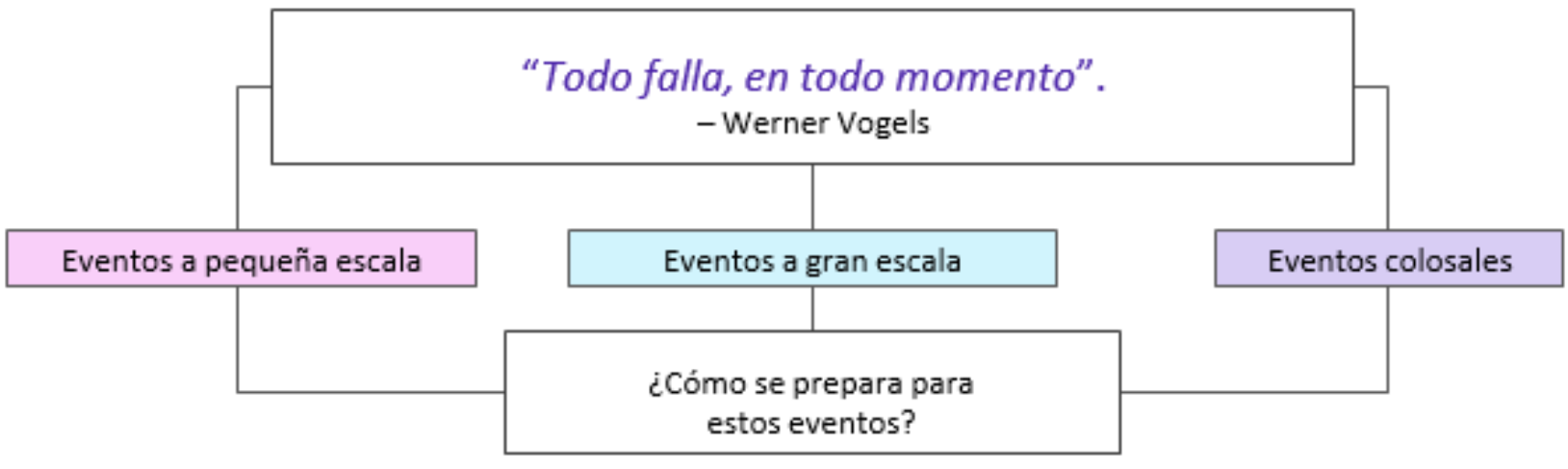
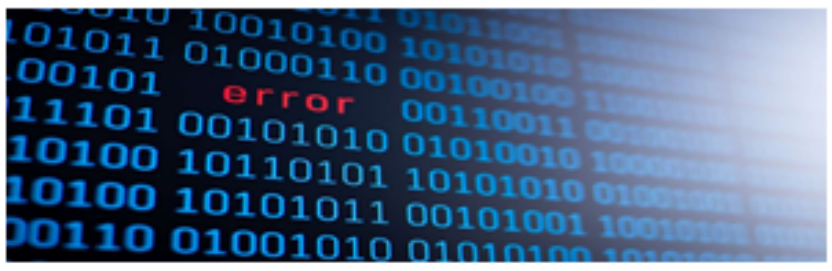
LECCIÓN 2: ESTRATEGIAS DE PLANIFICACIÓN PARA DESASTRES.

PLANIFICACIÓN PARA ERRORES





El director de tecnología (CTO) de AWS, Werner Vogels, ha dicho en más de una ocasión que: "Todo falla, en todo momento". Su enunciado ha ejercido influencia sobre el diseño arquitectónico de la informática en la nube durante muchos años porque expresa una verdad evidente.

Los errores no deberían considerarse una anormalidad poco probable. Por el contrario, se debe suponer que los errores, tanto de gran magnitud como de magnitud reducida, pueden ocurrir y así será. ¿Cómo se prepara para estos eventos?

Los errores pueden pertenecer a una de las siguientes tres categorías:

evento a pequeña escala:

Por ejemplo, un servidor dejó de responder o se desconectó

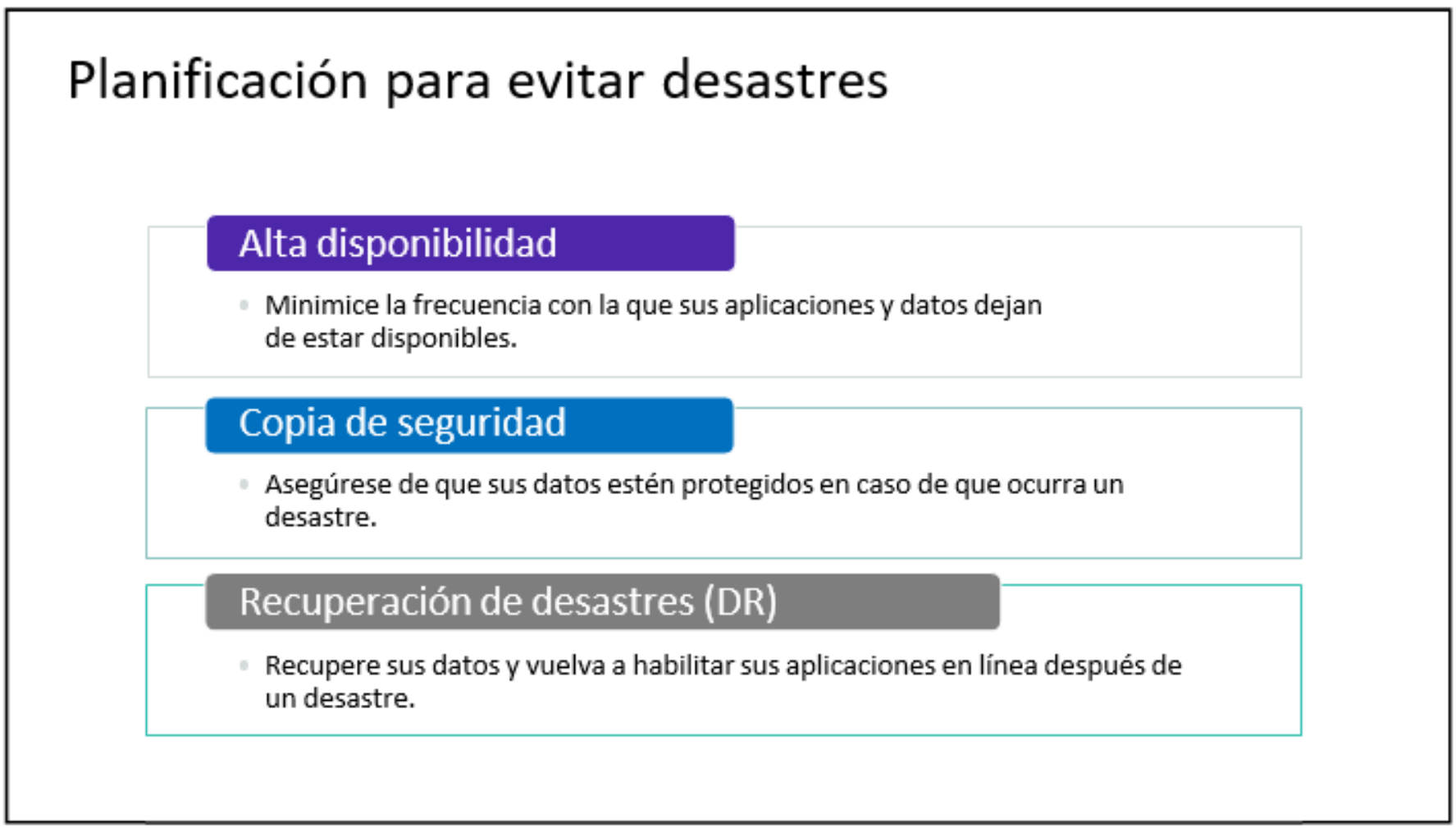
evento colosal:

En este caso, el error es generalizado y afecta a un gran número de usuarios y sistemas

evento a gran escala:

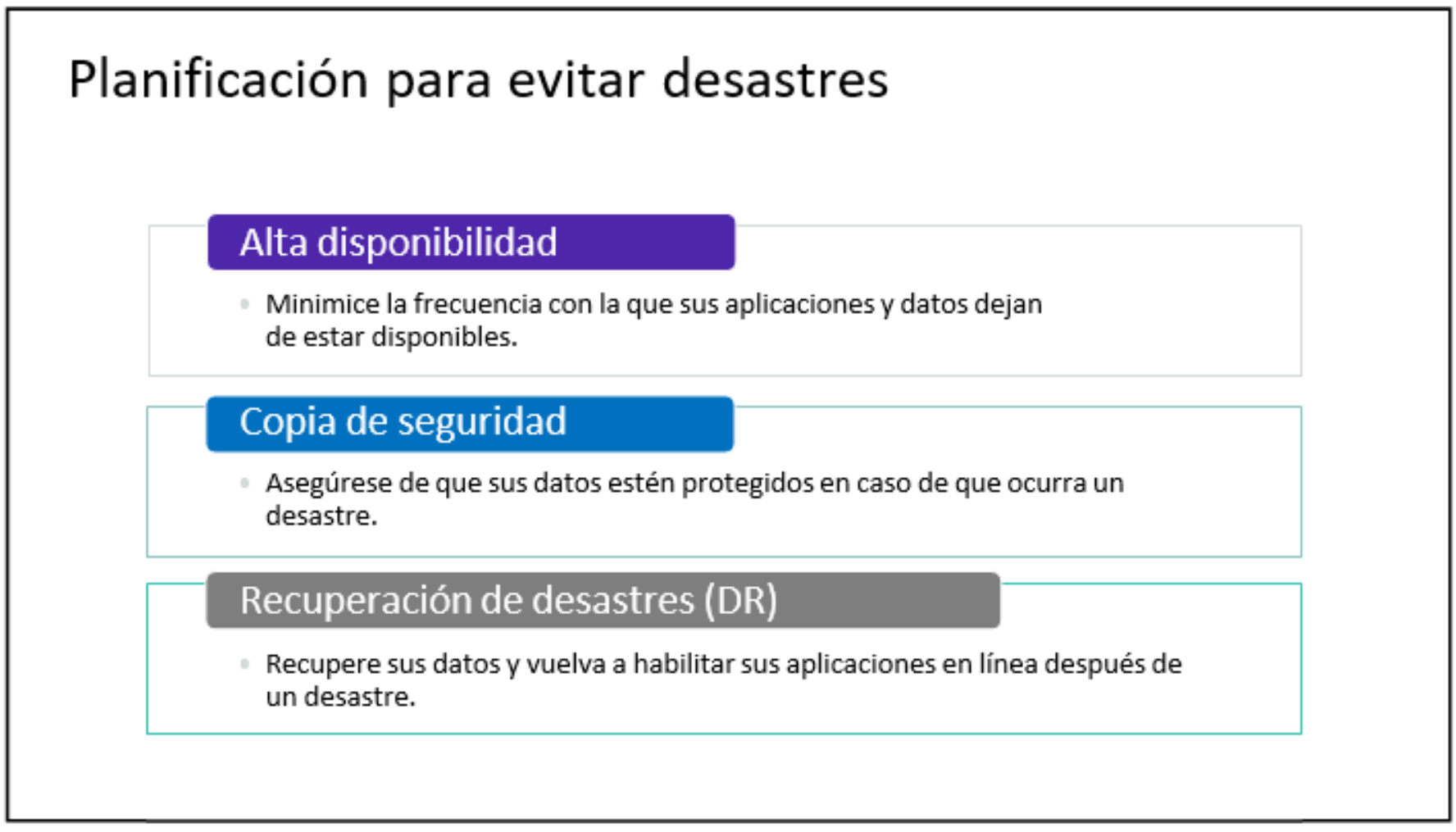
En este caso, varios recursos se vieron afectados, tal vez incluso en distintas zonas de disponibilidad dentro de una región

A fin de minimizar el impacto de un desastre, las organizaciones deben invertir tiempo y recursos en la planificación y la preparación, la capacitación de los empleados y la documentación y la actualización de los procesos. El monto de inversión destinado a la planificación para desastres de un sistema en particular puede variar drásticamente en función del costo de una posible interrupción.



Puede trabajar para evitar un desastre y prepararse para uno de tres maneras:

A fin de minimizar el impacto de un desastre, las organizaciones deben invertir tiempo y recursos en la planificación y la preparación, la capacitación de los empleados y la documentación y la actualización de los procesos. El monto de inversión destinado a la planificación para desastres de un sistema en particular puede variar drásticamente en función del costo de una posible interrupción.



Puede trabajar para evitar un desastre y prepararse para uno de tres maneras:

1

La alta disponibilidad proporciona redundancia y tolerancia a errores. Un sistema está altamente disponible cuando puede soportar la falla de un componente individual o de varios componentes (por ejemplo, discos duros, servidores o conectividad de red). Los sistemas de producción suelen tener requisitos de tiempo de actividad definidos.

La copia de seguridad es fundamental para proteger los datos y garantizar la continuidad del negocio. Sin embargo, puede ser un reto implementarla. El ritmo al que se generan los datos está creciendo de manera exponencial. Mientras tanto, la densidad y la durabilidad de los discos locales no están creciendo al mismo ritmo. Aun así, es fundamental mantener copias de seguridad de los datos críticos, por si ocurre desastre.

2

3

La recuperación de desastres (DR) consiste en prepararse para un desastre y recuperarse de él. Un desastre es cualquier evento que genera un impacto negativo en la continuidad del negocio o en las finanzas de una empresa. Tales eventos incluyen fallas en el hardware o el software, una interrupción de red, un corte de energía eléctrica o daños físicos a un edificio (como incendios o inundaciones). La causa puede ser un error humano o algún otro evento significativo. La recuperación de desastres consiste en un conjunto de políticas y procedimientos que permiten recuperar o mantener la infraestructura y los sistemas tecnológicos vitales después de un desastre.

PRINCIPIOS DE DISEÑO SELECCIONADOS DEL AWS WELL-ARCHITECTED FRAMEWORK

Pilar de excelencia operativa	Pilar de fiabilidad
• Prever errores • Mejorar los procedimientos con frecuencia	• Probar los procedimientos de recuperación • Recuperarse automáticamente de los errores

Considere algunos principios de diseño relacionados con el tema de la recuperación de desastres.

El pilar de excelencia operativa del AWS Well-Architected Framework expresa la importancia de prever los errores. Recomienda realizar ejercicios premortem para identificar los posibles orígenes de los errores, de manera que se puedan eliminar o mitigar. Debe probar los casos de error y validar su comprensión del impacto que estos tienen. AWS Well-
Architected Framework también describe los beneficios de perfeccionar sus procedimientos operativos con frecuencia para poder buscar oportunidades en las que se admitan mejoras. Entonces, a medida que mejora su carga de trabajo, puede perfeccionar sus procedimientos en consecuencia.

El pilar de fiabilidad describe la importancia de diseñar sus sistemas. Debe ser capaz de recuperarse de interrupciones en la infraestructura o el servicio, y mitigar dichas interrupciones, como errores en la configuración o problemas de red temporales.

Uno de los principios de diseño que menciona es probar los procedimientos de recuperación. Pruebe cómo falla el sistema y valide los procedimientos de recuperación. Puede utilizar la automatización para simular diferentes errores o para recrear casos que hayan dado lugar a errores en otras oportunidades. Esta prueba expone las rutas de error que puede probar y corregir antes de que se produzca un caso de error real. Reduce el riesgo de los componentes que no se hayan puesto a prueba antes de que fallen.

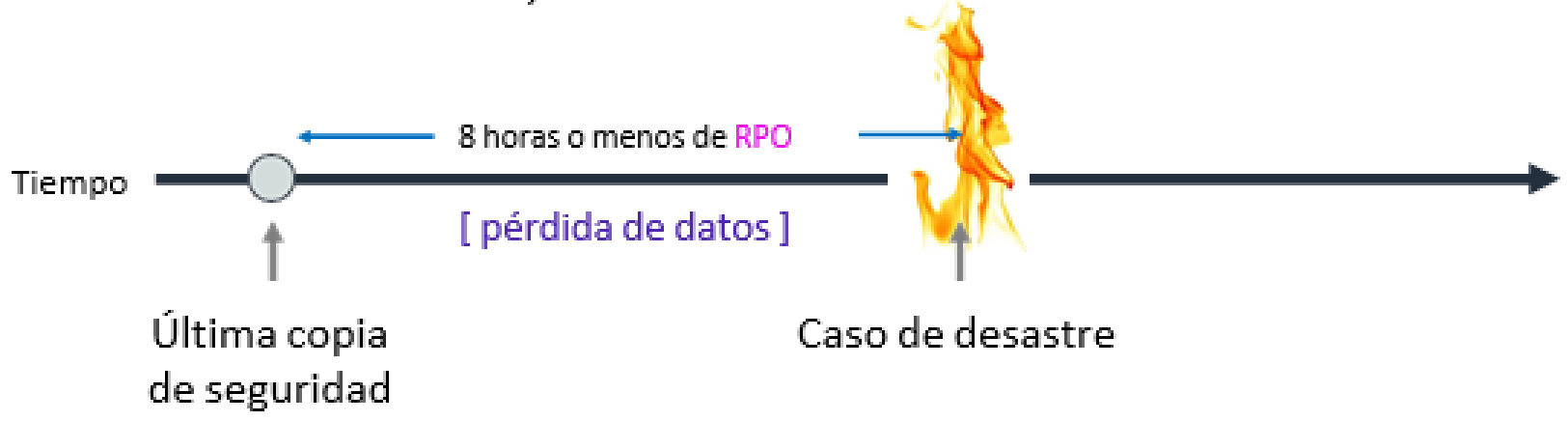
Otro principio de diseño es recuperarse automáticamente del error. Mediante el monitoreo
de un sistema en busca de indicadores clave de rendimiento (KPI), puede activar la automatización cuando se supere un límite. Estos KPI deben considerarse una medida del valor de negocio, no los aspectos técnicos sobre cómo funciona el servicio. La automatización podría proporcionar notificaciones y realizar un seguimiento de los errores y de los procesos de recuperación automatizados que evitan o reparan el error.

OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO)

El objetivo de punto de recuperación (RPO) es la máxima cantidad de pérdida de datos aceptable medida en el tiempo.

¿Con qué frecuencia se debe realizar una copia de seguridad de sus datos?

Ejemplo de RPO: *La empresa puede recuperarse de perder datos correspondientes a, como máximo, las últimas 8 horas.*



Las organizaciones de todos los tamaños, grandes y pequeñas, generalmente cuentan con un Plan de continuidad del negocio (BCP). Una parte típica del BCP es proporcionar continuidad del servicio de TI, incluida la planificación para la recuperación de desastres de TI.

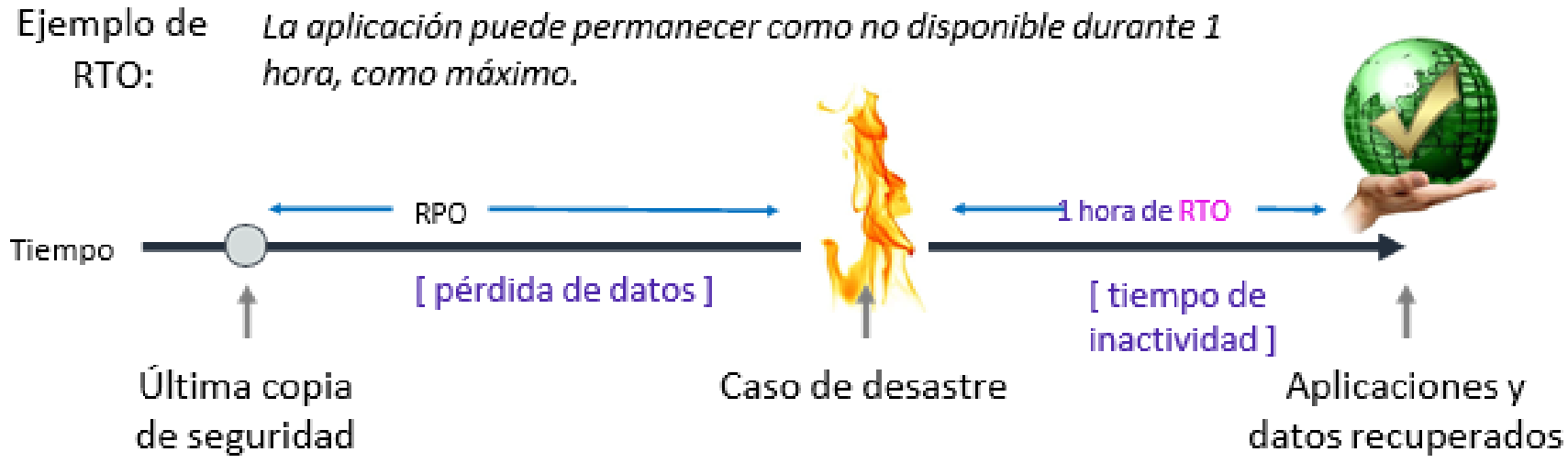
Una de las medidas más importantes de un plan de recuperación de desastres es definir el objetivo de punto de recuperación (RPO). Para calcular el RPO, primero determine qué cantidad de pérdida de datos sería aceptable de acuerdo con su BCP. Luego, descubra la rapidez con la que se produciría esa pérdida de datos, como una medida de tiempo.

Por ejemplo, supongamos que determina que los datos que genera la aplicación son importantes pero no críticos, de modo que la pérdida de 800 registros sería aceptable. Además, calcula que, incluso durante las horas pico, no se crean más de 100 registros en una hora. En este caso, decide que un RPO de 8 horas es suficiente para satisfacer sus necesidades. Si luego implementa un plan de recuperación de desastres que cumple este RPO, está seguro de realizar copias de seguridad de los datos al menos cada 8 horas. Entonces, si se produce un desastre a las 22:00, el sistema debería ser capaz de recuperar todos los datos que estaban en él antes de las 14:00.

OBJETIVO DE TIEMPO DE RECUPERACIÓN (RTO)

El objetivo de tiempo de recuperación (RTO) es la máxima cantidad de tiempo aceptable posterior a un desastre en la que un proceso empresarial puede permanecer fuera de servicio.

¿Con qué rapidez deben recuperarse sus aplicaciones y datos?

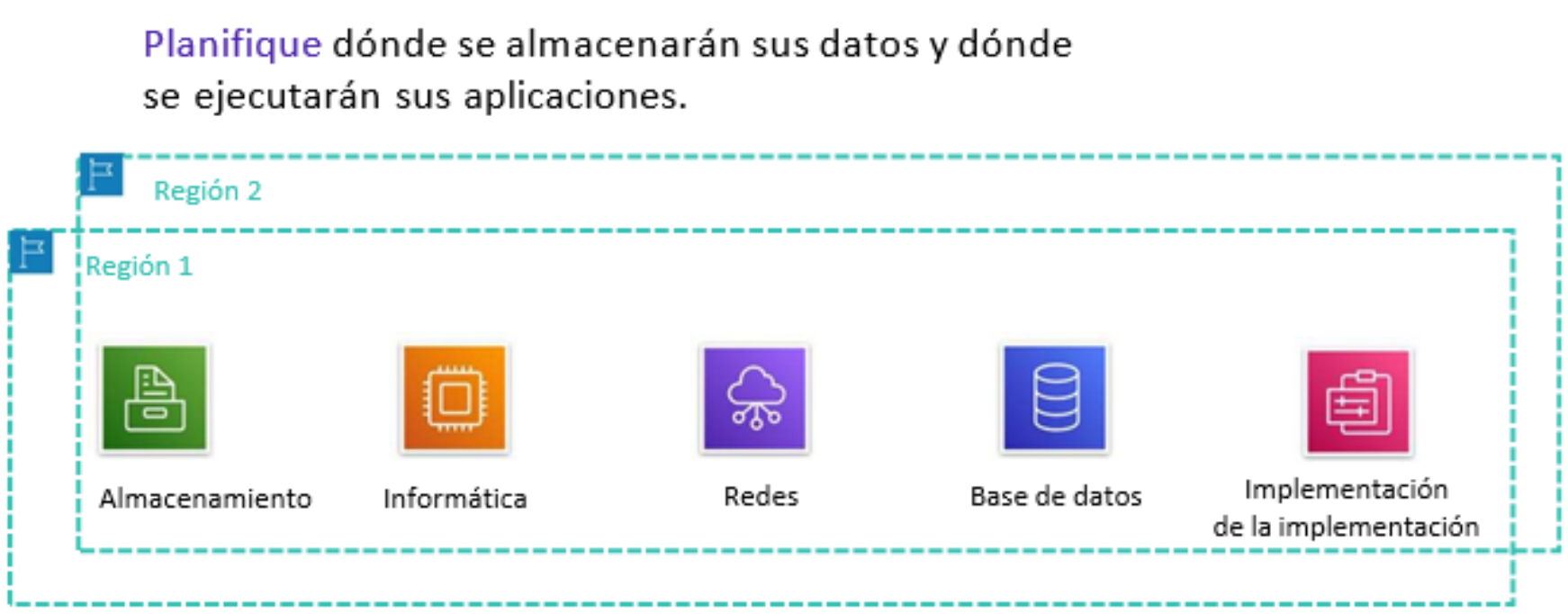


Otra medida importante de un plan de recuperación de desastres es definir el objetivo de tiempo de recuperación (RTO). El RTO es el tiempo que se tarda después de una interrupción en restaurar las aplicaciones y recuperar los datos. Para continuar con el ejemplo anterior, supongamos que se produce un desastre a las 22:00 y el RTO es de 1 hora. En ese caso, el proceso de recuperación de desastres tiene tiempo para restaurar el proceso empresarial al nivel de servicio aceptable hasta las 23:00.

Por lo general, una empresa determina cuáles son sus RPO y RTO aceptables en función del impacto financiero sobre el negocio que se produciría si los sistemas no estuviesen disponibles. La empresa determina el impacto financiero teniendo en cuenta muchos factores. Estos factores incluyen la pérdida de oportunidades de negocio y el daño a su reputación causados por el tiempo de inactividad y la falta de disponibilidad de los sistemas.

Es por eso que las organizaciones de TI planifican soluciones para proporcionar una recuperación del sistema rentable. Las soluciones se basan en el RPO en el marco del periodo y el nivel de servicio que establece el RTO.

PLAN PARA LA RECUPERACIÓN DE DESASTRES



Los planes de recuperación de desastres más sólidos abarcan más de una región.

Si desea determinar correctamente el alcance de la planificación para la recuperación de desastres, debe examinar de forma integral cómo emplea AWS. La mayoría de las organizaciones utilizan una combinación de servicios que se pueden clasificar en términos generales entre estas cinco áreas de categorías de servicios:

Almacenamiento

Informática

Redes

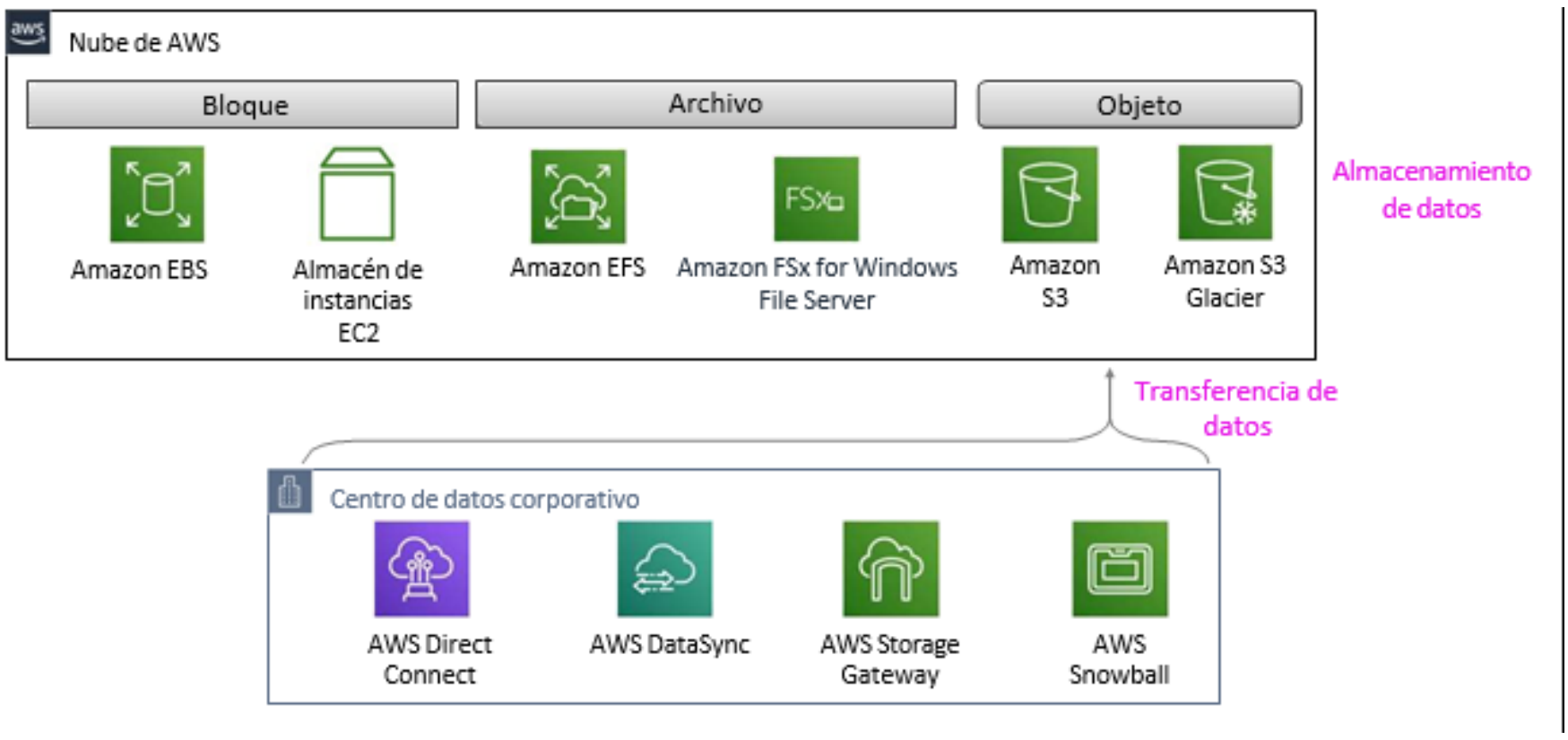
Bases de datos

Servicios de organización de la implementación

Si se produce un desastre, el RPO y el RTO serán la guía para los planes y los procedimientos de copia de seguridad y restauración en cada una de estas áreas de servicio. Posiblemente también afecten la arquitectura de implementación de producción.

Además, es importante tener en cuenta que, aunque es poco probable que una región no esté disponible, sería una posibilidad. Si un evento a gran escala afecta una región, por ejemplo, la caída de un meteorito, ¿seguirían disponibles los datos? ¿Seguiría siendo posible acceder a sus aplicaciones? AWS ofrece varias regiones en todo el mundo. Por eso, puede elegir la ubicación más adecuada para su sitio de recuperación de desastres, además del sitio donde se encuentra implementado todo su sistema.

COMPONENTES BÁSICOS DE ALMACENAMIENTO Y COPIA DE SEGURIDAD



En el diagrama, se hace referencia a los siguientes servicios:

- **Amazon Elastic Block Store (Amazon EBS)**
- **Amazon Elastic Compute Cloud (Amazon EC2)**
- **Amazon Elastic File System (Amazon EFS)**
- **Amazon Simple Storage Service (Amazon S3)**
- **Amazon Simple Storage Service Glacier (Amazon S3 Glacier)**

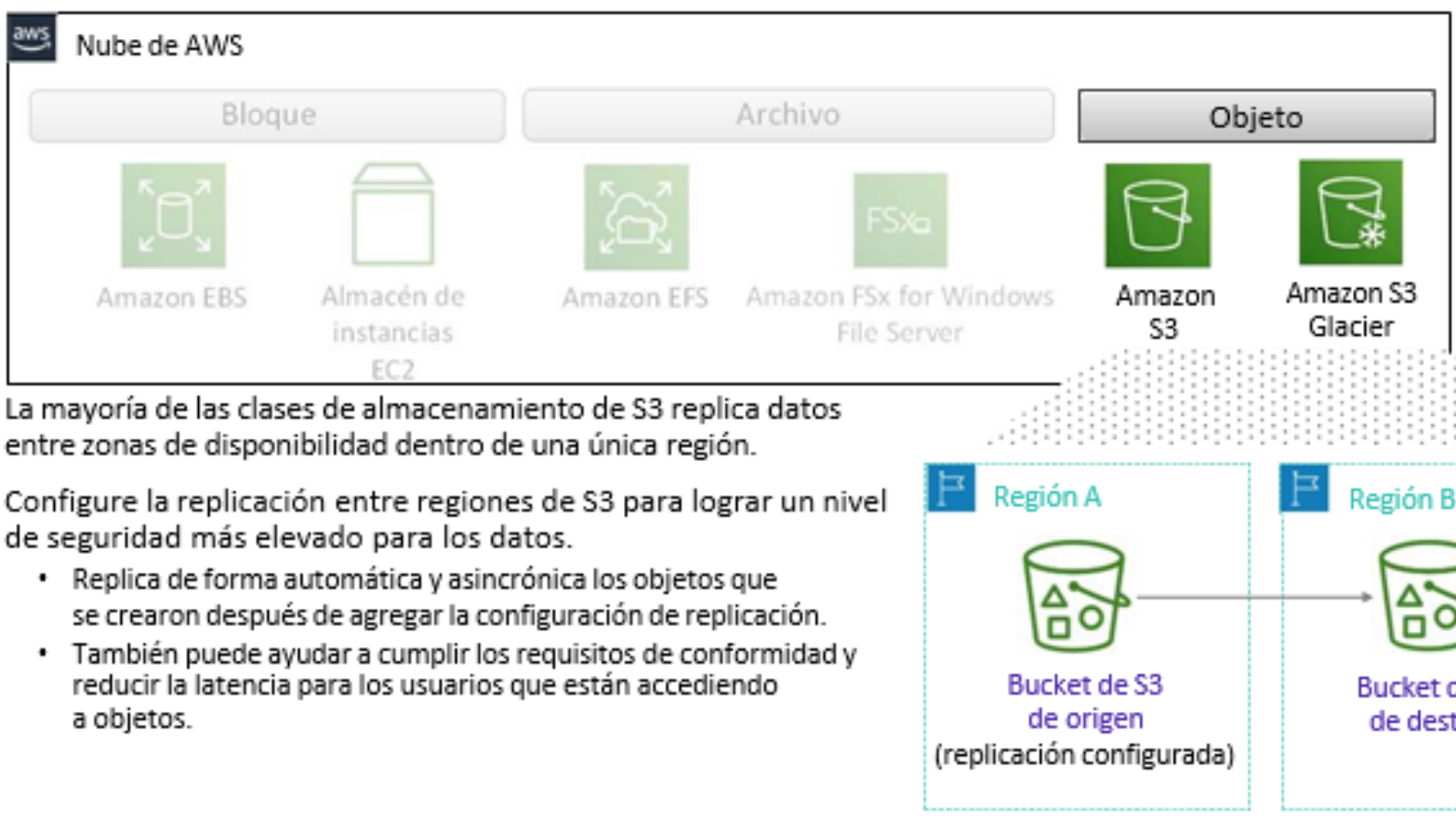
Si desea comenzar a planificar para desastres en detalle, observe la capa de almacenamiento de datos (posponga el análisis de la capa de base de datos por el momento).

El almacenamiento en la nube de AWS puede estar compuesto por una combinación de almacenamiento en bloque, de sistema de archivos y de objetos. Mientras tanto, su organización también podría utilizar servicios de AWS que conecten el centro de datos en las instalaciones a la nube de AWS.

En las siguientes diapositivas, aprenderá acerca de las prácticas recomendadas de alto nivel para cada una de estas tres áreas.

Un servicio que posiblemente no conozca es AWS DataSync. AWS DataSync permite mover grandes cantidades de datos en línea entre el almacenamiento en las instalaciones y Amazon S3, Amazon EFS o Amazon FSx for Windows File Server. Admite trabajos de copia generados por script y transferencias programadas de datos desde sistemas de archivos de red (NFS) en las instalaciones y almacenamiento de bloques de mensajes de servidor (SMB). También puede utilizar, opcionalmente, enlaces de AWS Direct Connect.

PRÁCTICA RECOMENDADA: REPLICACIÓN ENTRE REGIONES DE S3



- La mayoría de las clases de almacenamiento de S3 replica datos entre zonas de disponibilidad dentro de una única región.
- Configure la replicación entre regiones de S3 para lograr un nivel de seguridad más elevado para los datos.
  - Replica de forma automática y asincrónica los objetos que se crearon después de agregar la configuración de replicación.
  - También puede ayudar a cumplir los requisitos de conformidad y reducir la latencia para los usuarios que están accediendo a objetos.

Muchas organizaciones cuyos datos están almacenados en AWS conservan la mayor parte de ellos en Amazon S3, que proporciona almacenamiento de objetos.

Recuerde que los buckets de S3 existen en una región de AWS específica. Elige la región al crear el bucket. Amazon S3 ofrece 11 nueves (99,999999999 %) de durabilidad para las clases de almacenamiento S3 Estándar, S3 Estándar - Acceso poco frecuente, S3 Única zona - Acceso poco frecuente y Amazon S3 Glacier. Amazon S3 Estándar, S3 Estándar - Acceso poco frecuente y Amazon S3 Glacier están diseñadas para mantener los datos en el caso de que se produzca la pérdida total de una zona de disponibilidad de Amazon S3. Proporcionan esta estabilidad al almacenar automáticamente los objetos en al menos tres zonas de disponibilidad, separadas entre sí por millas, pero en una única región de AWS.

Para casos críticos de aplicaciones y datos en los que desee un nivel más alto de seguridad para los datos, una práctica recomendada es configurar la replicación entre regiones de S3. Si desea habilitar la replicación, debe agregar una configuración de replicación a su bucket de origen. La configuración mínima debe indicar el bucket de destino en el que desea que Amazon S3 replique todos los objetos o un subconjunto de todos los objetos. También debe incluir un rol de AWS Identity and Access Management (IAM) que otorgue permisos a Amazon S3 para copiar los objetos en el bucket de destino.

Los objetos copiados conservan sus metadatos. El bucket de destino puede pertenecer a otra clase de almacenamiento. Por ejemplo, el contenido de un bucket de S3 Estándar puede replicarse en un bucket de Amazon S3 Glacier. Puede asignar una propiedad diferente a los objetos en el bucket de destino. También puede utilizar el Control del tiempo de replicación de S3 (S3 RTC) para replicar los datos en diferentes regiones en un plazo predecible. S3 RTC replica 4 nueves (99,99 %) de los objetos nuevos almacenados en Amazon S3 en un plazo de 15 minutos (con el respaldo de un acuerdo de nivel de servicio).

PRÁCTICA RECOMENDADA: INSTANTÁNEAS DEL VOLUMEN DE EBS

En cuanto al almacenamiento en bloque, puede realizar copias de seguridad en Amazon S3 de los datos que estén en volúmenes de EBS al generar instantáneas en un momento específico. Las instantáneas son copias de seguridad graduales, lo que significa que solo se guardan los bloques del dispositivo que se hayan modificado desde la creación de la última instantánea. Esta arquitectura minimiza el tiempo que se necesita para crear la instantánea y ahorra costos de almacenamiento al no duplicar datos.

Cada instantánea contiene toda la información necesaria para restaurar los datos (desde el momento en que se tomó) en un volumen de EBS nuevo. Cuando se crea un volumen de EBS a partir de una instantánea, el volumen nuevo comienza como una réplica exacta del volumen original. Ese volumen original se utilizó para crear la instantánea. El volumen replicado carga los datos en segundo plano para que pueda comenzar a utilizarlo de inmediato. Si accede a datos que aún no se han cargado, el volumen inmediatamente descarga los datos solicitados de Amazon S3. Luego, sigue cargando el resto de los datos del volumen en segundo plano.

Los volúmenes de Amazon EBS proporcionan almacenamiento fuera de la instancia que persiste independientemente de cuánto dure la instancia y que se replica en varios servidores de una zona de disponibilidad. Los volúmenes evitan que se pierdan datos por errores en un componente individual. Después de crear una instantánea, finaliza la copia en Amazon S3 (cuando el estado de la instantánea ya está completo). A continuación, puede copiarla de una región de AWS a otra, o dentro de la misma región.

Puede usar Amazon Data Lifecycle Manager para automatizar la creación, la retención y la
eliminación de instantáneas que funcionan como copias de seguridad de los volúmenes de EBS. La administración automatizada de instantáneas lo ayuda a realizar lo siguiente:

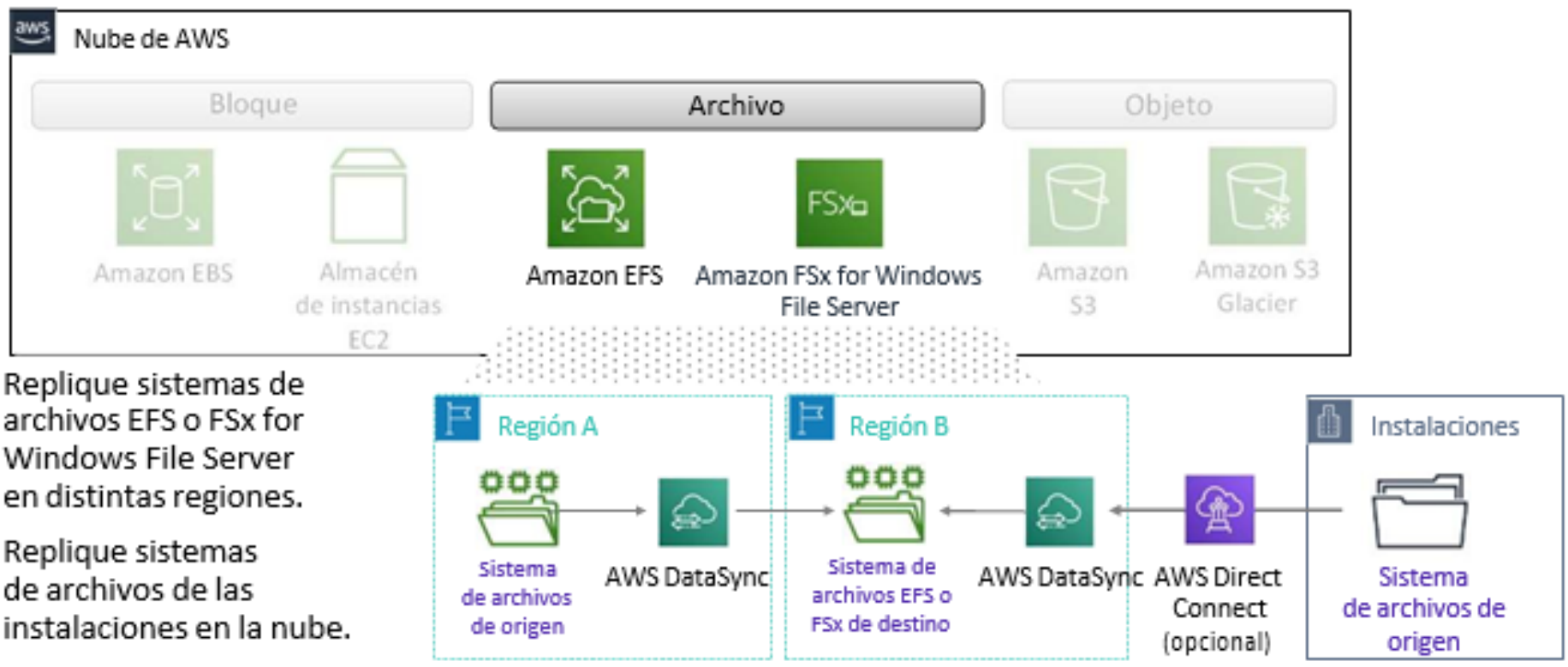
Proteger datos importantes aplicando una programación periódica de copias de seguridad

Conservar las copias de seguridad de acuerdo con los requisitos de los auditores o las políticas internas de conformidad

Reducir los costos de almacenamiento al eliminar las copias de seguridad obsoletas

No puede crear instantáneas de volúmenes de almacén de instancias EC2. Sin embargo, si debe realizar una copia de seguridad de los datos de un almacén de instancias, puede crear un nuevo volumen de EBS y darle formato. Así, monta el volumen nuevo en el sistema operativo invitado de la instancia EC2 y copia los datos del volumen de almacén de instancias en el volumen de EBS. Recuerde que los volúmenes de almacén de instancias proporcionan almacenamiento temporal a nivel de bloque que funciona bien para la información que cambia con frecuencia, como búferes, cachés y datos de pruebas. Es posible que deba realizar una copia de seguridad de los datos de un almacén de instancias. Si es así, tal vez deba reconsiderar por qué está almacenando esos datos en un volumen de almacén de instancias en primer lugar.

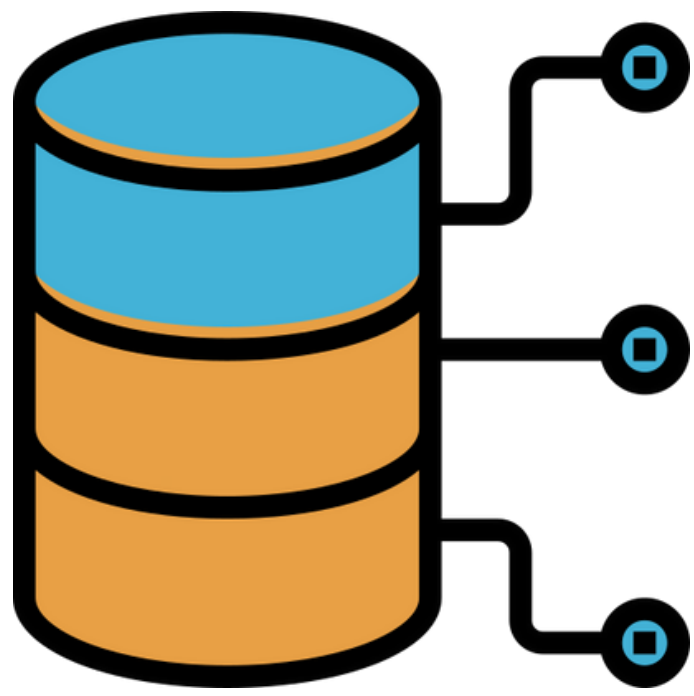
PRÁCTICA RECOMENDADA: REPLICACIÓN DEL SISTEMA DE ARCHIVOS



También se considera una práctica recomendada replicar el almacenamiento de archivos.

AWS DataSync hace que los datos se trasfieran más rápido entre dos sistemas de archivos EFS o Amazon FSx for Windows File Server, o entre almacenamiento en las instalaciones y almacenamiento de archivos de AWS. Puede utilizar DataSync para transferir conjuntos de datos a través de DX o Internet. Utilice el servicio para las migraciones de datos de una sola vez o para flujos de trabajo continuos con fines de protección y recuperación de los datos.

Puede obtener más información sobre cómo utilizar AWS Backup para administrar copias de seguridad de volúmenes de EBS y para automatizar las copias de los sistemas de archivos EFS.

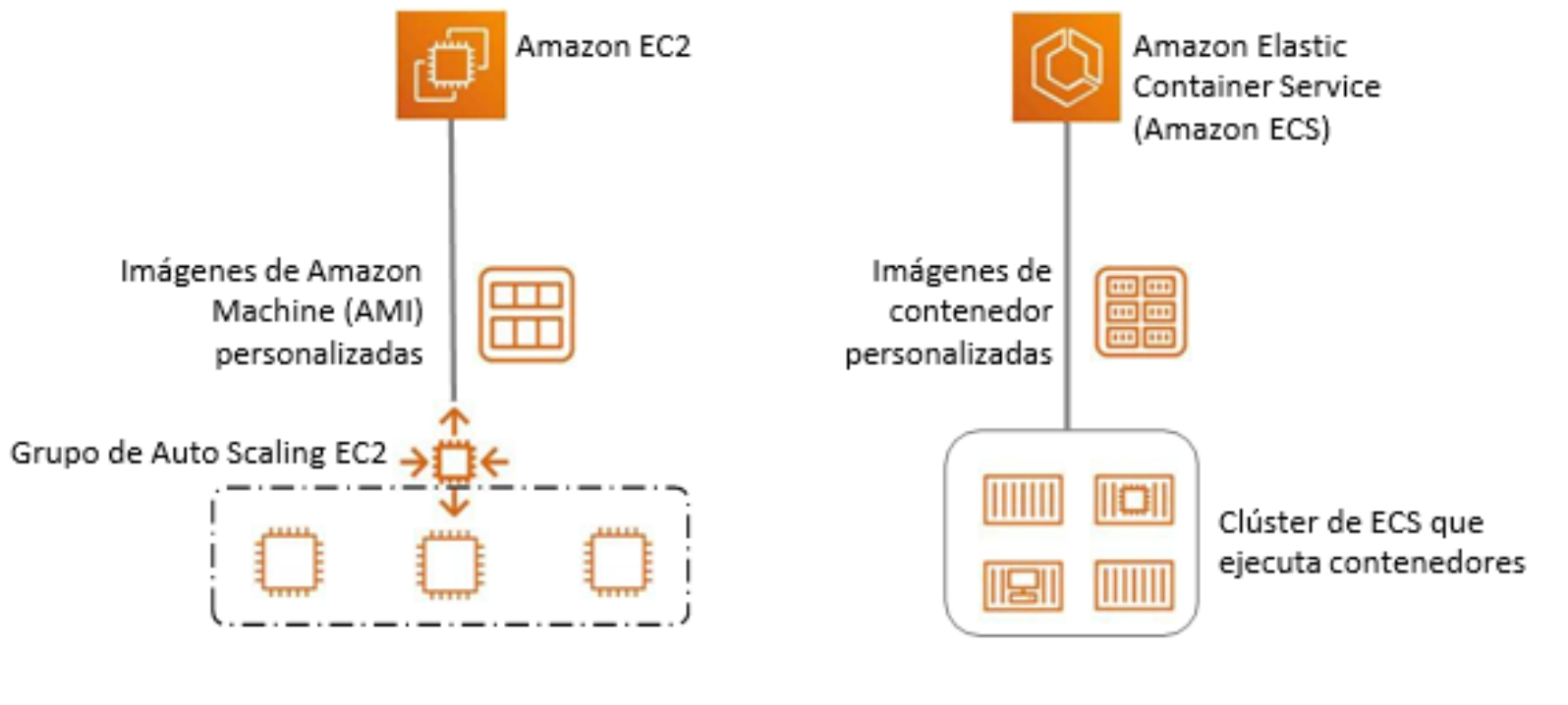


FSx for Windows File Server genera copias de seguridad automáticas de los sistemas de archivos a diario y le permite realizar más copias en cualquier momento. Amazon FSx almacena las copias de seguridad en Amazon S3. El intervalo de copia de seguridad diario es de 30 minutos y se especifica al crear el sistema de archivos. El periodo de retención de copia de seguridad diaria que se especifica para el sistema de archivos determina la cantidad de días que se conservan las copias de seguridad automáticas diarias. (Este número es 7 días de forma predeterminada).

Al igual que la mayoría de las clases de almacenamiento de Amazon S3, los sistemas de archivos de Amazon EFS y FSx for Windows File Server también replican datos entre zonas de disponibilidad. Sus requisitos de recuperación de desastres tal vez especifiquen que necesita una solución de recuperación de varias regiones. En ese caso, una práctica recomendada implica replicar los sistemas de archivos de Amazon EFS y FSx for Windows File Server en una segunda región. Puede utilizar AWS DataSync para obtener esta replicación. Para simplificar la transferencia de archivos entre dos sistemas de archivos EFS mediante DataSync, puede utilizar el inicio rápido y el programador en la nube de AWS DataSync.

LA CAPACIDAD DE CÓMPUTO DEBERÍA RECUPERARSE RÁPIDAMENTE

Obtenga y active nuevas instancias de servidor o contenedores en cuestión de minutos.



En el contexto de la recuperación de desastres, es fundamental poder crear máquinas virtuales que usted controle con rapidez. Al lanzar instancias en zonas de disponibilidad distintas, puede proteger sus aplicaciones de los errores que se produzcan en una sola ubicación.

Puede organizar la recuperación automática de una instancia EC2 cuando se detecta un error en la comprobación de estado del sistema correspondiente al hardware subyacente. La instancia se reinicia (en hardware nuevo, si es necesario), pero conserva su ID de instancia, direcciones IP, asociaciones de volumen de EBS y otros detalles de configuración. Si desea lograr una recuperación completa, asegúrese de que la instancia esté configurada para iniciar automáticamente cualquier servicio o aplicación como parte de su proceso de inicialización.

Las imágenes de Amazon Machine (AMI) están configuradas con antelación con sistemas operativos, y algunas AMI ya configuradas también pueden incluir pilas de aplicaciones. También puede configurar sus propias AMI personalizadas. En el contexto de la recuperación de desastres, AWS recomienda que configure e identifique sus propias AMI para que puedan lanzarse como parte del procedimiento de recuperación. Dichas AMI deben configurarse con antelación con el sistema operativo de su elección, además de las partes correspondientes de la pila de aplicaciones.

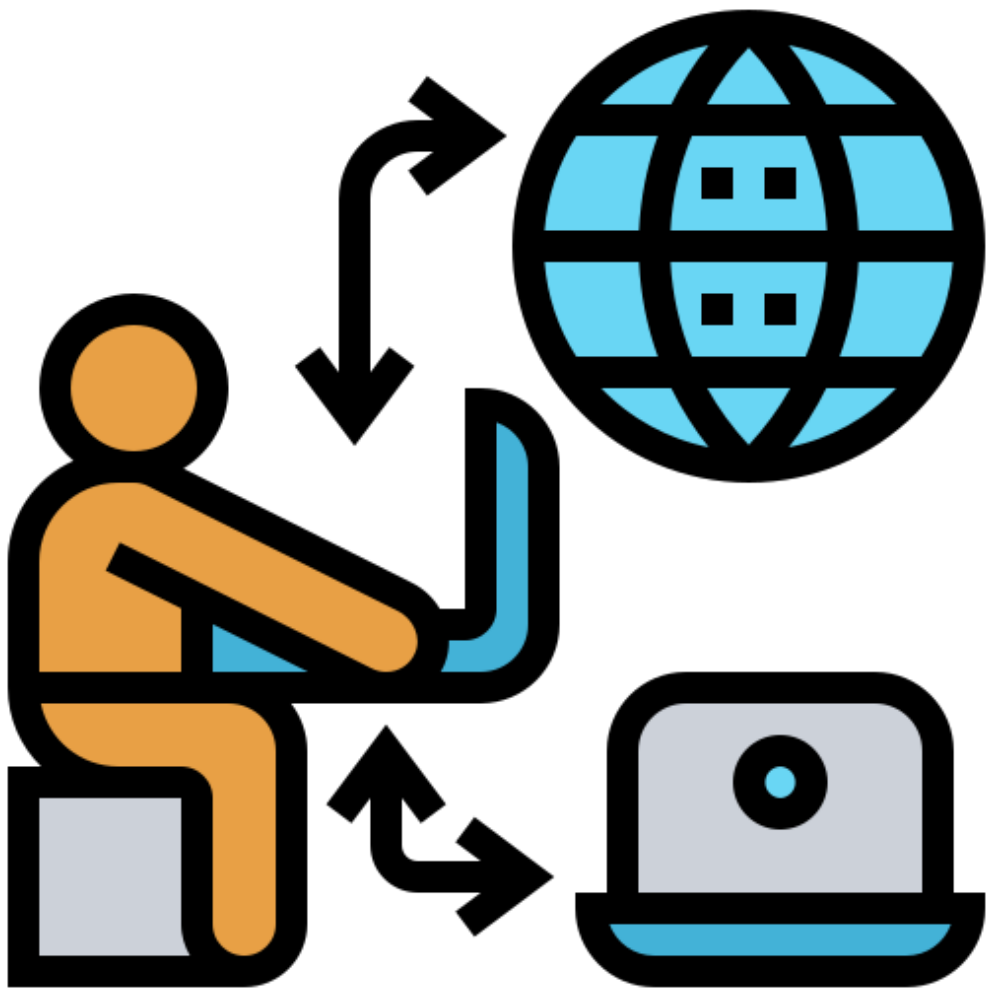
ESTRATEGIAS PARA LA RECUPERACIÓN DE DESASTRES INFORMÁTICOS

- Utilice la capacidad de crear instantáneas de Amazon EC2 para realizar copias de seguridad.
  - Las instantáneas se pueden generar manualmente o se pueden programar (por ejemplo, mediante AWS Lambda).
- Utilice copias de seguridad del sistema o del sistema a nivel de la instancia con poca frecuencia y como último recurso.
  - Eleva el costo del almacenamiento que se utiliza con rapidez.
  - Opte en cambio por la renovación automatizada de la compilación a partir de repositorios de código o configuración.
- Copias de AMI entre regiones
- Copias de instantáneas entre regiones
- Considere arquitecturas informáticas temporales
  - Almacene los datos esenciales fuera de la instancia.

Para la recuperación de desastres de recursos informáticos, probablemente desee utilizar la capacidad de crear instantáneas de Amazon EC2. Las instantáneas se pueden crear de manera manual o se pueden programar.

Si bien puede crear copias de seguridad del sistema o el sistema a nivel de la instancia, el uso exhaustivo de esta estrategia eleva los costos de almacenamiento. Una mejor estrategia consiste en configurar un proceso automatizado de renovación de la compilación, en el que el código fuente se almacena en un repositorio.

Es posible que desee replicar Amazon S3 entre regiones y probablemente también las AMI y las instantáneas más importantes.



Por último, considere la posibilidad de diseñar su propio uso de recursos informáticos de manera que se almacenen los datos esenciales fuera de las instancias. Como puede ver en el ejemplo, sus datos se pueden almacenar en un bucket de S3. Cuando deba realizar el procesamiento de datos, puede lanzar una o más instancias EC2 a partir de una AMI personalizada que ya esté configurada con software de aplicación. En cuanto se inicia la instancia, esta puede extraer los datos necesarios del bucket de S3 y procesarlos. Luego, puede escribir los datos de salida de nuevo en Amazon S3 (tal vez en otro bucket de S3). Una vez que la instancia complete sus tareas de cómputo, se puede terminar. Esta arquitectura, cuando todavía puede satisfacer las necesidades empresariales, facilita el diseño de la estrategia de recuperación de desastres. También puede ahorrar costos, ya que los servidores que no estén en uso constante pueden terminarse y luego volver a crearse cuando sean necesarios.

REDES: DISEÑO EN TORNO A LA RESILIENCIA Y LA RECUPERACIÓN

Amazon Route 53

- Distribución del tráfico
- Conmutación por error

Elastic Load Balancing

- Balanceo de carga
- Comprobaciones de estado y conmutación por error

Amazon Virtual Private Cloud (Amazon VPC)

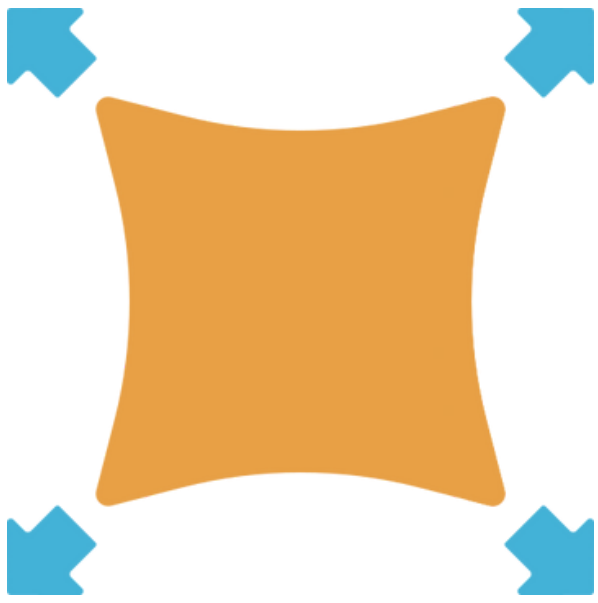
Amplíe la topología de red existente en las instalaciones a la nube.

AWS Direct Connect

Replicación y copia de seguridad uniformes y rápidas de grandes entornos en las instalaciones en la nube

Cuando trabaja para recuperarse de un desastre, es probable que deba modificar la configuración de redes para que el sistema conmute por error a otro sitio. AWS ofrece varios servicios y características que le permiten administrar y modificar la configuración de redes, algunos de los cuales se destacan a continuación.

Amazon Route 53 proporciona capacidades de balanceo de carga y direccionamiento de redes que le permiten distribuir el tráfico de red. También permite conmutar por error entre varios puntos de enlace e incluso a un sitio web estático que esté alojado en Amazon S3.



El servicio Elastic Load Balancing distribuye de manera automática el tráfico entrante de las aplicaciones entre varias instancias EC2. Le permite lograr la tolerancia a errores en sus aplicaciones al proporcionar la capacidad de balanceo de carga necesaria como respuesta al tráfico entrante de las aplicaciones. Puede asignar previamente un balanceador de carga para que su nombre de sistema de nombres de dominio (DNS) ya se conozca, lo que puede simplificar la implementación del plan de recuperación de desastres.

Puede utilizar Amazon Virtual Private Cloud (Amazon VPC) para extender una topología existente de redes en las instalaciones a la nube. Esta extensión puede ser sumamente adecuada cuando recupera aplicaciones empresariales que podrían estar alojadas en una red interna.

Por último, AWS Direct Connect simplifica la configuración de una conexión de red exclusiva
entre un centro de datos en las instalaciones y AWS. El uso de DX puede reducir los costos de redes, aumentar el rendimiento del ancho de banda y proporcionar una experiencia de red más uniforme que las conexiones basadas en Internet.

BASES DE DATOS: CARACTERÍSTICAS QUE ADMITEN LA RECUPERACIÓN

Amazon Relational Database Service (Amazon RDS)

- Tome los datos de la instantánea y guárdelos en una región independiente.
- Combine réplicas de lectura con implementaciones Multi-AZ para crear una estrategia resiliente de recuperación de desastres.
- Conserve las copias de seguridad automatizadas.

Amazon DynamoDB

- Realice copias de seguridad de tablas completas en cuestión de segundos.
- Utilice la recuperación a un momento dado para realizar copias de seguridad de las tablas de forma continua durante un máximo de 35 días.
- Inicie la realización de copias de seguridad con un solo clic en la consola o con una única llamada a la interfaz de programas de aplicaciones (API).
- Utilice tablas globales para crear una base de datos de varias regiones y maestros que proporcione rendimiento local rápido para aplicaciones que escalan de forma masiva y están distribuidas por todo el mundo.

AWS ofrece muchos servicios de base de datos. A continuación, se explican algunas características clave de Amazon RDS y Amazon DynamoDB que son relevantes para los casos de recuperación de desastres.

Considere la posibilidad de utilizar Amazon RDS en la fase de preparación de la recuperación de desastres para almacenar una copia de los datos críticos en una base de datos que ya se esté ejecutando. Luego, utilice Amazon RDS en la fase de recuperación de desastres para ejecutar la base de datos de producción.

Si implementa un plan de recuperación de desastres de varias regiones, Amazon RDS le permite almacenar datos de instantáneas que se registraron de una región en otra región. Puede compartir una instantánea manual con un máximo de 20 cuentas más de AWS.

Combinar réplicas de lectura con la implementación Multi-AZ le permite crear una estrategia de recuperación de desastres resiliente y simplificar el proceso de actualización del motor de base de datos. Mediante el uso de réplicas de lectura de Amazon RDS, puede crear una o más copias de solo lectura de la instancia de base de datos. Puede crear estas copias dentro de la misma región de AWS o en una región de AWS diferente. Las actualizaciones realizadas en la base de datos de origen se copian de forma asíncrona en las réplicas de lectura. Las réplicas de lectura se pueden promover para que se conviertan en una instancia de base de datos independiente, cuando sea necesario.

Utilice Amazon DynamoDB en la fase de preparación para copiar datos en DynamoDB en otra región o en Amazon S3. Durante la fase de recuperación de desastres, puede ampliarse de manera ascendente en cuestión de minutos. Las tablas globales de DynamoDB replican automáticamente las tablas de DynamoDB en las regiones de AWS que elija. Resuelven conflictos de actualización y permiten a las aplicaciones mantener un nivel alto de disponibilidad, incluso en el caso poco probable de que una región completa quede aislada o se vea afectada por degradación.

SERVICIOS DE AUTOMATIZACIÓN: REPLICACIÓN O REIMPLEMENTACIÓN RÁPIDAS DE ENTORNOS

AWS CloudFormation

- Utilice plantillas para implementar rápidamente colecciones de recursos según sea necesario.
- Duplique entornos de producción en una nueva región o VPC en cuestión de minutos.

AWS Elastic Beanstalk

- Vuelva a implementar rápidamente toda la pila con solo unos clics.

AWS OpsWorks

- Sustitución automática del alojamiento
- Combínelo con AWS CloudFormation en la etapa de recuperación.
- Aprovisione una pila nueva que admita el RTO definido.

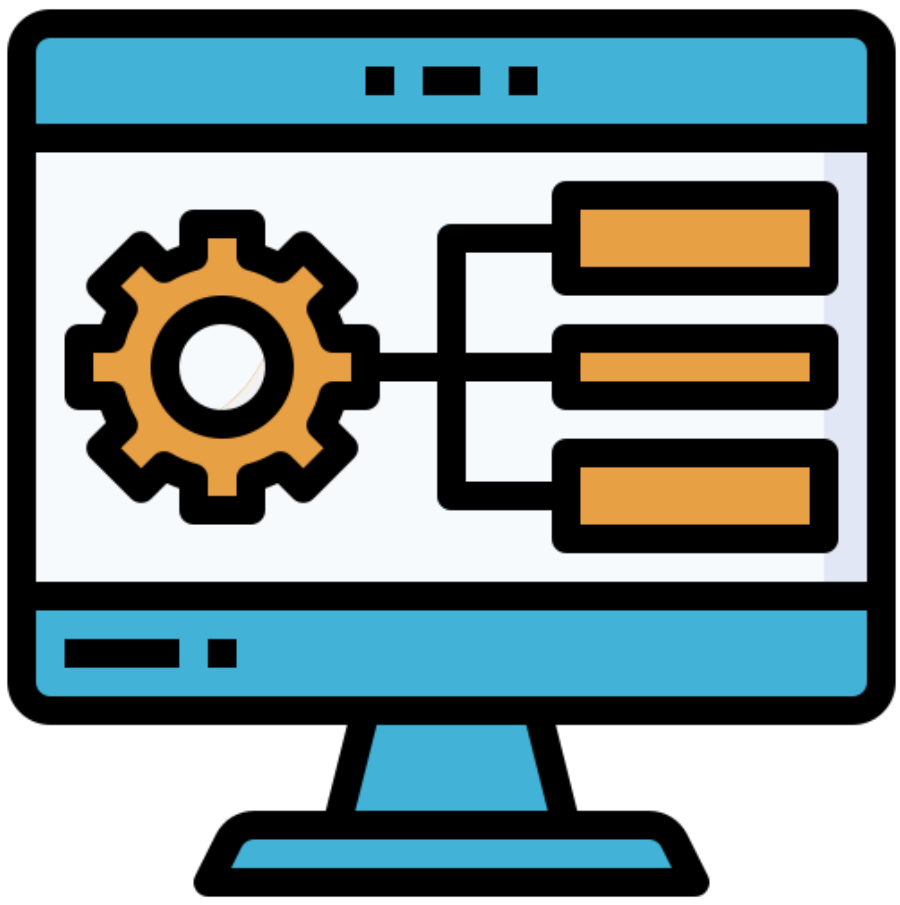
Cuando utiliza servicios de automatización, puede replicar o volver a implementar entornos con rapidez.

AWS CloudFormation le permite modelar e implementar toda la infraestructura en un archivo de texto. Esta plantilla puede convertirse en la única fuente de información para la infraestructura. Cuando utiliza AWS CloudFormation para administrar toda la infraestructura, también se convierte en una poderosa herramienta en el conjunto de herramientas de planificación para la recuperación de desastres. Permite que duplique entornos de producción complejos en cuestión de minutos, por ejemplo, en una nueva región o una nueva VPC.

AWS CloudFormation aprovisiona los recursos de manera repetible, lo que le permite crear una y otra vez su infraestructura y aplicaciones. No es necesario realizar acciones manuales ni escribir scripts personalizados.

Si utiliza AWS Elastic Beanstalk para alojar sus aplicaciones, puede cargar un paquete de origen de aplicaciones actualizadas e implementarlo en su entorno de AWS Elastic Beanstalk. Como alternativa, puede volver a implementar una versión de una aplicación que ya se haya cargado anteriormente. También puede implementar una versión de una aplicación que ya haya sido cargada con anterioridad en cualquiera de sus entornos.

Por último, AWS OpsWorks es un servicio de administración de aplicaciones que facilita la
implementación y la operación de aplicaciones de todo tipo y tamaño. Puede definir su entorno como una serie de capas y configurar cada una como un nivel de la aplicación.
AWS OpsWorks cuenta con sustitución automática del alojamiento, por lo que, si se produce un error en la instancia, se sustituye automáticamente. Puede utilizar AWS OpsWorks en la fase de preparación de la recuperación de desastres para generar una plantilla de su entorno y combinarla con AWS CloudFormation en la etapa de recuperación de desastres.



ESTOS SON ALGUNOS DE LOS APRENDIZAJES CLAVE DE ESTA LECCIÓN:

- **Para elegir la estrategia correcta de recuperación de desastres, primero identifique el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO).**

- **Utilice características, como la replicación entre regiones de S3, las instantáneas de volúmenes de EBS y las instantáneas de RDS, para proteger los datos.**

- **Utilice características de redes, como la conmutación por error de Route 53 y Elastic Load Balancing, para mejorar la disponibilidad de las aplicaciones.**

- **Utilice servicios de automatización, como AWS CloudFormation, como parte de su estrategia de recuperación de desastres para implementar rápidamente entornos duplicados siempre que sea necesario.**