch para recopilar, agregar y resumir las métricas y los registros de sus aplicaciones y microservicios en contenedores, o Lambda Insights de Amazon CloudWatch si utiliza funciones de AWS Lambda. Para crear una métrica de tasa de error agregada, puede sumar un contador cada vez que encuentre una respuesta o mensaje de error en los registros de sus componentes, o bien calcular el valor agregado de una métrica de tasa de error existente. Puede utilizar estos datos para generar histogramas que muestren el comportamiento final, como las solicitudes o los procesos con peor rendimiento. También puede escanear estos datos en tiempo real para detectar patrones anómalos mediante soluciones como la detección de anomalías de CloudWatch Logs. Esta información estratégica se puede colocar en los paneles de control para mantenerlos organizados de acuerdo con sus necesidades y preferencias.

La consulta de los registros puede ayudarlo a comprender cómo gestionaron las solicitudes específicas los componentes de la carga de trabajo y a revelar los patrones de las solicitudes u otro contexto que repercuta en la resiliencia de la carga de trabajo. Puede resultar útil investigar y preparar las consultas con antelación, en función de sus conocimientos sobre el comportamiento de sus aplicaciones y otros componentes, de forma que pueda ejecutarlas más fácilmente según sea necesario. Por ejemplo, con Información de registros de CloudWatch, puede buscar y analizar de forma interactiva los datos de registro almacenados en Registros de Amazon CloudWatch. También puede usar Amazon Athena para consultar registros de varias fuentes, incluidos muchos servicios de AWS, a escala de petabytes.

Al definir una política de retención de registros, tenga en cuenta el valor de los registros históricos. Los registros históricos pueden ayudar a identificar los patrones de uso y comportamiento a largo plazo, las regresiones y las mejoras en el rendimiento de la carga de trabajo. Los registros eliminados permanentemente no se pueden analizar más adelante. Sin embargo, el valor de los registros históricos tiende a disminuir durante largos periodos de tiempo. Elija una política que equilibre sus necesidades según corresponda y que cumpla con todos los requisitos legales o contractuales a los que pueda estar sujeto.

Pasos para la implementación

1. Elija mecanismos de recopilación, almacenamiento, análisis y visualización para sus datos de observabilidad.
2. Instale y configure los recopiladores de métricas y registros en los componentes correspondientes de su carga de trabajo (por ejemplo, en las instancias de Amazon EC2 y en los contenedores sidecar). Configure estos recopiladores para que se reinicien automáticamente si se detienen inesperadamente. Habilite el almacenamiento en búfer de disco o memoria para los recopiladores para que los errores de publicación temporales no afecten a sus aplicaciones ni provoquen la pérdida de datos.
3. Habilite el inicio de sesión en los servicios de AWS que utiliza como parte de sus cargas de trabajo y, si es necesario, reenvíe esos registros al servicio de almacenamiento que haya seleccionado. Consulte las guías de usuario o desarrollador de los servicios correspondientes para obtener instrucciones detalladas.
4. Defina las métricas operativas relevantes para sus cargas de trabajo en función de sus datos de telemetría. Podrían basarse en métricas directas emitidas por los componentes de la carga de trabajo, que pueden incluir métricas relacionadas con los KPI empresariales, o en los resultados de cálculos agregados, como sumas, tasas, percentiles o histogramas. Calcule estas métricas con su analizador de registros y colóquelas en los paneles según corresponda.
5. Prepare las consultas de registro adecuadas para analizar los componentes de la carga de trabajo, las solicitudes o el comportamiento de las transacciones, según sea necesario.
6. Defina y habilite una política de retención de registros para los registros de sus componentes. Elimine periódicamente los registros cuando sean más antiguos de lo que permite la política.

Recursos

Prácticas recomendadas relacionadas:

- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)

- REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)
- REL06-BP04 Automatización de las respuestas (procesamiento y alarmas en tiempo real)
- REL06-BP05 Análisis de registros
- REL06-BP06 Revisiones frecuentes
- REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema

Documentación relacionada:

- Funcionamiento de Amazon CloudWatch.
- Amazon Managed Prometheus
- Amazon Managed Grafana
- Analyzing Log Data with CloudWatch Logs Insights
- Lambda Insights de Amazon CloudWatch
- Información de contenedores de Amazon CloudWatch
- Consulta de métricas de CloudWatch con Información de métricas de CloudWatch
- AWS Distro para OpenTelemetry
- Amazon CloudWatch Logs Insights Sample Queries
- Debugging with Amazon CloudWatch Synthetics and AWS X-Ray
- Searching and Filtering Log Data
- Sending Logs Directly to Amazon S3
- Amazon Builders' Library: Instrumentación de los sistemas distribuidos para obtener visibilidad operativa

Talleres relacionados:

- One Observability Workshop

Herramientas relacionadas:

- AWS Distro para OpenTelemetry (GitHub)

REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)

Cuando las organizaciones detectan posibles problemas, envían notificaciones y alertas en tiempo real al personal y los sistemas correspondientes para poder responder de manera rápida y eficaz a estos problemas.

Resultado deseado: es posible responder rápidamente a los eventos operativos con la configuración de las alarmas correspondientes en función de las métricas del servicio y la aplicación. Cuando se superan los umbrales de alarma, se avisa al personal y a los sistemas adecuados para que puedan abordar los problemas subyacentes.

Patrones comunes de uso no recomendados:

- Las alarmas están configuradas con un umbral excesivamente alto, lo que impide que se envíen notificaciones vitales.
- Las alarmas están configuradas con un umbral demasiado bajo, lo que provoca inacción en las alertas importantes por el ruido que genera el exceso de notificaciones.
- Las alarmas y los umbrales no se actualizan cuando hay cambios de uso.
- En el caso de las alarmas que se abordan mejor con acciones automatizadas, en lugar de generar dichas acciones, se envían notificaciones al personal, lo que provoca un exceso de notificaciones.

Beneficios de establecer esta práctica recomendada: enviar notificaciones y alertas en tiempo real al personal y a los sistemas adecuados permite detectar problemas de forma temprana y responder rápidamente a los incidentes operativos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las cargas de trabajo deben estar equipadas con sistemas de procesamiento y generación de alarmas en tiempo real que permitan mejorar la capacidad de detección de problemas que podrían afectar a la disponibilidad de la aplicación y actúen como desencadenantes de una respuesta automatizada. Las organizaciones pueden llevar a cabo el procesamiento y generar alarmas en tiempo real mediante la creación de alertas con métricas definidas para recibir notificaciones siempre que ocurran eventos importantes o una métrica supere un umbral.

Amazon CloudWatch le permite crear alarmas de métricas y compuestas mediante alarmas de CloudWatch en función del umbral estático, la detección de anomalías y otros criterios. Para obtener más información sobre los tipos de alarmas que puede configurar con CloudWatch, consulte la sección de alarmas de la documentación de CloudWatch.

Puede crear vistas personalizadas de las métricas y alertas de los recursos de AWS para sus equipos mediante los paneles de CloudWatch. Las páginas de inicio personalizables de la consola de CloudWatch le permiten supervisar los recursos a través de una única vista de las diferentes regiones.

Las alarmas pueden llevar a cabo una o más acción, como enviar una notificación a un tema de Amazon SNS, ejecutar una acción de Amazon EC2 o una acción de Amazon EC2 Auto Scaling o crear un OpsItem o incidente en AWS Systems Manager.

Amazon CloudWatch usa Amazon SNS para enviar notificaciones cuando la alarma cambia de estado, lo que permite que los editores (productores) envíen mensajes a los suscriptores (consumidores). Para obtener más información sobre la configuración de las notificaciones de Amazon SNS, consulte Configuring Amazon SNS.

CloudWatch envía eventos a EventBridge cada vez que se crea, actualiza o elimina una alarma de CloudWatch o cambia su estado. Puede usar EventBridge con estos eventos para crear reglas que lleven a cabo acciones, como avisarle cada vez que cambie el estado de una alarma o que activen eventos en la cuenta de forma automática mediante la automatización de Systems Manager.

Manténgase informado con AWS Health. AWS Health es la fuente autorizada de información sobre el estado de los recursos de Nube de AWS. Use AWS Health para recibir notificaciones de cualquier evento de servicio confirmado, de modo que pueda tomar rápidamente medidas para mitigar cualquier impacto. Cree notificaciones de eventos de AWS Health adecuados para su propósito para los canales de correo electrónico y chat a través de AWS User Notifications e intégrelas mediante programación con las herramientas de supervisión y alertas a través de Amazon EventBridge. Si usa AWS Organizations, agregue eventos de AWS Health entre cuentas.

Cuándo debe utilizar EventBridge o Amazon SNS?

Tanto EventBridge como Amazon SNS se pueden utilizar para desarrollar aplicaciones basadas en eventos, así que la elección de uno u otro dependerá de sus necesidades específicas.

Se recomienda Amazon EventBridge si desea crear una aplicación que reaccione a los eventos de sus propias aplicaciones, aplicaciones SaaS y servicios de AWS. EventBridge es el único servicio

basado en eventos que se integra directamente con socios de SaaS externos. EventBridge también ingiere automáticamente eventos de más de 200 servicios de AWS sin que los desarrolladores tengan que crear ningún recurso en su cuenta.

EventBridge utiliza una estructura definida basada en JSON para los eventos y le ayuda a crear reglas que se aplican a todo el cuerpo del evento para seleccionar los eventos que se van a reenviar a un destino. Actualmente, EventBridge admite más de 20 servicios de AWS como destino, incluidos AWS Lambda, Amazon SQS, Amazon SNS, Amazon Kinesis Data Streams y Amazon Data Firehose.

Se recomienda usar Amazon SNS con aplicaciones que necesiten una gran distribución (miles o millones de puntos de conexión). Un patrón común que vemos con frecuencia es que los clientes usan Amazon SNS como destino de la regla para filtrar los eventos que necesitan y distribuirlos a diversos puntos de conexión.

Los mensajes no están estructurados y pueden estar en el formato que desee. Amazon SNS admite el reenvío de mensajes a seis tipos diferentes de destinos, incluidos Lambda, Amazon SQS, puntos de conexión HTTP/S, SMS, notificaciones push y correo electrónico. La latencia habitual de Amazon SNS es inferior a 30 milisegundos. Hay un gran número de servicios de AWS que envían mensajes de Amazon SNS si se configuran para ello (hay más de 30, incluidos Amazon EC2, Amazon S3 y Amazon RDS).

Pasos para la implementación

1. Cree una alarma con las alarmas de Amazon CloudWatch.
   a. Las alarmas de métricas supervisan una única métrica de CloudWatch o una expresión que depende de las métricas de CloudWatch. La alarma inicia una o varias acciones en función del valor de la métrica o de la expresión en comparación con un umbral durante varios intervalos de tiempo. La acción puede ser el envío de una notificación a un tema de Amazon SNS, la ejecución de una acción de Amazon EC2 o una acción de Amazon EC2 Auto Scaling o la creación de un OpsItem o incidente en AWS Systems Manager.
   b. Una alarma compuesta es una expresión de regla que tiene en cuenta las condiciones de otras alarmas que se han creado. La alarma compuesta solo entra en estado de alarma si se cumplen todas las condiciones de la regla. Las alarmas especificadas en la expresión de la regla de una alarma compuesta pueden ser alarmas de métricas y otras alarmas compuestas. Las alarmas compuestas pueden enviar notificaciones de Amazon SNS cuando cambian de estado y pueden crear OpsItems de Systems Manager o incidentes cuando entran en estado de alarma, pero no pueden llevar a cabo acciones de Amazon EC2 ni acciones de escalado automático.

2. Configure las notificaciones de Amazon SNS. Al crear una alarma de CloudWatch, puede incluir un tema de Amazon SNS para enviar una notificación cuando la alarma cambie de estado.
3. Cree reglas en EventBridge que coincidan con las alarmas de CloudWatch especificadas. Cada regla admite varios destinos, incluidas las funciones de Lambda. Por ejemplo, puede definir una alarma que se inicie cuando el espacio disponible en disco se esté agotando, lo que desencadenará una función de Lambda mediante una regla de EventBridge para limpiar el espacio. Para obtener más información sobre los objetivos de EventBridge, consulta los objetivos de EventBridge.

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL06-BP02 Definición y cálculo de métricas (agregación)
- REL12-BP01 Uso de manuales de estrategias para investigar los errores

Documentos relacionados:

- Amazon CloudWatch
- CloudWatch Logs insights
- Uso de las alarmas de Amazon CloudWatch
- Uso de paneles de Amazon CloudWatch
- Uso de métricas de Amazon CloudWatch
- Configuración de notificaciones de Amazon SNS
- Uso de la detección de anomalías de CloudWatch
- CloudWatch Logs data protection
- Amazon EventBridge
- Amazon Simple Notification Service

Videos relacionados:

- Videos sobre observabilidad de reinvent

- AWS re:Invent 2022 - Observability best practices at Amazon

Ejemplos relacionados:

- One Observability Workshop
- Amazon EventBridge to AWS Lambda with feedback control by Amazon CloudWatch Alarms

REL06-BP04 Automatización de las respuestas (procesamiento y alarmas en tiempo real)

Use la automatización para actuar cuando se detecte un evento, por ejemplo, para sustituir componentes defectuosos.

El procesamiento automatizado de las alarmas en tiempo real se implementa para que los sistemas puedan tomar medidas correctivas rápidas e intentar evitar fallos o que el servicio se degrade cuando se activan las alarmas. Entre las respuestas automatizadas a las alarmas, se podría incluir la sustitución de los componentes que fallan, el ajuste de la capacidad de computación, el redireccionamiento del tráfico a hosts, zonas de disponibilidad u otras regiones en buen estado y la notificación a los operadores.

Resultado deseado: se identifican las alarmas en tiempo real y se configura el procesamiento automatizado de las alarmas para invocar las acciones apropiadas que se necesitan para mantener los objetivos de nivel de servicio y los acuerdos de nivel de servicio (SLA). La automatización puede abarcar desde actividades de autorreparación de componentes individuales hasta la conmutación por error de todo el sitio.

Patrones comunes de uso no recomendados:

- No tener un inventario o catálogo claros de las principales alarmas en tiempo real.
- No tener respuestas automatizadas en las alarmas críticas (por ejemplo, cuando los recursos de computación están a punto de agotarse, se produce un escalado automático).
- Acciones de respuesta a alarmas contradictorias.
- No tener procedimientos operativos estándar (SOP) que los operadores puedan seguir cuando reciben notificaciones de alerta.
- No supervisar los cambios de configuración, ya que los cambios de configuración no detectados pueden provocar un tiempo de inactividad en las cargas de trabajo.

- No tener una estrategia para deshacer los cambios de configuración no deseados.

Beneficios de establecer esta práctica recomendada: la automatización del procesamiento de alarmas puede mejorar la resiliencia del sistema. El sistema aplica las medidas correctivas automáticamente, lo que reduce las actividades manuales que dan lugar a intervenciones humanas que son más susceptibles a errores. Las operaciones de carga de trabajo cumplen los objetivos de disponibilidad y reducen la interrupción del servicio.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Para administrar eficazmente las alertas y automatizar su respuesta, clasifique las alertas en función de su importancia y repercusión, documente los procedimientos de respuesta y planifique las respuestas antes de clasificar las tareas.

Identifique las tareas que requieren medidas específicas (suelen detallarse en los manuales de procedimientos) y examine todos los manuales de procedimientos y manuales de estrategias para determinar qué tareas se pueden automatizar. Si se pueden definir acciones, estas suelen poderse automatizar. Si las acciones no se pueden automatizar, documente los pasos manuales en un SOP y forme a los operadores sobre ellos. Analice continuamente los procesos manuales en busca de oportunidades de automatización en las que pueda establecer y mantener un plan para automatizar las respuestas a las alertas.

Pasos para la implementación

1. Creación de un inventario de alarmas: para obtener una lista de todas las alarmas, puede utilizar la AWS CLI con el comando de Amazon CloudWatch `describe-alarms`. Según el número de alarmas que haya configurado, puede que tenga que utilizar la paginación para recuperar un subconjunto de alarmas para cada llamada o, si lo prefiere, puede utilizar el AWS SDK para obtener las alarmas mediante una llamada a la API.
2. Documentación de todas las acciones de la alarma: actualice un manual de procedimientos con todas las alarmas y sus acciones, independientemente de si son manuales o automatizadas. AWS Systems Managerproporciona manuales de procedimientos predefinidos. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimiento, consulte View runbook content.

3. Configuración y administración de acciones de la alarma: para cualquiera de las alarmas que requieran una acción, especifique la acción automatizada mediante el SDK de CloudWatch. Por ejemplo, puede cambiar el estado de sus instancias de Amazon EC2 automáticamente en función de una alarma de CloudWatch. Para ello, cree y habilite acciones en una alarma o deshabilite acciones en una alarma.

   También se puede utilizar Amazon EventBridge para responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios en los recursos. Puede crear reglas para indicar qué eventos le resultan de interés, así como qué acciones se van a realizar cuando un evento cumpla una de las reglas. Entre las acciones que se pueden iniciar automáticamente, se incluye invocar una función de AWS Lambda, invocar el `Run Command` de Amazon EC2, transmitir el evento a Amazon Kinesis Data Streams y ver cómo se automatiza Amazon EC2 con EventBridge.
4. Procedimientos operativos estándar (SOP): en función de los componentes que tenga su aplicación, AWS Resilience Hub recomienda varias plantillas de SOP. Puede utilizar estos SOP para documentar todos los procesos que debe seguir un operador en caso de que se genere una alerta. También puede crear un SOP basado en recomendaciones de Resilience Hub cuando necesite una aplicación Resilience Hub con una política de resiliencia asociada, así como una evaluación de resiliencia histórica en relación con esa aplicación. Las recomendaciones para su SOP provienen de la evaluación de resiliencia.

   Resilience Hub funciona con Systems Manager para automatizar los pasos de sus SOP al proporcionar una serie de documentos SSM que puede utilizar como base para esos SOP. Por ejemplo, Resilience Hub puede recomendar un SOP para agregar espacio en disco en un documento de automatización de SSM existente.
5. Acciones automatizadas con Amazon DevOps Guru: puede utilizar Amazon DevOps Guru para supervisar automáticamente los recursos de la aplicación en busca de un comportamiento anómalo y ofrecer recomendaciones específicas para reducir el tiempo de identificación y resolución de problemas. Con DevOps Guru, puede supervisar secuencias de datos operativos casi en tiempo real desde múltiples orígenes, como métricas de Amazon CloudWatch, AWS Config, AWS CloudFormation y AWS X-Ray. También puede utilizar DevOps Guru para crear automáticamente OpsItems en OpsCenter y enviar eventos a EventBridge para una automatización adicional.

Recursos

Prácticas recomendadas relacionadas:

- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL06-BP02 Definición y cálculo de métricas (agregación)
- REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)
- REL08-BP01 Uso de manuales de procedimientos para actividades estándar como la implementación

Documentos relacionados:

- AWS Systems Manager Automation
- Creating an EventBridge Rule That Triggers on an Event from an AWS Resource
- One Observability Workshop
- Amazon Builders' Library: Instrumentación de los sistemas distribuidos para obtener visibilidad operativa
- What is Amazon DevOps Guru?
- Working with Automation Documents (Playbooks)

Videos relacionados:

- AWS re:Invent 2022 - Observability best practices at Amazon
- AWS re:Invent 2020: Automate anything with AWS Systems Manager
- Introduction to AWS Resilience Hub
- Create Custom Ticket Systems for Amazon DevOps Guru Notifications
- Enable Multi-Account Insight Aggregation with Amazon DevOps Guru

Ejemplos relacionados:

- Amazon CloudWatch and Systems Manager Workshop

REL06-BP05 Análisis de registros

Recopile archivos de registros e historiales de métricas y analícelos para identificar tendencias e información sobre las cargas de trabajo.

Información de registros de Amazon CloudWatch admite un lenguaje de consultas sencillo, pero potente, que se puede utilizar para analizar datos de registro. Registros de Amazon CloudWatch también admite suscripciones que permiten que los datos fluyan sin problemas a Amazon S3, donde puede usarlo o usar Amazon Athena para consultar los datos. También es compatible con consultas en una gran variedad de formatos. Consulte Formatos de SerDes y datos compatibles en la Guía del usuario de Amazon Athena para obtener más información. Para los análisis de conjuntos de archivos de registro enormes, puede ejecutar un clúster de Amazon EMR para ejecutar análisis en la escala de los petabytes.

Hay una serie de herramientas proporcionadas por socios de AWS y terceros que permiten la agregación, procesamiento, almacenamiento y análisis. Entre estas herramientas se incluyen New Relic, Splunk, Loggly, Logstash, CloudHealth y Nagios. Sin embargo, la generación fuera de los registros del sistema y las aplicaciones es exclusiva de cada proveedor de la nube y, a menudo, exclusiva de cada servicio.

Una parte del proceso de supervisión que a menudo se pasa por alto es la administración de datos. Necesita determinar los requisitos de retención para supervisar los datos y, luego, aplicar las políticas del ciclo de vida correspondientemente. Amazon S3 admite la gestión del ciclo de vida en el nivel de bucket de S3. Esta administración del ciclo de vida se puede aplicar de manera diferente a diferentes rutas en el bucket. Hacia el final del ciclo de vida, puede llevar a cabo la transición de datos a Amazon Glacier para el almacenamiento a largo plazo y vencimiento, una vez alcanzado el final del periodo de retención. La clase de almacenamiento S3 Intelligent-Tiering se ha diseñado para optimizar los costos de almacenamiento mediante el desplazamiento automático de los datos a la capa de acceso de almacenamiento más rentable, sin que afecte al rendimiento ni se produzca sobrecarga operativa.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

- Información de registros de CloudWatch le permite buscar y analizar de forma interactiva los datos de registro en Registros de Amazon CloudWatch.
  - Analyzing Log Data with CloudWatch Logs Insights
  - Amazon CloudWatch Logs Insights Sample Queries
- Use Registros de Amazon CloudWatch para enviar registros a Amazon S3, donde puede usar Amazon Athena para consultar los datos.
  - ¿Cómo analizo mis registros de acceso al servidor de Amazon S3 mediante Athena?

- Cree una política de ciclo de vida de S3 para su bucket de registros de acceso al servidor. Configure la política de ciclo de vida para que se eliminen periódicamente los archivos de registros. Esto reduce la cantidad de datos que Athena analiza para cada consulta.
  - ¿Cómo creo una política de ciclo de vida para un bucket de S3?

Recursos

Documentos relacionados:

- Amazon CloudWatch Logs Insights Sample Queries
- Analyzing Log Data with CloudWatch Logs Insights
- Debugging with Amazon CloudWatch Synthetics and AWS X-Ray
- ¿Cómo creo una política de ciclo de vida para un bucket de S3?
- ¿Cómo analizo mis registros de acceso al servidor de Amazon S3 mediante Athena?
- One Observability Workshop
- Amazon Builders' Library: Instrumentación de los sistemas distribuidos para obtener visibilidad operativa

REL06-BP06 Revisiones frecuentes

Revise frecuentemente cómo está implementada la supervisión de cargas de trabajo y actualícela a medida que su carga de trabajo y su arquitectura evolucionen. Las auditorías periódicas de su monitorización ayudan a reducir el riesgo de que los indicadores de problemas ignoren o se pasen por alto y, además, ayudan a que su carga de trabajo cumpla sus objetivos de disponibilidad.

Un monitoreo eficaz se basa en métricas empresariales clave, que evolucionan a medida que cambian las prioridades empresariales. Su proceso de revisión del monitoreo debe hacer hincapié en los indicadores de nivel de servicio (SLI) e incorporar información de su infraestructura, aplicaciones, clientes y usuarios.

Resultado deseado: cuenta con una estrategia de monitoreo eficaz que se revisa y actualiza periódicamente, así como después de cualquier evento o cambio significativo. Verifica que los indicadores clave del estado de las aplicaciones sigan siendo relevantes a medida que evolucionan su carga de trabajo y sus requisitos empresariales.

Patrones comunes de uso no recomendados:

- Recopila solo métricas predeterminadas.
- Establece una estrategia de monitoreo, pero nunca la revisa.
- No habla sobre el monitoreo cuando se implementan cambios importantes.
- Confía en métricas anticuadas para determinar el estado de la carga de trabajo.
- La carga de trabajo de sus equipos de operaciones es excesiva debido a las alertas de falsos positivos por la obsolescencia de las métricas y los umbrales.
- No tiene capacidad de observación de los componentes de la aplicación que no se monitorean.
- Se centra únicamente en las métricas técnicas de bajo nivel y excluye las métricas empresariales en su supervisión.

Beneficios de establecer esta mejor práctica: si revisa periódicamente su supervisión, puede anticipar los posibles problemas y comprobar que es capaz de detectarlos. También le permite descubrir puntos ciegos que podría haber pasado por alto durante las revisiones anteriores, lo que mejora aún más su capacidad para detectar problemas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Revise las métricas y el alcance del monitoreo durante el proceso de revisión de la preparación operativa (ORR). Realice revisiones periódicas de la preparación operativa siguiendo un cronograma coherente para evaluar si hay alguna brecha entre su carga de trabajo actual y la supervisión que ha configurado. Establezca una cadencia regular en las revisiones de rendimiento operativo y el intercambio de conocimientos para mejorar su capacidad de lograr un mayor rendimiento de sus equipos operativos. Compruebe si los umbrales de alerta existentes siguen siendo adecuados y compruebe si hay situaciones en las que los equipos operativos reciban alertas de falsos positivos o no supervisen los aspectos de la aplicación que deben supervisarse.

El Marco de análisis de la resiliencia proporciona una guía útil que puede ayudarlo a gestionar el proceso. El marco se centra en identificar los posibles modos de fallo y los controles preventivos y correctivos que puede utilizar para mitigar su impacto. Este conocimiento puede ayudar a identificar las métricas y los eventos correctos para monitorear y alertar sobre ellos.

Pasos para la implementación

1. Programe y lleve a cabo revisiones periódicas de los paneles de cargas de trabajo. Puede tener diferentes cadencias para el alcance de la inspección.

2. Inspeccione las tendencias en las métricas. Compare los valores de las métricas con los valores históricos para saber si hay tendencias que puedan indicar que algo necesita ser investigado. Algunos ejemplos son un aumento de la latencia, una reducción de la función empresarial principal y un aumento de las respuestas a los errores.
3. Compruebe si hay valores atípicos y anomalías en sus métricas, que pueden ocultarse mediante promedios o medianas. Examine los valores más altos y más bajos durante el periodo de tiempo e investigue las causas de las observaciones que exceden con creces los límites normales. Durante la eliminación de estas causas, podrá ajustar los límites métricos esperados en función de la mejora de la coherencia del rendimiento de sus cargas de trabajo.
4. Busque cambios bruscos en el comportamiento. Un cambio inmediato en la cantidad o en la dirección de una métrica podría indicar que se ha producido un cambio en la aplicación o factores externos que podrían necesitar la inclusión de métricas adicionales para su seguimiento.
5. Compruebe si la estrategia de supervisión actual sigue siendo relevante para la aplicación. Basándose en un análisis de incidentes anteriores (o en el marco de análisis de la resiliencia), evalúe si hay aspectos adicionales de la aplicación que deban incorporarse al ámbito de la supervisión.
6. Revise sus métricas de monitoreo de usuarios reales (RUM) para determinar si hay brechas en la cobertura de las funcionalidades de la aplicación.
7. Revise su proceso de administración de cambios. Actualice sus procedimientos si es necesario para incluir un paso de análisis de supervisión que deba realizarse antes de aprobar un cambio.
8. Implemente la supervisión y la revisión como parte de sus procesos de revisión de la preparación operativa y corrección de errores.

Recursos

Prácticas recomendadas relacionadas:

- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL06-BP02 Definición y cálculo de métricas (agregación)
- REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema
- REL12-BP02 Análisis después del incidente
- REL12-BP06 Planificación periódica de días de juego

Documentos relacionados:

- Why you should develop a correction of error (COE)
- Uso de paneles de Amazon CloudWatch
- La creación de paneles para la visibilidad operativa
- Advanced Multi-AZ Resilience Patterns - Gray failures
- Amazon CloudWatch Logs Insights Sample Queries
- Debugging with Amazon CloudWatch Synthetics and AWS X-Ray
- One Observability Workshop
- Amazon Builders' Library: Instrumentación de los sistemas distribuidos para obtener visibilidad operativa
- Uso de paneles de Amazon CloudWatch
- AWS Observability Best Practices
- Resilience analysis framework
- Marco de análisis de resiliencia: observabilidad
- Operational Readiness Review - ORR

REL06-BP07 Supervisión del seguimiento de las solicitudes de principio a fin en todo el sistema

Haga un seguimiento de las solicitudes a medida que se procesan a través de los componentes del servicio para que los equipos de producto puedan analizar y depurar los problemas con mayor facilidad y mejorar el rendimiento.

Resultado deseado: las cargas de trabajo con un seguimiento exhaustivo de todos los componentes son fáciles de depurar, lo que mejora el tiempo medio de recuperación (MTTR) de los errores y la latencia al simplificar la detección de la causa raíz. El rastreo integral reduce el tiempo necesario para descubrir los componentes afectados y analizar detalladamente las causas raíz de los errores o la latencia.

Patrones comunes de uso no recomendados:

- El rastreo se utiliza para algunos componentes, pero no para todos. Por ejemplo, si no se rastreara AWS Lambda, es posible que los equipos no entendieran con claridad la latencia que producen los arranques en frío en una carga de trabajo con picos.

- Los canarios sintéticos o la supervisión de usuarios reales (RUM) no tienen configurado el rastreo. Sin valores controlados ni RUM, la telemetría de interacción con el cliente se omite del análisis del rastreo, lo que da lugar a un perfil de rendimiento incompleto.
- Las cargas de trabajo híbridas incluyen herramientas de rastreo nativas en la nube y de terceros, pero no se han tomado medidas para integrar por completo una única solución de rastreo. En función de la solución de rastreo elegida, se deben utilizar SDK de rastreo nativos en la nube para instrumentar componentes que no sean nativos en la nube o se deben configurar herramientas de terceros para ingerir la telemetría de rastreo nativa en la nube.

Beneficios de establecer esta práctica recomendada: cuando los equipos de desarrollo reciben alertas sobre los problemas, ven una imagen completa de las interacciones entre los componentes del sistema, incluida la correlación componente por componente con el registro, el rendimiento y los errores. Dado que el rastreo facilita la identificación visual de las causas raíz, se dedica menos tiempo a investigar estas causas. Los equipos que conocen bien las interacciones de los componentes toman decisiones mejores y más rápidas a la hora de resolver problemas. Las decisiones, como cuándo invocar una conmutación por error de recuperación de desastres (DR) o cuál es la mejor forma de implementar las estrategias de autorreparación, se pueden mejorar mediante el análisis de los rastros de los sistemas y, en última instancia, puede mejorar la satisfacción del cliente con sus servicios.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Los equipos que utilizan aplicaciones distribuidas pueden utilizar herramientas de rastreo para establecer un identificador de correlación, recopilar rastros de las solicitudes y crear mapas de servicio de los componentes conectados. Todos los componentes de la aplicación deben incluirse en los rastros de solicitudes, como las puertas de enlace de middleware, los buses de eventos y los clientes del servicio, los componentes de computación y el almacenamiento, incluidos los almacenes de valores clave y las bases de datos. Incluya canarios sintéticos y la supervisión de usuarios reales en su configuración de rastreo integral para medir las interacciones y la latencia de los clientes remotos, de modo que pueda evaluar con precisión el rendimiento de sus sistemas en función de sus acuerdos y objetivos de nivel de servicio.

Puede utilizar AWS X-Ray y los servicios de instrumentación de supervisión de aplicaciones de Amazon CloudWatch para ofrecer una visión completa de las solicitudes a medida que pasan por la aplicación. X-Ray recopila la telemetría de las aplicaciones y le permite visualizarla y filtrarla

entre cargas útiles, funciones, rastros, servicios y API, y se puede activar para los componentes del sistema sin código o con poco código. La supervisión de aplicaciones de CloudWatch incluye ServiceLens para integrar sus rastros con métricas, registros y alarmas. La supervisión de aplicaciones de CloudWatch también incluye elementos sintéticos para supervisar los puntos de conexión y las API, así como la supervisión de usuarios reales para instrumentar los clientes de sus aplicaciones web.

Pasos para la implementación

- Use AWS X-Ray en todos los servicios nativos compatibles como Amazon S3, AWS Lambda y Amazon API Gateway. Estos servicios de AWS habilitan X-Ray con conmutadores de configuración que utilizan la infraestructura como código, AWS SDK o la Consola de administración de AWS.
- Aplicaciones de instrumento AWS Distro para OpenTelemetry y X-Ray o agentes recopiladores externos.
- Consulte la guía para desarrolladores de AWS X-Ray para obtener información sobre la implementación de lenguajes de programación específicos. En estas secciones de la documentación, se detalla cómo instrumentar las solicitudes HTTP, las consultas SQL y otros procesos específicos del lenguaje de programación de su aplicación.
- Utilice el rastreo de X-Ray para canarios de Amazon CloudWatch Synthetics y Amazon CloudWatch RUM para analizar la ruta de solicitud desde su cliente de usuario final hasta su infraestructura posterior de AWS.
- Configure métricas y alarmas de CloudWatch en función del estado de los recursos y la telemetría de canarios para que los equipos reciban alertas de los problemas rápidamente y, a continuación, puedan analizar en profundidad los rastros y los mapas de servicio con ServiceLens.
- Habilite la integración de X-Ray para herramientas de rastreo de terceros como Datadog, New Relic o Dynatrace si utiliza herramientas de terceros para su solución de rastreo principal.

Recursos

Prácticas recomendadas relacionadas:

- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores

Documentos relacionados:

- Qué es AWS X-Ray?
- Amazon CloudWatch: Application Monitoring
- Debugging with Amazon CloudWatch Synthetics and AWS X-Ray
- Amazon Builders' Library: Instrumentación de los sistemas distribuidos para obtener visibilidad operativa
- Integrating AWS X-Ray with other AWS services
- AWS Distro para OpenTelemetry y AWS X-Ray
- Amazon CloudWatch: Using synthetic monitoring
- Amazon CloudWatch: Use CloudWatch RUM
- Set up Amazon CloudWatch synthetics canary and Amazon CloudWatch alarm
- Availability and Beyond: Understanding and Improving the Resilience of Distributed Systems on AWS

Ejemplos relacionados:

- One Observability Workshop

Videos relacionados:

- AWS re:Invent 2022 - How to monitor applications across multiple accounts
- How to Monitor your AWS Applications

Herramientas relacionadas:

- AWS X-Ray
- Amazon CloudWatch
- Amazon Route 53

Diseño de su carga de trabajo para adaptarla a los cambios en la demanda

Una carga de trabajo escalable proporciona elasticidad para agregar o eliminar recursos automáticamente, de modo que se ajusten perfectamente a la demanda actual en cualquier momento dado.

Prácticas recomendadas

- REL07-BP01 Uso de la automatización al obtener o escalar recursos
- REL07-BP02 Obtención de recursos tras detectar un impedimento en una carga de trabajo
- REL07-BP03 Obtención de recursos tras detectar que se necesitan más recursos para una carga de trabajo
- REL07-BP04 Pruebas en su carga de trabajo

REL07-BP01 Uso de la automatización al obtener o escalar recursos

La fiabilidad en la nube se basa en aspectos clave como la definición programática, el aprovisionamiento y la administración de la infraestructura y los recursos. La automatización lo ayuda a optimizar el aprovisionamiento de recursos, facilitar las implementaciones coherentes y seguras y escalar los recursos en toda su infraestructura.

Resultado deseado: gestione su infraestructura como código (IaC). Define y mantiene su código de infraestructura en los sistemas de control de versiones (VCS). Puede delegar el aprovisionamiento de los recursos de AWS en mecanismos automatizados y aprovechar los servicios gestionados, como los grupos Equilibrador de carga de aplicación (ALB), Equilibrador de carga de red (NLB) y de escalado automático. Los recursos se aprovisionan mediante canalizaciones de integración y entrega continuas (CI/CD) para que los cambios de código inicien automáticamente las actualizaciones de los recursos, incluidas las actualizaciones de las configuraciones de escalado automático.

Patrones comunes de uso no recomendados:

- Los recursos se despliegan manualmente mediante la línea de comandos o la Consola de administración de AWS (también denominado click-ops).
- Combina estrechamente los componentes o los recursos de la aplicación y, como resultado, crea arquitecturas inflexibles.
- Implementa políticas de escalado inflexibles que no se adaptan a los cambiantes requisitos empresariales, a los patrones de tráfico o a los nuevos tipos de recursos.

- La capacidad se estima manualmente para satisfacer la demanda prevista.

Ventajas de establecer esta mejor práctica: la infraestructura como código (IaC) permite definir la infraestructura mediante programación. Esto ayuda a gestionar los cambios en la infraestructura durante el mismo ciclo de vida de desarrollo de software que los cambios en las aplicaciones, lo que promueve la coherencia y la repetibilidad y reduce el riesgo de realizar tareas manuales propensas a errores. Puede optimizar aún más el proceso de aprovisionamiento y actualización de los recursos mediante la implementación de la IaC con canalizaciones de entrega automatizadas. Puede implementar actualizaciones de infraestructura de manera fiable y eficiente sin necesidad de intervención manual. Esta agilidad es especialmente importante a la hora de escalar los recursos para satisfacer las demandas fluctuantes.

Puede lograr un escalado de recursos dinámico y automatizado junto con la IaC y las canalizaciones de entrega. Al monitorear las métricas clave y aplicar políticas de escalado predefinidas, el escalado automático puede aprovisionar o desaprovisionar recursos automáticamente según sea necesario, lo que mejora el rendimiento y la rentabilidad. Esto reduce la posibilidad de que se produzcan errores manuales o demoras en respuesta a los cambios en los requisitos de las aplicaciones o la carga de trabajo.

La combinación de IaC, canalizaciones de entrega automatizadas y escalado automático ayuda a las organizaciones a aprovisionar, actualizar y escalar sus entornos con confianza. Esta automatización es esencial para mantener una infraestructura en la nube con capacidad de respuesta, resiliente y gestionada de manera eficiente.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Para configurar la automatización con canalizaciones de CI/CD e infraestructura como código (IaC) para su arquitectura de AWS, elija un sistema de control de versiones como Git para almacenar las plantillas y la configuración de IaC. Estas plantillas se pueden escribir con herramientas como AWS CloudFormation. Para empezar, defina los componentes de su infraestructura (como las VPC de AWS, los grupos de Amazon EC2 Auto Scaling EC2 y las bases de datos de Amazon RDS) en estas plantillas.

A continuación, integre estas plantillas de IaC con una canalización de CI/CD para automatizar el proceso de implementación. AWS CodePipeline le ofrece una solución nativa de AWS perfecta, o puede utilizar otras soluciones de CI/CD de terceros. Cree una canalización que se active cuando

se produzcan cambios en su repositorio de control de versiones. Configure la canalización para que incluya etapas que analicen y validen sus plantillas de IaC, implementen la infraestructura en un entorno provisional, ejecuten pruebas automatizadas y, por último, las implementen en la producción. Incorpore los pasos de aprobación cuando sea necesario para mantener el control de los cambios. Esta canalización automatizada no solo acelera la implementación, sino que también facilita la coherencia y la fiabilidad en todos los entornos.

Configure el escalado automático de recursos como instancias de Amazon EC2, tareas de Amazon ECS y réplicas de bases de datos en su IaC para proporcionar escalado horizontal y escalado vertical automáticos según sea necesario. Esta estrategia mejora la disponibilidad y el rendimiento de las aplicaciones y optimiza los costes mediante el ajuste dinámico de los recursos en función de la demanda. Para obtener una lista de los recursos compatibles, consulte Amazon EC2 Auto Scaling y AWS Auto Scaling.

Pasos para la implementación

1. Cree y utilice un repositorio de código fuente para almacenar el código que controla la configuración de su infraestructura. Confirme los cambios en este repositorio para reflejar cualquier cambio en curso que desee realizar.
2. Seleccione una solución de infraestructura como código, por ejemplo, AWS CloudFormation, para mantener su infraestructura actualizada y detectar inconsistencias (desviaciones) con respecto al estado deseado.
3. Integre la plataforma IaC con la canalización de CI/CD para automatizar las implementaciones.
4. Determine y recopile las métricas adecuadas para el escalado automático de los recursos.
5. Configure el escalado automático de los recursos mediante políticas de escalado horizontal y vertical adecuadas para los componentes de la carga de trabajo. Plantéese la opción de utilizar el escalado programado para obtener patrones de uso predecibles.
6. Supervise las implementaciones para detectar errores y regresiones. Implemente mecanismos de reversión en su plataforma de CI/CD para revertir los cambios si es necesario.

Recursos

Documentos relacionados:

- AWS Auto Scaling: How Scaling Plans Work
- AWS Marketplace: productos que pueden usarse con escalado automático

- Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB
- Usar un equilibrador de carga con un grupo de escalado automático
- ¿Qué es AWS Global Accelerator?
- What Is Amazon EC2 Auto Scaling?
- Qué es AWS Auto Scaling?
- Qué es Amazon CloudFront?
- What is Amazon Route 53?
- Qué es Elastic Load Balancing?
- Qué es un equilibrador de carga de red?
- Qué es un equilibrador de carga de aplicación?
- Integrating Jenkins with AWS CodeBuild and AWS CodeDeploy
- Creating a four stage pipeline with AWS CodePipeline

Videos relacionados:

- Back to Basics: Deploy Your Code to Amazon EC2
- AWS Supports You | Starting Your Infrastructure as Code Solution Using AWS CloudFormation Templates
- Streamline Your Software Release Process Using AWS CodePipeline
- Monitor AWS Resources Using Amazon CloudWatch Dashboards
- Create Cross Account & Cross Region CloudWatch Dashboards | Amazon Web Services

REL07-BP02 Obtención de recursos tras detectar un impedimento en una carga de trabajo

Escale recursos de forma retroactiva cuando sea necesario si la disponibilidad se ve afectada para restaurar la disponibilidad de la carga de trabajo.

Primero debe configurar las comprobaciones de estado y los criterios de dichas comprobaciones para indicar cuándo se ve afectada la disponibilidad por falta de recursos. A continuación, notifique al personal pertinente para que escale manualmente el recurso o inicie la automatización, a fin de que el escalado se lleve a cabo de forma automática.

La escala puede ajustarse manualmente para su carga de trabajo (por ejemplo, se puede cambiar el número de instancias de EC2 en un grupo de escalado automático o se puede modificar el rendimiento de una tabla de DynamoDB mediante la Consola de administración de AWS o la AWS CLI). Sin embargo, la automatización debe usarse siempre que sea posible (consulte Usar la automatización al obtener o escalar recursos).

Resultado deseado: se inician las actividades de escalado (de forma automática o manual) para restablecer la disponibilidad al detectar un error o una experiencia del cliente degradada.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Implemente la observabilidad y la supervisión en todos los componentes de su carga de trabajo para supervisar la experiencia del cliente y detectar errores. Defina los procedimientos, manuales o automatizados, que escalan los recursos necesarios. Para obtener más información, consulte REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores.

Pasos para la implementación

- Defina los procedimientos, manuales o automatizados, que escalan los recursos requeridos.
  - Los procedimientos de escalado dependen de cómo estén diseñados los distintos componentes de la carga de trabajo.
  - Estos procedimientos también varían según la tecnología subyacente que se utilice.
    - Los componentes que utilizan AWS Auto Scaling pueden usar planes de escalado para configurar un conjunto de instrucciones para escalar los recursos. Si trabaja con AWS CloudFormation o agrega etiquetas a recursos de AWS, puede configurar planes de escalamiento para diferentes conjuntos de recursos por aplicación. Auto Scaling proporciona recomendaciones de estrategias de escalado personalizadas según cada recurso. Tras crear el plan de escalado, Auto Scaling combina el escalado dinámico y los métodos de escalado predictivos para ayudarle en su estrategia de escalado. Para obtener más información, consulte Cómo funcionan los planes de escalado.
    - Amazon EC2 Auto Scaling verifica que tenga el número correcto de instancias de Amazon EC2 disponibles para gestionar la carga de la aplicación. Crea colecciones de instancias EC2, denominadas grupo de escalado automático. Puede especificar el número mínimo y máximo de instancias en cada grupo de Auto Scaling y Amazon EC2 Auto Scaling garantiza que su grupo nunca tenga un tamaño por encima o por debajo de este límite. Para obtener más información, consulte ¿Qué es Amazon EC2 Auto Scaling?

- El escalado automático de Amazon DynamoDB usa el servicio Auto Scaling de aplicaciones de para ajustar de manera dinámica y automática la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para abastecer incrementos repentinos del tráfico sin limitaciones. Para obtener más información, consulte Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB.

Recursos

Prácticas recomendadas relacionadas:

- REL07-BP01 Uso de la automatización al obtener o escalar recursos
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores

Documentos relacionados:

- AWS Auto Scaling: How Scaling Plans Work
- Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB
- What Is Amazon EC2 Auto Scaling?

REL07-BP03 Obtención de recursos tras detectar que se necesitan más recursos para una carga de trabajo

Una de las características más valiosas de la computación en la nube es la capacidad de aprovisionar recursos de forma dinámica.

En los entornos informáticos tradicionales en las instalaciones, debe identificar y aprovisionar suficiente capacidad con antelación para atender los picos de demanda. Esto supone un problema porque resulta caro y supone un riesgo para la disponibilidad si se subestiman las necesidades de capacidad máxima de la carga de trabajo.

En la nube, no tiene que realizar esta acción. En su lugar, puede aprovisionar la capacidad de cómputo, la base de datos y otros recursos según sea necesario para satisfacer la demanda actual y prevista. Las soluciones automatizadas, como Amazon EC2 Auto Scaling y el escalamiento

automático de la aplicación, pueden poner los recursos en línea automáticamente en función de las métricas que especifique. Esto puede facilitar el proceso de escalado y hacerlo más predecible, así como mejorar la fiabilidad de su carga de trabajo al garantizar que haya recursos disponibles suficientes en todo momento.

Resultado deseado: configura el escalado automático de los recursos informáticos y otros recursos para satisfacer la demanda. Sus políticas de escalado ofrecen suficiente margen de maniobra para poder atender ráfagas de tráfico y, al mismo tiempo, poner en funcionamiento recursos adicionales.

Patrones comunes de uso no recomendados:

- Aprovisiona un número fijo de recursos escalables.
- Elige una métrica de escalado que no se correlaciona con la demanda real.
- No proporciona suficiente margen de maniobra en sus planes de escalado para adaptarse a las ráfagas de demanda.
- Sus políticas de escalado añaden capacidad demasiado tarde, lo que provoca el agotamiento de la capacidad y la degradación del servicio, a la vez que se ponen en línea recursos adicionales.
- No configura correctamente los recuentos de recursos mínimos y máximos, lo que provoca errores de escalado.

Ventajas de establecer esta práctica recomendada: disponer de recursos suficientes para satisfacer la demanda actual es fundamental para ofrecer una alta disponibilidad de la carga de trabajo y cumplir los objetivos de nivel de servicio (SLO) definidos. El escalado automático le permite proporcionar la cantidad adecuada de recursos informáticos, de bases de datos y de otro tipo que su carga de trabajo necesita para satisfacer la demanda actual y prevista. No es necesario determinar las necesidades de capacidad máxima ni asignar recursos de forma estática para atenderlas. En cambio, a medida que aumenta la demanda, puede asignar más recursos para adaptarla y, una vez que la demanda disminuya, puede desactivar los recursos para reducir los costes.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

En primer lugar, determine si el componente de la carga de trabajo es adecuado para el escalado automático. Estos componentes se denominan escalables horizontalmente porque proporcionan los mismos recursos y se comportan de forma idéntica. Entre los ejemplos de componentes escalables horizontalmente se incluyen las instancias de EC2 que están configuradas de forma similar, las tareas de Amazon Elastic Container Service (ECS) y los pods que se ejecutan en Amazon

Elastic Kubernetes Service (EKS). Estos recursos de cómputo suelen estar ubicados detrás de un equilibrador de carga y se denominan réplicas.

Otros recursos replicados pueden incluir réplicas de lectura de bases de datos, tablas de Amazon DynamoDB y clústeres de Amazon ElastiCache (Redis OSS). Para obtener una lista completa de los recursos admitidos, consulte los servicios de AWS que puede utilizar con el escalamiento automático de la aplicación.

En el caso de las arquitecturas basadas en contenedores, es posible que necesite escalar de dos maneras diferentes. En primer lugar, tal vez necesite escalar los contenedores que proporcionan servicios escalables horizontalmente. En segundo lugar, puede que necesite escalar los recursos informáticos para dejar espacio para nuevos contenedores. Existen diferentes mecanismos de escalado automático para cada capa. Para escalar las tareas de ECS, puede usar el escalamiento automático de la aplicación. Para escalar los pods de Kubernetes, puede usar el escalador automático de pods horizontal (HPA) o el escalado automático controlado por eventos de Kubernetes (KEDA). Para escalar los recursos de computación, puede usar los proveedores de capacidad para ECS o, para Kubernetes, puede usar Karpenter o el Cluster Autoscaler.

A continuación, seleccione cómo realizará el escalado automático. Hay tres opciones principales: el escalado basado en métricas, el escalado programado y el escalado predictivo.

Escalado basado en métricas

El escalado basado en métricas aprovisiona los recursos en función del valor de una o más métricas de escalado. Una métrica de escalado es aquella que corresponde a la demanda de su carga de trabajo. Una buena forma de determinar las métricas de escalado adecuadas es realizar pruebas de carga en un entorno que no sea de producción. Durante las pruebas de carga, mantenga fija la cantidad de recursos escalables y aumente lentamente la demanda (por ejemplo, el rendimiento, la simultaneidad o los usuarios simulados). A continuación, busque métricas que aumenten (o disminuyan) a medida que aumente la demanda y, a la inversa, que disminuyan (o aumenten) a medida que la demanda disminuya. Las métricas de escalado típicas incluyen el uso de la CPU, la profundidad de las colas de trabajo (como una cola de Amazon SQS), el número de usuarios activos y el rendimiento de la red.

> **Note**
>
> AWS ha observado que, en la mayoría de las aplicaciones, la utilización de la memoria aumenta a medida que la aplicación se calienta y, después, alcanza un valor estable. Cuando la demanda disminuye, la utilización de la memoria suele mantenerse elevada en

lugar de disminuir en consecuencia. Como la utilización de la memoria no se corresponde con la demanda en ambas direcciones (es decir, aumentando o disminuyendo según la demanda), piénseselo bien antes de seleccionar esta métrica para el escalado automático.

El escalado basado en métricas es una operación latente. Las métricas de utilización pueden tardar varios minutos en propagarse a los mecanismos de escalado automático y, por lo general, estos mecanismos esperan una señal clara de aumento de la demanda antes de reaccionar. Luego, a medida que el escalador automático crea nuevos recursos, es posible que tarde más tiempo en funcionar por completo. Por este motivo, es importante no fijar los objetivos de las métricas de escalado demasiado cerca de la plena utilización (por ejemplo, un 90 % de utilización de la CPU). Si lo hace, se corre el riesgo de agotar la capacidad de recursos existente antes de que se pueda poner en línea capacidad adicional. Los objetivos típicos de utilización de los recursos pueden oscilar entre el 50 % y el 70 % para lograr una disponibilidad óptima, en función de los patrones de demanda y del tiempo necesario para aprovisionar recursos adicionales.

Escalado programado

El escalado programado aprovisiona o elimina recursos según el calendario o la hora del día. Se usa con frecuencia para cargas de trabajo que tienen una demanda predecible, como los picos de uso durante el horario laboral de lunes a viernes o en eventos de ventas. Tanto Amazon EC2 Auto Scaling como el escalamiento automático de la aplicación admiten el escalado programado. El escalador cron de KEDA admite el escalado programado de los pods de Kubernetes.

Escalado predictivo

El escalado predictivo utiliza machine learning para escalar automáticamente los recursos en función de la demanda prevista. Analiza el valor histórico de la métrica de utilización que le proporcione y predice continuamente su valor futuro. A continuación, el valor previsto se utiliza para escalar el recurso hacia arriba o hacia abajo. Amazon EC2 Auto Scaling puede realizar un escalado predictivo.

Pasos para la implementación

1. En primer lugar, determine si el componente de la carga de trabajo es adecuado para el escalado automático.
2. Determine qué tipo de mecanismo de escalado es el más adecuado para la carga de trabajo: escalado basado en métricas, escalado programado o escalado predictivo.
3. Seleccione el mecanismo de escalado automático adecuado para el componente. Para instancias Amazon EC2, utilice Amazon EC2 Auto Scaling. Para otros servicios de AWS, utilice

el escalamiento automático de la aplicación. Para los pods de Kubernetes (como los que se ejecutan en un clúster de Amazon EKS), puede usar el escalador automático de pods horizontal (HPA) o el escalado automático controlado por eventos de Kubernetes (KEDA). Para los nodos de Kubernetes o EKS, puede usar Karpenter y Cluster Auto Scaler (CAS).

4. Para el escalado con métricas o programado, realice pruebas de carga para determinar las métricas de escalado y los valores objetivo adecuados para su carga de trabajo. Para el escalado programado, determine la cantidad de recursos necesarios en las fechas y horas que seleccione. Determine el número máximo de recursos necesarios para atender los picos de tráfico previstos.
5. Configure el escalador automático en función de la información recopilada anteriormente. Consulte la documentación del servicio de escalado automático para obtener información más detallada. Compruebe que los límites de escalado máximo y mínimo estén configurados correctamente.
6. Compruebe que la configuración de escalado funciona según lo esperado. Realice las pruebas de carga en un entorno que no sea de producción, observe cómo reacciona el sistema y haga los ajustes pertinentes. Cuando habilite el escalado automático en producción, configure las alarmas adecuadas para que le notifiquen cualquier comportamiento inesperado.

Recursos

Documentos relacionados:

- What Is Amazon EC2 Auto Scaling?
- Orientación normativa de AWS: aplicaciones de prueba de carga
- AWS Marketplace: productos que pueden usarse con escalado automático
- Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB
- Predictive Scaling for EC2, Powered by Machine Learning
- Scheduled Scaling for Amazon EC2 Auto Scaling
- Telling Stories About Little's Law

REL07-BP04 Pruebas en su carga de trabajo

Adopte una metodología de prueba de carga para medir si la actividad de escalado satisface los requisitos de la carga de trabajo.

Es importante llevar a cabo pruebas de carga sostenidas. Las pruebas de carga deben descubrir el punto de ruptura y probar el rendimiento de su carga de trabajo. AWS facilita la creación de entornos de prueba temporales que modelan la escala de su carga de trabajo de producción. En la nube, puede crear un entorno de prueba a escala de producción, completar sus pruebas y desmantelar los recursos. Debido a que solo paga por el entorno de prueba cuando se ejecuta, puede simular su entorno real por una fracción del costo de las pruebas en las instalaciones.

Las pruebas de carga en producción también deben considerarse como parte de los días de juegos en los que se estresa el sistema de producción, durante las horas de menor uso por parte de los clientes, con todo el personal a mano para interpretar los resultados y abordar cualquier problema que surja.

Patrones comunes de uso no recomendados:

- Hacer pruebas de carga en implementaciones que no tienen la misma configuración que su producción.
- Hacer pruebas de carga solo en elementos individuales de su carga de trabajo y no en toda la carga.
- Hacer pruebas de carga con un subconjunto de solicitudes y no con un conjunto representativo de solicitudes reales.
- Hacer pruebas de carga con un pequeño factor de seguridad por encima de la carga prevista.

Beneficios de establecer esta práctica recomendada: sabrá qué componentes de su arquitectura presentan errores bajo carga y podrá identificar qué métricas se deben vigilar para indicar que se está acercando a esa carga a tiempo para solucionar el problema, con lo que se evitará el impacto de ese error.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

- Haga pruebas de carga para identificar qué aspecto de su carga de trabajo indica que debe agregar o eliminar capacidad. Las pruebas de carga deben tener un tráfico representativo similar al que se recibe en producción. Aumente la carga mientras vigila las métricas que ha instrumentado para determinar qué métrica indica cuándo debe agregar o eliminar recursos.
  - Pruebas de carga distribuida en AWS: simular miles de usuarios conectados

- Identifique la combinación de solicitudes. Es posible que tenga una combinación variada de solicitudes, por lo que deberá tener en cuenta diversos periodos de tiempo a la hora de identificar la combinación de tráfico.
- Implemente un controlador de carga. Puede utilizar software de código personalizado, de código abierto o comercial para implementar un controlador de carga.
- Haga la prueba de carga inicialmente con una capacidad pequeña. Ve algunos efectos inmediatos al pasar la carga a una capacidad menor, posiblemente tan pequeña como una instancia o un contenedor.
- Lleve a cabo una prueba de carga con una capacidad mayor. Los efectos serán diferentes en una carga distribuida, por lo que debe efectuar las pruebas en un entorno lo más parecido al del producto.

Recursos

Documentos relacionados:

- Pruebas de carga distribuida en AWS: simular miles de usuarios conectados
- Aplicaciones de pruebas de carga

Videos relacionados:

- AWS Summit ANZ 2023: Accelerate with confidence through AWS Distributed Load Testing

Implementación de cambios

Los cambios controlados son necesarios para implementar nuevas funcionalidades y garantizar que las cargas de trabajo y el entorno operativo pongan en marcha software conocido debidamente revisado. Si estos cambios no se controlan, es difícil predecir su efecto o abordar los problemas que surjan a causa de ellos.

Otros patrones de implementación para minimizar el riesgo

Los indicadores de características (también conocidos como cambios de característica) son opciones de configuración de una aplicación. Puede implementar el software con una característica desactivada, para que los clientes no la vean. Luego puede activar la característica, como lo haría

para una implementación canario, o puede establecer el ritmo de cambio al 100 % para ver el efecto. Si la implementación tiene problemas, simplemente puede desactivar la característica sin restaurar.

Implementación por zonas aisladas de errores: una de las reglas más importantes que AWS ha establecido para sus propias implementaciones es evitar tocar múltiples zonas de disponibilidad dentro de una región al mismo tiempo. Esto es fundamental para garantizar que las zonas de disponibilidad sean independientes a los fines de nuestros cálculos de disponibilidad. Recomendamos que utilice consideraciones similares en las implementaciones.

Revisiones de preparación operativa (ORR)

AWS considera útil supervisar la preparación operativa para evaluar la integridad de las pruebas, la capacidad de supervisar y, lo que es más importante, la capacidad de auditar el rendimiento de las aplicaciones a sus SLA y proporcionar datos en caso de una interrupción u otra anomalía operativa. Se lleva a cabo una ORR formal antes de la implementación inicial de la producción. AWS repetirá las ORR periódicamente (una vez al año, o antes de los periodo de rendimiento crítico) para asegurarse de que no haya ningún desvío de las expectativas operacionales. Para obtener más información sobre la preparación operativa, consulte Pilar de excelencia operativa del Marco de AWS Well-Architected.

Prácticas recomendadas

- REL08-BP01 Uso de manuales de procedimientos para actividades estándar como la implementación
- REL08-BP02 Integración de las pruebas funcionales como parte de la implementación
- REL08-BP03 Integración de las pruebas de resiliencia como parte de la implementación
- REL08-BP04 Implementación mediante una infraestructura inmutable
- REL08-BP05 Implementación de cambios con automatización

REL08-BP01 Uso de manuales de procedimientos para actividades estándar como la implementación

Los manuales de procedimientos son procedimientos predefinidos para obtener resultados concretos. Use manuales de procedimientos para llevar a cabo actividades estándar manuales o automáticas. Algunos ejemplos incluyen implementar una carga de trabajo, aplicarle un parche a dicha carga de trabajo o hacer modificaciones de DNS.

Por ejemplo, establezca procesos para garantizar la seguridad de la reversión durante las implementaciones. Tener la garantía de poder dar marcha atrás en una implementación sin disrupciones para sus clientes es esencial a la hora de hacer que un servicio sea fiable.

Para los procedimientos del manual de procedimientos, comience con un proceso manual válido y efectivo, impleméntelo en código e invóquelo para que se ejecute automáticamente cuando corresponda.

Incluso en el caso de cargas de trabajo sofisticadas y altamente automatizadas, los manuales de procedimientos siguen siendo útiles para ejecutar los días de juego o para cumplir con los rigurosos requisitos de informes y auditoría.

Tenga en cuenta que los manuales de estrategias se usan en respuesta a incidentes específicos y los manuales de procedimientos se usan para conseguir resultados determinados. A menudo, los manuales de procedimientos son para actividades rutinarias, mientras que los manuales de estrategias se utilizan para responder a eventos no rutinarios.

Patrones comunes de uso no recomendados:

- Hacer cambios imprevistos en la configuración en producción.
- Omitir pasos del plan para que la implementación sea más rápida, lo que da lugar a una implementación errónea.
- Hacer cambios sin probar la revocación del cambio.

Beneficios de establecer esta práctica recomendada: la planificación eficaz de los cambios aumenta su capacidad de efectuar correctamente el cambio, ya que sabrá qué sistemas se verán afectados. Validar el cambio en los entornos de prueba aumenta la confianza.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

- Para obtener respuestas sistematizadas e inmediatas a eventos conocidos, documente los procedimientos en manuales de procedimientos.
- Use el principio de infraestructura como código para definir la infraestructura. Si usa AWS CloudFormation (o un tercero de confianza) para definir su infraestructura, puede utilizar software de control de versiones para crear versiones y hacer un seguimiento de los cambios.
  - Use AWS CloudFormation (o un proveedor tercero de confianza) para definir su infraestructura.

    - Qué es AWS CloudFormation?
- Cree plantillas singulares y desacopladas mediante buenos principios de diseño de software.
    - Determine los permisos, las plantillas y las partes responsables de su implementación.
        - Control de acceso con AWS Identity and Access Management
    - Utilice un sistema de administración de código fuente alojado basado en una tecnología popular como Git para almacenar el código fuente y la configuración de infraestructura como código (IaC).

Recursos

Documentos relacionados:

- Socio de APN: socios que pueden ayudarle a crear soluciones de implementación automatizadas
- AWS Marketplace: productos que pueden usarse para automatizar sus implementaciones
- Qué es AWS CloudFormation?

Ejemplos relacionados:

- Automating operations with Playbooks and Runbooks

REL08-BP02 Integración de las pruebas funcionales como parte de la implementación

Utilice técnicas como las pruebas unitarias y las pruebas de integración que validen la funcionalidad requerida.

Las pruebas unitarias son un proceso en el que se prueba la unidad funcional de código más pequeña para validar su comportamiento. Las pruebas de integración sirven para validar que cada característica de la aplicación funcione de acuerdo con los requisitos del software. Mientras que las pruebas unitarias se centran en probar parte de una aplicación de forma aislada, las pruebas de integración tienen en cuenta los efectos secundarios (por ejemplo, el efecto de la modificación de los datos mediante una operación de mutación). En cualquier caso, las pruebas se deben integrar en una canalización de implementación y, si no se cumplen los criterios de éxito, la canalización se detiene o se revierte. Estas pruebas se llevan a cabo en un entorno de preproducción, que se lleva a cabo antes de la producción en la canalización.

Los mejores resultados se obtienen cuando estas pruebas se ejecutan automáticamente como parte de las acciones de creación e implementación. Por ejemplo, con AWS CodePipeline, los desarrolladores confirman los cambios en un repositorio de origen, donde CodePipeline detecta automáticamente los cambios. Se crea la aplicación y se ejecutan las pruebas unitarias. Una vez completadas las pruebas unitarias, el código compilado se implementa en servidores de ensayo para su comprobación. En el servidor de ensayo, CodePipeline ejecuta pruebas adicionales, como pruebas de integración o carga. Una vez completadas correctamente estas pruebas, CodePipeline implementa el código probado y aprobado en instancias de producción.

Resultado deseado: utiliza la automatización para realizar pruebas unitarias y de integración a fin de validar que el código se comporta según lo previsto. Estas pruebas se integran en el proceso de implementación y, en caso de fallo de una prueba, se interrumpe la implementación.

Patrones comunes de uso no recomendados:

- Durante el proceso de implementación, se ignoran u omiten los errores y planes de las pruebas para acelerar el cronograma de implementación.
- Las pruebas se hacen manualmente fuera de la canalización de implementación.
- Omite los pasos de prueba de la automatización mediante flujos de trabajo de emergencia manuales.
- Las pruebas automatizadas se ejecutan en un entorno que no se parece mucho al entorno de producción.
- Crea un conjunto de pruebas que no es lo suficientemente flexible y que es difícil de mantener, actualizar o escalar a medida que la aplicación evoluciona.

Beneficios de establecer esta práctica recomendada: las pruebas automatizadas durante el proceso de implementación detectan los problemas de forma temprana, lo que reduce el riesgo de que se lance a producción con errores o un comportamiento inesperado. Las pruebas unitarias validan que el código se comporte como se desea y que se cumplan los contratos de la API. Las pruebas de integración validan que el sistema funcione de acuerdo con los requisitos especificados. Estos tipos de pruebas verifican de manera sistemática el orden de funcionamiento previsto de los componentes, como las interfaces de usuario, las API, las bases de datos y el código fuente.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Adopte una estrategia de desarrollo basada en pruebas (TDD) para desarrollar software que incluya casos de prueba para especificar y validar el código. Para empezar, cree casos de prueba para cada función. Si la prueba falla, escriba un código nuevo para superarla. Este enfoque ayuda a validar el resultado esperado de cada función. Ejecute pruebas unitarias y valide que se aprueben antes de enviar el código a un repositorio de código fuente.

Implemente pruebas unitarias o de integración como parte de las etapas de compilación, prueba e implementación de la canalización de CI/CD. Automatice las pruebas e inicie las pruebas automáticamente cada vez que haya una nueva versión de la aplicación lista para su implementación. Si no se satisfacen los criterios de éxito, la canalización se detiene o se revierte.

Si la aplicación es una aplicación web o móvil, realice pruebas de integración automatizadas en varios navegadores de escritorio o dispositivos reales. Este enfoque es particularmente útil para validar la compatibilidad y la funcionalidad de las aplicaciones móviles en una amplia gama de dispositivos.

Pasos para la implementación

1. Escriba pruebas unitarias antes de desarrollar código funcional (desarrollo basado en pruebas o TDD). Establezca pautas de código para que escribir y ejecutar pruebas unitarias sea un requisito de codificación no funcional.
2. Cree un conjunto de pruebas de integración automatizadas que cubran las funcionalidades comprobables identificadas. Estas pruebas deben simular las interacciones de los usuarios y validar los resultados esperados.
3. Cree el entorno de pruebas necesario para ejecutar las pruebas de integración. Esto puede incluir entornos de preparación o preproducción que imiten fielmente el entorno de producción.
4. Configuración de las etapas de origen, compilación, prueba e implementación mediante la consola de AWS CodePipeline o la AWS Command Line Interface (CLI).
5. Implemente la aplicación una vez que se haya creado y probado el código. AWS CodeDeploy puede implementarlo en sus entornos de puesta en escena (pruebas) y producción. Estos entornos pueden incluir instancias de Amazon EC2, funciones de AWS Lambda o servidores en las instalaciones. Se debe usar el mismo mecanismo de implementación para implementar la aplicación en todos los entornos.
6. Monitoree el progreso de la canalización y del estado de cada etapa. Utilice controles de calidad para bloquear la canalización en función del estado de las pruebas. También puede recibir

notificaciones cuando se produzca un fallo en una etapa de canalización o cuando se haya completado la canalización.

7. Supervise continuamente los resultados de las pruebas y busque patrones, regresiones o áreas que requieran más atención. Utilice esta información para mejorar el conjunto de pruebas, identificar las áreas de la aplicación que necesitan pruebas más sólidas y optimizar el proceso de implementación.

Recursos

Prácticas recomendadas relacionadas:

- REL07-BP04 Pruebas en su carga de trabajo
- REL08-BP03 Integración de las pruebas de resiliencia como parte de la implementación
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Documentos relacionados:

- Guía prescriptiva de AWS: automatización de pruebas
- Integración y entrega continuas
- Indicators for functional testing
- Monitorear canalizaciones
- Use AWS CodePipeline with AWS CodeBuild to test code and run builds
- AWS Device Farm

REL08-BP03 Integración de las pruebas de resiliencia como parte de la implementación

Para integrar las pruebas de resiliencia, cree fallos en el sistema de forma intencionada para medir su capacidad en caso de situaciones disruptivas. Las pruebas de resiliencia son diferentes de las pruebas unitarias y funcionales que suelen estar integradas en los ciclos de implementación, ya que se centran en la identificación de fallos imprevistos en el sistema. Aunque es seguro comenzar con la integración de pruebas de resiliencia en la fase de preproducción, fíjese el objetivo de implementar estas pruebas en producción como parte de sus días de juegos.

Resultado deseado: las pruebas de resiliencia ayudan a generar confianza en la capacidad del sistema para resistir la degradación en la producción. Los experimentos identifican los puntos débiles que podrían provocar fallos, lo que le ayuda a mejorar su sistema para mitigar de manera automática y eficiente los fallos y la degradación.

Patrones comunes de uso no recomendados:

- Falta de observabilidad y supervisión en los procesos de implementación
- Confianza en las personas para resolver fallos del sistema
- Mecanismos de análisis de mala calidad
- Centrarse en los problemas conocidos de un sistema y falta de experimentación para identificar cualquier elemento desconocido
- Identificación de fallos, pero sin ninguna resolución
- Falta de documentación de los resultados y manuales de procedimientos

Beneficios de establecer prácticas recomendadas: las pruebas de resiliencia integradas en las implementaciones ayudan a identificar problemas desconocidos en el sistema que, de otro modo, pasarían desapercibidos y que pueden provocar tiempos de inactividad en la producción. La identificación de estos elementos desconocidos en un sistema le ayuda a documentar los resultados, integrar las pruebas en su proceso de CI/CD y crear manuales de procedimientos, lo que simplifica la mitigación mediante mecanismos eficientes y repetibles.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Los formularios de pruebas de resiliencia más comunes que se pueden integrar en las implementaciones de su sistema son la recuperación de desastres y la ingeniería del caos.

- Incluya actualizaciones en sus planes de recuperación de desastres y procedimientos operativos estándar (SOP) en cualquier implementación importante.
- Integre las pruebas de fiabilidad en sus canalizaciones de implementación automatizadas. Estos servicios, como AWS Resilience Hub, se pueden integrar en su canalización de CI/CD para establecer evaluaciones de resiliencia continuas que se evalúen automáticamente como parte de cada implementación.
- Defina sus aplicaciones en AWS Resilience Hub. Las evaluaciones de resiliencia generan fragmentos de código que le ayudan a crear procedimientos de recuperación como documentos

de AWS Systems Manager para sus aplicaciones y proporcionan una lista de monitores y alarmas recomendados de Amazon CloudWatch.

- Una vez actualizados los planes de recuperación de desastres y los procedimientos operativos estándar, lleve a cabo las pruebas de recuperación de desastres para verificar que sean efectivos. Las pruebas de recuperación de desastres le ayudan a determinar si puede restaurar el sistema después de un evento y recuperar el funcionamiento normal. Puede simular varias estrategias de recuperación de desastres e identificar si su planificación es suficiente para cumplir sus requisitos de tiempo de actividad. Las estrategias comunes de recuperación de desastres incluyen copias de seguridad y restauración, el enfoque de luz piloto, la espera en frío, la espera semiactiva, la espera activa y la estrategia activa-activa, y todas difieren en costo y complejidad. Antes de llevar a cabo las pruebas de recuperación de desastres, le recomendamos que defina su objetivo de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO) para simplificar la elección de la estrategia que desee simular. AWS ofrece herramientas de recuperación de desastres, como AWS Elastic Disaster Recovery, que le ayudarán a empezar con la planificación y las pruebas.
- Los experimentos de ingeniería del caos introducen disrupciones en el sistema, como cortes de la red y fallos del servicio. Al ejecutar simulaciones con fallos controlados, puede descubrir las vulnerabilidades de su sistema y, al mismo tiempo, contener la repercusión de los fallos inyectados. Al igual que las demás estrategias, ejecute simulaciones de fallas controladas en entornos que no sean de producción utilizando servicios como AWS Fault Injection Service para ganar confianza antes de implementarlos en producción.

Recursos

Documentos relacionados:

- Experiment with failure using resilience testing to build recovery preparedness
- Continually assessing application resilience with AWS Resilience Hub and AWS CodePipeline
- Disaster recovery (DR) architecture on AWS, part 1: Strategies for recovery in the cloud
- Verify the resilience of your workloads using Chaos Engineering
- Principios de la ingeniería del caos
- Chaos Engineering Workshop

Videos relacionados:

- AWS re:Invent 2020: Testing Resilience using Chaos Engineering

- Improve Application Resilience with AWS Fault Injection Service
- Prepare & Protect Your Applications From Disruption With AWS Resilience Hub

REL08-BP04 Implementación mediante una infraestructura inmutable

La infraestructura inmutable es un modelo que exige que no haya actualizaciones, parches de seguridad ni cambios de configuración en las cargas de trabajo de producción. Cuando es necesario aplicar un cambio, la arquitectura se integra en una nueva infraestructura y se implementa en producción.

Utilice una estrategia de implementación de infraestructura inmutable para aumentar la fiabilidad, la coherencia y la reproducibilidad de las implementaciones de sus cargas de trabajo.

Resultado deseado: con una infraestructura inmutable, no se permiten modificaciones in situ para ejecutar los recursos de infraestructura dentro de una carga de trabajo. En su lugar, cuando es necesario hacer un cambio, se implementa en paralelo un nuevo conjunto de recursos de infraestructura actualizados que contienen todos los cambios que es necesario aplicar en los recursos existentes. Esta implementación se valida automáticamente y, si se efectúa correctamente, el tráfico se desplaza gradualmente al nuevo conjunto de recursos.

Esta estrategia de implementación se aplica a las actualizaciones de software, las revisiones de seguridad, los cambios de infraestructura, las actualizaciones de la configuración y las actualizaciones de las aplicaciones, entre otros.

Patrones comunes de uso no recomendados:

- Implementar cambios in situ en los recursos de infraestructura en ejecución.

Beneficios de establecer esta práctica recomendada:

- Mayor coherencia entre los entornos: dado que no hay diferencias en los recursos de infraestructura entre los entornos, la coherencia aumenta y las pruebas se simplifican.
- Reducción de las desviaciones de la configuración: al sustituir los recursos de infraestructura por una configuración conocida y controlada por versiones, la infraestructura se define en un estado conocido, probado y fiable, lo que evita desviaciones de la configuración.
- Implementaciones atómicas fiables: las implementaciones se completan correctamente o no cambia nada, lo que aumenta la coherencia y la fiabilidad del proceso de implementación.

- Implementaciones simplificadas: las implementaciones se simplifican porque no tienen que admitir actualizaciones. Las actualizaciones son simplemente nuevas implementaciones.
- Implementaciones más seguras con procesos de restauración y recuperación rápidos: las implementaciones son más seguras porque no se modifica la versión operativa anterior. Puede restaurarla si se detecta algún error.
- Mejora de la posición de seguridad: al no permitir cambios en la infraestructura, se pueden deshabilitar los mecanismos de acceso remoto (como SSH). Esto reduce el vector de ataque y mejora la posición de seguridad de su organización.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Automation

A la hora de definir una estrategia de implementación de infraestructura inmutable, se recomienda utilizar la automatización en la medida de lo posible para aumentar la reproducibilidad y minimizar la posibilidad de que se cometan errores humanos. Para obtener más información, consulte REL08-BP05 Implementación de cambios con automatización y Automatización de implementaciones seguras y sin intervención.

Con la infraestructura como código (IaC), los pasos de aprovisionamiento, orquestación e implementación de la infraestructura se definen de forma programática, descriptiva y declarativa y se almacenan en un sistema de control de código fuente. El uso de la infraestructura como código simplifica la automatización de la implementación de la infraestructura y ayuda a lograr la inmutabilidad de la infraestructura.

Patrones de implementación

Cuando es necesario hacer un cambio en la carga de trabajo, la estrategia inmutable de implementación de la infraestructura requiere la implementación de un nuevo conjunto de recursos de infraestructura que incluya todos los cambios necesarios. Es importante que este nuevo conjunto de recursos siga un patrón de implementación que minimice la repercusión en los usuarios. Hay dos estrategias principales para esta implementación:

Implementación canario: práctica que consiste en dirigir a un número reducido de clientes a la nueva versión, que normalmente se ejecuta en una instancia de servicio único (canario). A continuación, puede analizar en profundidad los errores o los cambios en el comportamiento que se hayan

generado. Puede eliminar el tráfico del canario si encuentra problemas críticos y enviar a los usuarios de vuelta a la versión anterior. Si la implementación se lleva a cabo correctamente, puede continuar implementando a la velocidad deseada y, al mismo tiempo, supervisar los cambios para detectar errores, hasta que esté completamente implementada. AWS CodeDeploy se puede configurar con una configuración de implementación que permita una implementación canario.

Implementación azul/verde: similar a la implementación canario, excepto que se implementa en paralelo una flota completa de la aplicación. Alterne sus implementaciones en las dos pilas (azul y verde). Una vez más, puede enviar tráfico a la nueva versión y volver a la versión anterior si observa problemas con la implementación. Por lo general, todo el tráfico se conmuta a la vez, pero también puede utilizar fracciones del tráfico en cada versión para acelerar la adopción de la nueva versión mediante las capacidades de enrutamiento de DNS ponderado de Amazon Route 53. AWS CodeDeploy y AWS Elastic Beanstalk se pueden establecer con una configuración de implementación que permita una implementación azul/verde.

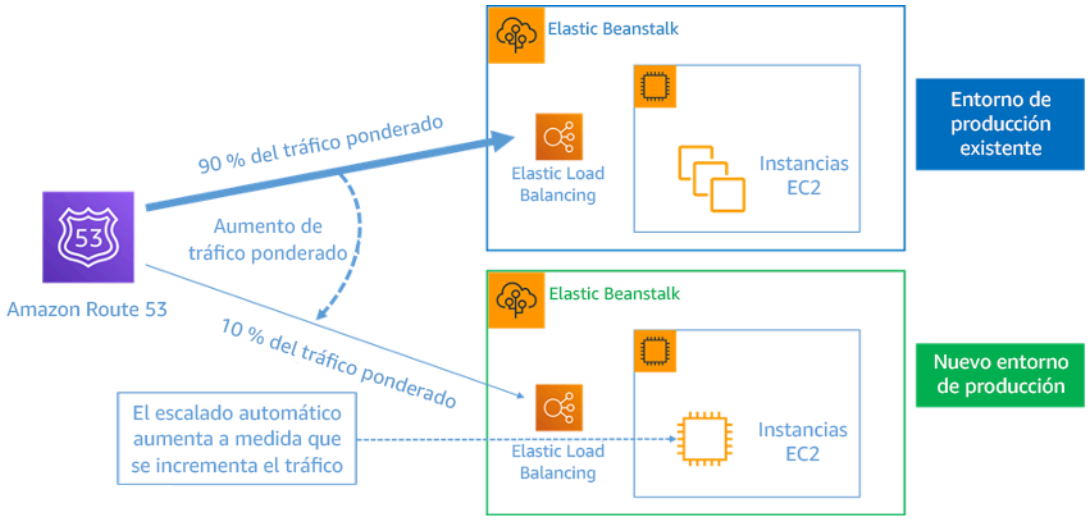


Figura 8: implementación azul/verde con AWS Elastic Beanstalk y Amazon Route 53

Detección de desviaciones

La desviación se define como cualquier cambio que provoque que un recurso de infraestructura tenga un estado o una configuración diferentes a los esperados. Cualquier tipo de cambio de configuración no administrado va en contra de la noción de infraestructura inmutable y debe detectarse y remediarse para que la infraestructura inmutable se implemente correctamente.

Pasos para la implementación

- No permita que se hagan modificaciones in situ de los recursos de la infraestructura en ejecución.

  - Puede usar AWS Identity and Access Management (IAM) para especificar quién o qué puede acceder a los servicios y recursos de AWS, administrar de forma centralizada los permisos detallados y analizar el acceso para refinar los permisos en AWS.
- Automatice la implementación de los recursos de la infraestructura para aumentar la reproducibilidad y minimizar la posibilidad de que se cometan errores humanos.
  - Como se describe en el documento técnico de introducción a DevOps en AWS, la automatización es la piedra angular de los servicios de AWS y es compatible internamente con todos los servicios, características y ofertas.
  - Preprocesar la Imagen de máquina de Amazon (AMI) puede acelerar el tiempo de lanzamiento. El Generador de imágenes de EC2 es un servicio totalmente administrado de AWS que le ayuda a automatizar la creación, el mantenimiento, la validación, el uso compartido y la implementación de AMI personalizadas, seguras y actualizadas para Linux o Windows.
  - Estos son algunos de los servicios que permiten la automatización:
    - AWS Elastic Beanstalk es un servicio para implementar y escalar rápidamente aplicaciones web desarrolladas con Java, .NET, PHP, Node.js, Python, Ruby, Go y Docker en servidores conocidos como, por ejemplo, Apache, NGINX, Passenger e IIS.
    - AWS Proton ayuda a los equipos de plataformas a conectar y coordinar todas las herramientas que sus equipos de desarrollo necesitan para el aprovisionamiento de infraestructuras, la implementación de código, la supervisión y las actualizaciones. AWS Proton permite una infraestructura automatizada, como el aprovisionamiento de código y la implementación de aplicaciones basadas en contenedores y sin servidor.
  - Usar la infraestructura como código facilita la automatización de su implementación y ayuda a lograr que sea inmutable. AWS proporciona servicios que permiten crear, implementar y mantener la infraestructura de forma programática, descriptiva y declarativa.
    - AWS CloudFormation ayuda a los desarrolladores a crear recursos de AWS de manera ordenada y predecible. Los recursos se escriben en archivos de texto en formato JSON o YAML. Las plantillas requieren una sintaxis y una estructura específicas que dependen de los tipos de recursos que se crean y administran. Los recursos se crean en JSON o YAML con cualquier editor de código, se registran en un sistema de control de versiones y, a continuación, CloudFormation crea los servicios especificados de una forma segura y repetible.
    - AWS Serverless Application Model (AWS SAM) es un marco de código abierto que se puede utilizar para crear aplicaciones sin servidor en AWS. AWS SAM se integra con otros servicios de AWS y es una extensión de CloudFormation.

  - Kit de desarrollo de la nube de AWS (AWS CDK) es un marco de desarrollo de software de código abierto para modelar y aprovisionar los recursos de sus aplicaciones en la nube mediante lenguajes de programación conocidos. Puede usar AWS CDK para modelar la infraestructura de las aplicaciones mediante TypeScript, Python, Java y .NET. AWS CDK utiliza CloudFormation en segundo plano para aprovisionar recursos de una forma segura y repetible.
  - API de control de nube de AWS presenta un conjunto común de API de creación, lectura, actualización, eliminación y enumeración (CRUDL) que ayudan a los desarrolladores a administrar su infraestructura en la nube de forma sencilla y coherente. Las API comunes de la API de control en la nube permiten a los desarrolladores administrar de manera uniforme el ciclo de vida de los servicios de AWS y de terceros.
- Aplique patrones de implementación que tengan la mínima repercusión en los usuarios.
  - Implementaciones canario:
    - Configuración de una implementación de un lanzamiento canario de API Gateway
    - Create a pipeline with canary deployments for Amazon ECS using AWS App Mesh
  - Implementaciones azul/verde: en el documento técnico sobre implementaciones azul/verde en AWS se describen técnicas de ejemplo para implementar estrategias de implementación azul/verde.
- Detecte desviaciones de la configuración o el estado. Para obtener más detalles, consulte Detectar cambios de configuración no administrados en pilas y recursos con detección de derivación.

Recursos

Prácticas recomendadas relacionadas:

- REL08-BP05 Implementación de cambios con automatización

Documentos relacionados:

- Automatización de implementaciones seguras y sin intervención
- Leveraging AWS CloudFormation to create an immutable infrastructure at Nubank
- Infraestructura como código
- Implementing an alarm to automatically detect drift in AWS CloudFormation stacks

Videos relacionados:

- AWS re:Invent 2020: Reliability, consistency, and confidence through immutability

REL08-BP05 Implementación de cambios con automatización

Las implementaciones y la aplicación de revisiones se automatizan para eliminar su impacto negativo.

Los cambios en los sistemas de producción son una de las mayores áreas de riesgo para muchas organizaciones. Consideramos que las implementaciones son un problema de primer orden que se debe resolver junto con los problemas empresariales que aborda nuestro software. Hoy en día, esto significa usar automatización en las operaciones siempre que resulte práctico, incluidas las pruebas y la implementación de cambios, la incorporación o eliminación de capacidad y la migración de datos.

Resultado deseado: incorpore la seguridad de la implementación automatizada en el proceso de lanzamiento con extensas pruebas de preproducción, reversiones automáticas e implementaciones de producción escalonadas. Esta automatización minimiza la posible repercusión en producción causada por implementaciones fallidas. Además, los desarrolladores ya no tienen que vigilar activamente las implementaciones en producción.

Patrones comunes de uso no recomendados:

- Los cambios se hacen de forma manual.
- Se salta los pasos de la automatización mediante flujos de trabajo de emergencia manuales.
- No sigue los planes y procesos establecidos en favor de plazos más rápidos.
- Lleva a cabo implementaciones de seguimiento rápidas sin dejar tiempo de incorporación.

Beneficios de establecer esta práctica recomendada: al utilizar la automatización para implementar todos los cambios, se elimina la posibilidad de que se produzcan errores humanos y se ofrece la posibilidad de llevar a cabo pruebas antes de cambiar de producción. Al llevar a cabo este proceso antes de la fase de producción, se verifica que los planes estén completos. Además, con la reversión automática al proceso de lanzamiento, se pueden identificar los problemas de producción y devolver la carga de trabajo a su estado operativo anterior.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Automatice su canalización de implementación. Las canalizaciones de implementación le permiten invocar pruebas automatizadas, detectar anomalías y detener la canalización en un paso determinado antes de la implementación en producción o revertir automáticamente un cambio. Una parte integral de esto es la adopción de la cultura de integración continua e implementación/entrega continua (CI/CD), en la que la confirmación o el cambio de código pasan por varias etapas automatizadas, desde las etapas de creación y prueba hasta la implementación en entornos de producción.

Aunque la sabiduría convencional sugiere que mantenga a las personas informadas sobre los procedimientos operativos más difíciles, le recomendamos que automatice los procedimientos más difíciles por esa misma razón.

Pasos para la implementación

Siga estos pasos de automatización de las implementaciones para eliminar las operaciones manuales:

- Configure un repositorio de código para almacenar su código de forma segura: utilice un sistema de administración de código fuente alojado basado en una tecnología popular como Git para almacenar el código fuente y la configuración de infraestructura como código (IaC).
- Configuración de un servicio de integración continua para compilar el código fuente, ejecución de pruebas y creación de artefactos de implementación: para configurar un proyecto de compilación con este fin, consulte Getting started with AWS CodeBuild using the console.
- Configuración de un servicio de implementación que automatice las implementaciones de aplicaciones y gestione la complejidad de las actualizaciones de las aplicaciones sin depender de implementaciones manuales propensas a errores: AWS CodeDeploy automatiza las implementaciones de software en múltiples servicios de computación, como Amazon EC2, AWS Fargate, AWS Lambda y sus servidores en las instalaciones. Para configurar estos pasos, consulte Getting started with CodeDeploy.
- Configuración de un servicio de entrega continua que automatice las canalizaciones de lanzamiento para lograr actualizaciones de infraestructuras y aplicaciones más rápidas y fiables: considere usar AWS CodePipeline para automatizar las canalizaciones de lanzamiento. Para obtener más información, consulte CodePipeline tutorials.

Recursos

Prácticas recomendadas relacionadas:

- OPS05-BP04 Uso de sistemas de administración de compilación e implementación
- OPS05-BP10 Automatización completa de la integración y la implementación
- OPS06-BP02 Implementaciones de prueba
- OPS06-BP04 Automatización de las pruebas y la reversión

Documentos relacionados:

- Continuous Delivery of Nested AWS CloudFormation Stacks Using AWS CodePipeline
- Socio de APN: socios que pueden ayudarle a crear soluciones de implementación automatizadas
- AWS Marketplace: productos que pueden usarse para automatizar sus implementaciones
- Automate chat messages with webhooks.
- Amazon Builders' Library: Asegurar la seguridad en las restauraciones durante las implementaciones
- Amazon Builders' Library: Evolución más rápida con la entrega continua
- Qué es AWS CodePipeline?
- What Is CodeDeploy?
- AWS Systems Manager Patch Manager
- What is Amazon SES?
- What is Amazon Simple Notification Service?

Videos relacionados:

- AWS Summit 2019: CI/CD on AWS

Administración de errores

> Los fallos son un hecho y, con el tiempo, todo fallará: desde los enrutadores hasta los discos duros, desde los sistemas operativos hasta las unidades de memoria que corrompen los paquetes TCP, desde los errores transitorios hasta los fallos permanentes. Esto es un hecho, ya sea que utilice hardware de la más alta calidad o los componentes más económicos: Werner Vogels, CTO, Amazon.com

Los fallos de componentes de hardware de bajo nivel son algo que hay que solucionar todos los días en un centro de datos en las instalaciones. Sin embargo, en la nube, debe protegerse contra la mayoría de estos tipos de errores. Por ejemplo, los volúmenes de Amazon EBS se colocan en una zona de disponibilidad específica, donde se replican automáticamente para protegerle en caso de error de un solo componente. Todos los volúmenes de EBS están diseñados para tener una disponibilidad del 99,999 %. Los objetos de Amazon S3 se almacenan en un mínimo de tres zonas de disponibilidad, lo que proporciona una durabilidad del 99,999999999 % durante un año natural. Independientemente del proveedor de servicios en la nube, existe la posibilidad de que los fallos afecten a su carga de trabajo. Por lo tanto, debe tomar medidas para implementar la resiliencia si necesita que su carga de trabajo sea fiable.

Un requisito previo para aplicar las prácticas que se analizan aquí es asegurarse de que las personas que diseñan, implementan y operan sus cargas de trabajo conozcan los objetivos empresariales y los objetivos de fiabilidad necesarios para lograrlos. Estas personas deben conocer estos requisitos de fiabilidad y haber recibido la formación para cumplir con ellos.

En las siguientes secciones se explican las prácticas recomendadas para gestionar los fallos y evitar que afecten a la carga de trabajo.

Temas

- Copia de seguridad de los datos
- Uso del aislamiento de errores para proteger su carga de trabajo
- Diseño de la carga de trabajo para que tolere los errores de los componentes
- Pruebas de fiabilidad
- Planificación de la recuperación de desastres (DR)

Copia de seguridad de los datos

Haga copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).

Prácticas recomendadas

- REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes
- REL09-BP02 Protección y cifrado de copias de seguridad
- REL09-BP03 Copias de seguridad automáticas de los datos
- REL09-BP04 Recuperación periódica de los datos para verificar la integridad de la copia de seguridad y los procesos

REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes

Comprenda y use las funciones de copia de seguridad de los servicios y recursos de datos usados por la carga de trabajo. La mayoría de los servicios ofrecen capacidades para crear copias de seguridad de los datos de la carga de trabajo.

Resultado deseado: se han identificado y clasificado los orígenes de datos según su criticidad. A continuación, establezca una estrategia de recuperación de datos basada en el RPO. Esta estrategia supone crear una copia de seguridad de estos orígenes de datos o tener la capacidad de reproducir datos desde otros orígenes. En el caso de pérdida de datos, la estrategia implementada permite recuperar o reproducir los datos dentro de los RPO y RTO definidos.

Fase de madurez de la nube: básica

Patrones comunes de uso no recomendados:

- No ser consciente de todos los orígenes de datos de la carga de trabajo y su nivel de gravedad.
- No crear copias de seguridad de los orígenes de datos críticos.
- Crear copias de seguridad solamente de algunos orígenes de datos sin usar la criticidad como criterio.

- RPO sin definir o una frecuencia de copias de seguridad que no puede ajustarse al RPO.
- No evaluar si una copia de seguridad es necesaria o si se pueden reproducir datos desde otros orígenes.

Beneficios de establecer esta práctica recomendada: identificar los lugares en los que se necesitan copias de seguridad e implementar un mecanismo para crearlas, o poder reproducir los datos desde un origen externo, mejora la capacidad de restaurar y recuperar los datos durante una interrupción.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Todos los almacenes de datos de AWS ofrecen capacidades de copia de seguridad. En los servicios como Amazon RDS y Amazon DynamoDB también se pueden hacer copias de seguridad automatizadas, lo que facilita la recuperación en un momento dado (PITR). De este modo, podrá restaurar una copia de seguridad a cualquier momento hasta cinco minutos (o menos) antes del momento actual. Muchos servicios de AWS ofrecen la posibilidad de copiar las copias de seguridad a otra Región de AWS. AWS Backup es una herramienta que le permite centralizar y automatizar la protección de datos en todos los servicios de AWS. AWS Elastic Disaster Recovery le permite copiar cargas de trabajo completas del servidor y mantener una protección continua de los datos en las instalaciones, entre zonas de disponibilidad o entre regiones, con un objetivo de punto de recuperación (RPO) medido en segundos.

Amazon S3 puede usarse como destino de las copias de seguridad para los orígenes de datos autoadministrados y administrados por AWS. Los servicios de AWS como Amazon EBS, Amazon RDS y Amazon DynamoDB tienen capacidades integradas para crear copias de seguridad. También se puede usar software de copias de seguridad de terceros.

Se pueden hacer copias de seguridad de los datos en las instalaciones en la Nube de AWS con AWS Storage Gateway o AWS DataSync. Los buckets de Amazon S3 se pueden utilizar para almacenar estos datos en AWS. Amazon S3 ofrece varios niveles de almacenamiento, como Amazon Glacier o Amazon Glacier Deep Archive, para reducir el costo del almacenamiento de datos.

Es posible que pueda satisfacer las necesidades de recuperación de datos mediante la reproducción de los datos desde otros orígenes. Por ejemplo, los nodos de réplica de Amazon ElastiCache o las réplicas de lectura de Amazon RDS podrían usarse para reproducir datos si se pierde el elemento principal. En aquellos casos en que los orígenes como este se puedan utilizar para cumplir su objetivo de punto de recuperación (RPO) y objetivo de tiempo de recuperación (RTO), es posible que

no necesite ninguna copia de seguridad. Otro ejemplo: si trabaja con Amazon EMR, puede que no sea necesario hacer copias de seguridad del almacén de datos de HDFS, siempre y cuando pueda reproducir los datos en Amazon EMR desde Amazon S3.

Al seleccionar una estrategia de copia de seguridad, piense en el tiempo que se necesita para recuperar los datos. El tiempo necesario para recuperar datos depende del tipo de copia de seguridad (en el caso de una estrategia de copia de seguridad) o de la complejidad del mecanismo de reproducción de datos. Este tiempo debería ajustarse al RTO de la carga de trabajo.

Pasos para la implementación

1. Identifique todos los orígenes de datos de la carga de trabajo. Los datos se pueden almacenar en varios recursos, como bases de datos, volúmenes, sistemas de archivos, sistemas de registro y almacenamiento de objetos. Consulte la sección Recursos para encontrar documentos relacionados sobre los diferentes servicios de AWS en los que se almacenan los datos y la capacidad de copia de seguridad que ofrecen estos servicios.
2. Clasifique los orígenes de datos según su criticidad. Los distintos conjuntos de datos tendrán diferentes niveles de criticidad para una carga de trabajo y, por tanto, distintos requisitos de resiliencia. Por ejemplo, algunos datos podrían ser críticos y requerir un RPO cercano a cero, mientras que otros datos podrían ser menos críticos y tolerar un RPO más alto y cierta pérdida de datos. Del mismo modo, los distintos conjuntos de datos podrían tener también diferentes requisitos en cuanto al RTO.
3. Uso de AWS o servicios de terceros para crear copias de seguridad de los datos. AWS Backup es un servicio administrado que permite crear copias de seguridad de diversos orígenes de datos en AWS. AWS Elastic Disaster Recovery administra la replicación automatizada de datos en menos de un segundo a una Región de AWS. La mayoría de los servicios de AWS también disponen de capacidades nativas para crear copias de seguridad. AWS Marketplace tiene muchas soluciones que ofrecen también estas capacidades. Consulte la sección Recursos que aparece a continuación para obtener información sobre cómo crear copias de seguridad de los datos de distintos servicios de AWS.
4. Establezca un mecanismo de reproducción de datos para los datos que no tengan copia de seguridad. Puede decidir no crear una copia de seguridad de datos que puedan reproducirse desde otros orígenes y por distintos motivos. Podría darse una situación en la que sea más barato reproducir datos de orígenes cuando sea necesario en lugar de crear una copia de seguridad, ya que podría existir un costo asociado con el almacenamiento de copias de seguridad. Otro ejemplo es cuando la restauración desde una copia de seguridad tarda más tiempo que la reproducción de los datos desde el origen, lo que implica un incumplimiento del RTO. En tales situaciones, sopese

los pros y los contras y establezca un proceso bien definido sobre cómo se pueden reproducir los datos desde estos orígenes cuando sea necesaria una recuperación de los datos. Por ejemplo, si ha cargado datos desde Amazon S3 en un almacenamiento de datos (como Amazon Redshift) o un clúster de MapReduce (como Amazon EMR) para analizar dichos datos, esto podría ser un ejemplo de datos que se pueden reproducir desde otros orígenes. Siempre y cuando los resultados de estos análisis se almacenen en algún lugar o sean reproducibles, no sufriría ninguna pérdida de datos por un error en el almacenamiento de datos o el clúster de MapReduce. Otros ejemplos que se pueden reproducir desde el origen son las cachés (como Amazon ElastiCache) o las réplicas de lectura de RDS.

5. Establezca una cadencia para hacer copias de seguridad de los datos. La creación de copias de seguridad de orígenes de datos es un proceso periódico y la frecuencia debería depender del RPO.

Nivel de esfuerzo para el plan de implementación: moderado

Recursos

Prácticas recomendadas relacionadas:

REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos

REL13-BP02 Uso de estrategias de recuperación definidas para cumplir los objetivos de recuperación

Documentos relacionados:

- Qué es AWS Backup?
- What is AWS DataSync?
- What is Volume Gateway?
- Socio de APN: socios que pueden ayudar con la copia de seguridad
- AWS Marketplace: productos que pueden usarse para la copia de seguridad
- Instantáneas de Amazon EBS
- Backing Up Amazon EFS
- Backing up Amazon FSx for Windows File Server
- Backup and Restore for ElastiCache for Redis

- Creating a DB Cluster Snapshot in Neptune
- Creación de una instantánea de base de datos
- Creating an EventBridge Rule That Triggers on a Schedule
- Replicación entre regiones con Amazon S3
- AWS Backup de EFS a EFS
- Exporting Log Data to Amazon S3
- Administración del ciclo de vida del almacenamiento
- Copia de seguridad y restauración bajo demanda para DynamoDB
- Recuperación a un momento dado en DynamoDB
- Working with Amazon OpenSearch Service Index Snapshots
- What is AWS Elastic Disaster Recovery?

Videos relacionados:

- AWS re:Invent 2021 - Backup, disaster recovery, and ransomware protection with AWS
- AWS Backup Demo: Cross-Account and Cross-Region Backup
- AWS re:Invent 2019: Deep dive on AWS Backup, ft. Rackspace (STG341)

REL09-BP02 Protección y cifrado de copias de seguridad

Controle y detecte el acceso a las copias de seguridad con autenticación y autorización. Evite que la integridad de los datos de las copias de seguridad se vea comprometida (y detecte los casos en los que así sea) mediante el cifrado.

Implemente controles de seguridad para evitar el acceso no autorizado a los datos de copia de seguridad. Cifre las copias de seguridad para proteger la confidencialidad y la integridad de los datos.

Patrones comunes de uso no recomendados:

- Tener el mismo acceso a las automatizaciones de las copias de seguridad y restauración que a los datos.
- No cifrar las copias de seguridad.

- No se implementa la inmutabilidad como protección contra la eliminación o la manipulación.
- Se usa el mismo dominio de seguridad para los sistemas de producción y de copia de seguridad.
- No se valida la integridad de las copias de seguridad mediante pruebas periódicas.

Beneficios de establecer esta práctica recomendada:

- La protección de las copias de seguridad impide que se manipulen los datos y el cifrado de los datos impide el acceso a esos datos si se exponen de forma accidental.
- Protección mejorada contra el ransomware y otras ciberamenazas que afectan a la infraestructura de copia de seguridad.
- Reducción del tiempo de recuperación tras un ciberincidente mediante procesos de recuperación validados.
- Capacidades de continuidad empresarial mejoradas durante los incidentes de seguridad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Controle y detecte el acceso a las copias de seguridad con autenticación y autorización, como AWS Identity and Access Management (IAM). Evite que la integridad de los datos de las copias de seguridad se vea comprometida (y detecte los casos en los que así sea) mediante el cifrado.

Amazon S3 admite varios métodos de cifrado de los datos en reposo. Con el cifrado del servidor, Amazon S3 acepta sus objetos como datos sin cifrar y después los cifra a medida que se almacenan. Con el cifrado del cliente, la aplicación de la carga de trabajo es la responsable de cifrar los datos antes de que se envíen a Amazon S3. Ambos métodos le permiten utilizar AWS Key Management Service (AWS KMS) para crear y almacenar la clave de los datos, o puede facilitar la suya propia, de la que será responsable. Con AWS KMS, puede establecer políticas con IAM sobre quién puede acceder a sus claves de datos y datos descifrados y quién no.

Para Amazon RDS, si ha decidido cifrar las bases de datos, sus copias de seguridad también estarán cifradas. Las copias de seguridad de DynamoDB siempre están cifradas. Al usar AWS Elastic Disaster Recovery, todos los datos en tránsito y en reposo están cifrados. Con la Recuperación de desastres elástica, los datos en reposo se pueden cifrar con la clave de cifrado de volumen predeterminada de Amazon EBS o una clave personalizada administrada por el cliente.

Consideraciones sobre la resiliencia cibernética

Para mejorar la seguridad de las copias de seguridad frente a las ciberamenazas, considere la posibilidad de implementar estos controles adicionales además del cifrado:

- Implemente la inmutabilidad mediante AWS Backup Vault Lock o el bloqueo de objetos de Amazon S3 para evitar que los datos de copia de seguridad se alteren o eliminen durante su periodo de retención, protegiéndolos contra el ransomware y la eliminación malintencionada.
- Establezca un aislamiento lógico entre los entornos de producción y de copia de seguridad con un almacén aislado lógicamente de AWS Backup para los sistemas críticos, lo que crea una separación que ayuda a evitar que ambos entornos se vean comprometidos simultáneamente.
- Valide la integridad de las copias de seguridad con regularidad mediante pruebas de restauración de AWS Backup para comprobar que las copias de seguridad no están dañadas y que se pueden restaurar correctamente tras un ciberincidente.
- Implemente la aprobación de varias partes para las operaciones de recuperación críticas mediante la aprobación de varias partes de AWS Backup para evitar intentos de recuperación no autorizados o malintencionados, exigiendo la autorización de varios aprobadores designados.

Pasos para la implementación

1. Use el cifrado en cada uno de los almacenes de datos. Si los datos de origen están cifrados, la copia de seguridad también estará cifrada.
   - Utilice el cifrado en Amazon RDS. Puede configurar el cifrado en reposo mediante AWS Key Management Service al crear una instancia de RDS.
   - Use el cifrado en volúmenes de Amazon EBS. Puede configurar el cifrado predeterminado o especificar una clave única al crear los volúmenes.
   - Use el cifrado de Amazon DynamoDB requerido. DynamoDB cifra todos los datos en reposo. Puede utilizar una clave de AWS propiedad de AWS KMS o una clave de KMS administrada por AWS, siempre que especifique una clave que esté almacenada en su cuenta.
   - Cifre los datos almacenados en Amazon EFS. Configure el cifrado cuando cree el sistema de archivos.
   - Configure el cifrado en las regiones de origen y destino. Puede configurar el cifrado en reposo en Amazon S3 con las claves almacenadas en KMS, pero las claves son específicas de la región. Puede especificar las claves de destino cuando configure la replicación.
   - Elija si desea utilizar el cifrado predeterminado o utilizar el cifrado personalizado de Amazon EBS para la Recuperación de desastres elástica. Esta opción cifrará sus datos replicados en reposo en los discos de la subred de la zona de preparación y en los discos replicados.

2. Implemente permisos de privilegio mínimo para acceder a las copias de seguridad. Siga las prácticas recomendadas para limitar el acceso a las copias de seguridad, instantáneas y réplicas de acuerdo con las prácticas recomendadas de seguridad.
3. Configure la inmutabilidad de las copias de seguridad críticas. En el caso de los datos críticos, implemente AWS Backup Vault Lock o el bloqueo de objetos de S3 para evitar que se eliminen o modifiquen durante el periodo de retención especificado. Para conocer los detalles de implementación, consulte AWS Backup Vault Lock.
4. Cree una separación lógica para los entornos de copia de seguridad. Implemente un almacén aislado lógicamente de AWS Backup para los sistemas críticos que requieren una protección mejorada contra las ciberamenazas. Para obtener una guía de implementación, consulte Building cyber resiliency with AWS Backup logically air-gapped vault.
5. Implemente procesos de validación de copias de seguridad. Configure las pruebas de restauración de AWS Backup para comprobar que las copias de seguridad no están dañadas y que se pueden restaurar correctamente tras un ciberincidente. Para obtener más información, consulte Validate recovery readiness with AWS Backup restore testing.
6. Configure la aprobación de varias partes para las operaciones de recuperación confidenciales. En el caso de los sistemas críticos, implemente la aprobación de varias partes de AWS Backup para solicitar la autorización de varios aprobadores designados antes de que pueda continuar con la recuperación. Para obtener información detallada sobre la implementación, consulte Improve recovery resilience with AWS Backup support for Multi-party approval.

Recursos

Documentos relacionados:

- AWS Marketplace: productos que pueden usarse para la copia de seguridad
- Amazon EBS Encryption
- Amazon S3: protección de los datos mediante el cifrado
- Configuración adicional de CRR: replicación de objetos creados con el cifrado del servidor (SSE) usando las claves de cifrado almacenadas en AWS KMS
- Cifrado en reposo en DynamoDB
- Encrypting Amazon RDS Resources
- Encrypting Data and Metadata in Amazon EFS
- Encryption for Backups in AWS

- Administración de tablas de cifrado
- Pilar de seguridad: Marco de AWS Well-Architected
- What is AWS Elastic Disaster Recovery?
- FSISEC11: ¿Cómo se protege contra el ransomware?
- Ransomware Risk Management on AWS Using the NIST Cyber Security Framework
- Building cyber resiliency with AWS Backup logically air-gapped vault
- Validate recovery readiness with AWS Backup restore testing
- Improve recovery resilience with AWS Backup support for Multi-party approval

Ejemplos relacionados:

- Implementing Bi-Directional Cross-Region Replication (CRR) for Amazon S3

REL09-BP03 Copias de seguridad automáticas de los datos

Configure las copias de seguridad para que se creen automáticamente con arreglo a un calendario periódico determinado por el objetivo de punto de recuperación (RPO) o cuando se produzcan cambios en el conjunto de datos. En el caso de los conjuntos de datos críticos con requisitos de pérdida de datos bajos, es necesario crear una copia de seguridad automática con frecuencia, mientras que en el de los datos menos críticos para los que resultan aceptables ciertas pérdidas, las copias de seguridad pueden ser menos frecuentes.

Resultado deseado: un proceso automatizado que crea copias de seguridad de los orígenes de datos con una cadencia establecida.

Patrones comunes de uso no recomendados:

- Hacer las copias de seguridad manualmente.
- Usar recursos que tengan la función de copia de seguridad, pero no incluir la copia de seguridad en la automatización.

Beneficios de establecer esta práctica recomendada: al automatizar las copias de seguridad, se comprueba que se hagan con regularidad en función del RPO y, si no se hacen, se avisa al usuario.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

AWS Backup se puede usar para crear copias de seguridad automatizadas de los datos de diversos orígenes de datos de AWS. Es posible crear copias de seguridad de las instancias de Amazon RDS casi de forma continua cada cinco minutos, y de los objetos de Amazon S3 cada quince minutos, lo que facilita una recuperación en un momento dado (PITR) a un punto específico del historial de copias de seguridad. Para otros orígenes de datos de AWS, como los volúmenes de Amazon EBS, las tablas de Amazon DynamoDB o los sistemas de archivos de Amazon FSx, AWS Backup puede ejecutar una copia de seguridad automatizada con una frecuencia que puede llegar a ser de una hora. Estos servicios también ofrecen capacidades de copia de seguridad nativas. Los servicios de AWS que ofrecen copias de seguridad automatizadas con recuperación en un momento dado son Amazon DynamoDB, Amazon RDS y Amazon Keyspaces (para Apache Cassandra), que se pueden restaurar a un momento específico del historial de copias de seguridad. La mayoría del resto de servicios de almacenamiento de datos de AWS ofrecen la capacidad de programar copias de seguridad periódicas, con una frecuencia que puede llegar a ser de una hora.

Amazon RDS y Amazon DynamoDB ofrecen copias de seguridad continuas con recuperación en un momento dado. El control de versiones de Amazon S3, una vez activado, es automático. Se puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de instantáneas de Amazon EBS. También puede automatizar la creación, copia, desuso y anulación de registro de imágenes de máquina de Amazon (AMI) basadas en Amazon EBS y sus instantáneas de Amazon EBS subyacentes.

AWS Elastic Disaster Recovery proporciona replicación continua en el nivel de bloque desde el entorno de origen (en las instalaciones o AWS) a la región de recuperación de destino. El servicio crea y administra automáticamente instantáneas de Amazon EBS de un momento dado.

Para obtener una vista centralizada de la automatización y el historial de sus copias de seguridad, AWS Backup proporciona una solución de copia de seguridad totalmente administrada y basada en políticas. Centraliza y automatiza la copia de seguridad de datos entre varios servicios de AWS en la nube y en el entorno en las instalaciones con AWS Storage Gateway.

De forma adicional al control de versiones, Amazon S3 incluye también replicación. Todo el bucket de S3 se puede replicar automáticamente en otro bucket de la misma Región de AWS o una diferente.

Pasos para la implementación

1. Identifique los orígenes de datos de los que se están haciendo copias de seguridad manualmente. Para obtener más información, consulte REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes.
2. Determine el RPO de la carga de trabajo. Para obtener más información, consulte REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos.
3. Use una solución de copia de seguridad automatizada o un servicio administrado. AWS Backup es un servicio totalmente administrado que facilita la centralización y automatización de la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones. Mediante planes de copia de seguridad en AWS Backup, cree reglas que definan de qué recursos se debe hacer copia de seguridad y con qué frecuencia deben crearse. Esta frecuencia debe determinarla el RPO establecido en el paso 2. Para obtener orientación práctica sobre cómo crear copias de seguridad automatizadas mediante AWS Backup, consulte Testing Backup and Restore of Data. La mayoría de los servicios de AWS que almacenan datos ofrecen capacidades de copia de seguridad nativas. Por ejemplo, se puede utilizar RDS para hacer copias de seguridad automatizadas con recuperación en un momento dado (PITR).
4. En el caso de los orígenes de datos que no sean compatibles con una solución de copia de seguridad automatizada o un servicio administrado, como los orígenes de datos en las instalaciones o las colas de mensajes, considere la posibilidad de utilizar una solución de terceros de confianza para crear copias de seguridad automatizadas. Como alternativa, puede crear una automatización que se encargue de esto con la AWS CLI o algún SDK. Puede usar funciones de AWS Lambda o AWS Step Functions para definir la lógica implicada en la creación de una copia de seguridad de datos y utilizar Amazon EventBridge para invocarla con una frecuencia basada en el RPO.

Nivel de esfuerzo para el plan de implementación: bajo

Recursos

Documentos relacionados:

- Socio de APN: socios que pueden ayudar con la copia de seguridad
- AWS Marketplace: productos que pueden usarse para la copia de seguridad
- Creating an EventBridge Rule That Triggers on a Schedule
- ¿Qué es AWS Backup?
- ¿Qué es AWS Step Functions?

- What is AWS Elastic Disaster Recovery?

Videos relacionados:

- AWS re:Invent 2019: Deep dive on AWS Backup, ft. Rackspace (STG341)

REL09-BP04 Recuperación periódica de los datos para verificar la integridad de la copia de seguridad y los procesos

Valide que su implementación del proceso de copia de seguridad cumpla con los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO) mediante una prueba de recuperación.

Resultado deseado: los datos de las copias de seguridad se recuperan periódicamente mediante mecanismos bien definidos para verificar que la recuperación sea posible dentro del objetivo de tiempo de recuperación (RTO) establecido para la carga de trabajo. Verifique que la restauración a partir de una copia de seguridad dé como resultado un recurso que contenga los datos originales sin que ninguno de ellos resulte dañado o inaccesible, y una pérdida de datos coherente con el objetivo de punto de recuperación (RPO).

Patrones comunes de uso no recomendados:

- Restaurar una copia de seguridad, pero no consultar ni recuperar ningún dato para comprobar que la restauración sea posible.
- Suponer que existe una copia de seguridad.
- Suponer que la copia de seguridad de un sistema está plenamente operativa y que es posible recuperar datos de ella.
- Suponer que el tiempo de restauración o recuperación de datos de una copia de seguridad entra dentro del RTO para la carga de trabajo.
- Suponer que los datos que contiene la copia de seguridad están dentro del RPO para la carga de trabajo
- Restaurar cuando sea necesario, sin usar un manual de procedimientos, o fuera de un procedimiento automatizado.

Beneficios de establecer esta práctica recomendada: al probar la recuperación de las copias de seguridad, se comprueba que los datos se pueden restaurar cuando sea necesario sin preocuparse

de que falten datos o estén dañados, de que la restauración y la recuperación sean posibles dentro del RTO de la carga de trabajo y que cualquier pérdida de datos recaiga dentro del RPO correspondiente a la carga de trabajo.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

La comprobación de la capacidad de copia de seguridad y restauración aumenta la confianza en la capacidad de llevar a cabo estas acciones durante una interrupción. Restaure periódicamente las copias de seguridad en una nueva ubicación y lleve a cabo pruebas para verificar la integridad de los datos. Algunas de las pruebas habituales que deberían efectuarse consisten en comprobar que todos los datos estén disponibles, no estén dañados, sean accesibles y si la pérdida de datos (si la hay) se ajusta al RPO de la carga de trabajo. Estas pruebas también pueden ayudar a determinar si los mecanismos de recuperación son lo suficientemente rápidos como para tener capacidad para el RTO de la carga de trabajo.

Con AWS, puede crear un entorno de pruebas y restaurar sus copias de seguridad para evaluar las capacidades en cuanto al RTO y al RPO y llevar a cabo pruebas sobre el contenido y la integridad de los datos.

Además, Amazon RDS y Amazon DynamoDB permiten la recuperación en un momento dado (PITR). Mediante la copia de seguridad continua, puede restaurar su conjunto de datos al estado en el que se encontraba en una fecha y hora específicas.

Si todos los datos están disponibles, no están dañados, son accesibles y la pérdida de datos (si la hay) se ajusta al RPO de la carga de trabajo. Estas pruebas también pueden ayudar a determinar si los mecanismos de recuperación son lo suficientemente rápidos como para tener capacidad para el RTO de la carga de trabajo.

AWS Elastic Disaster Recovery ofrece instantáneas de recuperación en un momento dado continuas de volúmenes de Amazon EBS. A medida que se replican los servidores de origen, los estados de un momento dado se cronifican en el tiempo en función de la política configurada. La Recuperación de desastres elástica ayuda a verificar la integridad de estas instantáneas mediante el lanzamiento de instancias con fines de prueba y simulacro sin redirigir el tráfico.

Pasos para la implementación

1. Identifique los orígenes de datos de los que se están haciendo copias de seguridad actualmente y dónde se almacenan dichas copias de seguridad. Para obtener una guía para la implementación,

consulte REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes.

2. Establezca los criterios de validación de datos para cada origen de datos. Los diferentes tipos de datos tendrán distintas propiedades, lo que podría requerir diferentes mecanismos de validación. Considere cómo se podrían validar estos datos antes de contar con la confianza suficiente para usarlos en producción. Algunas formas habituales de validar los datos son usar las propiedades de datos y copias de seguridad como el tipo de datos, el formato, la suma de comprobación, el tamaño o una combinación de ellas con lógica de validación personalizada. Por ejemplo, podría tratarse de una comparación de los valores de las sumas de comprobación entre el recurso restaurado y el origen de datos en el momento en que se creó la copia de seguridad.
3. Establezca el RTO y el RPO para restaurar los datos según su importancia. Para obtener una guía para la implementación, consulte REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos.
4. Evalúe su capacidad de recuperación. Revise su estrategia de copia de seguridad y restauración para comprender si se ajusta a su RTO y RPO y ajuste la estrategia según sea necesario. Con AWS Resilience Hub, puede evaluar la carga de trabajo. La evaluación compara la configuración de su aplicación con la política de resiliencia y notifica si se pueden cumplir los objetivos de RTO y RPO.
5. Ejecute una restauración de prueba con los procesos actualmente establecidos que se utilizan en la producción para la restauración de datos. Estos procesos dependen de cómo se haya creado la copia de seguridad del origen de datos, el formato y la ubicación del almacenamiento de la copia de seguridad, o de si los datos se reproducen desde otros orígenes. Por ejemplo, si utiliza un servicio administrado, como AWS Backup, podría ser tan sencillo como restaurar la copia de seguridad en un nuevo recurso. Si usó AWS Elastic Disaster Recovery, puede iniciar un simulacro de recuperación.
6. Valide la recuperación de datos del recurso restaurado en función de los criterios que estableció previamente para la validación de los datos. ¿Los datos restaurados y recuperados contienen el registro o elemento más reciente en el momento de la copia de seguridad? ¿Estos datos se ajustan al RPO de la carga de trabajo?
7. Calcule el tiempo necesario para la restauración y la recuperación y compárelo con el RTO establecido. ¿Este proceso se ajusta al RTO de la carga de trabajo? Por ejemplo, compare las marcas de tiempo del momento en que se inició el proceso de restauración y de cuando se completó la validación de la recuperación para calcular cuánto tarda este proceso. Todas las llamadas a la API de AWS llevan una marca de tiempo y esta información está disponible en AWS CloudTrail. Aunque esta información puede proporcionar detalles sobre cuándo se inició

el proceso de restauración, la marca de tiempo final del momento en que finalizó la validación debería quedar registrada mediante su lógica de validación. Si se utiliza un proceso automatizado, se pueden utilizar servicios como Amazon DynamoDB para almacenar esta información. Además, muchos servicios de AWS proporcionan un historial de eventos que facilita información con marcas de tiempo cuando ocurren determinadas acciones. En AWS Backup, las acciones de copia de seguridad y restauración se denominan trabajos, y estos trabajos contienen información sobre la marca de tiempo como parte de sus metadatos, que se puede utilizar para medir el tiempo necesario para la restauración y la recuperación.

8. Notifique a las partes interesadas si se produce un error en la validación de los datos o si el tiempo necesario para la restauración y la recuperación supera el RTO establecido para la carga de trabajo. Al implementar la automatización para que lo haga, como en este laboratorio, se pueden utilizar servicios como Amazon Simple Notification Service (Amazon SNS) para enviar notificaciones push, como correos electrónicos o SMS, a las partes interesadas. Estos mensajes también se pueden publicar en aplicaciones de mensajería como Amazon Chime, Slack o Microsoft Teams, o se pueden usar para crear tareas como OpsItems con el Centro de operaciones de AWS Systems Manager.
9. Automatice este proceso para que se ejecute periódicamente. Por ejemplo, se pueden usar servicios como AWS Lambda o una máquina de estados en AWS Step Functions para automatizar los procesos de restauración y recuperación, mientras que se puede usar Amazon EventBridge para invocar este flujo de trabajo de automatización periódicamente como se muestra en el siguiente diagrama de arquitectura. Obtenga información sobre cómo automatizar la validación de recuperación de datos con AWS Backup. Además, en este laboratorio de Well-Architected se ofrece una experiencia práctica sobre una forma de ejecutar la automatización de varios de los pasos que se describen aquí.

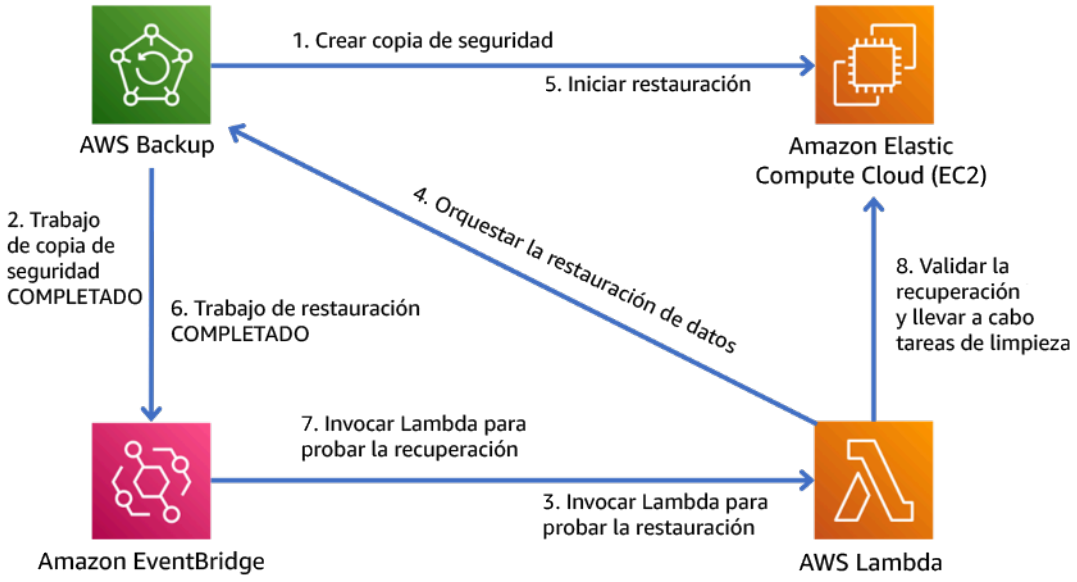


Figura 9. Proceso de copia de seguridad y restauración automatizado

Nivel de esfuerzo para el plan de implementación: de moderado a alto, según la complejidad de los criterios de validación.

Recursos

Documentos relacionados:

- Automate data recovery validation with AWS Backup
- Socio de APN: socios que pueden ayudar con la copia de seguridad
- AWS Marketplace: productos que pueden usarse para la copia de seguridad
- Creating an EventBridge Rule That Triggers on a Schedule
- Copia de seguridad y restauración bajo demanda para DynamoDB
- Qué es AWS Backup?
- Qué es AWS Step Functions?
- Qué es AWS Elastic Disaster Recovery
- AWS Elastic Disaster Recovery

Uso del aislamiento de errores para proteger su carga de trabajo

El aislamiento de fallos limita el impacto de un fallo en un componente o sistema a un límite definido. Mediante un aislamiento adecuado, los componentes que se encuentran fuera del límite no se ven

afectados por el error. Hacer que la carga de trabajo supere varios límites de aislamiento de fallos puede hacer que sea más resistente a los fallos.

Prácticas recomendadas

- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL10-BP02 Automatización de la recuperación de los componentes restringidos a una sola ubicación
- REL10-BP03 Uso de arquitecturas herméticas para limitar el alcance del impacto

REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones

Distribuya los datos y los recursos de la carga de trabajo entre varias zonas de disponibilidad o, si es necesario, entre varias Regiones de AWS.

Un principio fundamental para el diseño de servicios en AWS es evitar puntos únicos de error, incluida la infraestructura física subyacente. AWS proporciona recursos y servicios de computación en la nube a nivel internacional en múltiples ubicaciones geográficas denominadas regiones. Cada región es independiente física y lógicamente y consta de tres o más zonas de disponibilidad (AZ). Las zonas de disponibilidad están geográficamente cerca unas de otras, pero están físicamente separadas y aisladas. Cuando distribuye sus cargas de trabajo entre las zonas y regiones de disponibilidad, mitiga el riesgo de amenazas como incendios, inundaciones, desastres relacionados con el clima, terremotos y errores humanos.

Cree una estrategia de ubicación para ofrecer una alta disponibilidad que sea adecuada para las cargas de trabajo.

Resultado deseado: las cargas de trabajo de producción se distribuyen entre varias zonas de disponibilidad (AZ) o regiones para lograr la tolerancia a los errores y una alta disponibilidad.

Patrones comunes de uso no recomendados:

- La carga de trabajo de producción solo existe en una sola zona de disponibilidad.
- Se implementa una arquitectura multirregional cuando una arquitectura Multi-AZ podría cumplir los requisitos empresariales.
- Las implementaciones o los datos se desincronizan, lo que provoca cambios en la configuración o una replicación insuficiente de los datos.
- No se tienen en cuenta las dependencias entre los componentes de la aplicación si los requisitos de resiliencia y de múltiples ubicaciones difieren entre esos componentes.

Beneficios de establecer esta práctica recomendada:

- Su carga de trabajo es más resistente a los incidentes, como los cortes de energía o de control ambiental, los desastres naturales, los fallos del servicio previo o los problemas de red que afectan a una zona de disponibilidad o a toda una región.
- Puede acceder a un inventario más amplio de instancias de Amazon EC2 y reducir la probabilidad de que se produzcan InsufentCapacityExceptions (ICE) al lanzar tipos de instancias de EC2 específicos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Implemente y opere todas las cargas de trabajo de producción en al menos dos zonas de disponibilidad (AZ) en una región.

Uso de varias zonas de disponibilidad

Las zonas de disponibilidad son ubicaciones de alojamiento de recursos que están separadas físicamente entre sí para evitar fallos correlacionados debidos a riesgos como incendios, inundaciones y tornados. Cada zona de disponibilidad tiene una infraestructura física independiente, que incluye conexiones eléctricas de servicios públicos, fuentes de energía de emergencia, servicios mecánicos y conectividad de red. Esta disposición limita los errores en cualquiera de estos componentes únicamente a la zona de disponibilidad afectada. Por ejemplo, si un incidente en toda la zona de disponibilidad hace que las instancias de EC2 no estén disponibles en la zona de disponibilidad afectada, las instancias de la otra zona de disponibilidad seguirán disponibles.

A pesar de estar separadas físicamente, las zonas de disponibilidad de la misma Región de AWS están lo suficientemente cerca como para proporcionar redes de alto rendimiento y baja latencia (milisegundos de un solo dígito). Puede replicar los datos de forma sincrónica entre las zonas de disponibilidad para la mayoría de las cargas de trabajo sin que ello afecte significativamente a la experiencia del usuario. Esto significa que puede utilizar las zonas de disponibilidad en una configuración activa/activa o activa/en espera.

Toda la computación asociada a su carga de trabajo debe distribuirse entre varias zonas de disponibilidad. Esto incluye instancias de Amazon EC2, tareas de AWS Fargate y funciones de AWS Lambda conectadas a VPC. Los servicios de computación de AWS, incluidos EC2 Auto Scaling, Amazon Elastic Container Service (ECS) y Amazon Elastic Kubernetes Service (EKS), le

proporcionan formas de lanzar y administrar el procesamiento en todas las zonas de disponibilidad. Configúrelos para reemplazar automáticamente el procesamiento según sea necesario en una zona de disponibilidad diferente para mantener la disponibilidad. Para dirigir el tráfico a las zonas de disponibilidad disponibles, coloque un equilibrador de cargas delante del equipo, como un Equilibrador de carga de aplicación o un Equilibrador de carga de red. Los equilibradores de carga de AWS pueden redirigir el tráfico a las instancias disponibles en caso de que la zona de disponibilidad se vea afectada.

También debe replicar los datos de su carga de trabajo y ponerlos a disposición en varias zonas de disponibilidad. Algunos servicios de datos gestionados de AWS, como Amazon S3, Amazon Elastic File Service (EFS), Amazon Aurora, Amazon DynamoDB, Amazon Simple Queue Service (SQS) y Amazon Kinesis Data Streams, replican los datos en varias zonas de disponibilidad de forma predeterminada y son robustos frente al deterioro de la zona de disponibilidad. Con otros servicios de datos gestionados de AWS, como Amazon Relational Database Service (RDS), Amazon Redshift y Amazon ElastiCache, debe habilitar la replicación Multi-AZ. Una vez activados, estos servicios detectan automáticamente una alteración en la zona de disponibilidad, redirigen las solicitudes a una zona de disponibilidad disponible y vuelven a replicar los datos según sea necesario tras la recuperación sin la intervención del cliente. Familiarícese con la guía del usuario de cada servicio de datos gestionado de AWS que utilice para comprender las funciones, comportamientos y operaciones en zonas de disponibilidad múltiples.

Si utiliza un almacenamiento autogestionado, como los volúmenes de Amazon Elastic Block Store (EBS) o el almacenamiento de instancias de Amazon EC2, debe gestionar usted mismo la replicación en zonas de disponibilidad múltiples (Multi-AZ).

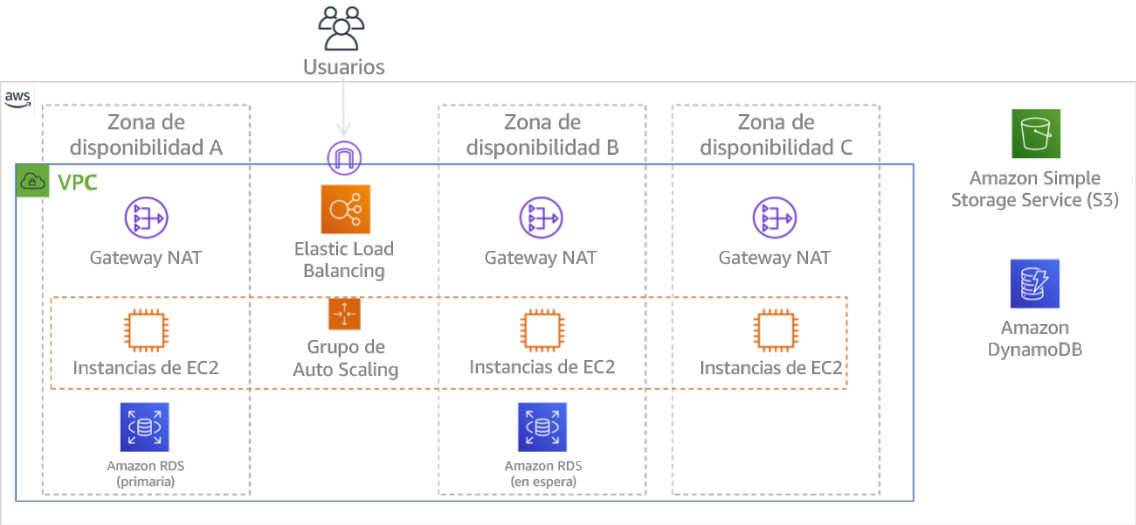


Figura 9: Arquitectura de varios niveles implementada en tres zonas de disponibilidad. Tenga en cuenta que Amazon S3 y Amazon DynamoDB siempre se implementan automáticamente en varias zonas de disponibilidad (Multi-AZ). El ELB también se implementa en las tres zonas.

Uso de múltiples Regiones de AWS

Si tiene cargas de trabajo que requieren una capacidad de recuperación extrema (como infraestructuras críticas, aplicaciones relacionadas con la salud o servicios con requisitos de disponibilidad estrictos u obligatorios por parte del cliente), es posible que necesite una disponibilidad adicional más allá de lo que puede ofrecer una sola Región de AWS. En este caso, debe implementar y operar su carga de trabajo en al menos dos Regiones de AWS (siempre que sus requisitos de residencia de datos lo permitan).

Las Regiones de AWS se encuentran en diferentes regiones geográficas de todo el mundo y en varios continentes. Las Regiones de AWS tienen una separación física y un aislamiento aún mayores que las zonas de disponibilidad por sí solas. Los servicios de AWS, con pocas excepciones, aprovechan este diseño para funcionar de forma totalmente independiente entre diferentes regiones (también conocidos como servicios regionales). El fallo de un servicio en una Región de AWS está diseñado para no afectar al servicio en una región diferente.

Cuando utilice su carga de trabajo en varias regiones, debe tener en cuenta requisitos adicionales. Como los recursos de las distintas regiones están separados y son independientes los unos de los otros, debe duplicar los componentes de la carga de trabajo en cada región. Esto incluye la infraestructura básica, como las VPC, además de los servicios de computación y de datos.

NOTA: Cuando se plantee un diseño multirregional, compruebe que su carga de trabajo sea capaz de ejecutarse en una sola región. Si crea dependencias entre regiones en las que un componente de una región depende de servicios o componentes de una región diferente, puede aumentar el riesgo de fallos y reducir considerablemente su nivel de fiabilidad.

Para facilitar las implementaciones multirregionales y mantener la coherencia, los AWS CloudFormation StackSets pueden replicar toda su infraestructura de AWS en varias regiones. AWS CloudFormation también puede detectar cambios en la configuración e informarle cuando los recursos de AWS de una región no estén sincronizados. Muchos servicios de AWS ofrecen replicación multirregional para activos de carga de trabajo importantes. Por ejemplo, Generador de imágenes de EC2 puede publicar sus imágenes de máquina (AMI) de EC2 después de cada compilación en cada región que utilice. Amazon Elastic Container Registry (ECR) puede replicar las imágenes del contenedor en las regiones seleccionadas.

También debe replicar los datos en cada una de las regiones que elija. Muchos servicios de datos gestionados de AWS ofrecen capacidad de replicación entre regiones, incluidos Amazon S3, Amazon DynamoDB, Amazon RDS, Amazon Aurora, Amazon Redshift, Amazon ElastiCache, y Amazon EFS. Las tablas globales de Amazon DynamoDB aceptan escrituras en cualquier región compatible y replicarán los datos en todas las demás regiones configuradas. Con otros servicios, debe designar una región principal para las escrituras, ya que otras regiones contienen réplicas de solo lectura. Para cada servicio de datos gestionado de AWS que utilice su carga de trabajo, consulte la guía del usuario y la guía para desarrolladores para comprender sus capacidades y limitaciones en varias regiones. Preste especial atención a dónde deben dirigirse las escrituras, a las capacidades y limitaciones de las transacciones, a cómo se lleva a cabo la replicación y a cómo supervisar la sincronización entre regiones.

AWS también ofrece la posibilidad de dirigir el tráfico de solicitudes a sus implementaciones regionales con gran flexibilidad. Por ejemplo, puede configurar sus registros de DNS con Amazon Route 53 para dirigir el tráfico a la región disponible más cercana al usuario. Como alternativa, puede configurar sus registros de DNS en una configuración activa/en espera, en la que designe una región como principal y recurra a una réplica regional solo si la región principal deja de estar en buen estado. Puede configurar las comprobaciones de estado de Route 53 para detectar puntos de conexión en mal estado y realizar una conmutación por error automática y, además, utilizar Amazon Application Recovery Controller (ARC) para proporcionar un control de enrutamiento de alta disponibilidad para redireccionar el tráfico manualmente según sea necesario.

Incluso si decide no operar en varias regiones por motivos de alta disponibilidad, considere la posibilidad de hacerlo en varias regiones como parte de su estrategia de recuperación ante desastres (DR). Si es posible, replique los datos y los componentes de la infraestructura de su carga de trabajo en una configuración de espera activa o piloto ligero en una región secundaria. En este diseño, se replica la infraestructura de referencia de la región principal, como las VPC, los grupos de escalado automático, los orquestadores de contenedores y otros componentes, pero se configuran los componentes de tamaño variable de la región en espera (como el número de instancias de EC2 y réplicas de bases de datos) para que tengan un tamaño operativo mínimo. También puede organizar la replicación continua de los datos desde la región principal a la región en espera. Si se produce un incidente, puede escalar horizontalmente o aumentar los recursos de la región en espera y, después, convertirla en la región principal.

Pasos para la implementación

1. Coordínese con las partes interesadas de la empresa y los expertos en residencia de datos para determinar qué Regiones de AWS se pueden utilizar para alojar sus recursos y datos.

2. Contacte con las partes interesadas tanto a nivel técnico como empresarial para evaluar su carga de trabajo y determinar si sus necesidades de resiliencia pueden satisfacerse mediante un método Multi-AZ (una sola Región de AWS) o si requieren un enfoque multirregional (si se permiten varias regiones). El uso de varias regiones puede proporcionar una mayor disponibilidad, pero también puede suponer una complejidad y un coste adicionales. Tenga en cuenta los siguientes factores en la evaluación:
   a. Objetivos empresariales y requisitos del cliente: ¿cuánto tiempo de inactividad se permite en caso de que se produzca un incidente que afecte a la carga de trabajo en una zona o región de disponibilidad? Evalúe los objetivos de puntos de recuperación, tal como se describe en REL13-BP01. Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos.
   b. Requisitos de recuperación ante desastres (DR): ¿Contra qué tipo de posible desastre quiere asegurarse? Plantéese la posibilidad de que se produzcan pérdidas de datos o una falta de disponibilidad prolongada en diferentes ámbitos de impacto, desde una sola zona de disponibilidad hasta una región completa. Si replica los datos y los recursos en todas las zonas de disponibilidad y una sola zona de disponibilidad sufre un error prolongado, puede recuperar el servicio en otra zona de disponibilidad. Si replica los datos y los recursos en todas las regiones, puede recuperar el servicio en otra región.
3. Implemente los recursos informáticos en varias zonas de disponibilidad.
   a. En la VPC, cree varias subredes en diferentes zonas de disponibilidad. Configure cada una de ellas para que sea lo suficientemente grande como para albergar los recursos necesarios para atender la carga de trabajo, incluso durante un incidente. Para obtener más información, consulte REL02-BP03 Garantía de que la asignación de subredes IP tenga en cuenta la expansión y la disponibilidad.
   b. Si utiliza instancias de Amazon EC2, utilice EC2 Auto Scaling para gestionar las instancias. Especifique las subredes que haya elegido en el paso anterior al crear los grupos de escalado automático.
   c. Si utiliza la computación de AWS Fargate para Amazon ECS o Amazon EKS, seleccione las subredes que haya elegido en el primer paso al crear un servicio de ECS, lanzar una tarea de ECS o crear un perfil de Fargate para EKS.
   d. Si utiliza funciones de AWS Lambda que deben ejecutarse en su VPC, seleccione las subredes que haya elegido en el primer paso al crear la función de Lambda. Para cualquier función que no tenga una configuración de VPC, AWS Lambda administra la disponibilidad automáticamente por usted.

   e. Coloque los directores de tráfico, como los equilibradores de carga, al frente de sus recursos informáticos. Si el equilibrio de carga entre zonas está activado, los equilibradores de carga de aplicaciones de AWS y los equilibradores de carga de red detectan si no es posible contactar con los destinos, como las instancias de EC2 y los contenedores, debido al deterioro de la zona de disponibilidad y redirigen el tráfico hacia los destinos que se encuentran en las zonas de disponibilidad en buen estado. Si inhabilita el equilibrio de carga entre zonas, utilice Amazon Application Recovery Controller (ARC) para proporcionar la capacidad de cambio de zona. Si utiliza un equilibrador de carga de terceros o ha implementado sus propios equilibradores de carga, configúrelos con múltiples interfaces en diferentes zonas de disponibilidad.

4. Replique los datos de la carga de trabajo en varias zonas de disponibilidad.
   a. Si utiliza un servicio de datos gestionado de AWS, como Amazon RDS, Amazon ElastiCache o Amazon FSx, consulte detenidamente su guía del usuario para conocer sus capacidades de replicación y resiliencia de datos. Habilite la replicación entre zonas de disponibilidad y la conmutación por error si es necesario.
   b. Si utiliza servicios de almacenamiento gestionados de AWS, como Amazon S3, Amazon EFS y Amazon FSx, evite utilizar configuraciones Single-AZ o One Zone para datos que requieran una gran durabilidad. Utilice una configuración Multi-AZ para estos servicios. Consulte la guía del usuario del servicio correspondiente para determinar si la replicación Multi-AZ está habilitada de forma predeterminada o si debe habilitarla.
   c. Si ejecuta una base de datos, una cola u otro servicio de almacenamiento autogestionado, organice la replicación en zonas de disponibilidad múltiples según las instrucciones o las prácticas recomendadas de la aplicación. Familiarícese con los procedimientos de conmutación por error de su aplicación.
5. Configure su servicio de DNS para detectar el deterioro de la zona de disponibilidad y redirigir el tráfico a una zona de disponibilidad en buen estado. Amazon Route 53, en combinación con Elastic Load Balancers, puede hacerlo automáticamente. Route 53 también se puede configurar con registros de conmutación por error que utilizan comprobaciones de estado para responder a las consultas únicamente con direcciones IP en buen estado. En el caso de cualquier registro de DNS que se utilice para la conmutación por error, especifique un valor de tiempo de vida (TTL) corto (por ejemplo, 60 segundos o menos) para evitar que el almacenamiento en caché de los registros impida la recuperación (los registros de alias de Route 53 le proporcionan los TTL adecuados).

Pasos adicionales cuando se utilizan varias Regiones de AWS

1. Replique todo el código del sistema operativo (SO) y de la aplicación que utilice su carga de trabajo en las regiones seleccionadas. Replique las imágenes de máquina de Amazon (AMI) que utilizan sus instancias de EC2 si es necesario mediante soluciones como Generador de imágenes de Amazon EC2. Replique las imágenes de contenedores almacenadas en los registros mediante soluciones como la replicación entre regiones de Amazon ECR. Habilite la replicación regional para cualquier bucket de Amazon S3 que se utilice para almacenar los recursos de la aplicación.
2. Implemente sus recursos informáticos y metadatos de configuración (como los parámetros almacenados en el almacén de parámetros de AWS Systems Manager) en varias regiones. Utilice los mismos procedimientos descritos en los pasos anteriores, pero replique la configuración para cada región que utilice para su carga de trabajo. Utilice la infraestructura como soluciones de código, tales como AWS CloudFormation, para reproducir uniformemente las configuraciones entre las regiones. Si utiliza una región secundaria en una configuración piloto sencilla para la recuperación ante desastres, puede reducir la cantidad de recursos informáticos a un valor mínimo para ahorrar costes, con el consiguiente aumento del tiempo de recuperación.
3. Replique los datos de la región principal en las regiones secundarias.
   a. Las tablas globales de Amazon DynamoDB proporcionan réplicas globales de sus datos que se pueden escribir desde cualquier región compatible. Con otros servicios de datos gestionados por AWS, como Amazon RDS, Amazon Aurora y Amazon Elasticache, se designa una región principal (lectura/escritura) y regiones de réplica (solo lectura). Consulte las guías de usuario y del desarrollador de los servicios respectivos para obtener más información sobre la replicación regional.
   b. Si ejecuta una base de datos autogestionada, organice la replicación en varias regiones siguiendo las instrucciones o las prácticas recomendadas de la aplicación. Familiarícese con los procedimientos de conmutación por error de su aplicación.
   c. Si la carga de trabajo utiliza AWS EventBridge, tal vez tenga que reenviar los eventos seleccionados de su región principal a las regiones secundarias. Para ello, especifique los buses de eventos de sus regiones secundarias como destinos de los eventos coincidentes en su región principal.
4. Piense si quiere utilizar claves de cifrado idénticas en todas las regiones y en qué medida. Un enfoque típico que equilibra la seguridad y la facilidad de uso consiste en utilizar claves de ámbito regional para los datos y la autenticación regionales y locales y utilizar claves de ámbito internacional para cifrar los datos que se replican entre distintas regiones. AWS Key Management Service (KMS) admite claves de varias regiones para distribuir y proteger de forma segura las claves compartidas entre las regiones.

5. Puede usar AWS Global Accelerator para mejorar la disponibilidad de la aplicación, que dirige el tráfico a regiones que contengan puntos de conexión en buen estado.

Recursos

Prácticas recomendadas relacionadas:

- REL02-BP03 Garantía de que la asignación de subredes IP tenga en cuenta la expansión y la disponibilidad
- REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal
- REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos

Documentos relacionados:

- AWS Infraestructura global de
- Documento técnico: AWS Fault Isolation Boundaries
- Resiliencia en Amazon EC2 Auto Scaling
- Amazon EC2 Auto Scaling: Ejemplo: Distribuir instancias entre zonas de disponibilidad
- Cómo funciona Generador de Imágenes de EC2
- Cómo coloca Amazon ECS las tareas en las instancias de contenedor (incluido Fargate)
- Resiliencia en AWS Lambda
- Amazon S3: información general de la replicación de objetos
- Replicación de imágenes privadas en Amazon ECR
- Tablas globales: replicación en varias regiones para DynamoDB
- Amazon Elasticache para Redis OSS: replicación en Regiones de AWS con almacenes de datos globales
- Resiliencia en Amazon RDS
- Uso de bases de datos globales de Amazon Aurora
- AWS Guía para desarrolladores de Global Accelerator
- Multi-Region keys in AWS KMS
- Amazon Route 53: configuración de la recuperación ante errores a nivel de DNS

- Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon (ARC)
- Sending and receiving Amazon EventBridge events between Regiones de AWS
- Serie de blogs Creating a Multi-Region Application with AWS Services
- Arquitectura de recuperación de desastres (DR) en AWS, parte I: estrategias de recuperación en la nube
- Disaster Recovery (DR) Architecture on AWS, Part III: Pilot Light and Warm Standby

Videos relacionados:

- AWS re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications
- AWS re:Invent 2019: Innovation and operation of the AWS global network infrastructure

REL10-BP02 Automatización de la recuperación de los componentes restringidos a una sola ubicación

Si los componentes de la carga de trabajo solo se pueden ejecutar en una zona de disponibilidad o en el centro de datos en las instalaciones, implemente la capacidad de volver a crear la carga de trabajo de acuerdo con los objetivos de recuperación definidos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Si la práctica recomendada de implementar la carga de trabajo en varias ubicaciones no es posible por limitaciones tecnológicas, debe implementar una ruta alternativa hacia la resiliencia. Debe automatizar la capacidad de recrear la infraestructura necesaria, volver a implementar las aplicaciones y volver a crear los datos necesarios para estos casos.

Por ejemplo, Amazon EMR lanza todos los nodos de un clúster determinado en la misma zona de disponibilidad, porque la ejecución de un clúster en la misma zona mejora el rendimiento de los flujos de trabajo, ya que ofrece una velocidad de acceso a los datos más alta. Si este componente resulta necesario para la resiliencia de la carga de trabajo, debe tener una forma de volver a implementar el clúster y sus datos. Además, para Amazon EMR, debería aprovisionar la redundancia de formas diferentes al uso de varias zonas de disponibilidad. Puede aprovisionar varios nodos. Con el sistema de archivos de EMR (EMRFS), los datos de EMR se pueden almacenar en Amazon S3, que a su vez se puede replicar en varias zonas de disponibilidad o Regiones de AWS.

De modo similar, en el caso de Amazon Redshift, el clúster se aprovisiona de forma predeterminada en una zona de disponibilidad seleccionada al azar dentro de la Región de AWS que haya seleccionado. Todos los nodos del clúster se aprovisionan en la misma zona.

Para cargas de trabajo basadas en servidores con estado implementadas en un centro de datos en las instalaciones, puede utilizar AWS Elastic Disaster Recovery para proteger sus cargas de trabajo en AWS. Si ya se aloja en AWS, puede usar la Recuperación de desastres elástica para proteger la carga de trabajo en una región o zona de disponibilidad alternativa. La Recuperación de desastres elástica utiliza la replicación continua en el nivel de bloque en un espacio de almacenamiento ligero para proporcionar una recuperación rápida y fiable de las aplicaciones en las instalaciones y basadas en la nube.

Pasos para la implementación

1. Implemente la autorrecuperación. Implemente sus instancias o contenedores con escalado automático siempre que sea posible. Si no puede usar el escalado automático, utilice la recuperación automática para instancias de EC2 o implemente la automatización de autorrecuperación basada en eventos de ciclo de vida del contenedor de Amazon EC2 o ECS.
   - Utilice grupos de Amazon EC2 Auto Scaling para instancias y cargas de trabajo de contenedor que no tengan requisitos de una sola dirección IP de instancia, dirección IP privada, dirección IP elástica y metadatos de instancia.
     - Los datos de usuario de la plantilla de lanzamiento se pueden usar para implementar una automatización que pueda solucionar la mayoría de las cargas de trabajo.
   - Utilice la recuperación automática de instancias de Amazon EC2 para cargas de trabajo que requieran una única dirección ID de instancia, dirección IP privada, dirección IP elástica y metadatos de instancia.
     - La recuperación automática enviará alertas de estado de recuperación a un tema de SNS cuando se detecte un error en la instancia.
   - Utilice los eventos del ciclo de vida de la instancia de Amazon EC2 o los eventos de Amazon ECS para automatizar la autorrecuperación cuando no se pueda utilizar el escalado automático ni la recuperación de EC2.
     - Utilice los eventos para invocar la automatización que reparará su componente de acuerdo con la lógica de proceso que necesita.
   - Proteja las cargas de trabajo con estado que están limitadas a una única ubicación con AWS Elastic Disaster Recovery.

Recursos

Documentos relacionados:

- Eventos de Amazon ECS
- Enlaces de ciclo de vida de Amazon EC2 Auto Scaling
- Recuperación de instancias.
- Escalado automático de su servicio
- What Is Amazon EC2 Auto Scaling?
- AWS Elastic Disaster Recovery

REL10-BP03 Uso de arquitecturas herméticas para limitar el alcance del impacto

La implementación de arquitecturas herméticas (también conocidas como arquitecturas basadas en celdas) restringe el efecto del fallo dentro de una carga de trabajo a un número limitado de componentes.

Resultado deseado: una arquitectura basada en celdas utiliza varias instancias aisladas de una carga de trabajo, donde cada instancia se conoce como celda. Cada celda es independiente, no comparte estado con otras celdas y gestiona un subconjunto de las solicitudes de la carga de trabajo global. Esto reduce la posible repercusión de un error, como una actualización de software incorrecta, en una celda individual y en las solicitudes que está procesando. Si una carga de trabajo utiliza 10 celdas para atender 100 solicitudes cuando se produce un error, el 90 % del total de las solicitudes no se verá afectado por el error.

Patrones comunes de uso no recomendados:

- Permitir que las celdas crezcan sin límites.
- Aplicar actualizaciones o implementaciones de código a todas las celdas al mismo tiempo.
- Compartir estado o componentes entre celdas (a excepción de la capa de enrutador).
- Agregar lógica compleja de negocio o de enrutamiento a la capa de enrutador.
- No minimizar las interacciones entre celdas.

Beneficios de establecer esta práctica recomendada: con las arquitecturas basadas en celdas, muchos tipos de fallos comunes se encuentran dentro de la propia celda, lo que proporciona un

aislamiento adicional de los fallos. Estos límites de los errores pueden favorecer la resiliencia frente a tipos de errores que, de otro modo, serían difíciles de contener, como implementaciones de código fallidas o solicitudes dañadas o que invocan un modo de error específico (también conocidas como solicitudes de píldora venenosa).

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

En un barco, los mamparos garantizan que una brecha en el casco quede contenida en una sola sección del casco. En los sistemas complejos, este modelo de contención suele imitarse para permitir el aislamiento de errores. Los límites aislados de los errores restringen el efecto de un error en una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo. En AWS, los clientes pueden utilizar varias zonas y regiones de disponibilidad para proporcionar aislamiento de errores, pero el concepto de aislamiento de errores también puede extenderse a la arquitectura de su carga de trabajo.

La carga de trabajo global se divide en celdas mediante una clave de partición. Esta clave tiene que alinearse con la corriente del servicio o con la forma natural en que la carga de trabajo de un servicio puede subdividirse con mínimas interacciones entre celdas. Algunos ejemplos de claves de partición son el ID de cliente, el ID de recurso o cualquier otro parámetro fácilmente accesible en la mayoría de las llamadas a la API. Una capa de enrutador de celdas distribuye las solicitudes a celdas individuales en función de la clave de partición y presenta un único punto de conexión a los clientes.

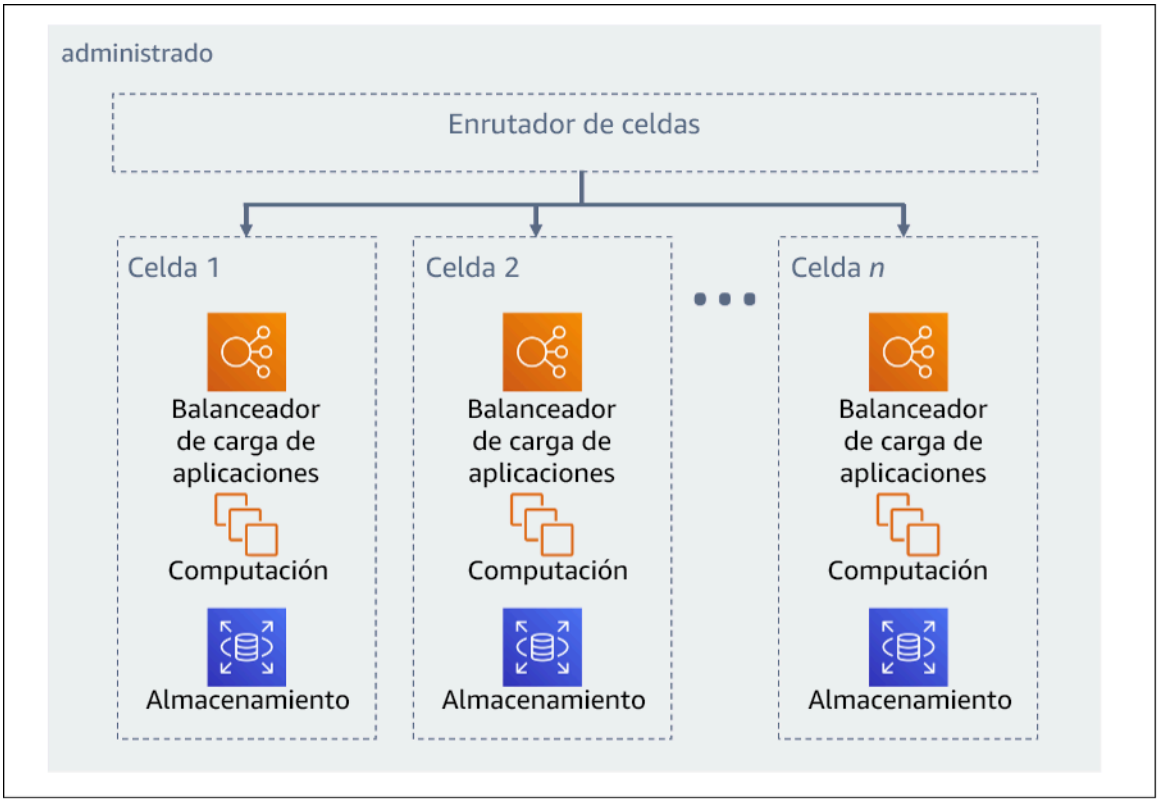


Figura 11: Arquitectura basada en celdas

Pasos para la implementación

Al diseñar una arquitectura basada en celdas, hay que tener en cuenta varias consideraciones de diseño:

1. Clave de partición: se debe tener especial cuidado al elegir la clave de partición.
   - Debe alinearse con la corriente del servicio o con la forma natural en que la carga de trabajo de un servicio puede subdividirse con mínimas interacciones entre celdas. Algunos ejemplos son `customer ID` o `resource ID`.
   - La clave de partición debe estar disponible en todas las solicitudes, ya sea de modo directo o de una manera que se pueda inferir con facilidad de forma determinista por otros parámetros.
2. Asignación persistente de celdas: los servicios ascendentes solo deberían interactuar con una única celda durante el ciclo de vida de sus recursos.
   - Según la carga de trabajo, puede ser necesaria una estrategia de migración de celda para migrar datos de una celda a otra. Un posible escenario en el que puede ser precisa una migración de celda es si un usuario o recurso concreto de la carga de trabajo crece demasiado y requiere una celda dedicada.

- Las celdas no deben compartir estados ni componentes entre ellas.
- En consecuencia, las interacciones entre celdas deben evitarse o mantenerse al mínimo, ya que dichas interacciones crean dependencias entre las celdas y, por lo tanto, disminuyen las ventajas en el aislamiento de errores.

3. Capa de enrutador: la capa de enrutador es un componente compartido entre las celdas y, por lo tanto, no puede seguir la misma estrategia de compartimentación que las celdas.
   - Se recomienda que la capa de enrutador distribuya las solicitudes a las celdas individuales mediante un algoritmo de asignación de particiones de una manera eficiente a nivel computacional, como la combinación de funciones hash criptográficas y aritmética modular para asignar claves de partición a las celdas.
   - Para evitar impactos multicelda, la capa de enrutador debe ser lo más simple y escalable horizontalmente posible, lo que requiere evitar una lógica de negocio compleja dentro de esta capa. Esto tiene la ventaja agregada de facilitar la comprensión de su comportamiento esperado en todo momento, lo que permite una comprobabilidad exhaustiva. Como explica Colm MacCárthaigh en Reliability, constant work, and a good cup of coffee, los diseños simples y los patrones de trabajo constantes producen sistemas fiables y reducen la antifragilidad.
4. Tamaño de la celda: las celdas deben tener un tamaño máximo y no debe permitirse que lo superen.
   - Para determinar el tamaño máximo, se deben llevar a cabo pruebas exhaustivas hasta que se alcancen puntos de ruptura y se establezcan márgenes de funcionamiento seguros. Para obtener más detalles sobre cómo implementar prácticas de prueba, consulte REL07-BP04 Pruebas en su carga de trabajo
   - La carga de trabajo global crecerá a medida que se agreguen celdas adicionales, lo que permite escalar la carga de trabajo con los aumentos de la demanda.
5. Estrategias de varias zonas de disponibilidad o de varias regiones: se deben aprovechar las diversas capas de resiliencia para protegerse contra diferentes dominios de error.
   - Para obtener resiliencia, debe utilizar un enfoque que cree capas de defensa. Una capa protege de las interrupciones más pequeñas y frecuentes mediante la creación de una arquitectura de alta disponibilidad con múltiples AZ. Otra capa de defensa está pensada para proteger de eventos poco frecuentes, como las catástrofes naturales generalizadas y las interrupciones a nivel regional. Esta segunda capa implica la arquitectura de su aplicación para que abarque múltiples Regiones de AWS. Implementar una estrategia multirregión para la carga de trabajo ayuda a protegerla de catástrofes naturales generalizadas que afecten a una región geográfica amplia de un país o de errores técnicos de alcance regional. Tenga en cuenta que implementar

una arquitectura multirregional puede ser significativamente complejo y no suele ser necesario para la mayoría de las cargas de trabajo. Para obtener más información, consulte REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones.

6. Implementación de código: debería preferirse una estrategia de implementación de código escalonada en lugar de implementar cambios de código en todas las celdas al mismo tiempo.
   - Esto ayuda a minimizar posibles errores en numerosas celdas provocados por una implementación incorrecta o a un error humano. Para obtener más detalles, consulte Automatización de implementaciones seguras y sin intervención.

Recursos

Prácticas recomendadas relacionadas:

- REL07-BP04 Pruebas en su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones

Documentos relacionados:

- Reliability, constant work, and a good cup of coffee
- AWS and Compartmentalization
- Aislamiento de las cargas de trabajo a través de la fragmentación aleatoria
- Automatización de implementaciones seguras y sin intervención

Videos relacionados:

- AWS re:Invent 2018: Close Loops and Opening Minds: How to Take Control of Systems, Big and Small
- AWS re:Invent 2018: How AWS Minimizes the Blast Radius of Failures (ARC338)
- Shuffle-sharding: AWS re:Invent 2019: Introducing The Amazon Builders' Library (DOP328)
- AWS Summit ANZ 2021 - Everything fails, all the time: Designing for resilience

Diseño de la carga de trabajo para que tolere los errores de los componentes

Las cargas de trabajo con un requisito de alta disponibilidad y un tiempo de recuperación (MTTR) bajo deben diseñarse para que sean resilientes.

Prácticas recomendadas

- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP02 Conmutación por error a recursos en buen estado
- REL11-BP03 Automatización de la reparación en todas las capas
- REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación
- REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal
- REL11-BP06 Envío de notificaciones cuando los eventos afecten a la disponibilidad
- REL11-BP07 Diseño de su producto para cumplir objetivos de disponibilidad y acuerdos de nivel de servicio (SLA) de tiempo de actividad

REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores

Supervise continuamente el estado de las cargas de trabajo para que usted y los sistemas automatizados sepan cuándo se produce degradaciones o errores en cuanto ocurran. Supervise los indicadores clave de rendimiento (KPI) en función del valor empresarial.

Todos los mecanismos de recuperación y corrección deben comenzar por la capacidad de detectar problemas rápidamente. Los fallos técnicos deberían detectarse en primer lugar para poder resolverse. Sin embargo, la disponibilidad se basa en la capacidad de su carga de trabajo para ofrecer valor empresarial, de modo que los indicadores clave de rendimiento (KPI) que midan esto tienen que formar parte de su estrategia de detección y corrección.

Resultado deseado: los componentes esenciales de una carga de trabajo se supervisan de forma independiente para detectar los errores en el momento y el lugar en que se producen y alertar sobre ellos.

Patrones comunes de uso no recomendados:

- No se han configurado alarmas, por lo que las interrupciones se producen sin notificación.
- Existen alarmas, pero en umbrales que no proporcionan el tiempo necesario para reaccionar.
- No se recopilan métricas con la suficiente regularidad para satisfacer el objetivo de tiempo de recuperación (RTO).
- Solo se supervisan activamente las interfaces de la carga de trabajo orientadas a los clientes.
- Solo se recopilan métricas técnicas, no métricas de funciones empresariales.
- No hay métricas que midan la experiencia del usuario con la carga de trabajo.
- Se crean demasiadas supervisiones.

Beneficios de establecer esta práctica recomendada: una supervisión adecuada de todas las capas le permite reducir el tiempo de recuperación al reducirse el tiempo de detección.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Identifique todas las cargas de trabajo que se revisarán para su supervisión. Una vez que haya identificado todos los componentes de la carga de trabajo que deberán supervisarse, tendrá que determinar el intervalo de supervisión. El intervalo de supervisión tendrá un impacto directo en la rapidez con la que se puede iniciar la recuperación en función del tiempo que se tarde en detectar un error. El tiempo medio de detección (MTTD) es el tiempo transcurrido entre la aparición de un error y el inicio de las operaciones de reparación. La lista de servicios debe ser amplia y completa.

La supervisión debe cubrir todas las capas de la pila de aplicaciones, incluidas la aplicación, la plataforma, la infraestructura y la red.

Su estrategia de supervisión debe considerar el impacto de los errores grises. Para obtener más información sobre los errores grises, consulte Gray failures en el documento técnico Advanced Multi-AZ Resilience Patterns.

Pasos para la implementación

- El intervalo de supervisión depende de la rapidez con la que deba recuperarse. El tiempo de recuperación depende del tiempo que tarde la recuperación, por lo que debe determinar la frecuencia de recopilación teniendo en cuenta este tiempo y el objetivo de tiempo de recuperación (RTO).
- Configure la supervisión detallada de los componentes y los servicios administrados.

  - Determine si son necesarios la supervisión detallada de las instancias de EC2 y el escalado automático. La supervisión detallada proporciona métricas en intervalos de un minuto y la supervisión predeterminada proporciona métricas en intervalos de cinco minutos.
  - Determine si se necesita la supervisión mejorada de RDS. La supervisión mejorada usa un agente en las instancias de RDS para obtener información útil sobre los diferentes procesos o subprocesos.
  - Determine los requisitos de supervisión de los componentes sin servidor cruciales para Lambda, API Gateway, Amazon EKS, Amazon ECS y todos los tipos de equilibradores de carga.
  - Determine los requisitos de supervisión de los componentes de almacenamiento para Amazon S3, Amazon FSx, Amazon EFS y Amazon EBS.
- Cree métricas personalizadas para medir los indicadores clave de rendimiento (KPI) del negocio. Las cargas de trabajo implementan funciones empresariales clave, que deben usarse como KPI para ayudar a identificar cuándo se produce un problema indirecto.
- Supervise la experiencia del usuario para detectar errores mediante canarios del usuario. Las pruebas de transacciones sintéticas (también denominadas “pruebas canario”, que no deben confundirse con las implementaciones canario) que puedan ejecutar y simular el comportamiento de los clientes son uno de los procesos de prueba más importantes. Ejecute estas pruebas constantemente en los puntos de conexión de las cargas de trabajo desde distintas ubicaciones remotas.
- Cree métricas personalizadas que controlen la experiencia del usuario. Si puede instrumentar la experiencia del cliente, puede determinar cuándo se degrada la experiencia del cliente.
- Defina alarmas para detectar cuándo alguna parte de la carga de trabajo no funciona correctamente y para indicar cuándo escalar automáticamente los recursos. Las alarmas pueden mostrarse visualmente en paneles, enviar alertas a través de Amazon SNS o por correo electrónico y trabajar con escalado automático para escalar o reducir verticalmente los recursos de la carga de trabajo.
- Cree paneles para visualizar las métricas. Se pueden usar paneles para visualizar las tendencias, los valores atípicos y otros indicadores de problemas potenciales, o para proporcionar una indicación de problemas que tal vez le convenga investigar.
- Cree una supervisión de rastreo distribuida para sus servicios. Con la supervisión distribuida, podrá saber cómo se comporta su aplicación y sus servicios subyacentes para identificar y resolver la causa raíz de los problemas y errores de rendimiento.
- Cree paneles de sistemas de supervisión (mediante CloudWatch o X-Ray) y recopilaciones de datos en una región y una cuenta independientes.

- Manténgase informado sobre las degradaciones del servicio con AWS Health. Cree notificaciones de eventos de AWS Health adecuados para su propósito para los canales de correo electrónico y chat a través de AWS User Notifications e intégrelas mediante programación con las herramientas de supervisión y alertas a través de Amazon EventBridge.

Recursos

Prácticas recomendadas relacionadas:

- Availability Definition
- REL11-BP06 Envío de notificaciones cuando los eventos afecten a la disponibilidad

Documentos relacionados:

- Amazon CloudWatch Synthetics le permite crear canarios de usuario
- Activar o desactivar el monitoreo detallado para las instancias
- Supervisión mejorada
- Monitoring Your Auto Scaling Groups and Instances Using Amazon CloudWatch
- Publicar métricas personalizadas
- Uso de las alarmas de Amazon CloudWatch
- Uso de paneles de CloudWatch
- Uso de paneles de CloudWatch entre regiones y entre cuentas
- Uso del rastreo de X-Ray entre regiones y entre cuentas
- Understanding availability

Videos relacionados:

- Mitigating gray failures

Ejemplos relacionados:

- One Observability Workshop: Explore X-Ray

Herramientas relacionadas:

- CloudWatch
- CloudWatch X-Ray

REL11-BP02 Conmutación por error a recursos en buen estado

Si un recurso fallara, los recursos en buen estado deberían seguir atendiendo las solicitudes. Para problemas de ubicación (como zonas de disponibilidad o Región de AWS), asegúrese de que disponga de sistemas para conmutar por error a recursos en buen estado en ubicaciones sin problemas.

Al diseñar un servicio, distribuya la carga entre los recursos, las zonas de disponibilidad o las regiones. De esta manera, el error de un recurso individual o el deterioro puede mitigarse al desplazar el tráfico a los recursos restantes en buen estado. Tenga en cuenta cómo se descubren los servicios y cómo se enruta a ellos en caso de que se produzca un error.

Tenga en cuenta la recuperación de errores al diseñar sus servicios. En AWS, diseñamos servicios para minimizar el tiempo de recuperación de los errores y el impacto en los datos. Nuestros servicios utilizan principalmente almacenes de datos que confirman las solicitudes solo después de que se almacenen de forma duradera en varias réplicas en una región. Se han diseñado para utilizar el aislamiento basado en celdas y el aislamiento de errores que proporcionan las zonas de disponibilidad. Utilizamos ampliamente la automatización en nuestros procedimientos operativos. También optimizamos nuestra funcionalidad de reemplazo y reinicio para recuperarnos rápidamente de las interrupciones.

Los patrones y diseños que permiten la conmutación por error varían para cada servicio de plataforma de AWS. Muchos servicios administrados nativos de AWS son zonas de disponibilidad múltiples de forma nativa (como Lambda o API Gateway). Otros servicios de AWS (como EC2 y EKS) requieren diseños específicos de las prácticas recomendadas para admitir la conmutación por error de los recursos o el almacenamiento de datos en las AZ.

La supervisión debe configurarse para que compruebe que el recurso de conmutación por error esté en buen estado, hacer un seguimiento del progreso de los recursos de conmutación por error y supervisar la recuperación de los procesos empresariales.

Resultado deseado: los sistemas son capaces de utilizar nuevos recursos de forma automática o manual para recuperarse de la degradación.

Patrones comunes de uso no recomendados:

- La planificación de errores no forma parte de la fase de planificación y diseño.
- No se establecen el RTO ni el RPO.
- Supervisión insuficiente para detectar recursos defectuosos.
- Aislamiento adecuado de los dominios de error.
- No se considera la conmutación por error multirregional.
- La detección de errores es demasiado sensible o agresiva a la hora de decidir efectuar una conmutación por error.
- No probar ni validar el diseño de la conmutación por error.
- Llevar a cabo la automatización de la recuperación automática, pero no notificar que se necesitaba una reparación.
- Ausencia de un periodo de amortiguación para evitar que la conmutación por error se lleve a cabo demasiado pronto.

Beneficios de establecer esta práctica recomendada: con una degradación uniforme y una recuperación rápida, puede crear sistemas más resilientes que mantengan la fiabilidad cuando se producen errores.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Los servicios de AWS, como Elastic Load Balancing y Amazon EC2 Auto Scaling, ayudan a distribuir la carga entre los recursos y las zonas de disponibilidad. Por lo tanto, el error de un recurso individual (como una instancia de EC2) o el deterioro de una zona de disponibilidad puede mitigarse si se desplaza el tráfico a los recursos restantes en buen estado.

Para las cargas de trabajo multirregionales, los diseños son más complicados. Por ejemplo, las réplicas de lectura entre regiones le permiten implementar sus datos en varias Regiones de AWS. Sin embargo, la conmutación por error sigue siendo necesaria para convertir la réplica de lectura en principal y, a continuación, dirigir el tráfico al nuevo punto de conexión. Amazon Route 53, el Controlador de recuperación de aplicaciones de (ARC), Amazon CloudFront y AWS Global Accelerator pueden ayudar a enrutar el tráfico en las Regiones de AWS.

Los servicios de AWS, como Amazon S3, Lambda, API Gateway, Amazon SQS, Amazon SNS, Amazon SES, Amazon Pinpoint, Amazon ECR, AWS Gestor de certificados, EventBridge o Amazon DynamoDB, se implementan automáticamente en varias zonas de disponibilidad mediante AWS.

En caso de error, estos servicios de AWS dirigen automáticamente el tráfico a ubicaciones en buen estado. Los datos se almacenan de forma redundante en varias zonas de disponibilidad y siguen estando disponibles.

Para Amazon RDS, Amazon Aurora, Amazon Redshift, Amazon EKS o Amazon ECS, Multi-AZ es una opción de configuración. AWS puede dirigir el tráfico a la instancia en buen estado si se inicia la conmutación por error. Esta acción de conmutación por error puede llevarla a cabo AWS o según lo requiera el cliente

Para las instancias de Amazon EC2, Amazon Redshift, las tareas de Amazon ECS o los pods de Amazon EKS, elige en qué zonas de disponibilidad deben implementarse. En algunos diseños, Elastic Load Balancing proporciona la solución para detectar instancias en zonas que no están en buen estado y dirigir el tráfico a las que sí están en buen estado. Elastic Load Balancing también puede dirigir el tráfico a componentes de su centro de datos en las instalaciones.

En cuanto a la conmutación por error del tráfico multirregional, el reenrutamiento puede utilizar Amazon Route 53, el Controlador de recuperación de aplicaciones de Amazon, AWS Global Accelerator, DNS privado de Route 53 para VPC o CloudFront para proporcionar una forma de definir dominios de Internet y asignar políticas de enrutamiento, incluidas comprobaciones de estado, para enrutar el tráfico a regiones en buen estado. AWS Global Accelerator proporciona direcciones IP estáticas que actúan como punto de entrada fijo a su aplicación; a continuación, se enrutan a los puntos de conexión de las Regiones de AWS que elija, mediante la red global de AWS en lugar de Internet para mejorar el rendimiento y la fiabilidad.

Pasos para la implementación

- Cree diseños de conmutación por error para todas las aplicaciones y servicios pertinentes. Aísle cada componente de la arquitectura y cree diseños de conmutación por error que satisfagan el RTO y el RPO de cada componente.
- Configure entornos inferiores (como los de desarrollo o prueba) con todos los servicios que sean necesarios para tener un plan de conmutación por error. Implemente las soluciones mediante la infraestructura como código (IaC) para garantizar la repetibilidad.
- Configure un sitio de recuperación, como una segunda región, para implementar y probar los diseños de conmutación por error. Si fuera necesario, los recursos para las pruebas se pueden configurar temporalmente para limitar los costos adicionales.
- Determine qué planes de conmutación por error se automatizan mediante AWS, cuáles pueden automatizarse mediante un proceso de DevOps y cuáles pueden ser manuales. Documente y mida el RTO y el RPO de cada servicio.

- Cree un manual de estrategias de conmutación por error e incluya todos los pasos de la conmutación por error de cada recurso, aplicación y servicio.
- Cree un manual de estrategias de conmutación por recuperación e incluya todos los pasos de la conmutación por recuperación (con plazos) de cada recurso, aplicación y servicio.
- Cree un plan para iniciar y ensayar el manual de estrategias. Utilice simulaciones y pruebas de caos para poner a prueba los pasos del manual de estrategias y la automatización.
- Para problemas de ubicación (como zonas de disponibilidad o Región de AWS), asegúrese de que disponga de sistemas para conmutar por error a recursos en buen estado en ubicaciones sin problemas. Compruebe la cuota, los niveles de escalado automático y los recursos en ejecución antes de llevar a cabo la prueba de conmutación por error.

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- REL13: Plan para DR
- REL10: Uso del aislamiento de errores para proteger la carga de trabajo

Documentos relacionados:

- Setting RTO and RPO Targets
- Failover using Route 53 Weighted routing
- Disaster Recovery with Amazon Application Recovery Controller
- EC2 with autoscaling
- EC2 Deployments - Multi-AZ
- ECS Deployments - Multi-AZ
- Switch traffic using Amazon Application Recovery Controller
- Lambda con un equilibrador de carga de aplicación y conmutación por error
- ACM Replication and Failover
- Parameter Store Replication and Failover
- ECR cross region replication and Failover
- Secrets manager cross region replication configuration

- Enable cross region replication for EFS and Failover
- EFS Cross Region Replication and Failover
- Conmutación por error de red
- S3 Endpoint failover using MRAP
- Creación de replicación entre regiones para S3
- Guidance for Cross Region Failover and Graceful Failback on AWS
- Failover using multi-region global accelerator
- Failover with DRS

Ejemplos relacionados:

- Disaster Recovery on AWS
- Elastic Disaster Recovery on AWS

REL11-BP03 Automatización de la reparación en todas las capas

Cuando se detecte un error, utilice las funciones automatizadas para tomar medidas correctivas. Las degradaciones pueden repararse automáticamente a través de mecanismos de servicio interno o requerir que los recursos se reinicien o eliminen a través de medidas de corrección.

Para las aplicaciones autoadministradas y la reparación entre regiones, los diseños de recuperación y los procesos de reparación automatizados se pueden extraer de las prácticas recomendadas existentes.

La capacidad de reiniciar o eliminar un recurso es una herramienta importante para corregir los errores. Una práctica recomendada es convertir los servicios en servicios sin estado siempre que sea posible. Esto evita la pérdida de datos o disponibilidad tras el reinicio del recurso. En la nube, puede (y generalmente debería) sustituir todo el recurso (por ejemplo, la instancia de computación o la función sin servidor) como parte del reinicio. El reinicio en sí es una forma sencilla y fiable de recuperarse de un error. En las cargas de trabajo ocurren muchos tipos de errores diferentes. Los errores pueden ocurrir en el hardware, el software, las comunicaciones y el funcionamiento.

El reinicio o el reintento también se aplican a las solicitudes de red. Se aplica el mismo enfoque de recuperación tanto a un tiempo de espera de la red como a un error en la dependencia, en el que la dependencia devuelve un error. Ambos eventos tienen un efecto similar en el sistema, por lo que,

en lugar de intentar convertir cada uno en un caso especial, se aplicaría una estrategia similar de reintento con retroceso exponencial y fluctuación. La capacidad de reiniciar es un mecanismo de recuperación que aparece en la computación orientada a la recuperación y en las arquitecturas de clústeres de alta disponibilidad.

Resultado deseado: se llevan a cabo medidas automatizadas para corregir la detección de un error.

Patrones comunes de uso no recomendados:

- Aprovisionar recursos sin escalado automático.
- Implementar las aplicaciones en instancias o contenedores individualmente.
- Implementar aplicaciones que no se pueden implementar en varias ubicaciones sin usar la recuperación automática.
- Reparar manualmente las aplicaciones que el escalado automático y la recuperación automática no pueden reparar.
- No hay automatización de las bases de datos de conmutación por error.
- Carencia de métodos automatizados para redirigir el tráfico a nuevos puntos de conexión.
- No hay replicación del almacenamiento.

Beneficios de establecer esta práctica recomendada: la reparación automática puede reducir el tiempo medio de recuperación y mejorar la disponibilidad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Los diseños de Amazon EKS u otros servicios de Kubernetes deben incluir conjuntos de réplicas o con estado mínimo y máximo y el tamaño mínimo del clúster y los grupos de nodos. Estos mecanismos proporcionan una cantidad mínima de recursos de procesamiento disponibles de forma continua y, al mismo tiempo, corrigen automáticamente cualquier error mediante el plano de control de Kubernetes.

Los patrones de diseño a los que se accede a través de un equilibrador de carga mediante clústeres de computación deben utilizar los grupos de escalado automático. Elastic Load Balancing (ELB) distribuye automáticamente el tráfico de aplicaciones entrante entre varios destinos y dispositivos virtuales en una o más zonas de disponibilidad (AZ).

Los diseños basados en computación en clúster que no utilizan el equilibrio de carga deben tener un diseño de tamaño que dé cabida a la pérdida de al menos un nodo. Esto permitirá que el servicio siga funcionando con una capacidad potencialmente reducida mientras recupera un nuevo nodo. Algunos servicios son Mongo, el Acelerador de DynamoDB, Amazon Redshift, Amazon EMR, Cassandra, Kafka, MSK-EC2, Couchbase, ELK y Amazon OpenSearch Service. Muchos de estos servicios se pueden diseñar con características adicionales de autorreparación. Algunas tecnologías de clústeres deben generar una alerta tras la pérdida de un nodo, lo que desencadena un flujo de trabajo automático o manual para recrear un nuevo nodo. Este flujo de trabajo se puede automatizar con AWS Systems Manager para corregir los problemas rápidamente.

Se puede usar Amazon EventBridge para supervisar y filtrar los eventos, como las alarmas de CloudWatch o cambios en el estado en otros servicios de AWS. En función de la información del evento, se puede invocar a AWS Lambda, Automatización de Systems Manager u otros destinos para ejecutar una lógica de corrección personalizada en la carga de trabajo. Amazon EC2 Auto Scaling se puede configurar para comprobar el estado de la instancia de EC2. Si el estado de la instancia es cualquier otro estado distinto de En ejecución o si el estado del sistema es Dañado, Amazon EC2 Auto Scaling considera que la instancia tiene un estado incorrecto y lanza una instancia de reemplazo. Para sustituciones a gran escala (como la pérdida de toda una zona de disponibilidad), se prefiere la estabilidad estática para la alta disponibilidad.

Pasos para la implementación

- Use grupos de escalado automático para implementar niveles en una carga de trabajo. El escalado automático puede llevar a cabo una reparación automática de aplicaciones sin estado y agregar o eliminar capacidad.
- En el caso de las instancias de computación indicadas anteriormente, utilice el equilibrio de carga y elija el tipo de equilibrador de carga adecuado.
- Considere la reparación para Amazon RDS. Con las instancias en espera, defina la configuración de la conmutación por error automática en la instancia en espera. Para la réplica de lectura de Amazon RDS, se requiere un flujo de trabajo automatizado para convertir una réplica de lectura en principal.
- Implemente la recuperación automática en instancias de EC2 que tengan aplicaciones implementadas que no se puedan implementar en varias ubicaciones y puedan tolerar el reinicio tras un error. La recuperación automática se puede usar para reemplazar hardware defectuoso y reiniciar la instancia cuando la aplicación no se puede implementar en varias ubicaciones. Los metadatos de la instancia y las direcciones IP asociadas se conservan, así como los volúmenes de EBS y los puntos de montaje en Amazon Elastic File System o File Systems para Lustre y

Windows. Con AWS OpsWorks, puede configurar la reparación automática de las instancias de EC2 en el nivel de capa.

- Implemente la recuperación automática mediante AWS Step Functions y AWS Lambda cuando no pueda usar el escalado automático ni la recuperación automática o cuando la recuperación automática produzca un error. Cuando no pueda usar el escalado automático ni la recuperación automática, o esta produzca un error, puede automatizar la reparación con AWS Step Functions y AWS Lambda.
- Se puede usar Amazon EventBridge para supervisar y filtrar los eventos, como las alarmas de CloudWatch o cambios en el estado en otros servicios de AWS. En función de la información del evento, se puede invocar AWS Lambda (u otros destinos) para ejecutar una lógica de corrección personalizada en su carga de trabajo.

Recursos

Prácticas recomendadas relacionadas:

- Availability Definition
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores

Documentos relacionados:

- Funcionamiento de AWS Auto Scaling
- Recuperación automática de Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic File System (Amazon EFS)
- What is Amazon FSx for Lustre?
- What is Amazon FSx for Windows File Server?
- AWS OpsWorks: Using Auto Healing to Replace Failed Instances
- Qué es AWS Step Functions?
- Qué es AWS Lambda?
- Qué es Amazon EventBridge?
- Using Amazon CloudWatch Alarms
- Amazon RDS Failover
- SSM - Systems Manager Automation

- Resilient Architecture Best Practices

Videos relacionados:

- Automatically Provision and Scale OpenSearch Service
- Amazon RDS Failover Automatically

Ejemplos relacionados:

- Amazon RDS Failover Workshop

Herramientas relacionadas:

- CloudWatch
- CloudWatch X-Ray

REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación

Los planos de control proporcionan las API administrativas que se utilizan para crear, leer y describir, actualizar, eliminar y enumerar los recursos (CRUDL), mientras que los planos de datos gestionan el tráfico de servicio diario. Al implementar respuestas de recuperación o mitigación a eventos que puedan afectar a la resiliencia, céntrese en utilizar un número mínimo de operaciones del plano de control para recuperar, reescalar, restaurar, reparar o conmutar por error el servicio. La acción del plano de datos debe reemplazar cualquier actividad durante estos eventos de degradación.

Por ejemplo, las siguientes son todas las acciones del plano de control: lanzar una nueva instancia de computación, crear almacenamiento en bloques y describir los servicios de colas. Al lanzar instancias de computación, el plano de control debe hacer varias tareas, como encontrar un host físico con capacidad, asignar interfaces de red, preparar los volúmenes de almacenamiento en bloques locales, generar credenciales y agregar reglas de seguridad. Los planos de control suelen tener una orquestación complicada.

Resultado deseado: cuando un recurso entra en un estado deteriorado, el sistema es capaz de recuperarse automática o manualmente al cambiar el tráfico de recursos deteriorados a recursos en buen estado.

Patrones comunes de uso no recomendados:

- Depender de cambiar los registros de DNS para redirigir el tráfico.
- Depender de las operaciones de escalado del plano de control para reemplazar los componentes dañados debido a que no se han aprovisionado suficientes recursos.
- Confiar en amplias acciones del plano de control de varios servicios y varias API para corregir cualquier categoría de deterioro.

Beneficios de establecer esta práctica recomendada: el aumento de la tasa de éxito de la corrección automatizada puede reducir el tiempo medio de recuperación y mejorar la disponibilidad de la carga de trabajo.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio (para determinados tipos de degradaciones del servicio, los planos de control se ven afectados). Si se depende del uso extensivo del plano de control para la corrección, se puede aumentar el tiempo de recuperación (RTO) y el tiempo medio de recuperación (MTTR).

Guía para la implementación

Para limitar las acciones del plano de datos, evalúe cada servicio para determinar qué acciones son necesarias para restablecer el servicio.

Use el Controlador de recuperación de aplicaciones de Amazon para cambiar el tráfico de DNS. Estas características supervisan continuamente la capacidad de la aplicación de recuperarse de los errores y le permiten controlar la recuperación de la aplicación en las distintas Regiones de AWS, zonas de disponibilidad y en las instalaciones.

Las políticas de enrutamiento de Route 53 utilizan el plano de control, por lo que no debe confiar en él para la recuperación. Los planos de datos de Route 53 responden a consultas de DNS y llevan a cabo y evalúan comprobaciones de estado. Están distribuidos por todo el mundo y están diseñados para cumplir con un acuerdo de nivel de servicio (SLA) con una disponibilidad del 100 %.

Las API de administración de Route 53 y las consolas en las que se crean, actualizan y eliminan recursos de Route 53 se ejecutan en planos de control diseñados para dar prioridad a la sólida coherencia y durabilidad que necesita al administrar DNS. Para conseguirlo, los planos de control se encuentran en una única región: Este de EE. UU. (Norte de Virginia). Aunque ambos sistemas se han diseñado para ser muy fiables, los planos de control no están incluidos en el SLA. Podría haber eventos poco frecuentes en los que el diseño resiliente del plano de datos permita mantener la disponibilidad mientras que los planos de control no lo permitan. Con los mecanismos de

recuperación de desastres y conmutación por error, utilice las funciones del plano de datos para proporcionar la mejor fiabilidad posible.

Diseñe su infraestructura informática para que sea estable desde el punto de vista estático a fin de evitar el uso del plano de control durante un incidente. Por ejemplo, si utiliza instancias de Amazon EC2, evite aprovisionar nuevas instancias manualmente o dar instrucciones a los grupos de escalado automático para que agreguen instancias en respuesta. Para obtener los niveles más altos de resiliencia, aprovisione suficiente capacidad en el clúster utilizado para la conmutación por error. Si este umbral de capacidad debe limitarse, establezca limitaciones en todo el sistema de principio a fin para limitar de forma segura el tráfico total que llega al conjunto limitado de recursos.

En el caso de los servicios como Amazon DynamoDB, Amazon API Gateway, los equilibradores de carga y sin servidor de AWS Lambda, el uso de esos servicios utiliza el plano de datos. Sin embargo, la creación de nuevas funciones, equilibradores de carga, puertas de enlace de API o tablas de DynamoDB es una acción del plano de control y debe completarse antes de la degradación como preparación para un evento y ensayo de las acciones de conmutación por error. En el caso de Amazon RDS, las acciones del plano de datos permiten el acceso a los datos.

Para obtener más información sobre planos de datos, planos de control y cómo AWS crea servicios para cumplir los objetivos de alta disponibilidad, consulte Estabilidad estática con zonas de disponibilidad.

Comprenda qué operaciones están en el plano de datos y cuáles están en el plano de control.

Pasos para la implementación

Para cada carga de trabajo que deba restaurarse después de un evento de degradación, evalúe el manual de procedimientos de conmutación por error, el diseño de alta disponibilidad, el diseño de reparación automática o el plan de restauración de recursos de alta disponibilidad. Identifique cada acción que pueda considerarse una acción del plano de control.

Considere cambiar la acción de control por una acción del plano de datos:

- Escalado automático (plano de control) a los recursos de Amazon EC2 preescalados (plano de datos)
- Escalado de instancias de Amazon EC2 (plano de control) a escalado de AWS Lambda (plano de datos)
- Evalúe cualquier diseño con Kubernetes y la índole de las acciones del plano de control. Agregar pods es una acción del plano de datos en Kubernetes. Las acciones deben limitarse a agregar

pods y no a agregar nodos. Usar nodos sobreaprovisionados es el método preferido para limitar las acciones del plano de control

Tenga en cuenta los enfoques alternativos que permiten que las acciones del plano de datos afecten a la misma corrección.

- Cambio de registro de Route 53 (plano de control) o Controlador de recuperación de aplicaciones de Amazon (plano de datos)
- Comprobaciones de estado de Route 53 para obtener actualizaciones más automatizadas

Considere algunos servicios en una región secundaria, en caso de que el servicio sea crítico, para permitir más acciones del plano de control y el plano de datos en una región no afectada.

- Amazon EC2 Auto Scaling o Amazon EKS en una región principal en comparación con Amazon EC2 Auto Scaling o Amazon EKS en una región secundaria y enrutamiento del tráfico a una región secundaria (acción del plano de control)
- Hacer réplicas de lectura en la región principal secundaria o intentar la misma acción en la región principal (acción del plano de control)

Recursos

Prácticas recomendadas relacionadas:

- Availability Definition
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores

Documentos relacionados:

- Socio de APN: socios que pueden ayudar con la automatización de su tolerancia a errores
- AWS Marketplace: productos que pueden usarse para tolerancia a errores
- Amazon Builders' Library: Avoiding overload in distributed systems by putting the smaller service in control
- API de Amazon DynamoDB (plano de control y plano de datos)
- Ejecuciones de AWS Lambda (divididas entre el plano de control y el plano de datos)
- Plano de datos de AWS Elemental MediaStore

- Building highly resilient applications using Amazon Application Recovery Controller, Part 1: Single-Region stack
- Building highly resilient applications using Amazon Application Recovery Controller, Part 2: Multi-Region stack
- Creating Disaster Recovery Mechanisms Using Amazon Route 53
- What is Amazon Application Recovery Controller
- Kubernetes Control Plane and data plane

Videos relacionados:

- Back to Basics - Using Static Stability
- Building resilient multi-site workloads using AWS global services

Ejemplos relacionados:

- Introducing Amazon Application Recovery Controller
- Amazon Builders' Library: Avoiding overload in distributed systems by putting the smaller service in control
- Building highly resilient applications using Amazon Application Recovery Controller, Part 1: Single-Region stack
- Building highly resilient applications using Amazon Application Recovery Controller, Part 2: Multi-Region stack
- Estabilidad estática con zonas de disponibilidad

Herramientas relacionadas:

- Amazon CloudWatch
- AWS X-Ray

REL11-BP05 Uso de la estabilidad estática para evitar el comportamiento bimodal

Las cargas de trabajo deben ser estáticamente estables y funcionar solo en un único modo normal. El comportamiento bimodal se produce cuando la carga de trabajo presenta un comportamiento diferente en los modos normal y de error.

Por ejemplo, puede intentar recuperarse de un error en una zona de disponibilidad mediante el lanzamiento de nuevas instancias en una zona de disponibilidad distinta. Esto puede dar como resultado una respuesta bimodal durante un modo de error. En lugar de ello, debe crear cargas de trabajo que sean estables estáticamente y funcionen en un solo modo. En este ejemplo, esas instancias deben haberse aprovisionado en la segunda zona de disponibilidad antes del error. Este diseño de estabilidad estática verifica que la carga de trabajo solo funcione en un único modo.

Resultado deseado: las cargas de trabajo no muestran un comportamiento bimodal durante los modos normal y de error.

Patrones comunes de uso no recomendados:

- Suponer que los recursos siempre se pueden aprovisionar independientemente del alcance del error.
- Intentar adquirir recursos de forma dinámica durante un error.
- No aprovisionar los recursos adecuados en todas las zonas o regiones hasta que se produzca un error.
- Considerar diseños estáticos estables solo para recursos de computación.

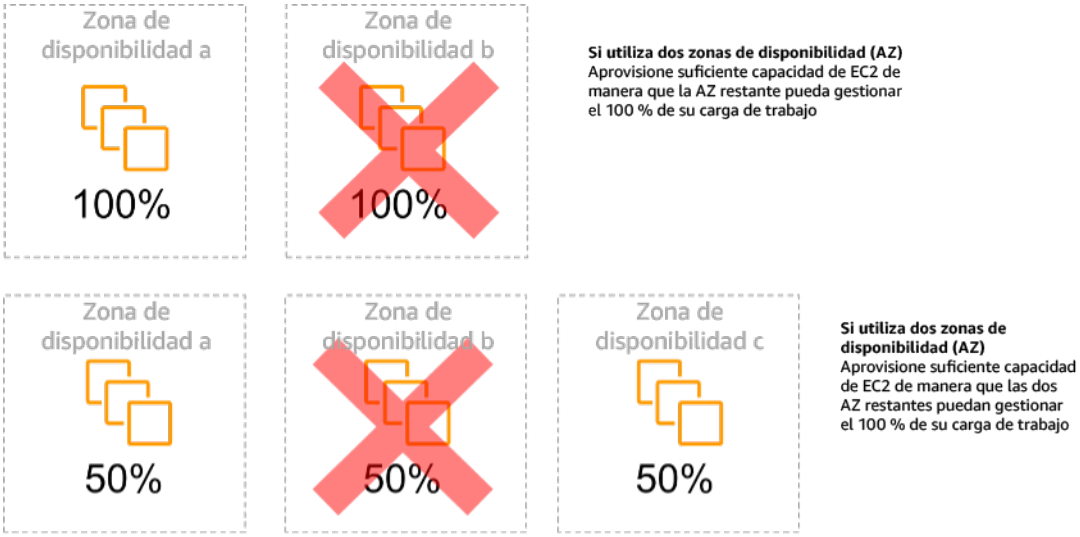
Beneficios de establecer esta práctica recomendada: las cargas de trabajo que se ejecutan con diseños estáticamente estables pueden tener resultados predecibles durante eventos normales y de error.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

El comportamiento bimodal ocurre cuando la carga de trabajo exhibe diferentes comportamientos en los modos normal y de error (como confiar en el lanzamiento de nuevas instancias si se produce un error en una zona de disponibilidad). Un ejemplo de comportamiento bimodal ocurre cuando los

diseños de Amazon EC2 estables aprovisionan suficientes instancias en cada zona de disponibilidad para gestionar la carga de trabajo si se eliminara una zona de disponibilidad. Se comprobaría el estado de Elastic Load Balancing o Amazon Route 53 para desviar una carga de las instancias dañadas. Una vez desviado el tráfico, use AWS Auto Scaling para sustituir de manera asíncrona las instancias de la zona con errores y lanzarlas en las zonas en buen estado. La estabilidad estática para implementaciones de computación (como instancias de EC2 o contenedores) da como resultado la máxima fiabilidad.



Estabilidad estática de las instancias de EC2 entre zonas de disponibilidad

Esto debe ponderarse en comparación con el costo de este modelo y el valor empresarial de mantener la carga de trabajo en todos los casos de resiliencia. Es menos costoso aprovisionar menos capacidad de computación y confiar en el lanzamiento de nuevas instancias en caso de error, pero en el caso de errores a gran escala (como un deterioro regional o de zona de disponibilidad), este enfoque es menos eficaz porque se basa tanto en un plano operativo como en la disponibilidad de recursos suficientes en las zonas o regiones no afectadas.

Su solución también debe ponderar la fiabilidad en comparación con los costos necesarios para la carga de trabajo. Las arquitecturas de estabilidad estática se aplican a una variedad de arquitecturas, incluidas las instancias de computación distribuidas en las zonas de disponibilidad, los diseños de réplicas de lectura de bases de datos, los diseños de clústeres de Kubernetes (Amazon EKS) y las arquitecturas de conmutación por error multirregional.

También es posible implementar un diseño más estable desde el punto de vista estático mediante el uso de más recursos en cada zona. Al agregar más zonas, reduce la cantidad de procesamiento adicional que necesita para la estabilidad estática.

Un ejemplo de comportamiento bimodal sería un tiempo de espera de la red que podría provocar que un sistema intente actualizar el estado de configuración de todo el sistema. Se agregaría una carga inesperada a otro componente, lo que podría hacer que se produzca un error y desencadene otras consecuencias inesperadas. Este bucle de retroalimentación negativa afecta a la disponibilidad de su carga de trabajo. En lugar de ello, puede crear cargas de trabajo que sean estables estáticamente y funcionen en un solo modo. Un diseño estáticamente estable haría un trabajo constante y actualizaría continuamente el estado de configuración a una cadencia establecida. Cuando una llamada genera un error, la carga de trabajo utiliza el valor previamente almacenado en caché e inicia una alarma.

Otro ejemplo de comportamiento bimodal es permitir que los clientes omitan la caché de la carga de trabajo si se produce un error. Esto podría parecer una solución para satisfacer las necesidades del cliente, pero puede cambiar notablemente la demanda de la carga de trabajo y es probable que produzca errores.

Evalúe las cargas de trabajo críticas para determinar cuáles requieren este tipo de diseño de resiliencia. Se debe revisar cada componente de la aplicación en las cargas que se consideren cruciales. Algunos tipos de servicios que requieren evaluaciones de estabilidad estática son:

- Computación: Amazon EC2, EKS-EC2, ECS-EC2, EMR-EC2
- Bases de datos: Amazon Redshift, Amazon RDS, Amazon Aurora
- Almacenamiento: Amazon S3 (zona única), Amazon EFS (montajes), Amazon FSx (montajes)
- Equilibradores de carga: según diseños determinados

Pasos para la implementación

- Cree cargas de trabajo que sean estables estáticamente y funcionen en un solo modo. En este caso, aprovisione suficientes instancias en cada región o zona de disponibilidad para gestionar la capacidad de la carga de trabajo en caso de que se eliminara una región o zona de disponibilidad. Puede usar una variedad de servicios para el enrutamiento a recursos en buen estado, como:
  - Cross Region DNS Routing
  - MRAP Amazon S3 MultiRegion Routing
  - AWS Global Accelerator
  - Controlador de recuperación de aplicaciones de Amazon
- Configure las réplicas de lectura de base de datos de modo que tengan en cuenta la pérdida de una única instancia principal o una réplica de lectura. Si las réplicas de lectura atienden el tráfico,

la cantidad en cada zona de disponibilidad y cada región debe ser igual a la necesidad general en caso de que se produzca un error en la zona o región.

- Configure los datos cruciales en el almacenamiento de Amazon S3 que está diseñado para ser estáticamente estable para los datos almacenados en caso de que se produzca un error en la zona de disponibilidad. Si se utiliza la clase de almacenamiento Amazon S3 One Zone-IA, no debe considerarse estable desde el punto de vista estático, ya que la pérdida de esa zona minimiza el acceso a los datos almacenados.
- Los equilibradores de carga a veces están configurados incorrectamente o por diseño para prestar servicio a una zona de disponibilidad específica. En este caso, el diseño estáticamente estable podría consistir en distribuir una carga de trabajo entre varias zonas de disponibilidad en un diseño más complejo. El diseño original se puede utilizar para reducir el tráfico entre zonas por motivos de seguridad, latencia o costo.

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- Availability Definition
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación

Documentos relacionados:

- Minimizing Dependencies in a Disaster Recovery Plan
- Amazon Builders' Library: estabilidad estática con zonas de disponibilidad
- Fault Isolation Boundaries
- Estabilidad estática con zonas de disponibilidad
- RDS multizona
- Minimizing Dependencies in a Disaster Recovery Plan
- Cross Region DNS Routing
- MRAP Amazon S3 MultiRegion Routing
- AWS Global Accelerator
- Controlador de recuperación de aplicaciones de Amazon
- Amazon S3 de zona única

- Cross Zone Load Balancing

Videos relacionados:

- Static stability in AWS: AWS re:Invent 2019: Introducing The Amazon Builders' Library (DOP328)

REL11-BP06 Envío de notificaciones cuando los eventos afecten a la disponibilidad

Se envían notificaciones cuando se detecta que se han superado los umbrales, incluso si el evento que causó el problema se ha resuelto automáticamente.

La corrección automática permite que la carga de trabajo sea fiable. Sin embargo, también puede ocultar problemas subyacentes que deberían abordarse. Implemente una supervisión y unos eventos adecuados para poder detectar patrones de problemas, incluidos los que pueden abordarse mediante corrección automática, para que pueda resolver los problemas de la causa fundamental.

Los sistemas resilientes están diseñados para que los eventos de degradación se comuniquen inmediatamente a los equipos correspondientes. Estas notificaciones deben enviarse a través de uno o varios canales de comunicación.

Resultado deseado: las alertas se envían inmediatamente a los equipos de operaciones cuando se superan los umbrales, como las tasas de error, la latencia u otras métricas cruciales de los indicadores clave de rendimiento (KPI), para que estos problemas se resuelvan lo antes posible y se evite o minimice el impacto en los usuarios.

Patrones comunes de uso no recomendados:

- Enviar demasiadas alarmas.
- Enviar alarmas que no son procesables.
- Establecer umbrales de alarma demasiado altos (muy sensibles) o demasiado bajos (poco sensibles).
- No enviar alarmas para dependencias externas.
- No considerar los errores grises al diseñar la supervisión y las alarmas.
- Llevar a cabo la automatización de la reparación, pero sin notificar al equipo adecuado que se necesita una reparación.

Beneficios de establecer esta práctica recomendada: las notificaciones de recuperación permiten que los equipos operativos y empresariales estén al tanto de las degradaciones del servicio para que puedan reaccionar de inmediato y minimizar tanto el tiempo medio de detección (MTTD) como el tiempo medio de reparación (MTTR). Las notificaciones de los eventos de recuperación también garantizan que no se ignoren problemas que ocurren con poca frecuencia.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio. Si no se implementan los mecanismos adecuados de supervisión y notificación de eventos, es posible que no se detecten patrones de problemas, incluidos los que pueden abordarse mediante la corrección automática. El equipo solo descubrirá la degradación del sistema cuando los usuarios se pongan en contacto con el servicio de atención al cliente o por casualidad.

Guía para la implementación

Al definir una estrategia de supervisión, la activación de una alarma es un evento frecuente. Es probable que este evento contenga un identificador de la alarma, el estado de la alarma (como `IN ALARM` o `OK`) y los detalles de lo que la desencadenó. En muchos casos, se debe detectar el evento de alarma y enviar una notificación por correo electrónico. Este es un ejemplo de una acción en una alarma. La notificación de alarmas es fundamental en la observabilidad, ya que informa a las personas adecuadas de que existe un problema. Sin embargo, cuando la acción sobre los eventos madura en su solución de observabilidad, puede solucionar el problema automáticamente sin necesidad de intervención humana.

Una vez que se hayan establecido las alarmas de supervisión de los KPI, se deben enviar alertas a los equipos correspondientes cuando se superen los umbrales. Esas alertas también se pueden usar para activar procesos automatizados que intentarán corregir la degradación.

Para una supervisión de umbrales más compleja, se deben considerar las alarmas compuestas. Las alarmas compuestas utilizan una serie de alarmas de supervisión de KPI para crear una alerta basada en la lógica empresarial operativa. Las alarmas de CloudWatch se pueden configurar para enviar correos electrónicos o para registrar incidentes en sistemas de seguimiento de incidentes de terceros mediante la integración con Amazon SNS o Amazon EventBridge.

Pasos para la implementación

Cree varios tipos de alarmas en función de la forma en que se supervisan las cargas de trabajo, como, por ejemplo:

- Las alarmas de las aplicaciones se utilizan para detectar cuando alguna parte de la carga de trabajo no funciona correctamente.

- Las alarmas de la infraestructura indican cuándo escalar los recursos. Las alarmas se pueden mostrar visualmente en paneles, enviar alertas a través de Amazon SNS o por correo electrónico y trabajar con el escalado automático para reducir o escalar horizontalmente los recursos de la carga de trabajo.
- Se pueden crear alarmas estáticas sencillas para supervisar cuando una métrica supera un umbral estático durante un número específico de periodos de evaluación.
- Las alarmas compuestas pueden abarcar alarmas complejas de numerosos orígenes.
- Una vez creada la alarma, cree los eventos de notificación adecuados. Puede invocar directamente una API de Amazon SNS para enviar notificaciones y vincular cualquier automatización para su corrección o comunicación.
- Manténgase informado sobre las degradaciones del servicio con AWS Health. Cree notificaciones de eventos de AWS Health adecuados para su propósito para los canales de correo electrónico y chat a través de AWS User Notifications e intégrelas mediante programación con las herramientas de supervisión y alertas a través de Amazon EventBridge.

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- Availability Definition

Documentos relacionados:

- Cree una alarma de CloudWatch basada en un umbral estático
- Qué es Amazon EventBridge?
- What is Amazon Simple Notification Service?
- Publicar métricas personalizadas
- Uso de las alarmas de Amazon CloudWatch
- Configuración de alarmas compuestas de CloudWatch
- What's new in AWS Observability at re:Invent 2022

Herramientas relacionadas:

- CloudWatch

- CloudWatch X-Ray

REL11-BP07 Diseño de su producto para cumplir objetivos de disponibilidad y acuerdos de nivel de servicio (SLA) de tiempo de actividad

Diseñe el producto para que cumpla con los objetivos de disponibilidad y los acuerdos de nivel de servicio (SLA) de tiempo de actividad. Si publica o acuerda en privado objetivos de disponibilidad o SLA de tiempo de actividad, verifique que su arquitectura y procesos operativos están diseñados para admitirlos.

Resultado deseado: cada aplicación tiene un objetivo definido de disponibilidad y un SLA para las métricas de rendimiento, que se pueden supervisar y mantener para cumplir con los resultados comerciales.

Patrones comunes de uso no recomendados:

- Diseño e implementación de cargas de trabajo sin establecer acuerdos de nivel de servicio.
- Las métricas de los SLA se fijan en niveles demasiado altos sin justificación ni requisitos empresariales.
- Establecimiento de SLA sin tener en cuenta las dependencias y sus SLA subyacentes.
- Los diseños de aplicaciones se crean sin tener en cuenta el Modelo de responsabilidad compartida para la resiliencia.

Beneficios de establecer esta práctica recomendada: diseñar aplicaciones en función de los objetivos clave de resiliencia ayuda a cumplir los objetivos empresariales y las expectativas de los clientes. Estos objetivos contribuyen a impulsar el proceso de diseño de aplicaciones que evalúa diferentes tecnologías y tiene en cuenta varios compromisos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

El diseño de aplicaciones debe tener en cuenta una serie de requisitos derivados de objetivos empresariales, operativos y financieros. Dentro de los requisitos operativos, las cargas de trabajo deben tener objetivos concretos de métricas de resiliencia para que se puedan supervisar y respaldar adecuadamente. Las métricas de resiliencia no deben establecerse ni derivarse después de implementar la carga de trabajo. En cambio, deben definirse durante la fase de diseño y ayudar a orientar diversas decisiones y compensaciones.

- Cada carga de trabajo debe tener su propio conjunto de métricas de resiliencia. Esas métricas pueden ser diferentes de las de otras aplicaciones empresariales.
- Reducir las dependencias puede tener un impacto positivo en la disponibilidad. Cada carga de trabajo debe considerar sus dependencias y sus SLA. En general, seleccione dependencias con objetivos de disponibilidad iguales o superiores a los objetivos de su carga de trabajo.
- Siempre que sea posible, examine diseños de acoplamiento débil para que la carga de trabajo pueda funcionar correctamente a pesar del deterioro de las dependencias.
- Reduzca las dependencias del plano de control, especialmente durante la recuperación o una degradación. Evalúe diseños que sean estáticamente estables para las cargas de trabajo críticas. Utilice el ahorro de recursos para aumentar la disponibilidad de esas dependencias en una carga de trabajo.
- La observabilidad y la instrumentación son fundamentales para alcanzar los SLA al reducir el tiempo medio de detección (MTTD) y el tiempo medio de reparación (MTTR).
- Los tres factores que se utilizan para mejorar la disponibilidad en los sistemas distribuidos son una menor frecuencia de errores (MTBF más largo), tiempos de detección de errores más cortos (MTTD más corto) y tiempos de reparación más cortos (MTTR más corto).
- Establecer y cumplir las métricas de resiliencia para una carga de trabajo es una parte imprescindible de todo diseño eficaz. Estos diseños deben tener en cuenta las compensaciones de la complejidad del diseño, las dependencias de los servicios, el rendimiento, la escalabilidad y los costos.

Pasos para la implementación

- Revise y documente el diseño de la carga de trabajo con las siguientes preguntas en mente:
  - ¿Dónde se utilizan los planos de control en la carga de trabajo?
  - ¿Cómo implementa la carga de trabajo la tolerancia a errores?
  - ¿Cuáles son los patrones de diseño para el escalado, el escalado automático, la redundancia y los componentes de alta disponibilidad?
  - ¿Cuáles son los requisitos de coherencia y disponibilidad de los datos?
  - ¿Se tiene en cuenta el ahorro de recursos o la estabilidad estática de los recursos?
  - ¿Cuáles son las dependencias de los servicios?
- Defina las métricas de los SLA en función de la arquitectura de la carga de trabajo mientras trabaja con las partes interesadas. Considere los SLA de todas las dependencias que utiliza la carga de trabajo.

- Una vez establecido el objetivo del SLA, optimice la arquitectura para que cumpla el SLA.
- Una vez establecido el diseño que cumplirá el SLA, implemente cambios operativos, automatización de procesos y manuales de procedimientos que también se centren en reducir el MTTD y el MTTR.
- Una vez implementado, supervise y cree informes del SLA.

Recursos

Prácticas recomendadas relacionadas:

- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- REL10-BP01 Implementación de la carga de trabajo en varias ubicaciones
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL11-BP03 Automatización de la reparación en todas las capas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos
- REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos
- Comprender el estado de la carga de trabajo

Documentos relacionados:

- Disponibilidad con redundancia
- Pilar de fiabilidad: disponibilidad
- Measuring availability
- AWS Fault Isolation Boundaries
- Modelo de responsabilidad compartida para la resiliencia
- Estabilidad estática con zonas de disponibilidad
- Acuerdos de nivel de servicios (SLA) de AWS
- Guidance for Cell-based Architecture on AWS
- AWS infrastructure
- Documento técnico Advanced Multi-AZ Resilience Patterns

Servicios relacionados:

- Amazon CloudWatch
- AWS Config
- AWS Trusted Advisor

Pruebas de fiabilidad

Una vez diseñada la carga de trabajo para que sea resiliente al estrés de producción, las pruebas son la única forma de garantizar que funcionará según lo previsto y proporcionará la resiliencia esperada.

Haga pruebas para comprobar que su carga de trabajo cumpla con los requisitos funcionales y no funcionales, ya que los errores o los cuellos de botella en el rendimiento pueden afectar a la fiabilidad de la carga de trabajo. Pruebe la resiliencia de su carga de trabajo para poder encontrar errores latentes que solo aparecen en la producción. Haga estas pruebas regularmente.

Prácticas recomendadas

- REL12-BP01 Uso de manuales de estrategias para investigar los errores
- REL12-BP02 Análisis después del incidente
- REL12-BP03 Requisitos de escalado y rendimiento de las pruebas
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos
- REL12-BP05 Planificación periódica de días de juego

REL12-BP01 Uso de manuales de estrategias para investigar los errores

Permite obtener respuestas sistemáticas e inmediatas a escenarios de error que no se comprendan bien mediante la documentación del proceso de investigación en guías de estrategias. Los manuales de estrategias son pasos predefinidos hechos para identificar los factores que contribuyen a un escenario de error. Los resultados de cualquier paso del proceso se utilizan para determinar los siguientes pasos, hasta que el problema se identifique o escale.

El manual de estrategias es una planificación proactiva que debe hacer para poder tomar medidas reactivas de manera efectiva. Cuando se produzcan situaciones de error que no estén contempladas en el manual de estrategias, aborde primero el problema (resuelva la crisis). A continuación, repase los pasos que ha seguido para solucionar el problema y utilícelos para agregar una nueva entrada al manual de estrategias.

Tenga en cuenta que los manuales de estrategias se usan en respuesta a incidentes específicos, mientras que los manuales de procedimientos se usan para conseguir resultados específicos. A menudo, los manuales de procedimientos se utilizan para actividades rutinarias, mientras que los manuales de estrategias se utilizan para responder a eventos no rutinarios.

Patrones comunes de uso no recomendados:

- Planificar la implementación de una carga de trabajo sin conocer los procesos para diagnosticar los problemas o responder a los incidentes.
- Decisiones no planificadas acerca de qué sistemas se recopilan registros y métricas cuando se investiga un evento.
- No retener las métricas y los eventos el tiempo suficiente para poder recuperar los datos.

Beneficios de establecer esta práctica recomendada: la captura de esta información en manuales de estrategias garantiza que el proceso pueda seguirse sistemáticamente. La creación de manuales de estrategias limita la introducción de errores de la actividad manual. La automatización de manuales de estrategias reduce el tiempo para responder a un evento, ya que se elimina el requisito de intervención de un miembro del equipo o se dispone de información adicional al inicio de su intervención.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

- Use manuales de estrategias para identificar problemas. Los manuales de estrategias son procesos documentados para investigar problemas. Permita las respuestas sistemáticas e inmediatas a escenarios de error mediante la documentación de los procesos en manuales de estrategias. Los manuales de estrategias deben contener la información y las instrucciones necesarias para que alguien con la formación adecuada reúna la información correspondiente, identifique las posibles fuentes de error, aísle los errores y determine los factores que han contribuido al problema (hacer un análisis después del incidente).
  - Implemente manuales de estrategias como código. Efectúe sus operaciones como código mediante scripts de sus manuales de estrategias para garantizar la sistematicidad y reducir los errores provocados por los procesos manuales. Los manuales de estrategias pueden constar de varios scripts que representen los diferentes pasos que podrían ser necesarios para identificar los factores que contribuyen a un problema. Se pueden invocar o llevar a cabo actividades del

manual de procedimientos como parte de las actividades de un manual de estrategias, o se puede solicitar la ejecución de un manual de estrategias en respuesta a eventos identificados.

- Automatice sus manuales operativos con AWS Systems Manager
- AWS Systems Manager Run Command
- AWS Systems Manager Automation
- ¿Qué es AWS Lambda?
- ¿Qué es Amazon EventBridge?
- Uso de las alarmas de Amazon CloudWatch

Recursos

Documentos relacionados:

- AWS Systems Manager Automation
- AWS Systems Manager Run Command
- Automatice sus manuales operativos con AWS Systems Manager
- Uso de las alarmas de Amazon CloudWatch
- Uso de canarios (Amazon CloudWatch Synthetics)
- ¿Qué es Amazon EventBridge?
- ¿Qué es AWS Lambda?

Ejemplos relacionados:

- Automating operations with Playbooks and Runbooks

REL12-BP02 Análisis después del incidente

Revise los eventos que afectan a los clientes e identifique los factores que contribuyen al evento y las medidas preventivas. Use esta información para desarrollar un plan de mitigación que limite o evite la reaparición del problema. Desarrolle procedimientos para proporcionar respuestas rápidas y eficaces. Comunique los factores que han contribuido al problema y las medidas correctivas según corresponda, adaptados al público de destino. Disponga de un método para comunicar estas causas a otros usuarios según sea necesario.

Evalúe por qué las pruebas existentes no han detectado el problema. Agregue pruebas para este caso si no hay pruebas ya establecidas.

Resultado deseado: sus equipos tienen un enfoque coherente y consensuado para gestionar el análisis posterior al incidente. Un mecanismo es el proceso de corrección de errores (COE). El proceso de COE ayuda a los equipos a identificar, comprender y abordar las causas fundamentales de los incidentes, a la vez que crea mecanismos y barreras de protección para limitar la probabilidad de que se repita el mismo incidente.

Patrones comunes de uso no recomendados:

- Buscar los factores que han contribuido al problema, pero no seguir investigando si existen otros problemas potenciales o enfoques que mitigar.
- Identificar solo los errores humanos y no proporcionar ninguna formación o automatización que pueda evitar estos errores.
- Concentrarse en determinar la culpa en lugar de en conocer la causa fundamental, lo que da lugar a una cultura de miedo y obstaculiza la comunicación abierta.
- No intercambiar información, lo que hace que los resultados del análisis de incidentes los conozca solo un grupo pequeño y evita que otros se beneficien de las lecciones aprendidas.
- No existe ningún mecanismo para capturar el conocimiento institucional, por lo que se pierde información valiosa al no preservar las lecciones aprendidas en forma de actualizaciones de las prácticas recomendadas y, por lo tanto, se repiten incidentes con la misma causa fundamental o una similar

Beneficios de establecer esta práctica recomendada: hacer análisis después de un incidente y compartir los resultados permite que el riesgo se mitigue en otras cargas de trabajo si estas tienen implementadas los mismos factores que han contribuido al problema, y permite también implementar la mitigación o la recuperación automatizada antes de que se produzca un incidente.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Un buen análisis posterior a un incidente ofrece oportunidades de proponer soluciones comunes para problemas con patrones de arquitectura que se utilizan en otros lugares de los sistemas.

Un aspecto clave del proceso de COE es documentar y resolver los problemas. Es recomendable definir una forma estandarizada de documentar las causas fundamentales críticas y garantizar que

estas se revisan y solucionan. Asigne una responsabilidad clara al proceso de análisis posterior al incidente. Nombre un equipo o persona responsable que supervise las investigaciones y el seguimiento de los incidentes.

Fomente una cultura que se centre en el aprendizaje y la mejora en lugar de en la culpa. Haga hincapié en que el objetivo es prevenir futuros incidentes, no penalizar a las personas.

Desarrolle procedimientos bien definidos para llevar a cabo análisis posteriores a los incidentes. En estos procedimientos, se deben describir los pasos que hay que seguir, la información que se va a recopilar y las preguntas clave que se abordarán durante el análisis. Investigue los incidentes a fondo y vaya más allá de las causas inmediatas para identificar las causas fundamentales y los factores que contribuyen a ellos. Utilice técnicas como los cinco porqués para profundizar en los problemas subyacentes.

Mantenga un repositorio de las lecciones aprendidas de los análisis de incidentes. Este conocimiento institucional puede servir como referencia para incidentes futuros e iniciativas de prevención. Comparta los resultados y la información de los análisis posteriores a los incidentes y considere la posibilidad de celebrar reuniones de revisión de invitación abierta después de los incidentes para analizar las lecciones aprendidas.

Pasos para la implementación

- Al hacer un análisis posterior al incidente, asegúrese de que en el proceso no se culpe a nadie. Esto permite que las personas involucradas en el incidente se muestren imparciales con respecto a las medidas correctivas propuestas, además de fomentar una autoevaluación honesta y la colaboración entre los equipos.
- Defina una forma estandarizada de documentar los problemas críticos. Un ejemplo de estructura para dicho documento es el siguiente:
  - ¿Qué ha pasado?
  - ¿Cómo ha afectado a los clientes y a la empresa?
  - ¿Cuál ha sido la causa fundamental?
  - ¿Qué datos tiene para corroborarlo?
    - Por ejemplo, métricas y gráficos
  - ¿Qué pilares básicos estuvieron implicados, con especial atención a la seguridad?
    - Al diseñar cargas de trabajo, se hacen concesiones entre pilares según el contexto del negocio. Estas decisiones de negocio puede impulsar sus prioridades de diseño. Podría dar preferencia a reducir el costo a expensas de la fiabilidad en el desarrollo de entornos o, para

soluciones críticas, podría optimizar la fiabilidad con un aumento de los costos. La seguridad siempre es la tarea primordial, ya que sus clientes deben estar protegidos.

  - ¿Qué lecciones aprendió?
  - ¿Qué medidas correctivas va a tomar?
    - Elementos de acción
    - Elementos relacionados
- Cree procedimientos operativos estándar bien definidos para llevar a cabo análisis posteriores a los incidentes.
- Configure un proceso estandarizado de notificación de incidentes. Documente todos los incidentes de manera exhaustiva, incluido el informe inicial del incidente, los registros, las comunicaciones y las medidas tomadas durante el incidente.
- Recuerde que un incidente no requiere una interrupción. Podría tratarse de un cuasi incidente o de un sistema que funciona de una forma inesperada, pero que cumple su función.
- Mejore continuamente su proceso de análisis posterior a un incidente en función de los comentarios y las lecciones aprendidas.
- Registre los resultados clave en un sistema de administración del conocimiento y considere cualquier patrón que deba agregarse a las guías para desarrolladores o a las listas de verificación previas a la implementación.

Recursos

Documentos relacionados:

- Why you should develop a correction of error (COE)

Videos relacionados:

- Amazon’s approach to failing successfully
- AWS re:Invent 2021 - Amazon Builders’ Library: Operational Excellence at Amazon

REL12-BP03 Requisitos de escalado y rendimiento de las pruebas

Utilice técnicas, como las pruebas de carga, para validar que la carga de trabajo satisface los requisitos de escalado y rendimiento.

En la nube, puede crear un entorno de pruebas a escala de producción bajo demanda para la carga de trabajo. En lugar de confiar en un entorno de pruebas reducido, lo que podría provocar predicciones inexactas de los comportamientos de producción, puede utilizar la nube para proporcionar un entorno de pruebas que refleje fielmente el entorno de producción esperado. Este entorno lo ayuda a realizar pruebas en una simulación más precisa de las condiciones reales a las que se enfrenta su aplicación.

Además de las pruebas de rendimiento que intente llevar a cabo, asegúrese de validar que los recursos básicos, la configuración de escalado, las cuotas de servicio y el diseño de resiliencia funcionen según lo esperado bajo carga. Este enfoque holístico verifica que su aplicación pueda escalarse y funcionar de manera confiable según sea necesario, incluso en las condiciones más exigentes.

Resultado deseado: su carga de trabajo mantiene el comportamiento esperado incluso cuando está sujeta a picos de carga. Aborda de forma proactiva cualquier problema relacionado con el rendimiento que pueda surgir a medida que la aplicación crece y evoluciona.

Patrones comunes de uso no recomendados:

- Utiliza entornos de prueba que no coinciden estrechamente con el entorno de producción.
- Considera las pruebas de carga como una actividad independiente y única, y no como una parte integrada del proceso de integración continua (CI) de la implementación.
- No se definen requisitos de rendimiento claros y mensurables, como el tiempo de respuesta, el rendimiento y los objetivos de escalabilidad.
- Realiza pruebas con escenarios de carga poco realistas o insuficientes, y no realiza pruebas para detectar picos de carga, picos repentinos y cargas elevadas sostenidas.
- No se pone a prueba la carga de trabajo usando límites de carga esperados excesivos.
- Utilizas herramientas de pruebas de carga y elaboración de perfiles de rendimiento inadecuadas.
- Carece de sistemas integrales de supervisión y alerta para realizar un seguimiento de las métricas de rendimiento y detectar anomalías.

Beneficios de establecer esta práctica recomendada:

- Las pruebas de carga lo ayudan a identificar posibles obstáculos en el rendimiento de su sistema antes de que entre en producción. Al simular el tráfico y las cargas de trabajo en la producción, puede identificar las áreas en las que el sistema puede tener dificultades para gestionar la carga, como los tiempos de respuesta lentos, la escasez de recursos o los fallos del sistema.

- Probar el sistema en distintas condiciones de carga lo ayudará a comprender mejor los requisitos de recursos necesarios para respaldar su carga de trabajo. Esta información puede ayudarlo a tomar decisiones fundamentadas sobre la asignación de recursos y a evitar el aprovisionamiento excesivo o insuficiente de los recursos.
- Para identificar los posibles puntos de fallo, puede observar el rendimiento de su carga de trabajo en condiciones de carga elevada. Esta información lo ayuda a mejorar la fiabilidad y la resiliencia de su carga de trabajo mediante la implementación de mecanismos de tolerancia a fallos, estrategias de conmutación por error y medidas de redundancia, según corresponda.
- Puede identificar y abordar los problemas de rendimiento anticipadamente y evitar así el elevado coste de las interrupciones del sistema, la lentitud de los tiempos de respuesta y la insatisfacción de los usuarios.
- Los datos de rendimiento detallados y la información de creación de perfiles recopilados durante las pruebas pueden ayudarlo a solucionar los problemas relacionados con el rendimiento que puedan surgir en la producción. Esto puede acelerar la respuesta y la resolución de los incidentes, lo que reduce el impacto en los usuarios y en las operaciones de la organización.
- En algunos sectores, las pruebas de rendimiento proactivas pueden ayudar a que su carga de trabajo cumpla con los estándares de conformidad, lo que reduce el riesgo de sanciones o problemas legales.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

El primer paso es definir una estrategia de pruebas integral que abarque todos los aspectos de los requisitos de escalado y rendimiento. Para empezar, defina claramente los objetivos de nivel de servicio (SLO) de su carga de trabajo en función de las necesidades de su empresa, como el rendimiento, el histograma de latencia y la tasa de errores. A continuación, diseñe un conjunto de pruebas que puedan simular varios escenarios de carga, desde un uso medio hasta picos repentinos y picos de carga sostenidos, y compruebe que el comportamiento de la carga de trabajo cumpla con sus SLO. Estas pruebas deben automatizarse e integrarse en la canalización de integración e implementación continuas para detectar las regresiones de rendimiento al principio del proceso de desarrollo.

Para probar de forma eficaz el escalado y el rendimiento, invierta en las herramientas y la infraestructura adecuadas. Esto incluye herramientas de pruebas de carga que pueden generar un tráfico de usuarios realista, herramientas de creación de perfiles de rendimiento para identificar los

cuellos de botella y soluciones de supervisión para realizar un seguimiento de las métricas clave. Por otro lado, es muy importante comprobar que sus entornos de prueba se ajusten perfectamente al entorno de producción en términos de infraestructura y condiciones ambientales para que los resultados de las pruebas sean lo más precisos posible. Para facilitar la replicación y el escalado fiables de configuraciones similares a las de producción, utilice la infraestructura como código y aplicaciones basadas en contenedores.

Las pruebas de escalado y rendimiento son un proceso continuo, no una actividad que se realiza una sola vez. Implemente la supervisión y las alertas de manera exhaustiva para realizar un seguimiento del rendimiento de la aplicación en producción y utilice estos datos para perfeccionar continuamente sus estrategias de prueba y sus esfuerzos de optimización. Analice periódicamente los datos de rendimiento para identificar los problemas que surjan, pruebe nuevas estrategias de escalado e implemente optimizaciones para mejorar la eficiencia y la fiabilidad de la aplicación. Si adopta un enfoque iterativo y aprende constantemente de los datos de producción, puede comprobar que su aplicación puede adaptarse a las demandas variables de los usuarios y mantener la resiliencia y un rendimiento óptimo a lo largo del tiempo.

Pasos para la implementación

1. Establezca requisitos de rendimiento claros y mensurables, como el tiempo de respuesta, el rendimiento y los objetivos de escalabilidad. Estos requisitos deben basarse en los patrones de uso de la carga de trabajo, las expectativas de los usuarios y las necesidades empresariales.
2. Seleccione y configure una herramienta de pruebas de carga que pueda imitar con precisión los patrones de carga y el comportamiento de los usuarios en su entorno de producción.
3. Configure un entorno de pruebas que se ajuste perfectamente al entorno de producción, incluidas las condiciones de la infraestructura y el entorno, para mejorar la precisión de los resultados de las pruebas.
4. Cree un conjunto de pruebas que abarque una amplia gama de escenarios, desde patrones de uso promedio hasta picos de carga, picos rápidos y cargas elevadas sostenidas. Integre las pruebas en la canalización de integración e implementación continuas para detectar las regresiones de rendimiento al principio del proceso de desarrollo.
5. Realice pruebas de carga para simular el tráfico de usuarios del mundo real y comprender cómo se comporta su aplicación en diferentes condiciones de carga. Para someter la aplicación a una prueba de estrés, supere la carga esperada y observe su comportamiento, como la degradación del tiempo de respuesta, el agotamiento de los recursos o los fallos del sistema. Esto ayuda a identificar el punto de ruptura de su aplicación y a determinar las estrategias de escalado. Evalúe la escalabilidad de su carga de trabajo aumentando gradualmente la carga y mida el impacto en

el rendimiento para identificar los límites de escalado y planificar las necesidades de capacidad futuras.

6. Implemente la supervisión y las alertas de manera exhaustiva para realizar un seguimiento de las métricas de rendimiento, detectar anomalías e iniciar acciones de escalado o notificaciones cuando se superen los umbrales.
7. Supervise y analice continuamente los datos de rendimiento para identificar las áreas de mejora. Repita sus estrategias de prueba y sus esfuerzos de optimización.

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP04 Supervisión y administración de cuotas
- REL06-BP01 Supervisión de todos los componentes de la carga de trabajo (generación)
- REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)

Documentos relacionados:

- Aplicaciones de pruebas de carga
- Pruebas de carga distribuidas en AWS
- Supervisión del rendimiento de las aplicaciones
- Amazon EC2 Testing Policy

Ejemplos relacionados:

- Pruebas de carga distribuidas en AWS (GitHub)

Herramientas relacionadas:

- Generador de perfiles de Amazon CodeGuru
- Amazon CloudWatch RUM
- Apache JMeter
- K6
- Vegeta

- Hey
- ab
- wrk
- Pruebas de carga distribuidas en AWS

REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos

Haga experimentos de caos con regularidad en entornos que estén en producción o lo más cerca posible de ella para entender cómo responde su sistema a condiciones adversas.

Resultado deseado:

La resiliencia de la carga de trabajo se verifica regularmente aplicando la ingeniería del caos en forma de experimentos de inyección de errores o inyección de carga inesperada, además de las pruebas de resiliencia que validan el comportamiento esperado conocido de su carga de trabajo durante un evento. Combine la ingeniería del caos y las pruebas de resiliencia para tener la seguridad de que su carga de trabajo puede sobrevivir a los errores de los componentes y puede recuperarse de las interrupciones inesperadas con un impacto mínimo o nulo.

Patrones comunes de uso no recomendados:

- Diseñar para lograr la resiliencia, pero no verificar cómo funciona la carga de trabajo en su conjunto cuando se producen errores.
- No experimentar nunca en condiciones reales y con la carga prevista.
- No tratar los experimentos como código ni mantenerlos durante el ciclo de desarrollo.
- No ejecutar experimentos de caos tanto como parte de su canalización de CI/CD, así como fuera de las implementaciones.
- No utilizar los análisis posteriores a los incidentes a la hora de determinar los errores con los que experimentar.

Beneficios de establecer esta práctica recomendada: inyectar errores para verificar la resiliencia de la carga de trabajo permite tener seguridad de que los procedimientos de recuperación de su diseño resiliente funcionarán en caso de un error real.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

La ingeniería del caos proporciona a sus equipos capacidades para inyectar continuamente interrupciones del mundo real (simulaciones) de forma controlada según el proveedor de servicios, infraestructura, carga de trabajo y componentes, con un impacto mínimo o nulo para sus clientes. Permite que sus equipos aprendan de los errores y observen, midan y mejoren la resiliencia de las cargas de trabajo, además de validar que las alertas se activen y que los equipos reciban notificaciones en caso de algún evento.

Cuando se hace de forma continua, la ingeniería del caos puede poner de manifiesto deficiencias en las cargas de trabajo que, si no se abordan, podrían afectar negativamente a la disponibilidad y al funcionamiento.

> **Note**
>
> La ingeniería del caos es la disciplina que consiste en experimentar en un sistema para generar confianza en la capacidad del sistema de resistir condiciones adversas en producción. – Principios de la ingeniería del caos

Si un sistema puede soportar estas interrupciones, el experimento del caos debe mantenerse como una prueba de regresión automatizada. De este modo, los experimentos de caos deben hacerse como parte de su ciclo de vida de desarrollo de sistemas (SDLC) y como parte de su canalización de CI/CD.

Para garantizar que la carga de trabajo puede sobrevivir a los errores de los componentes, inyecte eventos reales como parte de los experimentos. Por ejemplo, experimente con la pérdida de instancias de Amazon EC2 o la conmutación por error de la instancia primaria de la base de datos de Amazon RDS y verifique que la carga de trabajo no se ve afectada (o solo en un mínimo). Utilice una combinación de errores de componentes para simular los eventos que puede causar una interrupción en una zona de disponibilidad.

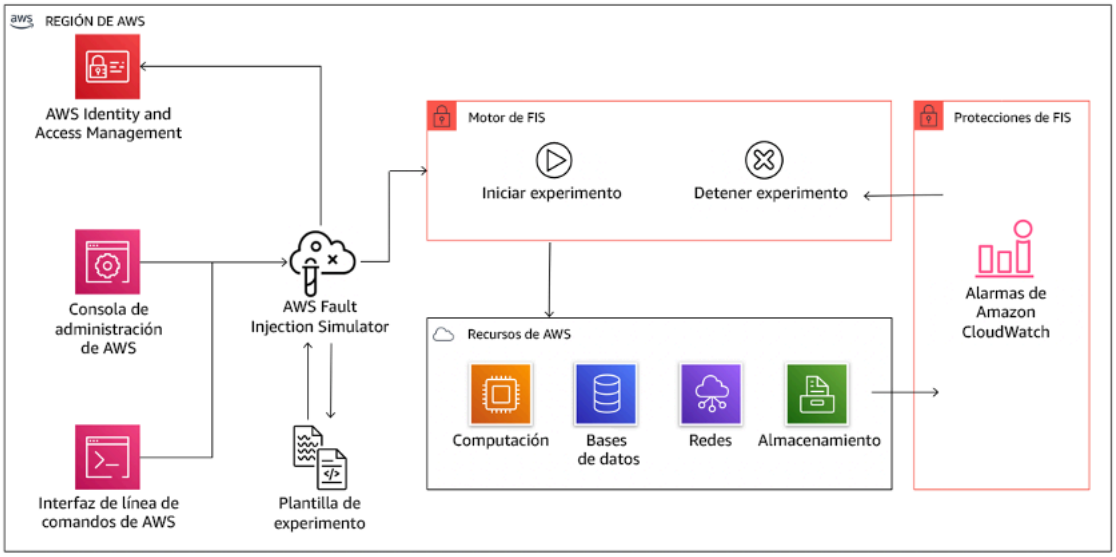
Para los errores a nivel de aplicación (como las caídas), se puede empezar con factores de estrés como el agotamiento de la memoria y la CPU.

Para validar los mecanismos de respaldo y de conmutación por error para las dependencias externas debido a interrupciones intermitentes de la red, sus componentes deben simular un evento de este tipo mediante el bloqueo del acceso a los proveedores de terceros durante una duración especificada que puede durar desde segundos hasta horas.

Otros modos de degradación podrían provocar una funcionalidad reducida y respuestas lentas, lo que a menudo da como resultado una interrupción de los servicios. Los orígenes comunes de esta degradación son una mayor latencia en los servicios críticos y una comunicación de red poco fiable (paquetes omitidos). Los experimentos con estos errores, como, por ejemplo, efectos de red como la latencia, los mensajes perdidos y los errores de DNS, podrían incluir la incapacidad de resolver un nombre, alcanzar el servicio DNS o establecer conexiones con servicios dependientes.

Herramientas de ingeniería del caos:

AWS Fault Injection Service (AWS FIS) es un servicio completamente administrado para hacer experimentos de inyección de errores que puede utilizarse como parte de su canalización de CD. AWS FIS es una buena opción para usar durante los días de simulación de ingeniería del caos. Admite la introducción simultánea de errores en distintos tipos de recursos, tales como Amazon EC2, Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) y Amazon RDS. Estos errores incluyen la terminación de los recursos, forzado de conmutación por error, estrés de CPU o memoria, limitación, latencia y pérdida de paquetes. Al estar integrado con las alarmas de Amazon CloudWatch, puede configurar las condiciones de detención como barreras de protección para revertir un experimento si provoca un impacto inesperado.



AWS Fault Injection Service se integra con recursos de AWS para permitirle ejecutar experimentos de inyección de errores para las cargas de trabajo.

También hay varias opciones de terceros para los experimentos de inyección de errores. Entre estas se incluyen herramientas de código abierto como Chaos Toolkit, Chaos Mesh y Litmus Chaos, así como opciones comerciales como Gremlin. Para ampliar el número de errores que se pueden inyectar en AWS, AWS FIS se integra con Chaos Mesh y Litmus Chaos, lo que le permite coordinar

los flujos de trabajo de inyección de errores entre varias herramientas. Por ejemplo, puede ejecutar una prueba de estrés en la CPU de un pod mediante errores de Chaos Mesh o Litmus, además de terminar un porcentaje seleccionado al azar de nodos del clúster mediante acciones de error de AWS FIS.

Pasos para la implementación

1. Determine qué errores se van a utilizar en los experimentos.

   Evalúe el diseño de su carga de trabajo para la resiliencia. Estos diseños (creados mediante las prácticas recomendadas del Marco de Well-Architected) tienen en cuenta los riesgos en función de las dependencias críticas, los eventos pasados, los problemas conocidos y los requisitos de cumplimiento. Enumere cada elemento del diseño destinado a mantener la resiliencia y los errores que pretende mitigar. Para obtener más información sobre la creación de dichas listas, consulte el documento técnico sobre revisión de la preparación operativa, que guía sobre cómo crear un proceso para evitar que se repitan incidentes anteriores. El proceso de análisis de modos de error y efectos (FMEA) le proporciona un marco para hacer un análisis de los errores de componentes y cómo afectan a la carga de trabajo. Adrian Cockcroft describe con más detalle el FMEA en Failure Modes and Continuous Resilience.

2. Asigne una prioridad a cada error.

   Comience con una categorización amplia, como alta, media o baja. Para evaluar la prioridad, hay que tener en cuenta la frecuencia del error y su impacto en la carga de trabajo global.

   Al considerar la frecuencia de un determinado error, analice los datos anteriores de esta carga de trabajo cuando estén disponibles. Si no están disponibles, utilice datos de otras cargas de trabajo que se ejecuten en un entorno similar.

   Cuando se considera el impacto de un error determinado, cuanto mayor sea el alcance del error, generalmente mayor será el impacto. También hay que tener en cuenta el diseño y la finalidad de la carga de trabajo. Por ejemplo, la capacidad de acceder a los almacenes de datos de origen es fundamental para una carga de trabajo que haga transformaciones y análisis de datos. En este caso, se daría prioridad a los experimentos de errores de acceso, así como al acceso limitado y a la inserción de latencia.

   Los análisis posteriores a los incidentes son un buen origen de datos para comprender tanto la frecuencia como el impacto de los modos de error.

Utilice la prioridad asignada para determinar con qué errores experimentar primero y en qué orden desarrollar nuevos experimentos de inyección de errores.

3. En cada experimento que haga, siga la ingeniería del caos y el volante de resiliencia continua en la figura siguiente.

Volante de ingeniería del caos y de resiliencia continua, con el método científico de Adrian Hornsby.

a. Defina el estado estable como un resultado medible de una carga de trabajo que indica un comportamiento normal.

   Su carga de trabajo exhibe un estado estable si está operando de manera fiable y como se espera. Por tanto, valide que su carga de trabajo tenga un buen estado antes de definir el estado estable. El estado estable no significa necesariamente que no haya impacto en la carga de trabajo cuando se produce un error, ya que un cierto porcentaje en los errores podría estar

dentro de los límites aceptables. El estado estable es la línea de base que observará durante el experimento, que pondrá de manifiesto las anomalías si su hipótesis definida en el siguiente paso no resulta de la forma esperada.

Por ejemplo, un estado estable de un sistema de pagos puede definirse como el procesamiento de 300 TPS con una tasa de éxito del 99 % y un tiempo de ida y vuelta de 500 ms.

b. Formule una hipótesis sobre cómo reaccionará la carga de trabajo ante el error.

Una buena hipótesis se basa en cómo se espera que la carga de trabajo mitigue el error para mantener el estado estable. La hipótesis establece que, dado el error de un tipo específico, el sistema o la carga de trabajo continuará en estado estable, porque la carga de trabajo se diseñó con mitigaciones específicas. En la hipótesis deben especificarse el tipo específico de error y las mitigaciones.

Se puede utilizar la siguiente plantilla para la hipótesis (pero también se acepta otra redacción):

> **Note**
>
> Si se produce un *`error específico`*, el *`nombre de la carga de trabajo describirá los controles de mitigación`* para mantener el *`impacto de las métricas empresariales o técnicas`*.

Por ejemplo:

- Si el 20 % de los nodos del grupo de nodos de Amazon EKS se eliminan, la API de creación de transacciones sigue sirviendo el percentil 99 de peticiones en menos de 100 ms (estado estable). Los nodos de Amazon EKS se recuperarán en cinco minutos y los pods se programarán y procesarán el tráfico en ocho minutos tras el inicio del experimento. Las alertas se activan en tres minutos.
- Si se produce un error de instancia de Amazon EC2, la comprobación de estado de Elastic Load Balancing del sistema de pedidos hará que Elastic Load Balancing solo envíe solicitudes a las instancias en buen estado restantes mientras Amazon EC2 Auto Scaling sustituye la instancia con error, manteniendo un aumento inferior al 0,01 % en los errores del servidor (5xx) (estado estable).
- Si se produce un error en la instancia de la base de datos principal de Amazon RDS, la carga de trabajo de recopilación de datos de la cadena de suministro se conmutará por error y

se conectará a la instancia de la base de datos de Amazon RDS en espera para mantener menos de 1 minuto de errores de lectura o escritura en la base de datos (estado estable).

c. Inyecte el error para hacer el experimento.

Un experimento debe ser de manera predeterminada a prueba de errores y tolerado por la carga de trabajo. Si sabe que se producirá un error en la carga de trabajo, no haga el experimento. Debe utilizarse la ingeniería del caos para encontrar incógnitas conocidas o incógnitas desconocidas. Las incógnitas desconocidas son aspectos que conoce, pero que no comprende del todo, y las incógnitas desconocidas son aspectos que no conoce ni comprende del todo. Experimentar con una carga de trabajo que se sabe que está descompuesta no proporcionará información nueva. El experimento se debe planificar con cuidado, tener un alcance claro del impacto y proporcionar un mecanismo de retroceso que pueda aplicarse en caso de turbulencias inesperadas. Si su diligencia demuestra que la carga de trabajo debe sobrevivir al experimento, siga adelante. Hay varias opciones para inyectar los errores. Para las cargas de trabajo en AWS, AWS FIS proporciona diversas simulaciones de errores predefinidas que se denominan acciones. También puede definir acciones personalizadas que se ejecuten en AWS FIS, mediante documentos de AWS Systems Manager.

Desaconsejamos el uso de scripts personalizados para los experimentos de caos, a menos que los scripts tengan la capacidad de entender el estado actual de la carga de trabajo, sean capaces de emitir registros y proporcionen mecanismos para retrocesos y condiciones de parada cuando sea posible.

Un marco o conjunto de herramientas eficaz que apoye la ingeniería del caos debe hacer el seguimiento del estado actual de un experimento, emitir registros y proporcionar mecanismos de reversión para apoyar la ejecución controlada de un experimento. Comience con un servicio establecido como AWS FIS que permite hacer experimentos con un alcance claramente definido y mecanismos de seguridad que reviertan el experimento si este introduce turbulencias inesperadas. Para obtener información sobre una variedad más amplia de experimentos mediante AWS FIS, consulte también el laboratorio Resilient and Well-Architected Apps with Chaos Engineering. Además, AWS Resilience Hub analizará la carga de trabajo y creará experimentos que puede elegir para implementar y ejecutar en AWS FIS.

> **Note**
>
> Para cada experimento, comprenda claramente el alcance y su impacto. Recomendamos que los errores se simulen primero en un entorno de no producción antes de ejecutarlos en producción.

Cuando sea posible, los experimentos deben ejecutarse en un entorno de producción en condiciones reales, mediante implementaciones canario que permitan implementar un sistema de control y uno experimental. Ejecutar los experimentos durante las horas de menor actividad es una buena práctica para mitigar el impacto potencial cuando se experimenta por primera vez en producción. Además, si utilizar el tráfico real del cliente supone demasiado riesgo, puede hacer experimentos con tráfico sintético en la infraestructura de producción en las implementaciones de control y experimentales. Cuando no sea posible utilizar la producción, ejecute los experimentos en entornos de preproducción que sean lo más parecidos posible a la producción.

Debe establecer y supervisar las barreras de protección para garantizar que el experimento no afecte al tráfico de producción o a otros sistemas más allá de los límites aceptables. Establezca condiciones de parada para detener un experimento si alcanza un umbral en una métrica de barrera de protección que usted defina. Esto debe incluir las métricas para el estado estable de la carga de trabajo, así como la métrica en comparación con los componentes en los que está inyectando el error. Un monitor sintético (también conocido como canario de usuario) es una métrica que normalmente debe incluir como proxy de usuario. Las condiciones de parada para AWS FIS se admiten como parte de la plantilla del experimento, lo que permite hasta cinco condiciones de parada por plantilla.

Uno de los principios del caos es minimizar el alcance del experimento y su impacto:

Aunque hay que tener en cuenta algún impacto negativo a corto plazo, es responsabilidad y obligación del ingeniero del caos garantizar que las consecuencias de los experimentos se minimicen y contengan.

Un método para verificar el alcance y el impacto potencial es hacer el experimento primero en un entorno que no sea de producción, y verificar que los umbrales para las condiciones de parada se activan como se espera durante un experimento y la observabilidad está disponible para detectar una excepción, en lugar de experimentar directamente en producción.

Cuando se hagan experimentos de inyección de errores, verifique que todas las partes responsables estén bien informadas. Comuníquese con los equipos adecuados, como los equipos de operaciones, los equipos de fiabilidad del servicio y el servicio de atención al cliente, para informarles de cuándo se llevarán a cabo los experimentos y qué pueden esperar. Proporcione herramientas de comunicación a estos equipos para que informen a quienes dirigen el experimento si observan algún efecto adverso.

Debe restablecer la carga de trabajo y sus sistemas subyacentes al estado original de funcionalidad comprobada. A menudo, el diseño resistente de la carga de trabajo se autorrepara. No obstante, algunos diseños de errores o experimentos con errores pueden dejar la carga de trabajo en un estado de error inesperado. Al final del experimento, debe ser consciente de ello y restablecer la carga de trabajo y los sistemas. Con AWS FIS puede establecer una configuración de reversión (también llamada acción posterior) en los parámetros de la acción. Una acción posterior devuelve el destino al estado en el que se encontraba antes de que se ejecutara la acción. Ya sean automatizadas (como con AWS FIS) o manuales, estas acciones posteriores deben formar parte de una guía de estrategias que describa cómo detectar y gestionar los errores.

d. Verifique la hipótesis.

Principios de la ingeniería del caos ofrece estas directrices sobre cómo verificar el estado estable de su carga de trabajo:

Céntrese en los resultados medibles de un sistema, más que en sus atributos internos. Las mediciones de esos resultados durante un corto periodo constituyen una aproximación al estado estable del sistema. El rendimiento global del sistema, las tasas de error y los percentiles de latencia podrían ser métricas de interés que representen el comportamiento del estado estable. Al centrarse en los patrones de comportamiento sistémico durante los experimentos, la ingeniería del caos verifica que el sistema funcione, en lugar de intentar validar su funcionamiento.

En nuestros dos ejemplos anteriores, incluimos las métricas de estado estable de menos del 0,01 % de aumento de errores del servidor (5xx) y menos de un minuto de errores de lectura y escritura en la base de datos.

Los errores 5xx son una buena métrica porque son una consecuencia del modo de error que experimentará directamente un cliente de la carga de trabajo. La medición de los errores de la base de datos es buena como consecuencia directa del error, pero también

debe complementarse con una medición del impacto en el cliente, como las solicitudes con errores de los clientes o los errores que aparecen en el cliente. Además, incluya un monitor sintético (también conocido como canario de usuario) en cualquier API o URI al que acceda directamente el cliente de su carga de trabajo.

e. Mejora del diseño de la carga de trabajo para la resiliencia.

   Si el estado estable no se mantuvo, investigue cómo se puede mejorar el diseño de la carga de trabajo para mitigar el error y aplique las prácticas recomendadas del pilar de fiabilidad de AWS Well-Architected. Puede encontrar orientación y recursos adicionales en la AWS Builders' Library, que contiene artículos sobre cómo mejorar las comprobaciones de estado o utilizar los reintentos con retroceso en el código de la aplicación, entre otros temas.

   Una vez aplicados estos cambios, vuelva a hacer el experimento (mostrado por la línea de puntos en el volante de ingeniería del caos) para determinar su eficacia. Si el paso de verificación indica que la hipótesis es cierta, entonces la carga de trabajo estará en estado estable y el ciclo continúa.

4. Lleve a cabo experimentos periódicos.

   Un experimento de caos es un ciclo y los experimentos deben hacerse regularmente como parte de la ingeniería del caos. Después de que una carga de trabajo cumpla con la hipótesis del experimento, este debe automatizarse para ejecutarse continuamente como parte de la regresión de su canalización de CI/CD. Para obtener información sobre cómo hacerlo, consulte este blog sobre cómo hacer experimentos de AWS FIS con AWS CodePipeline. Este laboratorio sobre experimentos recurrentes de AWS FIS en una canalización de CI/CD le permite trabajar de forma práctica.

   Los experimentos de inyección de errores también forman parte de los días de simulación (consulte REL12-BP05 Planificación periódica de días de juego). En los días de simulación se simula un error o evento para verificar los sistemas, los procesos y las respuestas de los equipos. El objetivo es llevar a cabo las acciones que llevaría a cabo el equipo si se produjera un evento excepcional.

5. Capture y almacene los resultados de los experimentos.

   Los resultados de los experimentos de inyección de errores deben capturarse y persistir. Incluya todos los datos necesarios (como el tiempo, la carga de trabajo y las condiciones) para poder analizar posteriormente los resultados y las tendencias del experimento. Algunos ejemplos de resultados pueden ser capturas de pantalla de paneles, volcados en CSV de la base de datos

de métricas o un registro escrito a mano de los eventos y las observaciones del experimento. El registro de experimentos con AWS FIS puede ser parte de esta captura de datos.

Recursos

Prácticas recomendadas relacionadas:

- REL08-BP03 Integración de las pruebas de resiliencia como parte de la implementación
- REL13-BP03 Prueba de la implementación de recuperación de desastres para validarla

Documentos relacionados:

- Qué es AWS Fault Injection Service?
- Qué es AWS Resilience Hub?
- Principios de la ingeniería del caos
- Chaos Engineering: Planning your first experiment
- Resilience Engineering: Learning to Embrace Failure
- Chaos Engineering stories
- Evitar los planes alternativos en los sistemas distribuidos
- Canary Deployment for Chaos Experiments

Videos relacionados:

- AWS re:Invent 2020: Testing resiliency using chaos engineering (ARC316)
- AWS re:Invent 2019: Improving resiliency with chaos engineering (DOP309-R1)
- AWS re:Invent 2019: Performing chaos engineering in a serverless world (CMY301)

Herramientas relacionadas:

- AWS Fault Injection Service
- AWS Marketplace: Gremlin Chaos Engineering Platform
- Chaos Toolkit
- Chaos Mesh

- Litmus

REL12-BP05 Planificación periódica de días de juego

Organice días de juego para poner en práctica con regularidad sus procedimientos de respuesta a los eventos y deficiencias que afecten a la carga de trabajo. Incluya a los mismos equipos que se encargarían de gestionar los escenarios de producción. Estos ejercicios ayudan a aplicar medidas para evitar que los eventos de producción afecten a los usuarios. Si practica sus procedimientos de respuesta en condiciones realistas, podrá identificar y abordar cualquier laguna o punto débil antes de que se produzca un suceso real.

En los días de juego, se simulan eventos en entornos de producción para probar los sistemas, los procesos y las respuestas de los equipos. El objetivo es poner en práctica las acciones que llevaría a cabo el equipo si se produjera realmente un evento. Estos ejercicios lo ayudan a comprender dónde se pueden efectuar mejoras y a desarrollar la experiencia de la organización a la hora de gestionar eventos y deficiencias. Deben hacerse periódicamente, para que el equipo desarrolle hábitos sobre cómo responder.

Los días de juego preparan a los equipos para que puedan abordar los eventos de producción con mayor confianza. Los equipos que tienen mucha experiencia son más capaces de detectar y responder rápidamente a varios escenarios. Esto se traduce en una postura de preparación y resiliencia significativamente mejorada.

Resultado deseado: organiza los días de juego de resiliencia de forma constante y programada. Estos días de juego se integran armoniosamente en la actividad empresarial. Su organización ha creado una cultura de preparación y, cuando se producen problemas de producción, sus equipos están bien preparados para responder con eficacia, resolver los problemas de manera eficiente y mitigar las repercusiones para los clientes.

Patrones comunes de uso no recomendados:

- Documenta los procedimientos, pero no los llega a poner en práctica.
- En los ejercicios de prueba se excluye a los responsables de la toma de decisiones empresariales.
- Organiza un día de juego, pero no informa a todas las partes interesadas pertinentes.
- Se centra únicamente en los fallos técnicos, pero no incluye a las partes interesadas de la empresa.
- No incorpora las lecciones aprendidas de los días de juego en sus procesos de recuperación.

- Culpa a los equipos de los fallos o los errores.

Beneficios de establecer esta práctica recomendada:

- Mejorar las habilidades de respuesta: durante los días de juego, los equipos practican sus tareas y ponen a prueba sus mecanismos de comunicación durante los eventos simulados, lo que permite una respuesta más coordinada y eficiente en situaciones de producción.
- Identificar y abordar las dependencias: los entornos complejos suelen conllevar dependencias intrincadas entre varios sistemas, servicios y componentes. Los días de juego pueden ayudar a identificar y abordar estas dependencias, y a comprobar que los manuales de procedimientos abordan sus sistemas y servicios críticos debidamente, así como que puedan ampliarse o recuperarse de forma oportuna.
- Fomentar una cultura de resiliencia: los días de juego pueden ayudar a cultivar una mentalidad de resiliencia en una organización. Al implicar a equipos multidisciplinarios y a las partes interesadas, estos ejercicios fomentan la concienciación, la colaboración y una comprensión compartida de la importancia de la resiliencia en toda la organización.
- Mejorar y adaptarse continuamente: los días de juego practicados con regularidad ayudan a evaluar y adaptar continuamente las estrategias de resiliencia, de modo que sigan siendo relevantes y eficaces aunque cambien las circunstancias.
- Aumentar la confianza en el sistema: los días de juego ejecutados correctamente pueden ayudar a generar confianza en la capacidad del sistema para resistir las interrupciones y recuperarse de ellas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Una vez que haya diseñado e implementado las medidas de resiliencia necesarias, organice un día de juego para comprobar que todo funciona según lo previsto durante la fase de producción. Un día de juego, sobre todo el primero, debe incluir a todos los miembros del equipo, y se debe informar con antelación a todas las partes interesadas y participantes sobre la fecha, la hora y los escenarios simulados.

Durante el día de juego, los equipos participantes simulan varios eventos y posibles escenarios de acuerdo con los procedimientos prescritos. Los participantes monitorean y evalúan de cerca el impacto de estos eventos simulados. Si el sistema funciona según lo diseñado, los mecanismos

automatizados de detección, escalado y recuperación automática deberían activarse y tener un impacto mínimo o nulo en los usuarios. Si el equipo observa algún impacto negativo, anula la prueba y soluciona los problemas identificados, ya sea mediante medios automatizados o mediante una intervención manual documentada en los manuales aplicables.

Para mejorar continuamente la resiliencia, es fundamental documentar e incorporar las lecciones aprendidas. Este proceso es un ciclo de retroalimentación que recopila de forma sistemática la información obtenida durante los días de juego y la utiliza para mejorar los sistemas, los procesos y las capacidades de los equipos.

Para ayudarlo a reproducir situaciones reales en las que los componentes o servicios del sistema podrían fallar inesperadamente, utilice la simulación de fallos como ejercicio para un día de juego. Los equipos pueden probar la resiliencia y la tolerancia a los fallos de sus sistemas y simular sus procesos de respuesta y recuperación ante incidentes en un entorno controlado.

En AWS, los días de juego se pueden llevar a cabo con réplicas de su entorno de producción utilizando la infraestructura como código. Mediante este proceso, puede realizar las pruebas en un entorno seguro que se parece mucho a su entorno de producción. Puede utilizar AWS Fault Injection Service para crear diferentes escenarios de error. Use servicios como Amazon CloudWatch y AWS X-Ray para monitorear el comportamiento del sistema durante los días de juego. Use AWS Systems Manager para administrar y ejecutar guías de estrategia, y utilice AWS Step Functions para organizar los flujos de trabajo recurrentes del día del juego.

Pasos para la implementación

- Establezca un programa para los días de juego: desarrolle un programa estructurado que defina la frecuencia, el alcance y los objetivos de los días de juego. Incluya a las principales partes interesadas y a los expertos en la materia en la planificación y ejecución de estos ejercicios.
- Prepare el día de juego:
  1. Identifique los principales servicios críticos para la empresa en los que se centrará el día de juego. Catalogue y mapee las personas, los procesos y las tecnologías que respaldan esos servicios.
  2. Establezca la agenda para el día de juego y prepare a los equipos implicados para que participen en el evento. Prepare sus servicios de automatización para simular los escenarios planificados y ejecutar los procesos de recuperación adecuados. Los servicios de AWS, como AWS Fault Injection Service, AWS Step Functions y AWSSystems Manager pueden ayudarlo a automatizar varios aspectos de los días de juego, como la inyección de errores y el inicio de las acciones de recuperación.

- Ejecute su simulación: el día de juego, ejecute el escenario planificado. Observe y documente cómo reaccionan las personas, los procesos y las tecnologías ante el evento simulado.
- Realice revisiones después del ejercicio: después del día de juego, realice una sesión retrospectiva para repasar las lecciones aprendidas. Identifique las áreas de mejora y cualquier acción necesaria para mejorar la resiliencia operativa. Documente sus resultados y realice un seguimiento de los cambios necesarios para mejorar sus estrategias de resiliencia y su preparación para llevarlas a cabo.

Recursos

Prácticas recomendadas relacionadas:

- REL12-BP01 Uso de manuales de estrategias para investigar los errores
- REL12-BP04 Pruebas de resiliencia mediante ingeniería del caos
- OPS04-BP01 Identificación de los indicadores clave de rendimiento
- OPS07-BP03 Uso de manuales de procedimientos para llevar a cabo los procedimientos
- OPS10-BP01 Uso de un proceso para la administración de eventos, incidentes y problemas

Documentos relacionados:

- ¿Qué es AWS GameDay?

Videos relacionados:

- AWS re:Invent 2023 - Practice like you play: How Amazon scales resilience to new heights

Ejemplos relacionados:

- AWS Workshop - Navigate the storm: Unleashing controlled chaos for resilient systems
- Build Your Own Game Day to Support Operational Resilience

Planificación de la recuperación de desastres (DR)

Disponer de copias de seguridad y de componentes de cargas de trabajo redundantes es el principio de su estrategia de DR. El RTO y el RPO son los objetivos de restauración de las cargas de trabajo.

Estos se definen en función de las necesidades del negocio. Implemente una estrategia para satisfacer estos objetivos teniendo en cuenta las ubicaciones y la función de los recursos de las cargas de trabajo y los datos. La probabilidad de una interrupción y el costo de recuperación son también factores clave que ayudan a conocer el valor empresarial de proporcionar recuperación de desastres para una carga de trabajo.

Tanto la disponibilidad como la recuperación de desastres se basan en las mismas prácticas recomendadas, como la supervisión de los fallos, la implementación en varias ubicaciones y la conmutación por error automática. Sin embargo, la disponibilidad se centra en los componentes de la carga de trabajo, mientras que la recuperación de desastres se centra en las copias independientes de toda la carga de trabajo. La recuperación de desastres tiene objetivos diferentes a los de la disponibilidad y se centra en el tiempo de recuperación después de un desastre.

Prácticas recomendadas

- REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos
- REL13-BP02 Uso de estrategias de recuperación definidas para cumplir los objetivos de recuperación
- REL13-BP03 Prueba de la implementación de recuperación de desastres para validarla
- REL13-BP04 Administración de la desviación de la configuración en el sitio o región de DR
- REL13-BP05 Automatización de la recuperación

REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos

Los errores pueden afectar a su empresa de varias maneras. En primer lugar, los errores pueden provocar la interrupción del servicio (tiempo de inactividad). En segundo lugar, pueden provocar la pérdida de datos, su incoherencia o su obsolescencia. Para orientar la forma de responder y recuperarse ante los errores, defina un objetivo de tiempo de recuperación (RTO) y un objetivo de punto de recuperación (RPO) para cada carga de trabajo. El objetivo de tiempo de recuperación (RTO) es el tiempo máximo aceptable entre la interrupción del servicio y su restablecimiento. El objetivo de punto de recuperación (RPO) es el tiempo máximo aceptable tras el último punto de recuperación de datos.

Resultado deseado: cada carga de trabajo tiene un RTO y un RPO designados en función de las circunstancias técnicas y de repercusión para la empresa.

Patrones comunes de uso no recomendados:

- No ha designado objetivos de recuperación.
- Selecciona objetivos de recuperación arbitrarios.
- Selecciona objetivos de recuperación demasiado permisivos que no cumplen los objetivos de la empresa.
- No ha evaluado las consecuencias del tiempo de inactividad y la pérdida de datos.
- Selecciona objetivos de recuperación poco realistas, como un tiempo de recuperación nulo o una pérdida de datos nula, que la configuración de la carga de trabajo tal vez no pueda alcanzar.
- Selecciona objetivos de recuperación más estrictos que los objetivos empresariales reales. Esto obliga a hacer implementaciones de recuperación más costosas y complejas que lo que necesita la carga de trabajo.
- Selecciona objetivos de recuperación incompatibles con los de una carga de trabajo dependiente.
- No tiene en cuenta los requisitos normativos y de cumplimiento.

Beneficios de establecer esta práctica recomendada: al definir los RTO y los RPO para sus cargas de trabajo, establece objetivos de recuperación claros y medibles en función de las necesidades de su empresa. Una vez que haya establecido esos objetivos, puede crear planes de recuperación ante desastres (DR) para alcanzar dichos objetivos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Elabore una matriz o una hoja de trabajo que le sirva de guía para planificar la recuperación ante desastres. En su matriz, cree diferentes categorías o niveles de carga de trabajo en función de cómo afecten a su empresa (de nivel crítico, alto, medio y bajo, por ejemplo) y los RTO y RPO asociados a los que desee asignar cada uno de ellos. En la siguiente matriz se muestra un ejemplo (tenga en cuenta que los valores de RTO y RPO pueden diferir) que puede seguir:

Matriz de recuperación de desastres						
		Objetivo de punto de recuperación				
		< 1 minuto	< 1 hora	< 6 horas	< 1 día	Más de 1 día
Objetivo de tiempo de recuperación	< 10 minutos	Crítico	Crítico	Alto	Medio	Medio
	< 2 horas	Crítico	Alto	Medio	Medio	Bajo
	< 8 horas	Alto	Medio	Medio	Bajo	Bajo
	< 24 horas	Medio	Medio	Bajo	Bajo	Bajo
	Más de 24 horas	Medio	Bajo	Bajo	Bajo	Bajo

Ejemplo de matriz de recuperación ante desastres

Para cada carga de trabajo, debe comprender como afectan el tiempo de inactividad y la pérdida de datos a su empresa. Por lo general, el impacto aumenta con el tiempo de inactividad y la pérdida de datos, pero la forma del impacto puede variar según el tipo de carga de trabajo. Por ejemplo, un tiempo de inactividad de hasta una hora puede tener un impacto mínimo, pero después ese impacto podría aumentar rápidamente. Puede afectar de muchas maneras; por ejemplo, a nivel financiero (como la pérdida de ingresos), operativo (como la falta de nóminas o la disminución de la productividad) o normativo, así como en la reputación (incluida la pérdida de la confianza de los clientes). Una vez completado, asigne la carga de trabajo al nivel adecuado.

Tenga en cuenta las siguientes preguntas al analizar el impacto de un error:

1. ¿Durante cuánto tiempo se puede desactivar la carga de trabajo como máximo antes de que afecte gravemente a la empresa?
2. ¿En qué medida afecta a la empresa una interrupción de la carga de trabajo y de qué modo? Tenga en cuenta todos los tipos de impacto, a nivel financiero, operativo, normativo y en la reputación.
3. ¿Cuántos datos se pueden perder como máximo antes de que la empresa se vea gravemente afectada?
4. ¿Se pueden volver a crear los datos perdidos a partir de otras fuentes (también conocidos como datos derivados)? Si es así, incluya también los RPO de todos los datos de origen utilizados para volver a crea los datos de la carga de trabajo.
5. ¿Cuáles son los objetivos de recuperación y las expectativas de disponibilidad de las cargas de trabajo de las que depende (en sentido descendente)? Los objetivos de su carga de trabajo deben

poder alcanzarse gracias a las capacidades de recuperación de sus dependencias posteriores. Puede usar soluciones alternativas o mitigaciones de las dependencias posteriores que puedan mejorar la capacidad de recuperación de esta carga de trabajo.

6. ¿Cuáles son los objetivos de recuperación y las expectativas de disponibilidad de las cargas de trabajo de las que depende (en sentido ascendente)? Los objetivos de la carga de trabajo anterior pueden requerir que esta carga de trabajo tenga capacidades de recuperación más estrictas de lo que parece a primera vista.
7. ¿Existen diferentes objetivos de recuperación en función del tipo de incidente? Por ejemplo, puede haber diferentes RTO y RPO en función de que el incidente afecte a una zona de disponibilidad o a toda una región.
8. ¿Cambian sus objetivos de recuperación durante determinados eventos o épocas del año? Por ejemplo, es posible que tenga diferentes RTO y RPO en función de las temporadas de compras navideñas, los eventos deportivos, las rebajas especiales y los lanzamientos de nuevos productos.
9. ¿Cómo se acompasan los objetivos de recuperación con las posibles estrategias de recuperación ante desastres de su línea de negocio y de su organización?
10. ¿Hay que tener en cuenta las ramificaciones legales o contractuales? Por ejemplo, ¿tiene una obligación contractual de prestar un servicio con un RTO o RPO determinado? ¿A qué sanciones podría enfrentarse por no cumplirlas?
11. ¿Tiene obligación de mantener la integridad de los datos para cumplir con los requisitos normativos o de conformidad?

La siguiente hoja de trabajo puede ayudarlo a evaluar cada carga de trabajo. Puede modificar esta hoja de trabajo para adaptarla a sus necesidades específicas, por ejemplo, agregar otras preguntas.

Paso 2: Preguntas principales	¿Se aplica a la carga de trabajo?	RTO de carga de trabajo	RPO de carga de trabajo	Ajuste de RTO	Ajuste de RPO	Instrucciones
[1] tiempo máximo que puede estar inoperativa la carga de trabajo						medido en tiempo desde el inicio de la interrupción hasta la recuperación
[2] cantidad máxima de datos que se pueden perder						medido en tiempo desde el último conjunto de datos restaurable correcto conocido
[3a] dependencias upstream						introduzca los objetivos de recuperación upstream más estrictos
[3b] dependencias downstream						introduzca los objetivos de recuperación downstream menos estrictos
[3a] dependencias upstream reconciliadas						Si el valor upstream es menor que los valores actuales y el valor downstream es mayor,
[3b] dependencias downstream reconciliadas						trabaje con las dependencias para reconciliarlas e introducir aquí los valores reconciliados
[3] dependencias						reduzca los valores para ajustarse a las dependencias upstream o auméntelos en función de las capacidades de dependencias downstream
Paso 2: Preguntas adicionales						Indique si se aplica la pregunta. Si no se aplica, omítala
RTO/RPO base						Traslade los valores de RTO y RPO de arriba aquí
[4] tipo de interrupción	[ ]S / [ ]N					Introduzca los objetivos de recuperación del tipo de evento con los requisitos más estrictos
[5] objetivos específicos basados en el tiempo	[ ]S / [ ]N					Introduzca los objetivos de recuperación de tiempo con los requisitos más estrictos
[6] clientes afectados	[ ]S / [ ]N					Realice un gráfico de los clientes afectados en función del tiempo de inactividad o de los datos perdidos. Utilícelo para introducir los RTO y RPO máximos permisibles en función del impacto sobre los clientes
[7] impacto reputacional	[ ]S / [ ]N					Trabaje con la empresa para determinar los RTO y RPO máximos en función del impacto sobre la reputación
[8] impacto operativo	[ ]S / [ ]N					Introduzca los RTO y RPO máximos en función del impacto operativo
[9] alineación organizativa	[ ]S / [ ]N					Introduzca los RTO y RPO máximos para cargas de trabajo de este tipo según los requisitos organizativos y de LOB
[10] obligaciones contractuales	[ ]S / [ ]N					Introduzca los RTO y RPO máximos en función de las obligaciones contractuales
[11] conformidad normativa	[ ]S / [ ]N					Introduzca los RTO y RPO máximos en función de la conformidad normativa pertinente
objetivo basado en preguntas adicionales						Tome el valor mínimo (valor más estricto) de entre Q 4-11 e introdúzcalo aquí
objetivo ajustado						Si no se puede dar cabida a los objetivos de la línea anterior, colabore con los interesados para transigir en los límites e introduzca aquí un nuevo valor mínimo
RTO/RPO ajustados						Introduzca los valores base de RPO/RTO o el objetivo ajustado, el menor de los valores
Paso 3						
Mapa a categoría o nivel predefinidos						Ajuste ambos valores a la baja (lo más estricto) para alinearlos con el nivel definido más cercano

Hoja de trabajo

Pasos para la implementación

1. Identifique cuáles son las partes interesadas de la empresa y los equipos técnicos responsables de cada carga de trabajo y contacte con ellos.
2. Cree categorías o niveles de importancia crítica del impacto de la carga de trabajo en su organización. Entre las categorías de ejemplo se incluyen las siguientes: crítico, alto, medio y bajo. Para cada categoría, elija un RTO y un RPO que reflejen los objetivos y requisitos de su empresa.
3. Asigne una de las categorías de impacto que ha creado en el paso anterior a cada carga de trabajo. Para decidir cómo se asigna una carga de trabajo a una categoría, tenga en cuenta la importancia de la carga de trabajo para la empresa y el impacto de la interrupción o la pérdida de datos. Las preguntas anteriores pueden guiarle. De este modo, obtendrá un RTO y un RPO para cada carga de trabajo.
4. Tenga en cuenta el RTO y el RPO para cada carga de trabajo determinada en el paso anterior. Incluya a los equipos técnicos y empresariales de la carga de trabajo para determinar si se deben ajustar los objetivos. Por ejemplo, las partes interesadas de la empresa podrían determinar que se requieren objetivos más estrictos. Si lo prefiere, los equipos técnicos podrían determinar si los

objetivos deberían modificarse para que se puedan alcanzar con los recursos disponibles y las limitaciones tecnológicas.

Recursos

Prácticas recomendadas relacionadas:

- REL09-BP04 Recuperación periódica de los datos para verificar la integridad de la copia de seguridad y los procesos
- REL12-BP01 Uso de manuales de estrategias para investigar los errores
- REL13-BP02 Uso de estrategias de recuperación definidas para cumplir los objetivos de recuperación
- REL13-BP03 Prueba de la implementación de recuperación ante desastres para validarla

Documentos relacionados:

- AWS Architecture Blog: Disaster Recovery Series
- Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube (documento técnico de AWS)
- Administrar las políticas de resiliencia con AWS Resilience Hub
- Socio de APN: socios que pueden ayudar con la recuperación ante desastres
- AWS Marketplace: productos que pueden usarse para la recuperación ante desastres

Videos relacionados:

- AWS re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications
- Disaster Recovery of Workloads on AWS

REL13-BP02 Uso de estrategias de recuperación definidas para cumplir los objetivos de recuperación

Defina una estrategia de recuperación de desastres (DR) que se ajuste a los objetivos de recuperación de su carga de trabajo. Elija una estrategia como copia de seguridad y restauración, estado de espera (activa/pasiva) o activa/activa.

Resultado deseado: para cada carga de trabajo, hay una estrategia de DR definida e implementada que permite que la carga de trabajo alcance los objetivos de DR. Las estrategias de DR entre cargas de trabajo emplean patrones reutilizables (como las estrategias descritas anteriormente).

Patrones comunes de uso no recomendados:

- Implementar procedimientos de recuperación incoherentes para cargas de trabajo con objetivos de DR similares.
- Dejar la estrategia de DR para implementarla ad hoc cuando se produzca un desastre.
- No tener un plan de recuperación de desastres.
- Depender de las operaciones del plano de control durante la recuperación.

Beneficios de establecer esta práctica recomendada:

- El uso de estrategias de recuperación definidas le permite emplear herramientas y procedimientos de prueba comunes.
- El uso de estrategias de recuperación definidas mejora el intercambio de conocimiento entre equipos y la implementación de la DR en las cargas de trabajo que se encuentran bajo su responsabilidad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto. Sin una estrategia de DR planificada, implementada y probada, es poco probable que consiga sus objetivos de recuperación en caso de desastre.

Guía para la implementación

Una estrategia de DR depende de la capacidad de poner en marcha su carga de trabajo en un sitio de recuperación si su ubicación principal deja de estar disponible para la ejecución de dicha carga de trabajo. Los objetivos de recuperación más comunes son el RTO y el RPO, como explicamos en REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos.

Una estrategia de DR en varias zonas de disponibilidad (AZ) en una única Región de AWS puede ofrecer mitigación contra eventos de desastres como incendios, inundaciones y cortes de suministro eléctrico considerables. Si es necesario implementar medidas de protección contra un evento poco probable que evite que su carga de trabajo pueda ejecutarse en una Región de AWS determinada, puede seguir una estrategia de DR que abarque múltiples regiones.

A la hora de diseñar una estrategia de DR en varias regiones, debe elegir una de las siguientes estrategias. Se enumeran en orden ascendente de costo y complejidad, y en orden descendente de RTO y RPO. La región de recuperación se refiere a una Región de AWS distinta de la principal que se utiliza para la carga de trabajo.

Figura 17: Estrategias de recuperación de desastres (DR)

- Copia de seguridad y restauración (RPO en horas, RTO en 24 horas o menos): haga una copia de seguridad de los datos y aplicaciones en la región de recuperación. El uso de copias de seguridad automatizadas o continuas permitirá la recuperación en un momento dado (PITR), lo que puede reducir el RPO a hasta 5 minutos en algunos casos. En caso de desastre, implementará la infraestructura (mediante la infraestructura como código para reducir el RTO), implementará el código y restaurará los datos desde la copia de seguridad para recuperarse del desastre en la región de recuperación.
- Luz piloto (RPO en minutos, RTO en decenas de minutos): aprovisione una copia de la infraestructura de carga de trabajo principal en la región de recuperación. Replique los datos en la región de recuperación y cree allí copias de seguridad de estos. Los recursos necesarios para permitir la replicación y copia de seguridad de los datos, como el almacenamiento de bases de datos y objetos, están siempre disponibles. Otros elementos, como los servidores de aplicaciones o la computación sin servidor, no se implementan, pero pueden crearse cuando sea necesario con la configuración y el código de aplicación pertinentes.
- Espera semiactiva (RPO en segundos, RTO en minutos): mantenga una versión reducida, pero completamente funcional de la carga de trabajo que se ejecute siempre en la región de

recuperación. Los sistemas críticos se duplican en su totalidad y siempre están activos, pero con una flota reducida. Los datos se replican y están activos en la región de recuperación. Cuando llegue el momento de la recuperación, el sistema se ampliará rápidamente para asumir la carga de producción. Cuanto mayor sea la escala de la espera semiactiva, menor será el RTO y la fiabilidad del plano de control. Cuando se amplía por completo, esto se conoce como espera activa.

- Activo-activo en varias regiones (varios sitios) (RPO cercano a cero, RTO potencialmente nulo): la carga de trabajo se implementa en varias Regiones de AWS y atiende de manera activa el tráfico procedente de estas. Esta estrategia requiere que sincronice datos entre regiones. Los posibles conflictos causados por escrituras en el mismo registro en dos réplicas regionales diferentes deben evitarse o gestionarse, lo que puede resultar complejo. La replicación de datos es útil para la sincronización de datos y es una protección ante algunos tipos de desastres, pero no ante el daño o la destrucción de datos, a no ser que su solución incluya también opciones para una recuperación en un momento dado.

> **Note**
>
> La diferencia entre la luz piloto y la espera semiactiva a veces puede ser difícil de comprender. Ambos métodos incluyen un entorno en su región de recuperación con copias de los activos de su región principal. La distinción es que la luz piloto no puede procesar solicitudes sin tomar primero medidas adicionales, mientras que la espera semiactiva puede gestionar el tráfico (a niveles de capacidad reducidos) inmediatamente. La luz piloto exige que active servidores, posiblemente que implemente infraestructura adicional (no principal) y que escale verticalmente, mientras que la espera semiactiva solo requiere que escale verticalmente (ya está todo implementado y en ejecución). Elija una de estas opciones en función de sus necesidades de RTO y RPO.
> Cuando el costo sea una preocupación y desee alcanzar unos objetivos de RPO y RTO similares a los definidos en la estrategia de espera semiactiva, podría plantearse soluciones nativas en la nube, como AWS Elastic Disaster Recovery, que adoptan el enfoque de luz piloto y ofrecen objetivos de RPO y RTO mejorados.

Pasos para la implementación

1. Determine una estrategia de recuperación de desastres que satisfaga los requisitos de recuperación de esta carga de trabajo.

La selección de una estrategia de DR requiere alcanzar un punto de equilibrio entre la reducción del tiempo de inactividad y la pérdida de datos (RTO y RPO) y los costos y la complejidad de implementar la estrategia. Debe evitar implementar una estrategia que sea más exigente de lo necesario, ya que esto supone costos innecesarios.

Por ejemplo, en el siguiente diagrama, la empresa ha determinado su RTO máximo permisible y el límite de gasto en su estrategia de restauración del servicio. Dados los objetivos de la empresa, las estrategias de DR de luz piloto o espera semiactiva satisfarán tanto el RTO como los criterios de costo.

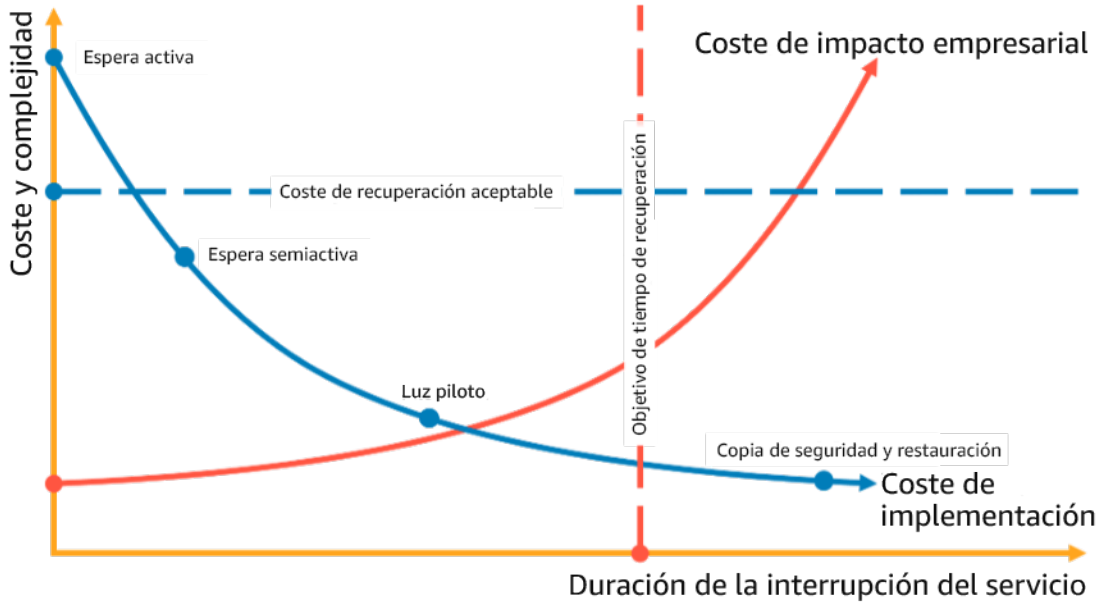


Figura 18: Selección de una estrategia de DR en función del RTO y costo

Para más información, consulte el Plan de continuidad del negocio (BCP).

2. Revise los patrones de cómo se puede implementar la estrategia de DR seleccionada.

   Este paso implica comprender cómo implementará la estrategia seleccionada. Las estrategias se explican mediante las Regiones de AWS para determinar un sitio principal y otro de recuperación. Sin embargo, también puede decidir utilizar zonas de disponibilidad en una única región como estrategia de DR, que utiliza los elementos de varias de estas estrategias.

   En los siguientes pasos, puede aplicar la estrategia a su carga de trabajo específica.

   Copia de seguridad y restauración

La copia de seguridad y restauración son la estrategia menos compleja de implementar, pero requerirán más tiempo y esfuerzo para restaurar la carga de trabajo, lo que generará un RTO y un RPO más altos. Se recomienda hacer siempre copias de seguridad de los datos y copiarlas en otro sitio (por ejemplo, otra Región de AWS).

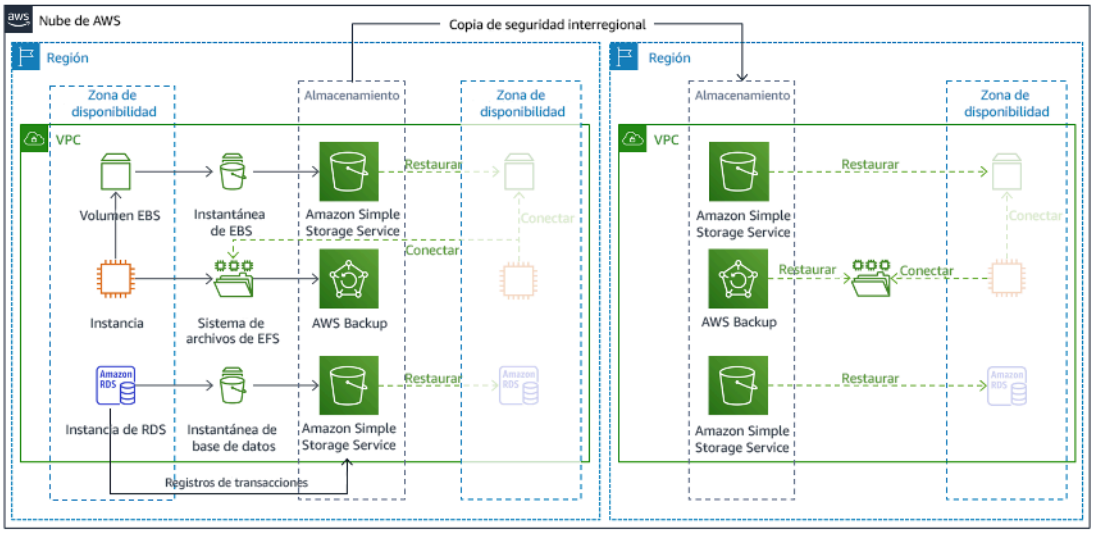


Figura 19: Arquitectura de copia de seguridad y restauración

Para obtener más información sobre esta estrategia, consulte [Disaster Recovery (DR) Architecture on AWS, Part II: Backup and Restore with Rapid Recovery](#).

Luz piloto

Con el enfoque de luz piloto, se replican los datos de la región principal a la región de recuperación. Los recursos principales utilizados para la infraestructura de la carga de trabajo se implementan en la región de recuperación; sin embargo, se siguen necesitando recursos adicionales y las dependencias pertinentes para que esta pila sea funcional. Por ejemplo, en la figura 20 no se implementan instancias de computación.

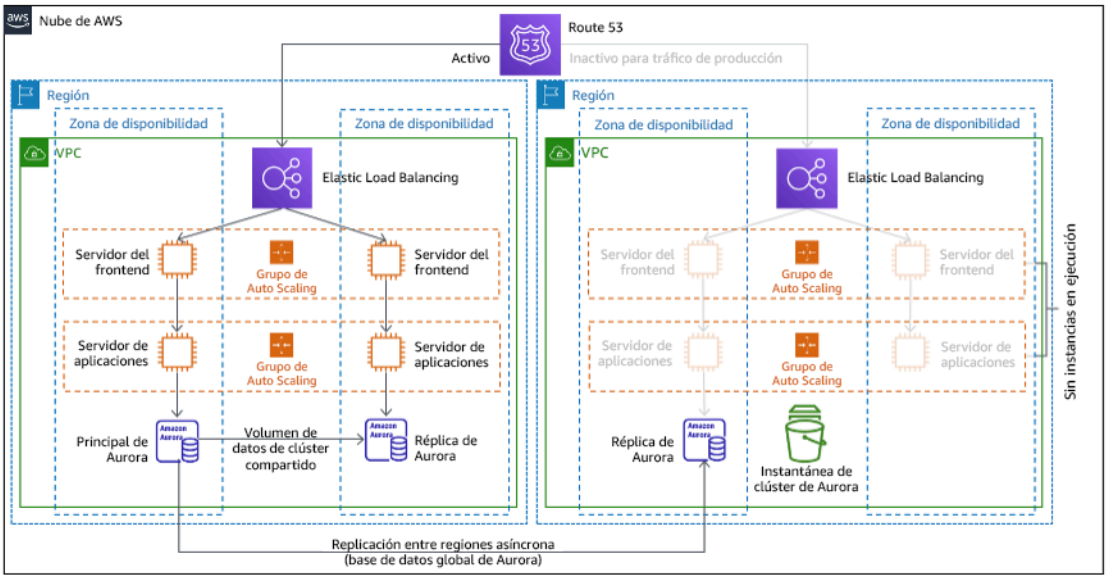


Figura 20: Arquitectura de luz piloto

Para obtener más información sobre esta estrategia, consulte Disaster Recovery (DR) Architecture on AWS, Part III: Pilot Light and Warm Standby.

Espera semiactiva

El enfoque de espera semiactiva implica garantizar que haya una copia reducida, pero completamente funcional, del entorno de producción en otra región. Este enfoque extiende el concepto de luz piloto y reduce el tiempo de recuperación, ya que su carga de trabajo tiene disponibilidad permanente en otra región. Si la región de recuperación se implementa al máximo de su capacidad, esto se conoce como modo de espera activa.

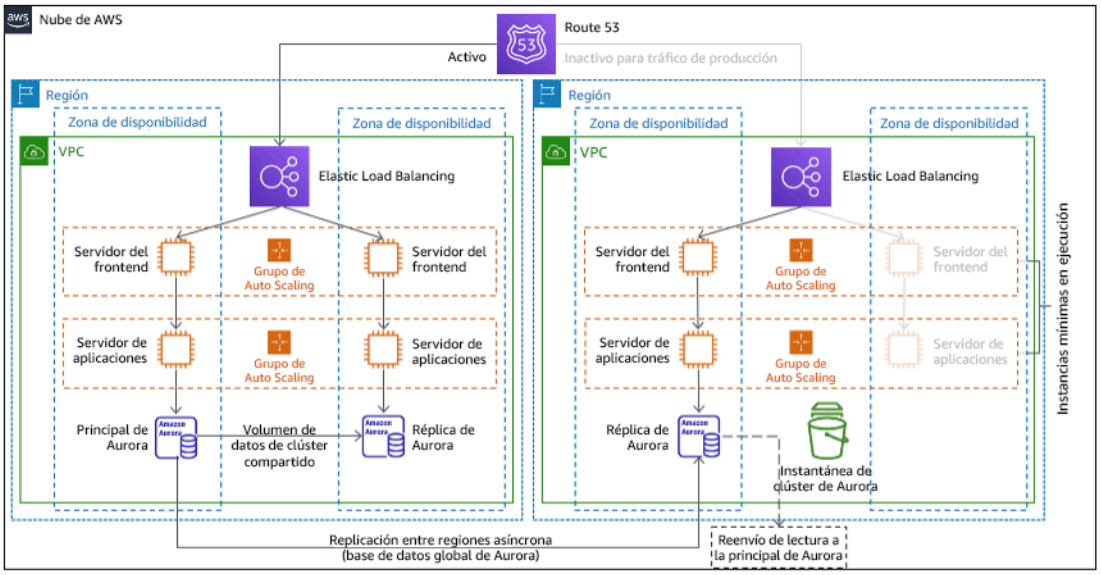


Figura 21: Arquitectura de espera semiactiva

El uso de los enfoques de espera semiactiva o luz piloto requiere escalar verticalmente los recursos en la región de recuperación. Para comprobar que la capacidad esté disponible cuando sea necesaria, considere la posibilidad de utilizar reservas de capacidad para las instancias de EC2. Si se utiliza AWS Lambda, la simultaneidad aprovisionada puede proporcionar entornos de tiempo de ejecución para que estén preparados para responder a las invocaciones de la función.

Para obtener más información sobre esta estrategia, consulte Disaster Recovery (DR) Architecture on AWS, Part III: Pilot Light and Warm Standby.

Activa-activa multisitio

Puede ejecutar la carga de trabajo de forma simultánea en varias regiones como parte de una estrategia activa-activa multisitio. La estrategia activa-activa multisitio suministra tráfico desde todas las regiones en las que se implementa. Los clientes podrían seleccionar esta estrategia por motivos ajenos a la DR. Se puede utilizar para aumentar la disponibilidad o cuando se implementa una carga de trabajo para una audiencia global (para colocar el punto de conexión más cerca de los usuarios o para implementar pilas localizadas para la audiencia de esa región). Como estrategia de DR, si la carga de trabajo no es compatible en una de las Regiones de AWS en la que se implemente, esa región se evacúa y las regiones restantes se utilizar para mantener la disponibilidad. La estrategia activa-activa multisitio es la más compleja de las estrategias de DR a nivel operativo y solo se debe seleccionar cuando los requisitos empresariales lo exijan.

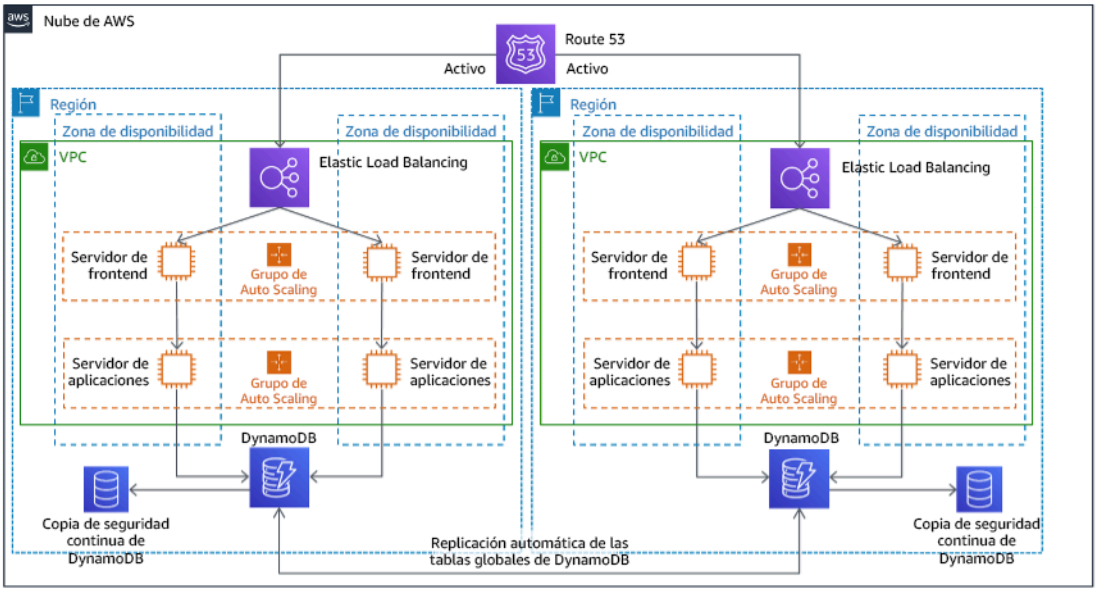


Figura 22: Arquitectura activa-activa multisitio

Para obtener más información sobre esta estrategia, consulte Disaster Recovery (DR) Architecture on AWS, Part IV: Multi-site Active/Active.

AWS Elastic Disaster Recovery

Si está considerando la posibilidad de adoptar la estrategia de luz piloto o espera semiactiva en caso de recuperación de desastres, AWS Elastic Disaster Recovery podría proporcionar un enfoque alternativo con mejores beneficios. La Recuperación de desastres elástica puede ofrecer un objetivo de RPO y RTO similar al de los sistemas de espera semiactiva, pero mantiene el enfoque de bajo costo de luz piloto. La Recuperación de desastres elástica replica los datos de la región principal a la región de recuperación y utiliza una protección de datos continua para lograr un RPO medido en segundos y un RTO que se puede medir en minutos. En la región de recuperación se implementan solo los recursos necesarios para replicar los datos, lo que mantiene los costos bajos, de forma similar a la estrategia de luz piloto. Al utilizar Recuperación de desastres elástica, el servicio coordina y organiza la recuperación de los recursos de computación cuando se inicia como parte de una conmutación por error o un simulacro.

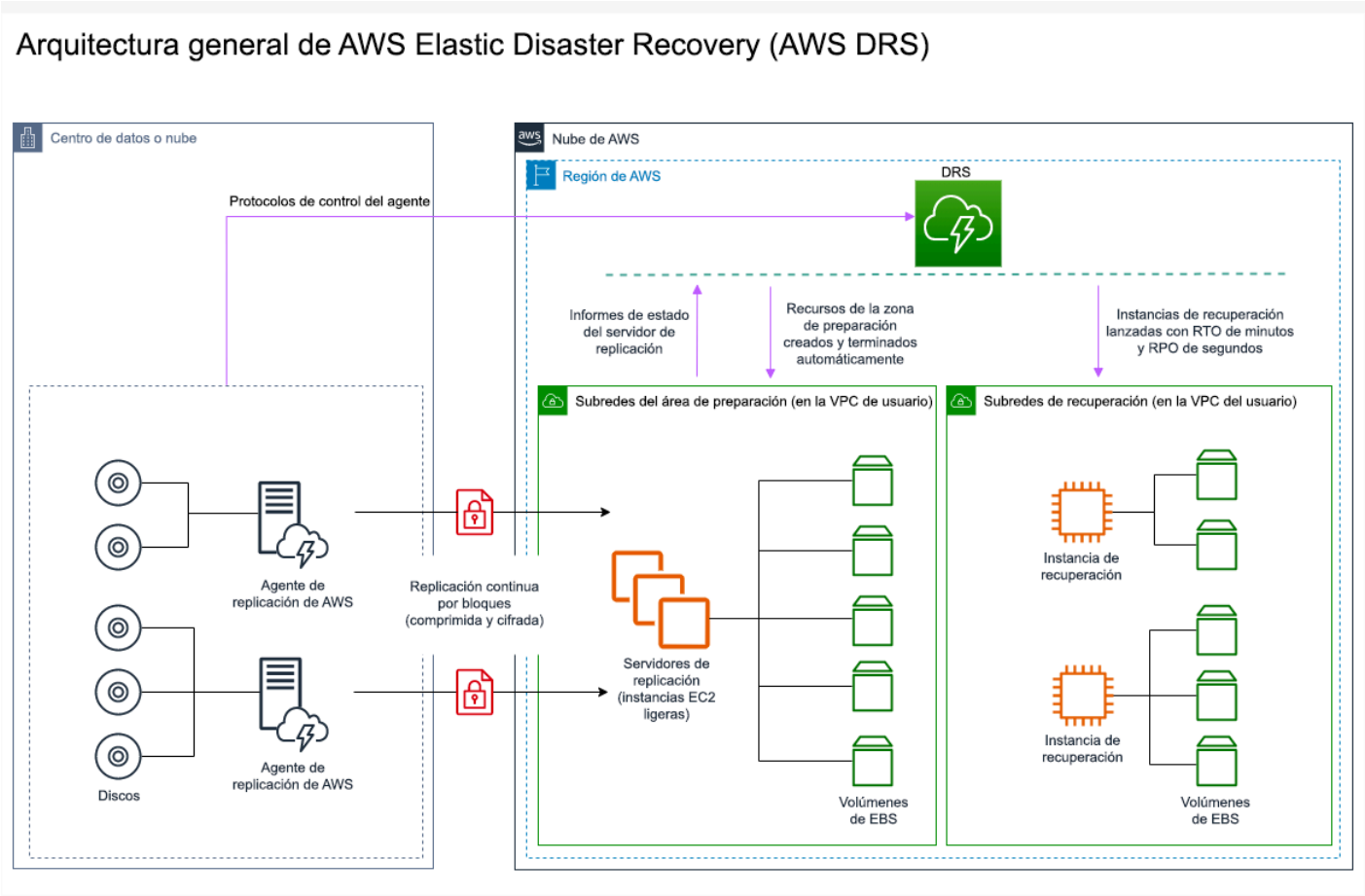


Figura 23: Arquitectura de AWS Elastic Disaster Recovery

Prácticas adicionales para la protección de los datos

Con todas las estrategias, también debe mitigar los posibles desastres de datos. La replicación de datos continua le brindará protección ante algunos tipos de desastres, pero no ante el daño o la destrucción de datos, a no ser que su estrategia incluya también control de versiones para una recuperación en un momento dado. También debe hacer una copia de seguridad de los datos replicados en el sitio de recuperación para crear copias de seguridad en un momento dado además de las réplicas.

Uso de varias zonas de disponibilidad (AZ) en una sola Región de AWS

Al usar varias AZ en una única región, la implementación de DR utiliza varios elementos de las estrategias anteriores. Primero, debe crear una arquitectura de alta disponibilidad con varias AZ, como se muestra en la figura 23. Esta arquitectura utiliza un enfoque activo-activo multisitio, ya que las instancias de Amazon EC2 y el equilibrador de carga elástico tienen recursos

implementados en varias zonas de disponibilidad y gestionan las solicitudes de forma activa. La arquitectura también muestra el modo de espera activa, donde, si se produce un error en la instancia principal de Amazon RDS (o se produce un error en la propia AZ), la instancia en espera pasa a ser principal.

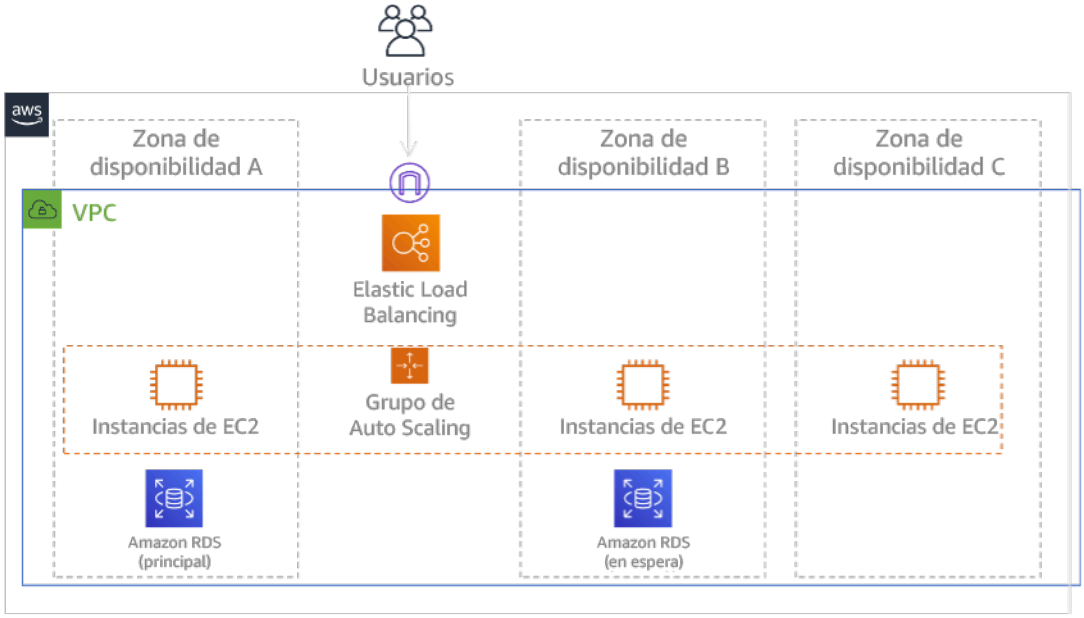


Figura 24: Arquitectura multi-AZ

Además de esta arquitectura de alta disponibilidad, debe agregar copias de seguridad con todos los datos necesarios para ejecutar la carga de trabajo. Esto es especialmente importante para los datos que están restringidos a una sola zona, como los volúmenes de Amazon EBS o los clústeres de Amazon Redshift. Si se produce un error en una AZ, tendrá que restaurar estos datos en otra AZ. Siempre que sea posible, deberá copiar las copias de seguridad de los datos en otra Región de AWS como capa de protección adicional.

Un enfoque alternativo menos común para la DR de una sola región de varias zonas de disponibilidad se ilustra en la entrada del blog Building highly resilient applications using Amazon Application Recovery Controller, Part 1: Single-Region stack. Aquí, la estrategia es mantener la máxima cantidad posible de aislamiento entre las AZ, tal y como funcionan las regiones. Al utilizar esta estrategia alternativa, puede elegir un enfoque activo-activo o activo-pasivo.

> **Note**
>
> Algunas cargas de trabajo tienen requisitos normativos de residencia de datos. Si esto se aplica a su carga de trabajo en una ubicación que actualmente tenga solo una Región

de AWS, el enfoque multirregión no se adaptará a sus necesidades empresariales. Las estrategias de multi-AZ ofrecen una buena protección contra la mayoría de los desastres.

3. Evalúe los recursos de la carga de trabajo y cuál será su configuración en la región de recuperación antes de la conmutación por error (durante el funcionamiento normal).

   Para la infraestructura y los recursos de AWS, utilice la infraestructura como código, por ejemplo, AWS CloudFormation o herramientas de terceros, como Hashicorp Terraform. Para efectuar la implementación en varias cuentas y regiones en una sola operación, puede utilizar AWS CloudFormation StackSets. En el caso de las estrategias activa-activa multisitio o espera activa, la infraestructura implementada en la región de recuperación tiene los mismos recursos que la región principal. En las estrategias de luz piloto y espera semiactiva, la infraestructura implementada requerirá acciones adicionales para prepararse para la producción. Con los parámetros y la lógica condicional de CloudFormation, puede controlar si una pila implementada está activa o en espera con una sola plantilla. Al utilizar la Recuperación de desastres elástica, el servicio replicará y orquestará la restauración de las configuraciones de las aplicaciones y los recursos de computación.

   Todas las estrategias de DR requieren que se haga una copia de seguridad de los orígenes de datos en la Región de AWS y, a continuación, que esas copias de seguridad se copien en la región de recuperación. AWS Backup proporciona una vista centralizada en la que se pueden configurar, programar y supervisar las copias de seguridad de estos recursos. Para los enfoques de luz piloto, espera semiactiva y activo-activo multisitio, también debe replicar los datos de la región principal en los recursos de datos de la región de recuperación, como las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS) o las tablas de Amazon DynamoDB. De esta forma, estos recursos de datos estarán activos y preparados para responder a solicitudes en la región de recuperación.

   Para más información sobre el funcionamiento de los servicios de AWS en las regiones, consulte esta serie de blogs en Creating a Multi-Region Application with AWS Services.

4. Determine e implemente cómo preparará la región de recuperación para la conmutación por error cuando sea necesario (durante un desastre).

   En el caso de la opción activa-activa multisitio, la conmutación por error implica evacuar una región y recurrir a las regiones activas restantes. En general, esas regiones están listas para aceptar tráfico. En las estrategias de luz piloto y espera semiactiva, las acciones de recuperación tendrán que implementar los recursos faltantes, como las instancias de EC2 en la figura 20, además de otros recursos faltantes.

En todas las estrategias anteriores, es posible que tenga que promover instancias de solo lectura de bases de datos para que se conviertan en la instancia de lectura y escritura principal.

En copias de seguridad y restauración, la restauración de datos desde una copia de seguridad crea recursos para esos datos, como volúmenes de EBS, instancias de bases de datos de RDS y tablas de DynamoDB. También tiene que restaurar la infraestructura e implementar el código. Puede utilizar AWS Backup para restaurar datos en la región de recuperación. Consulte REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes para obtener más detalles. Volver a crear la infraestructura incluye la creación de recursos, como instancias de EC2, además de Amazon Virtual Private Cloud (Amazon VPC), las subredes y los grupos de seguridad necesarios. Puede automatizar gran parte del proceso de restauración. Consulte esta entrada de blog para obtener más información.

5. Determine e implemente cómo redirigirá el tráfico a la conmutación por error cuando sea necesario (durante un desastre).

   Esta operación de conmutación por error se puede iniciar automática o manualmente. La conmutación por error iniciada automáticamente en función de comprobaciones de estado o alarmas se debe utilizar con cuidado, ya que una conmutación por error innecesaria (falsa alarma) supone ciertos inconvenientes, como la falta de disponibilidad y la pérdida de datos. Por tanto, la conmutación por error iniciada manualmente es la que se suele utilizar. En este caso, debe seguir automatizando los pasos de la conmutación por error, de modo que la iniciación manual sea como pulsar un botón.

   Hay varias opciones de administración del tráfico que tener en cuenta al utilizar servicios de AWS. Una opción es utilizar Amazon Route 53. Al utilizar Amazon Route 53, puede asociar varios puntos de conexión de IP en una o varias Regiones de AWS a un nombre de dominio de Route 53. Para implementar la conmutación por error iniciada manualmente, puede utilizar el Controlador de recuperación de aplicaciones de Amazon, que proporciona una API de plano de datos de alta disponibilidad para redirigir el tráfico a la región de recuperación. Al implementar la conmutación por error, utilice las operaciones del plano de datos y evite las del plano de control, como se describe en REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación.

   Para más información sobre esta y otras opciones, consulte esta sección del documento técnico sobre recuperación de desastres.

6. Diseñe un plan sobre cómo se recuperará su carga de trabajo.

La conmutación por recuperación se produce cuando se devuelve la operación de una carga de trabajo a la región principal una vez disminuido un desastre. Por lo general, el aprovisionamiento de la infraestructura y el código en la región principal sigue los mismos pasos que se utilizaron inicialmente y se basa en la infraestructura como código y en las canalizaciones de implementación del código. El reto que plantea la conmutación por recuperación es restaurar los almacenes de datos y garantizar que sean coherentes con la región de recuperación en funcionamiento.

En el estado de conmutación por error, las bases de datos en la región de recuperación están activas y tienen los datos actualizados. El objetivo es volver a efectuar la sincronización desde la región de recuperación a la región principal, lo que garantiza que está actualizada.

Algunos servicios de AWS harán esto automáticamente. Si utiliza las tablas globales de Amazon DynamoDB, aunque la tabla de la región principal no esté disponible, cuando vuelva a estar en línea, DynamoDB reanudará la propagación de las escrituras pendientes. Si utiliza la Base de datos global de Amazon Aurora y la conmutación por error planificada administrada, se mantiene la topología de reproducción existente de la base de datos global de Aurora. Por tanto, la instancia de lectura y escritura anterior en la región principal se convertirá en una réplica y recibirá actualizaciones desde la región de recuperación.

En los casos en los que esto no se haga automáticamente, tendrá que restablecer la base de datos en la región principal como una réplica de la base de datos en la región de recuperación. En muchos casos, esto supondrá eliminar la antigua base de datos principal y crear nuevas réplicas.

Tras una conmutación por error, si puede seguir operando en su región de recuperación, considere la posibilidad de convertir esta región en la nueva región principal. Seguiría completando los pasos anteriores para hacer que la antigua región principal fuera una región de recuperación. Algunas organizaciones llevan a cabo una rotación programada y cambian sus regiones principal y de recuperación periódicamente (por ejemplo, cada tres meses).

Todos los pasos necesarios para la conmutación por error y conmutación por recuperación deben mantenerse en una guía de estrategias disponible para todos los miembros del equipo que se revise periódicamente.

Al utilizar la Recuperación de desastres elástica, el servicio ayudará a organizar y automatizar el proceso de conmutación por recuperación. Para obtener más información, consulte Performing a failback.

Nivel de esfuerzo para el plan de implementación: alto

Recursos

Prácticas recomendadas relacionadas:

- the section called “REL09-BP01 Identificación de todos los datos de los que se debe hacer una copia de seguridad, creación de la copia de seguridad o reproducción de los datos a partir de los orígenes”
- the section called “REL11-BP04 Confianza en el plano de datos y no en el plano de control durante la recuperación”
- the section called “REL13-BP01 Definición de objetivos de recuperación para el tiempo de inactividad y la pérdida de datos”

Documentos relacionados:

- AWS Architecture Blog: Disaster Recovery Series
- Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube (documento técnico de AWS)
- Opciones de recuperación de desastres en la nube
- Build a serverless multi-region, active-active backend solution in an hour
- Multi-region serverless backend — reloaded
- RDS: replicación de una réplica de lectura entre regiones
- Route 53: Configuring DNS Failover
- S3: replicación entre regiones
- Qué es AWS Backup?
- What is Amazon Application Recovery Controller?
- AWS Elastic Disaster Recovery
- HashiCorp Terraform: Get Started - AWS
- Socio de APN: socios que pueden ayudar con la recuperación de desastres
- AWS Marketplace: productos que pueden usarse para la recuperación ante desastres

Videos relacionados:

- Disaster Recovery of Workloads on AWS

- AWS re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications (ARC209-R2)
- Get Started with AWS Elastic Disaster Recovery | Amazon Web Services

REL13-BP03 Prueba de la implementación de recuperación de desastres para validarla

Compruebe periódicamente la conmutación por error de su sitio de recuperación para verificar que funcione adecuadamente y que se cumplan el RTO y el RPO.

Patrones comunes de uso no recomendados:

- No llevar a cabo nunca conmutaciones por error en producción.

Beneficios de establecer esta práctica recomendada: las pruebas periódicas del plan de recuperación de desastres verifican que el plan funcione cuando llegue el momento y que su equipo sepa cómo llevar a cabo la estrategia.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Un patrón que debe evitarse es el desarrollo de rutas de recuperación que se pongan en práctica pocas veces. Por ejemplo, puede tener un almacén de datos secundario que se utilice para consultas de solo lectura. Cuando escribe en un almacén de datos y se produce un error del almacén principal, es posible que quiera conmutar por error al almacén de datos secundario. Si no se prueba frecuentemente esta conmutación por error, es posible que sus suposiciones sobre las capacidades del almacén de datos secundario sean incorrectas. Es posible que la capacidad del almacén de datos secundario, que quizás fuera suficiente cuando se probó por última vez, ya no pueda tolerar la carga en esta situación. Nuestra experiencia ha demostrado que la única forma de recuperación de errores que funciona es aquella que se prueba constantemente. Por ello, es mejor tener un número reducido de rutas de recuperación. Puede establecer patrones de recuperación y probarlos con frecuencia. Si tiene una ruta de recuperación compleja o crítica, todavía debe llevar a efecto ese error en producción periódicamente para asegurarse de que la ruta funcione. En el ejemplo que acabamos de comentar, se debe conmutar por error al modo de espera con regularidad, sin importar si es necesario.

Pasos para la implementación

1. Diseñe sus cargas de trabajo para que se puedan recuperar. Pruebe regularmente sus rutas de recuperación. La computación orientada a la recuperación identifica las características de los sistemas que mejoran la recuperación: aislamiento y redundancia, capacidad en todo el sistema para revertir los cambios, capacidad para supervisar y determinar el estado, capacidad para proporcionar diagnósticos, recuperación automatizada, diseño modular y capacidad para reiniciar. Ponga en práctica la ruta de recuperación para verificar que pueda llevar a cabo la recuperación en el tiempo especificado para el estado especificado. Use sus manuales de procedimientos durante esta recuperación para documentar los problemas y encontrar soluciones para estos antes de la próxima prueba.
2. En el caso de las cargas de trabajo basadas en Amazon EC2, utilice AWS Elastic Disaster Recovery para implementar y lanzar instancias de simulacro para la estrategia de DR. AWS Elastic Disaster Recovery ofrece la posibilidad de ejecutar simulacros de forma eficiente, lo que ayuda a prepararse para un evento de conmutación por error. También puede lanzar con frecuencia sus instancias mediante Recuperación de desastres elástica para hacer pruebas y simulacros sin redirigir el tráfico.

Recursos

Documentos relacionados:

- Socio de APN: socios que pueden ayudar con la recuperación de desastres
- AWS Architecture Blog: Disaster Recovery Series
- AWS Marketplace: productos que pueden usarse para la recuperación de desastres
- AWS Elastic Disaster Recovery
- Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube (documento técnico de AWS)
- AWS Elastic Disaster Recovery Preparing for Failover
- The Berkeley/Stanford recovery-oriented computing project
- What is AWS Fault Injection Simulator?

Videos relacionados:

- AWS re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications
- AWS re:Invent 2019: Backup-and-restore and disaster-recovery solutions with AWS

REL13-BP04 Administración de la desviación de la configuración en el sitio o región de DR

Para llevar a cabo un procedimiento de recuperación ante desastres (DR) correctamente, su carga de trabajo debe poder reanudar las operaciones normales de manera oportuna sin pérdida relevante de funcionalidad o datos una vez que el entorno de DR se haya puesto en funcionamiento. Para lograr este objetivo, es esencial mantener una infraestructura, datos y configuraciones consistentes entre el entorno de DR y el entorno principal.

Resultado deseado: la configuración y los datos de su sitio de recuperación ante desastres son iguales a los del sitio principal, lo que facilita una recuperación rápida y completa cuando es necesario.

Patrones comunes de uso no recomendados:

- No se actualizan las ubicaciones de recuperación cuando se realizan cambios en las ubicaciones principales, lo que se traduce en configuraciones desactualizadas que podrían dificultar los esfuerzos de recuperación.
- No tiene en cuenta las posibles limitaciones, como las diferencias de los servicios entre las ubicaciones principales y de recuperación, que pueden provocar fallos inesperados durante la conmutación por error.
- Confía en los procesos manuales para actualizar y sincronizar el entorno de recuperación ante desastres, lo que aumenta el riesgo de errores humanos e incoherencias.
- No se detectan desviaciones en la configuración, lo que genera una falsa sensación de que el sitio de recuperación ante desastres está preparado antes de que se produzca un incidente.

Beneficios de establecer esta mejor práctica: la coherencia entre el entorno de recuperación ante desastres y el entorno principal mejora considerablemente las probabilidades de una recuperación satisfactoria tras un incidente y reduce el riesgo de que se produzca un error en el procedimiento de recuperación.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Un enfoque integral de la administración de la configuración y la preparación para la conmutación por error puede ayudarlo a comprobar que el sitio de recuperación ante desastres se actualiza

constantemente y está preparado para asumir el control en caso de que se produzca un fallo en el sitio principal.

Para lograr la coherencia entre su entorno principal y el de recuperación ante desastres (DR), compruebe que sus canales de entrega distribuyen las aplicaciones tanto en el sitio principal como en el de recuperación ante desastres. Despliegue los cambios en los sitios de recuperación ante desastres después de un periodo de evaluación adecuado (también conocido como despliegues escalonados) para detectar problemas en el sitio principal y detener la implementación antes de que se propaguen. Implemente la supervisión para detectar desviaciones en la configuración y lleve un seguimiento de los cambios y el cumplimiento en todos sus entornos. Realice correcciones automatizadas en el sitio de recuperación ante desastres para mantener la máxima coherencia y que esté listo para funcionar en caso de que se produzca un incidente.

Pasos para la implementación

1. Valide que la región de recuperación ante desastres contenga los servicios y las características de AWS necesarios para ejecutar correctamente el plan de recuperación ante desastres.
2. Utilice infraestructura como código (IaC). Mantenga la precisión de sus plantillas de configuración de aplicaciones e infraestructura de producción y aplíquelas periódicamente a su entorno de recuperación ante desastres. AWS CloudFormationpuede detectar una desviación entre lo que especifican las plantillas de CloudFormation y lo que realmente se implementa.
3. Configure las canalizaciones de CI/CD para implementar aplicaciones y actualizaciones de infraestructura en todos los entornos, incluidos los sitios principales y de recuperación ante desastres. Las soluciones de CI/CD, como AWS CodePipeline, pueden automatizar el proceso de implementación, lo que reduce el riesgo de cambios en la configuración.
4. Distribuya las implementaciones entre el entorno principal y el de recuperación ante desastres. Este enfoque permite implementar y probar las actualizaciones inicialmente en el entorno principal, lo que aísla los problemas en el sitio principal antes de que se propaguen al sitio de DR. Así se evita que los defectos se transmitan simultáneamente a la planta de producción y al centro de recuperación ante desastres y mantiene la integridad del entorno de recuperación ante desastres.
5. Supervise continuamente las configuraciones de los recursos en los entornos principal y de DR. Soluciones como AWS Config pueden ayudar a garantizar el cumplimiento de la configuración y detectar desviaciones, lo que ayuda a mantener la coherencia de las configuraciones en todos los entornos.
6. Implemente mecanismos de alerta para rastrear y notificar cualquier cambio en la configuración o interrupción o retraso en la replicación de datos.

7. Automatice la corrección de las desviaciones de configuración detectadas.
8. Programe auditorías y comprobaciones de conformidad periódicas para verificar la alineación continua entre las configuraciones principal y de recuperación ante desastres. Las revisiones periódicas ayudan a mantener el cumplimiento de las normas definidas e identificar cualquier discrepancia que deba abordarse.
9. Compruebe si hay discrepancias en la capacidad aprovisionada, las cuotas de servicio, los límites de aceleración y las discrepancias de configuración y versión de AWS.

Recursos

Prácticas recomendadas relacionadas:

- REL01-BP01 Conocimiento de las cuotas y restricciones del servicio
- REL01-BP02 Administración de cuotas de servicio en cuentas y regiones
- REL01-BP04 Supervisión y administración de cuotas
- REL13-BP03 Prueba de la implementación de recuperación ante desastres para validarla

Documentos relacionados:

- Remediating Noncompliant AWS Resources by Reglas de AWS Config
- AWS Systems Manager Automation
- AWS CloudFormation: Detección de cambios de configuración no administrados en pilas y recursos
- AWS CloudFormation: Detección de desviaciones en una pila de CloudFormation completa
- AWS Systems Manager Automation
- Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube (documento técnico de AWS)
- How do I implement an Infrastructure Configuration Management solution on AWS?
- Remediating Noncompliant AWS Resources by Reglas de AWS Config

Videos relacionados:

- AWS re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications (ARC209-R2)

Ejemplos relacionados:

- CloudFormation Registro
- Monitor de cuotas para AWS
- Implemente la corrección automática de desviaciones para AWS CloudFormation mediante Amazon CloudWatch y AWS Lambda
- AWS Architecture Blog: Disaster Recovery Series
- AWS Marketplace: productos que pueden usarse para la recuperación ante desastres
- Automatización de implementaciones seguras y sin intervención

REL13-BP05 Automatización de la recuperación

Implemente mecanismos de recuperación comprobados y automatizados que sean fiables, observables y reproducibles para reducir el riesgo y el impacto empresarial de los fallos.

Resultado deseado: ha implementado un flujo de trabajo de automatización bien documentado, estandarizado y probado exhaustivamente para los procesos de recuperación. La automatización de la recuperación corrige automáticamente los problemas menores que suponen un bajo riesgo de pérdida de datos o de falta de disponibilidad. Puede invocar rápidamente a los procesos de recuperación en caso de incidentes graves, observar el comportamiento de corrección mientras están en funcionamiento y finalizar los procesos si observa situaciones peligrosas o fallos.

Patrones comunes de uso no recomendados:

- Como parte de su plan de recuperación, depende de los componentes o mecanismos que se encuentran en un estado defectuoso o degradado.
- Los procesos de recuperación requieren una intervención manual, como el acceso a la consola (también conocido como operaciones de clic).
- Los procedimientos de recuperación se inician automáticamente en situaciones que presentan un alto riesgo de pérdida de datos o de falta de disponibilidad.
- No incluye un mecanismo para interrumpir un procedimiento de recuperación (similar a un sistema Andon o a un botón rojo de parada de emergencia) que no funciona o que plantea riesgos adicionales.

Beneficios de establecer esta práctica recomendada:

- Mayor fiabilidad, previsibilidad y consistencia de las operaciones de recuperación.
- Capacidad para cumplir objetivos de recuperación más estrictos, como el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO).
- Menor probabilidad de fallos en la recuperación durante un incidente.
- Reducción del riesgo de fallos asociados a los procesos de recuperación manual que son propensos a errores humanos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Para implementar la recuperación automatizada, necesita un enfoque integral que utilice los servicios de AWS y las prácticas recomendadas. Para empezar, identifique los componentes críticos y los posibles puntos de fallo de su carga de trabajo. Desarrolle procesos automatizados que puedan recuperar sus cargas de trabajo y datos en caso de fallos sin intervención humana.

Desarrolle la automatización de la recuperación mediante los principios de la infraestructura como código (IaC). Esto hace que su entorno de recuperación sea coherente con el entorno de origen y permita controlar las versiones de sus procesos de recuperación. Para organizar flujos de trabajo de recuperación complejos, puede usar soluciones como AWSSystems Manager Automation o AWS Step Functions.

La automatización de los procesos de recuperación ofrece beneficios importantes y puede ayudar a alcanzar el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) con mayor facilidad. Sin embargo, pueden encontrarse con situaciones inesperadas que tal vez provoquen fallos o creen nuevos riesgos por su parte, como un mayor tiempo de inactividad y la pérdida de datos. Para mitigar este riesgo, ofrezca la posibilidad de detener rápidamente una automatización de la recuperación en curso. Una vez detenida, puede investigar y tomar medidas correctivas.

En el caso de las cargas de trabajo compatibles, puede probar soluciones como la recuperación elástica ante desastres de AWS (AWS DRS) para proporcionar una conmutación por error automatizada. AWS DRS replica continuamente las máquinas (incluido el sistema operativo, la configuración del estado del sistema, las bases de datos, las aplicaciones y los archivos) en un área provisional de su cuenta de Cuenta de AWS de destino y en la región preferida. Si se produce un incidente, AWS DRS automatiza la conversión de los servidores replicados en cargas de trabajo totalmente aprovisionadas en la región de recuperación en AWS.

El mantenimiento y la mejora de la recuperación automática son un proceso continuo. Pruebe y perfeccione continuamente sus procedimientos de recuperación en función de las lecciones aprendidas y manténgase al tanto de los nuevos servicios y características de AWS que pueden mejorar sus capacidades de recuperación.

Pasos para la implementación

1. Planifique una recuperación automatizada
   a. Realice una revisión exhaustiva de la arquitectura, los componentes y las dependencias de su carga de trabajo para identificar y planificar los mecanismos de recuperación automatizados. Clasifique las dependencias de su carga de trabajo en dependencias estrictas y flexibles. Las dependencias estrictas son imprescindibles y sin ellas la carga de trabajo no puede funcionar; además, no se puede ofrecer ninguna alternativa. Las dependencias flexibles son aquellas que suele utilizar la carga de trabajo, pero que pueden sustituirse por sistemas o procesos alternativos de manera temporal o que pueden gestionarse mediante una degradación estable.
   b. Establezca procesos para identificar y recuperar los datos dañados o ausentes.
   c. Defina los pasos para confirmar un estado estable recuperado una vez finalizadas las acciones de recuperación.
   d. Considere cualquier acción necesaria para que el sistema recuperado esté listo para funcionar plenamente, como precalentar y llenar las cachés.
   e. Considere los problemas que podrían surgir durante el proceso de recuperación y cómo detectarlos y solucionarlos.
   f. Plantéese situaciones en las que no se pueda acceder al sitio principal y a su plano de control. Compruebe que las acciones de recuperación se puedan realizar de forma independiente sin depender del sitio principal. Puede usar soluciones como el controlador de recuperación de aplicaciones de Amazon (ARC) para redirigir el tráfico sin necesidad de mutar manualmente los registros de DNS.
2. Desarrolle un proceso de recuperación automatizado
   a. Implemente mecanismos automatizados de detección de fallos y conmutación por error para una recuperación sin intervención manual. Cree paneles de control, como Amazon CloudWatch, para informar sobre el progreso y el estado de los procedimientos de recuperación automatizados. Incluya procedimientos para validar una recuperación correcta. Proporcione un mecanismo para interrumpir una recuperación en curso.
   b. Cree guías de estrategia como un proceso alternativo para los errores que no permitan una recuperación automática y tenga en cuenta su plan de recuperación ante desastres.

   c. Pruebe los procesos de recuperación tal y como se describe en REL13-BP03.

3. Prepárese para la recuperación
   a. Evalúe el estado de su sitio de recuperación e implemente los componentes críticos en él con antelación. Para obtener más información, consulte REL13-BP04.
   b. Defina funciones, responsabilidades y procesos de toma de decisiones claros para las operaciones de recuperación, con la participación de las partes interesadas y los equipos pertinentes de toda la organización.
   c. Defina las condiciones para iniciar los procesos de recuperación.
   d. Cree un plan para revertir el proceso de recuperación y vuelva a su sitio principal si es necesario o después de considerarlo seguro.

Recursos

Prácticas recomendadas relacionadas:

- REL07-BP01 Uso de la automatización al obtener o escalar recursos
- REL11-BP01 Supervisión de todos los componentes de la carga de trabajo para detectar errores
- REL13-BP02 Uso de estrategias de recuperación definidas para cumplir los objetivos de recuperación
- REL13-BP03 Prueba de la implementación de recuperación ante desastres para validarla
- REL13-BP04 Administración de la desviación de la configuración en el sitio o región de DR

Documentos relacionados:

- AWS Architecture Blog: Disaster Recovery Series
- Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube (documento técnico de AWS)
- Orchestrate Disaster Recovery Automation using Amazon Route 53 ARC and AWS Step Functions
- Build AWS Systems Manager Automation runbooks using AWS CDK
- AWS Marketplace: productos que pueden usarse para la recuperación ante desastres
- AWS Systems Manager Automation
- AWS Elastic Disaster Recovery
- Using Elastic Disaster Recovery for Failover and Failback

- AWS Elastic Disaster Recovery Resources
- Socio de APN: socios que pueden ayudar con la recuperación ante desastres

Videos relacionados:

- AWS re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications (ARC209-R2)
- AWS re:Invent 2022: AWS On Air ft. AWS Failback for AWS Elastic Disaster Recovery

Conclusión

Ya sea un novato en los temas de disponibilidad y fiabilidad o un veterano experimentado que busca información para maximizar la disponibilidad de su carga de trabajo crítica, esperamos que este documento técnico haya retado su mente, ofrecido una nueva idea o introducido una nueva línea de preguntas. Esperamos que esto conduzca a una comprensión más profunda del nivel correcto de disponibilidad basado en las necesidades de su negocio y cómo diseñar la fiabilidad para lograrlo. Le recomendamos que aproveche las recomendaciones de diseño, operativas y orientadas a la recuperación que se ofrecen aquí, así como el conocimiento y la experiencia de nuestros arquitectos de soluciones de AWS. Nos encantaría conocer su opinión, especialmente sus historias de éxito que logran altos niveles de disponibilidad en AWS. Contacte con el equipo de cuentas o utilice la opción Contacto en nuestro sitio web.

Colaboradores

Los colaboradores de este documento son:

- Michael Fischer, Principal Solutions Architect, Amazon Web Services
- Seth Eliot, Principal Developer Advocate, Amazon Web Services
- Mahanth Jayadeva, Solutions Architect – Well-Architected, Amazon Web Services
- Amulya Sharma, Principal Solutions Architect, Amazon Web Services
- Jason DiDomenico, Senior Solutions Architect – Cloud Foundations, Amazon Web Services
- Marcin Bednarz, Principal Solutions Architect, Amazon Web Services
- Tyler Applebaum, Senior Solutions Architect, Amazon Web Services
- Rodney Lester, Principal Solutions Architect, Amazon Web Services
- Joe Chapman, Senior Solutions Architect, Amazon Web Services
- Adrian Hornsby, Principal System Development Engineer, Amazon Web Services
- Kevin Miller, Vice President – S3, Amazon Web Services
- Shannon Richards, Principal Technical Program Manager, Amazon Web Services
- Laurent Domb, Chief Technologist - Fed Fin, Amazon Web Services
- Kevin Schwarz, Sr. Solutions Architect, Amazon Web Services
- Rob Martell, Principal Cloud Resilience Architect, Amazon Web Services
- Priyam Reddy, Senior Solutions Architect Manager DR, Amazon Web Services
- Jeff Ferris, Principal Technologist, Amazon Web Services
- Matias Battaglia, Senior Solutions Architect, Amazon Web Services

Documentación adicional

Para obtener información adicional, consulte:

- Marco de AWS Well-Architected
- Centro de arquitectura de AWS

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Actualización de las directrices de prácticas recomendadas	Las prácticas recomendadas se han actualizado con nuevas guías en las siguientes áreas: REL 1, REL 2, REL 4, REL 6, REL 7, REL 8, REL 10, REL 12 y REL 13. La guía se ha ampliado y aclarado en todo el pilar. Se han fusionado las guías de REL10-BP0 2 y REL12-BP03 en otras prácticas recomendadas. Se han actualizado los recursos de todo el pilar.	6 de noviembre de 2024
Actualización de las directrices de prácticas recomendadas	Pequeñas actualizaciones de las prácticas recomendadas en REL 2, 4, 5, 6, 7 y 8.	27 de junio de 2024
Actualización de las directrices de prácticas recomendadas	Las prácticas recomendadas se actualizaron con nuevas directrices en las siguientes áreas: Diseño de las interacci ones en un sistema distribui do para evitar los errores, Diseño de interacciones en un sistema distribuido para mitigar o tolerar errores, Supervisión de los recursos de la carga de trabajo, Diseño de la carga de trabajo para que	6 de diciembre de 2023

	se adapte a los cambios de la demanda, Implementación de cambios y Pruebas de fiabilidad.	
Actualización de las directrices de prácticas recomendadas	Las prácticas recomendadas se actualizaron con nuevas directrices en las siguientes áreas: Supervisión de los recursos de la carga de trabajo y Diseño de la carga de trabajo para que tolere los errores de los componentes.	3 de octubre de 2023
Actualización de las directrices de prácticas recomendadas	Las prácticas recomendadas se actualizaron con nuevas directrices en las siguientes áreas: Diseño de la arquitectura de servicio de su carga de trabajo, Diseño de interacciones en un sistema distribuido para mitigar o tolerar errores y Supervisión de los recursos de la carga de trabajo.	13 de julio de 2023
Actualización menor	Eliminación del lenguaje no inclusivo.	13 de abril de 2023
Actualizaciones del nuevo marco	Se actualizaron las prácticas recomendadas con una guía prescriptiva y se agregaron nuevas prácticas recomendadas.	10 de abril de 2023
Documento técnico actualizado	Se actualizaron las prácticas recomendadas con una nueva guía de implementación.	15 de diciembre de 2022

Actualizaciones menores	Corrección de cifras y cambios menores en todo el documento.	17 de noviembre de 2022
Documento técnico actualizado	Se ampliaron las prácticas recomendadas y se agregaron planes de mejora.	20 de octubre de 2022
Documento técnico actualizado	Se agregaron dos nuevas prácticas recomendadas al pilar de fiabilidad en las secciones Uso del aislamiento de errores para proteger su carga de trabajo y Diseño de la carga de trabajo para que tolere los errores de los componentes.	5 de mayo de 2022
Documento técnico actualizado	Se actualizó la guía de recuperación de desastres para incluir el Controlador de recuperación de aplicaciones de Route 53. Se agregaron referencias a DevOps Guru. Se actualizaron varios enlaces de recursos y se hicieron otros cambios editoriales menores.	26 de octubre de 2021
Actualización menor	Se agregó información sobre AWS Fault Injection Service (AWS FIS).	15 de marzo de 2021
Actualización menor	Actualización de texto menor.	4 de enero de 2021

Documento técnico actualizado	Actualización del apéndice A en relación con el objetivo de diseño de la disponibilidad para Amazon SQS, Amazon SNS y Amazon MQ; reordenación de las filas de la tabla para facilitar la búsqueda; mejora de la explicación de las diferencias entre la disponibilidad y la recuperación de desastres y de cómo ambas contribuyen a la resiliencia; ampliación de la cobertura de las arquitecturas multirregión (para la disponibilidad) y de las estrategias multirregión (para la recuperación de desastres); actualización del libro de referencia a la última versión; ampliación de los cálculos de la disponibilidad para incluir el cálculo basado en las solicitudes y los cálculos abreviados; mejora de la descripción de los días de juego.	7 de diciembre de 2020
Actualización menor	Se actualizó el Apéndice A para modificar el objetivo de diseño de disponibilidad para AWS Lambda	27 de octubre de 2020
Actualización menor	Se actualizó el Apéndice A para agregar el objetivo de diseño de disponibilidad para AWS Global Accelerator	24 de julio de 2020

Actualizaciones del nuevo marco	Actualizaciones sustanciales y contenido nuevo o revisado, que incluyen lo siguiente : se agregó la sección de prácticas recomendadas “Arquitectura de la carga de trabajo”; se reorganizaron las prácticas recomendadas en las secciones Administración de cambios y Administración de errores; se actualizó la sección Recursos para incluir los recursos y servicios de AWS más recientes, como AWS Global Accelerator, AWS Service Quotas y AWS Transit Gateway; se agregaron o actualizaron las definicio nes de fiabilidad, disponibi lidad y resiliencia; se alineó mejor el documento técnico con AWS Well-Architected Tool (preguntas y prácticas recomendadas) que se usa para las revisiones de Well-Architected; se reordenar on los principios de diseño; se trasladó Recuperación automática de un error antes de Prueba de procedimi entos de recuperación; se actualizaron los diagramas y los formatos de las ecuacione s; se eliminaron las secciones Servicios clave y se integraron las referencias a los servicios	8 de julio de 2020

	clave de AWS en las prácticas recomendadas.	
Actualización menor	Corrección del enlace que no funciona	1 de octubre de 2019
Documento técnico actualizado	Se actualizó el Apéndice A	1 de abril de 2019
Documento técnico actualizado	Se agregaron recomendaciones específicas de redes de AWS Direct Connect y objetivos de diseño de servicio adicionales	1 de septiembre de 2018
Documento técnico actualizado	Se agregaron las secciones Principios de diseño y Administración de límites. Se actualizaron los enlaces, se eliminó la ambigüedad de la terminología ascendente/descendente y se agregaron referencias explícitas a los temas restantes del Pilar de fiabilidad en las situaciones de disponibilidad.	1 de junio de 2018
Documento técnico actualizado	Se cambió la solución de la región DynamoDB Cross a DynamoDB Global Tables. Se agregaron objetivos de diseño de servicio.	1 de marzo de 2018
Actualizaciones menores	Corrección menor en el cálculo de disponibilidad para incluir la disponibilidad de la aplicación	1 de diciembre de 2017

Documento técnico actualizado	Se actualizó el documento para proporcionar orientación sobre diseños de alta disponibilidad, como conceptos, prácticas recomendadas e implementaciones de ejemplo.	1 de noviembre de 2017
Publicación inicial	Se publicó Pilar de fiabilidad: Marco de AWS Well-Architected.	1 de noviembre de 2016

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene sólo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

© 2023 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.