
# El uso de AWS para recuperación ante desastres

***Octubre de 2011***

***Actualizado en enero de 2012***

***Glen Robinson, Ianni Vamvadelis y Attila Narin***



# Contenido

# Resumen

En caso de desastre, puede rápidamente lanzar recursos de Amazon Web Services (AWS) para garantizar la continuidad del negocio. El documento resalta las características y los servicios de AWS relevantes que puede utilizar para los procesos de DR y muestra casos de ejemplo sobre cómo recuperarse de un desastre. Además, proporciona recomendaciones sobre cómo puede mejorar su plan de DR y aprovechar todo el potencial de AWS para los procesos de recuperación ante desastres.

# Introducción

La recuperación ante desastres (DR) consiste en preparar los recursos necesarios para poder recuperar los datos ante un desastre. Cualquier evento que tenga un impacto negativo en la continuidad o la contabilidad del negocio puede considerarse un desastre. Puede tratarse de un error de hardware o software, de una interrupción de la red, de un corte eléctrico, de daños físicos producidos en un edificio como un incendio o una inundación, de un error humano o de otro desastre importante.

Para minimizar el impacto que puede tener un desastre en el negocio, las empresas invierten tiempo y recursos en planear, preparar, ensayar, documentar, formar y actualizar procesos para gestionar los eventos. El volumen de inversiones para la planificación de recuperación ante desastres de un sistema particular puede variar significativamente en función del coste de una interrupción potencial. En el presente documento se describen los enfoques típicos que abarcan desde las inversiones mínimas hasta la disponibilidad de escala total y de tolerancia a fallos.

Es un requisito disponer de una fase de preparación adecuada para casos de DR y, por tanto, en el presente documento se describen algunas de las prácticas recomendadas para mejorar los planes y los procesos de DR.

La recuperación ante desastres consiste en un proceso continuo de análisis y mejora, a medida que evolucionan las empresas y los sistemas. Para cada servicio empresarial, los clientes deben establecer un punto y tiempo de recuperación aceptables y, a continuación, planificar una solución de DR adecuada.

En un entorno físico tradicional, un enfoque típico implicaría normalmente la duplicación de la infraestructura para garantizar la disponibilidad de capacidad productiva en un escenario de desastre. Esta infraestructura ha de adquirirse, instalarse y mantenerse de forma que esté preparada para satisfacer cualquier necesidad de capacidad anticipada. En circunstancias operativas normales, esta infraestructura quedaría infrautilizada o aprovisionada de forma excesiva.

AWS le permite ampliar la infraestructura en función de las necesidades. Puede obtener acceso a la misma infraestructura de alta escalabilidad, fiabilidad, seguridad, rapidez y rentabilidad que Amazon utiliza para ejecutar su propia red global de sitios web y pagar solo por lo que utilice. Para una solución de recuperación ante desastres (DR), esto ofrece ahorros importantes. Esto también ofrece mayor agilidad para cambiar y optimizar los recursos durante un escenario de recuperación ante desastres.

El error humano es la causa de una gran parte de la inactividad del sistema. AWS ofrece herramientas para permitir una distribución de tareas a fin de permitir un diseño basado en *privilegios mínimos*[1]. AWS le permite automatizar la implementación de entornos completos, permitiendo configuraciones predecibles y repetibles. La prueba de los entornos de DR se puede configurar con gran rapidez y, además, puede tratarlos como un recurso desechable. Esto permite que las organizaciones puedan probar los cambios de configuración en un entorno duplicado antes de introducirlos en la fase de producción, sin que sea necesario un entorno de pruebas específico de escala completa, que podría verse infrautilizado con frecuencia.

[1] http://en.wikipedia.org/wiki/Principle_of_least_privilege

# Tiempo objetivo de recuperación y punto objetivo de recuperación

Este documento utiliza dos términos comunes del sector para la planificación ante desastres:

**Tiempo objetivo de recuperación** (RTO)[2]: se corresponde con la duración del tiempo y el nivel de servicio al que se debe restablecer un proceso empresarial después de un desastre (o interrupción) a fin de impedir consecuencias inaceptables asociadas con la interrupción de la continuidad del negocio. Por ejemplo, si un desastre se produce a las 12:00 p.m. (mediodía) y el RTO es de 8 horas, el proceso de recuperación ante desastres garantizaría que la recuperación del nivel de servicio aceptable fuera posible a las 8:00 p. m.

**Punto objetivo de recuperación** (RPO)[3]: describe el volumen aceptable de datos perdidos medido por tiempo. Por ejemplo, si el RPO ha sido de 1 hora después de la recuperación del sistema, contendría todos los datos hasta el punto temporal que no sea anterior a las 11:00 a. m., ya que el desastre ocurrió a mediodía.

Una empresa normalmente decide acerca del RTO y RPO aceptables en función del impacto financiero que tengan para el negocio cuando los sistemas no están disponibles. El impacto financiero se evalúa normalmente al considerar muchos factores, como la pérdida que supone para el negocio y hasta qué punto repercute la situación en su reputación debido al tiempo de inactividad y a la falta de disponibilidad de los sistemas.

Las organizaciones de TI deben programar soluciones para ofrecer de forma rentable una recuperación del sistema basada en el RPO dentro de una línea temporal y el nivel de servicio establecido por el RTO.

# Prácticas tradicionales de inversión en DR

Un enfoque tradicional con respecto a la recuperación ante desastres ofrece diferentes niveles de duplicación exterior de los datos y la infraestructura. Los servicios importantes para la empresa se configuran y mantienen en esta infraestructura y se prueban a intervalos regulares. La infraestructura de origen y la ubicación del entorno de recuperación ante desastres deben tener una distancia física importante a fin de garantizar que dicho entorno quede aislado de errores que podrían repercutir en el sitio de origen.

La infraestructura necesaria para admitir el entorno duplicado incluiría, entre otras cosas:

- Instalaciones para alojar la infraestructura, incluida la alimentación y la refrigeración.
- Seguridad para garantizar la protección física de los recursos.
- Capacidad adecuada para escalar el entorno.
- Soporte para reparar, sustituir y actualizar la infraestructura.
- Acuerdos contractuales con un proveedor de servicios de Internet (ISP) para ofrecer conexión a Internet que pueda soportar la utilización del ancho de banda para el entorno en una situación de carga máxima.
- Infraestructura de red, como firewalls, enrutadores, conmutadores y equilibradores de carga.
- Capacidad del servidor suficiente para ejecutar todos los servicios de vital importancia, incluidos los dispositivos de almacenamiento para respaldar los datos y los servidores para ejecutar aplicaciones y servicios back-end como la autenticación de usuarios, el sistema de nombres de dominio (DNS), el protocolo de configuración dinámica de host (DHCP), la supervisión y las alertas.

En función de la importancia de los servicios, el entorno duplicado puede configurarse de forma tolerante a fallos. Esto suele implicar la duplicación de toda la infraestructura mencionada anteriormente.

[2] Información extraída de http://en.wikipedia.org/wiki/Recovery_time_objective
[3] Información extraída de http://en.wikipedia.org/wiki/Recovery_point_objective

# Servicios y funciones esenciales de AWS para la recuperación ante desastres

Antes de hablar acerca de los diferentes enfoques relacionados con la DR, cabe revisar las funciones y los servicios de AWS más importantes para la recuperación ante desastres. En esta sección se ofrece un resumen.

En la fase de preparación de la DR, es fundamental considerar el uso de servicios y funciones que respalden la migración de datos y el almacenamiento duradero, ya que estos servicios permiten restablecer datos de los que se hayan realizado copias de seguridad en AWS cuando se produce algún desastre. También se requerirán recursos informáticos para algunos escenarios que conlleven una implementación reducida o de escala completa del sistema en AWS.

A la hora de reaccionar frente a un desastre, es fundamental designar rápidamente recursos informáticos para ejecutar el sistema en AWS u organizar la conmutación por error para los recursos que ya se están ejecutando en AWS. Las partes esenciales de la infraestructura en este contexto incluyen DNS, las funciones de red y las distintas funciones de Amazon Elastic Compute Cloud (Amazon EC2) que se describen a continuación.

### Regiones

Los servicios de Amazon Web Services se encuentran disponibles en varias regiones, por lo que puede elegir la ubicación más adecuada para el sitio de recuperación ante desastres, además del entorno en que el sistema se implementa por completo. En el momento de la publicación de esta información, AWS se encuentra disponible en cinco regiones: EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Norte de California), UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio).

### Almacenamiento

Amazon Simple Storage Service (Amazon S3) proporciona una infraestructura de almacenamiento de alta durabilidad diseñada para almacenamiento de vital importancia para su negocio y datos principales. Los objetos se almacenan de forma redundante en varios dispositivos en varias instalaciones dentro de una región. AWS ofrece protección adicional para la retención y el archivado de datos a través del control de versiones en Amazon S3, AWS Multi-Factor Authentication, las políticas sobre depósitos e Identity and Access Management (IAM).

Amazon Elastic Block Store (Amazon EBS) ofrece la capacidad de crear instantáneas puntuales de los volúmenes de datos. Estas instantáneas se pueden utilizar como punto de partida para nuevos volúmenes de Amazon EBS y para proteger los datos que se desean conservar a largo plazo. Después de crear un volumen, este se puede enlazar con una instancia que se ejecute en Amazon EC2. Los volúmenes Amazon EBS ofrecen un almacenamiento fuera de la instancia que persiste con independencia de la vida de una instancia.

AWS Import/Export acelera la transferencia de grandes cantidades de datos hacia y desde AWS, utilizando dispositivos de almacenamiento portátiles para su transporte. AWS extrae de y transfiere sus datos a dispositivos de almacenamiento utilizando la red interna de alta velocidad de Amazon, sin tener que pasar por Internet. En el caso de que se trate de conjuntos de datos de un volumen importante, AWS Import/Export suele resultar más rápido que la transferencia a través de Internet y más rentable que actualizar la conectividad. Puede utilizar AWS Import/Export para migrar datos dentro y fuera de los depósitos de Amazon S3 o en las instantáneas de Amazon EBS.

AWS Storage Gateway permite una perfecta migración de datos bidireccional entre el almacenamiento en nube de AWS y las aplicaciones de la instalación. AWS Storage Gateway almacena datos de volumen de forma local en su infraestructura y en AWS. Gracias a esto, las aplicaciones de la instalación pueden almacenar datos sin ningún problema en la infraestructura de almacenamiento rentable, segura y duradera de AWS sin perder el acceso de baja latencia a estos datos.

## Procesamiento de datos

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática de tamaño variable en la nube. En cuestión de minutos, puede crear instancias de EC2, que son máquinas virtuales sobre las que tiene pleno control. En el contexto de la recuperación ante desastres, es de vital importancia tener esta posibilidad de crear rápidamente equipos virtuales que pueda controlar. La descripción de cada función de Amazon EC2 no es una cuestión que recaiga dentro del ámbito de aplicación del presente documento; por tanto, nos centraremos en los aspectos de Amazon EC2 que resulten más relevantes para la DR.

Las imágenes de máquina de Amazon (AMI) se encuentran configuradas previamente con los sistemas operativos y algunas AMI preconfiguradas también pueden incluir pilas de aplicaciones. También puede configurar sus propias AMI. En el contexto de la DR, recomendamos encarecidamente que tenga configuradas e identificadas su propias AMI para que puedan iniciarse como parte del procedimiento de recuperación. Dichas AMI deben estar preconfiguradas con el sistema operativo que elija, además de los componentes apropiados de la pila de aplicaciones.

Las instancias reservadas de Amazon EC2, que suelen utilizarse para obtener un descuento importante en el coste de ejecución de una instancia de EC2, además ofrecen la ventaja de que resultan especialmente importantes para la DR. Las instancias reservadas ayudan a garantizar que la capacidad que precisa se encuentre disponible cuando la necesite.

Las zonas de disponibilidad son regiones diferentes que están diseñadas para estar aisladas de fallos que se produzcan en otras zonas de disponibilidad, y que proporcionan conectividad de red de baja latencia a otras zonas de disponibilidad de la misma región. Al iniciar instancias en zonas de disponibilidad distintas, puede proteger a sus aplicaciones en caso de que se produzca algún error en una única ubicación. Las regiones se componen de una o varias zonas de disponibilidad.

La función de importación de VM de Amazon EC2 permite importar imágenes de equipos virtuales desde el entorno con el que cuenta el cliente a instancias de Amazon EC2.

## Redes

Al tratar una situación de desastre, es muy probable que tenga que modificar la configuración de red cuando conmute el error a otro entorno.

Amazon Route 53 es un servicio web DNS (Sistema de nombres de dominio) escalable y de alta disponibilidad. Está diseñado para ofrecer a los desarrolladores y a las empresas una forma sumamente fiable y rentable de remitir a los usuarios finales a las aplicaciones en Internet.

Las direcciones IP elásticas son direcciones IP estáticas diseñadas para la informática dinámica en nube. Al contrario que las tradicionales direcciones IP estáticas, las direcciones IP elásticas permiten disimular los errores en instancias o zonas de disponibilidad, al reasignar de forma programada sus direcciones IP públicas a cualquier instancia de su cuenta en una región determinada. En los casos de DR, también puede preasignar algunas direcciones IP para los sistemas más importantes, de forma que se conozcan las direcciones IP antes de que se produzca el desastre. De esta forma, se puede simplificar la ejecución del plan de DR.

Elastic Load Balancing distribuye automáticamente el tráfico entrante de las aplicaciones entre varias instancias de Amazon EC2. Permite conseguir aún más tolerancia a fallos en sus aplicaciones, al proporcionar la capacidad de equilibrio de carga necesaria como respuesta al tráfico entrante de aplicaciones. Del mismo modo que puede preasignar direcciones IP elásticas, también puede preasignar el Elastic Load Balancer para que ya se conozca su nombre DNS, una operación que puede simplificar el plan de DR.

Amazon Virtual Private Cloud (Amazon VPC) permite disfrutar de una sección privada y aislada de la nube de Amazon Web Services donde podrá lanzar recursos de AWS en una red virtual que defina. Usted controla todos los aspectos de su entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de rutas y puertas de enlace de red. Esto le permitirá crear una conexión VPN entre el centro de datos corporativo y la VPC, además de poder utilizar la nube de AWS como una extensión del centro de datos corporativo. En el contexto de DR, puede utilizar Amazon VPC para ampliar la topología existente de la red a la nube; esto puede resultar especialmente útil para recuperar las aplicaciones empresariales típicas de la red interna.

Amazon Direct Connect facilita el establecimiento de una conexión de red dedicada desde sus instalaciones a AWS. En muchos casos, esto puede reducir los costes de red, aumentar el rendimiento del ancho de banda y ofrecer una experiencia de red más coherente que las conexiones basadas en Internet.

### Bases de datos

Para satisfacer las necesidades de su base de datos, considere la posibilidad de utilizar los servicios de AWS:

Con Amazon Relational Database Service (Amazon RDS), es más fácil configurar, gestionar y escalar una base de datos relacional en la nube. Puede utilizar Amazon RDS en la fase de preparación para DR para tener listos los datos importantes en una base de datos en ejecución o en la fase de recuperación para ejecutar su base de datos de producción.

Amazon SimpleDB es un almacén de datos no relacionales de alta disponibilidad y flexible que descarga el trabajo de administración de bases de datos. También se puede utilizar en la fase de preparación y de recuperación de un proceso de DR.

También puede instalar y ejecutar un software de base de datos de su elección en Amazon EC2 y, además, puede elegir entre una serie de sistemas de base de datos principales.

Para obtener información detallada acerca de las opciones de bases de datos de AWS, consulte Ejecución de bases de datos en AWS.

### Organización de la implementación

En Amazon EC2 se pueden utilizar herramientas y procesos de instalación/configuración de software después del inicio y para la automatización de la implementación. Se recomienda encarecidamente invertir en este ámbito. Esto puede resultar realmente útil en la fase de recuperación para crear el conjunto de recursos necesarios de forma automática.

AWS CloudFormation ofrece a desarrolladores y administradores de sistemas un método sencillo de crear una colección de recursos de AWS relacionados entre sí para ofrecerlos de una manera ordenada y predecible. Puede crear plantillas para sus entornos e implementar conjuntos asociados de recursos (conocidos como pilas), según sea necesario.

### Seguridad

Hay muchas funciones relacionadas con la seguridad en los servicios de AWS. Recomendamos a los clientes que consulten el documento técnico Security Best Practices. AWS también ofrece información adicional sobre riesgos y conformidad legal en el Centro de seguridad de AWS. La información completa sobre seguridad no recae dentro el ámbito de este documento.

# Ejemplo de escenarios de recuperación ante desastres con AWS

En esta sección se describen cuatro escenarios de DR en los que se destaca el uso de AWS y se compara AWS con otros métodos tradicionales de DR:

- Copia de seguridad y restablecimiento
- Luz piloto para la recuperación simple en AWS
- Solución de estado de espera semiactiva
- Solución multisitio

Amazon Web Services permite que los clientes puedan desarrollar de forma rentable cada una de estas estrategias de ejemplo de DR. Cabe destacar que se trata solo de ejemplos de posibles enfoques, por lo que pueden existir variaciones y combinaciones de estos.

## Copia de seguridad y restablecimiento

En los entornos más tradicionales, las copias de seguridad de los datos se almacenan en una cinta y se envían fuera del sitio con regularidad. El tiempo de recuperación será el más largo con la utilización de este método. Amazon S3 es un destino ideal para las copias de seguridad de los datos, ya que se trata de una solución diseñada para ofrecer una durabilidad de los objetos del 99,999999999% (11 nueves) durante un año determinado. La transferencia de datos entrantes y salientes de Amazon S3 se realiza normalmente a través de la red y, por tanto, se puede acceder desde cualquier ubicación. Existen muchas soluciones de copia de seguridad comerciales y de código abierto que realizan copias de seguridad en Amazon S3. El servicio AWS Import/Export permite realizar transferencias de conjuntos de datos muy grandes enviando los dispositivos de almacenamiento directamente a AWS.

El servicio AWS Storage Gateway permite copiar de forma transparente instantáneas de los volúmenes de datos de la instalación a Amazon S3 para realizar copias de seguridad. A partir de estas instantáneas se pueden crear volúmenes locales o volúmenes de AWS EBS.

En el caso de los sistemas que se ejecutan en AWS, los clientes también realizan copias de seguridad en Amazon S3. Las instantáneas de los volúmenes de Elastic Block Store (EBS) y las copias de seguridad de Amazon RDS se almacenan en Amazon S3. De forma alternativa, puede copiar los archivos directamente en Amazon S3 o puede optar por crear archivos de copia de seguridad y copiarlos en Amazon S3. Hay muchas soluciones de copia de seguridad que almacenan datos de copia de seguridad en Amazon S3 y estos se pueden utilizar también desde los sistemas de Amazon EC2.

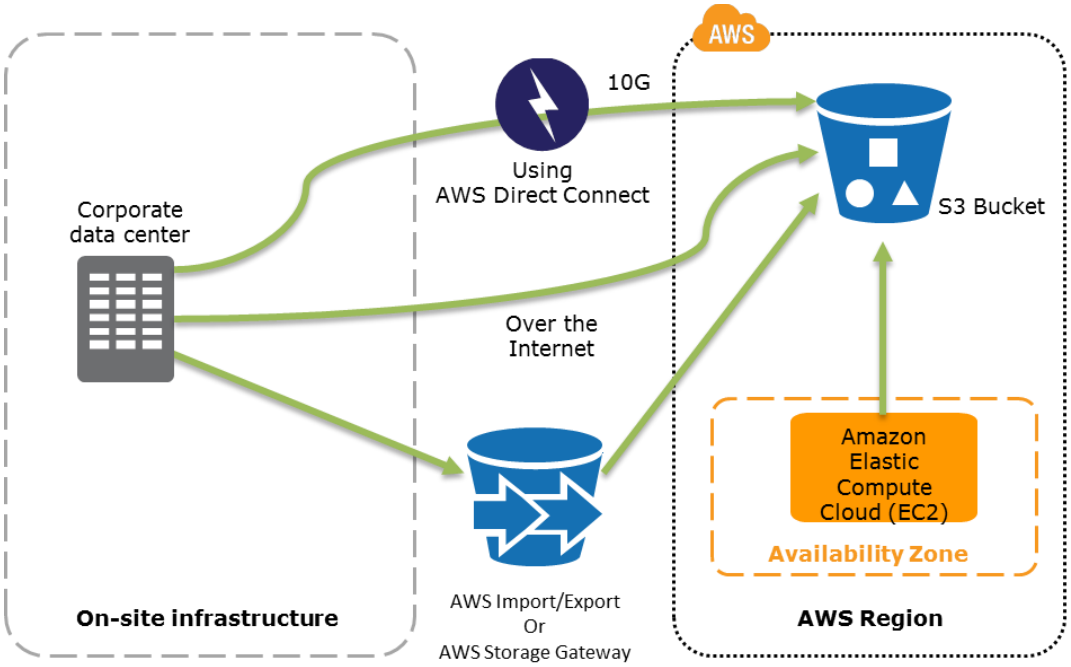


*Ilustración 1: Opciones de copia de seguridad de datos en S3 desde infraestructuras locales o desde AWS.*

La copia de seguridad de los datos constituye solo el 50% del proceso. La recuperación de los datos en un escenario de desastre ha de probarse y conseguirse de forma rápida y fiable. Los clientes deben de asegurarse de que sus sistemas estén configurados para una retención adecuada de los datos y para preservar la seguridad de los mismos, así como de que se hayan probado los procesos de recuperación de datos.

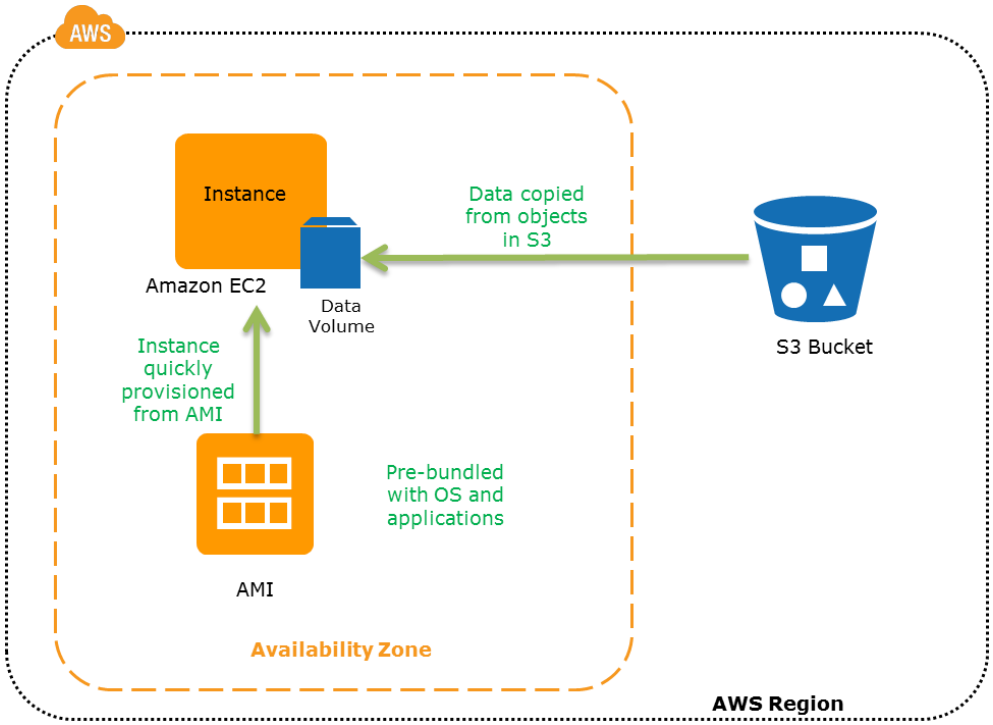


*Ilustración 2: Restablecimiento de un sistema a partir de copias de seguridad de S3 en AWS EC2*

Pasos clave para copias de seguridad y restablecimiento:

- Seleccione una herramienta o un método adecuados para realizar copias de seguridad de los datos en AWS.
- Asegúrese de que dispone de una política adecuada de retención para estos datos.
- Asegúrese de que dispone de las medidas de seguridad adecuadas para estos datos, incluidas políticas de acceso y cifrado.
- Pruebe regularmente la recuperación de estos datos y el restablecimiento del sistema.

## Luz piloto para la recuperación rápida en AWS

La idea de la luz piloto es una analogía que surge del calentador de gas. En un calentador de gas, una llama inactiva pequeña que está siempre encendida puede encender rápidamente la caldera para calentar una casa según sea necesario. Este escenario es similar a un escenario de copia de seguridad y restablecimiento; no obstante, debe asegurarse de que cuenta con los elementos principales más importantes del sistema que ya estén configurados y en ejecución en AWS (la luz piloto). Cuando llega el momento de la recuperación, dispondrá rápidamente de un entorno de producción a escala completa en torno al núcleo principal.

Los elementos de la infraestructura de la luz piloto incluyen normalmente los servidores de la base de datos, que replicarían los datos en Amazon EC2. En función de cuál sea el sistema, cabe la posibilidad de que haya datos importantes fuera de la base de datos que se tengan que replicar en AWS. Se trata del núcleo principal del sistema (la luz piloto) en torno al cual todos los demás elementos de la infraestructura de AWS pueden aprovisionarse rápidamente (el resto del equipo) para restablecer el sistema completo.

Para aprovisionar al resto de la infraestructura para restablecer los servicios de vital importancia para el negocio, normalmente debería contar con servidores preconfigurados y agrupados como imágenes de máquina de Amazon (AMI), que estén listas para iniciarse en el momento de la notificación. Cuando empieza la recuperación, las instancias de estas AMI se inician rápidamente y encuentran su función en la implementación en torno a la luz piloto. Desde el punto de vista de la red, puede utilizar las direcciones IP elásticas (que pueden preasignarse en la fase de preparación de DR) y asociarlas con sus instancias, o utilizar la función de Elastic Load Balancing para distribuir el tráfico entre varias instancias. Posteriormente, puede actualizar los registros DNS para identificar la instancia de Amazon EC2 o apuntar hacia el Elastic Load Balancing usando un CNAME.

Para sistemas menos importantes, puede asegurarse de que dispone de los paquetes de instalación y de la información de configuración en AWS, por ejemplo, en forma de una instantánea de EBS. De esta forma, se agilizará la configuración del servidor de la aplicación, ya que puede crear rápidamente varios volúmenes en varias zonas de disponibilidad para enlazarlos con instancias de EC2. A continuación, puede instalarlos y configurarlos según proceda.

El método de la luz piloto le ofrecerá un tiempo de recuperación más corto que el escenario anterior de "copia de seguridad y restablecimiento", ya que los elementos principales del sistema ya se están ejecutando y se mantienen continuamente actualizados. Aún hay algunas tareas de instalación y configuración que se han de desarrollar para poder recuperar las aplicaciones por completo. AWS le permite automatizar el aprovisionamiento y la configuración de los recursos de la infraestructura, que pueden resultar realmente beneficiosos para ahorrar tiempo y ayudar a protegerse frente a errores humanos.

**Fase de preparación:**

En la siguiente ilustración se muestra la fase de preparación, en la que necesita disponer de datos modificados regularmente que se hayan replicado con el método de la luz piloto, el núcleo pequeño en torno al cual se iniciará el entorno completo en la fase de recuperación. Los datos actualizados con menor frecuencia, como los sistemas operativos y las aplicaciones, se pueden actualizar periódicamente y almacenarse como imágenes de máquina de Amazon (AMI).

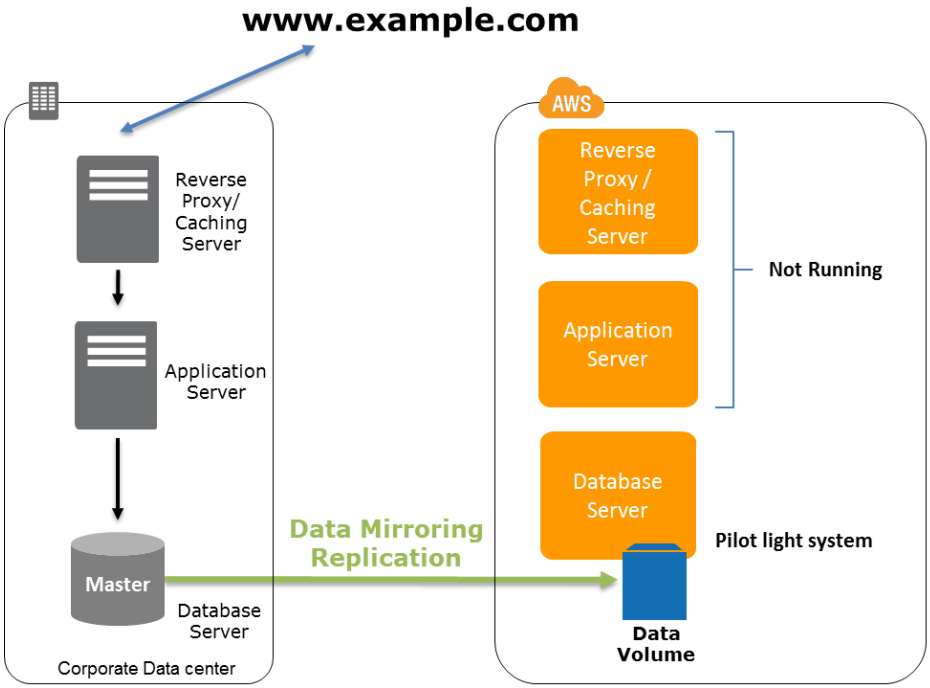


*Ilustración 3: La fase de preparación del escenario de la luz piloto*

Puntos clave de la fase de preparación:

- Configure las instancias de EC2 para replicar o realizar una copia en espejo de los datos.
- Asegúrese de tener disponible en AWS todos los paquetes de soporte de software personalizados.
- Cree y mantenga las imágenes de máquina de Amazon (AMI) de los servidores clave en los que se precisa de una recuperación rápida.
- Ejecute estos servidores con regularidad y aplique cualquier actualización y cambios de configuración del software.
- Considere automatizar el aprovisionamiento de los recursos de AWS.

**Fase de recuperación:**

Para recuperar el resto del entorno relativo a la luz piloto, debería iniciar los sistemas a partir de las imágenes de máquina de Amazon (AMI) en cuestión de minutos sobre los tipos de instancia adecuados. Para los servidores de datos dinámicos, puede adaptar el tamaño para gestionar los volúmenes de producción según sea necesario o añadir capacidad según proceda. El escalado horizontal, si es posible, suele ser la forma más rentable y el enfoque más escalable para añadir capacidad a un sistema; no obstante, también es posible elegir tipos de instancias de EC2 más grandes y así aplicar un escalado vertical. Desde la perspectiva de la red, las actualizaciones necesarias de DNS se pueden realizar de forma paralela.

Después de que se haya completado la recuperación, debe asegurarse de que se restablezca la redundancia lo más rápidamente posible. Aunque es poco probable que su entorno de DR falle poco después de que falle el entorno de producción, ha de ser consciente de este riesgo. Siga realizando copias de seguridad regulares del sistema y considere la opción de añadir redundancia en la capa de datos.

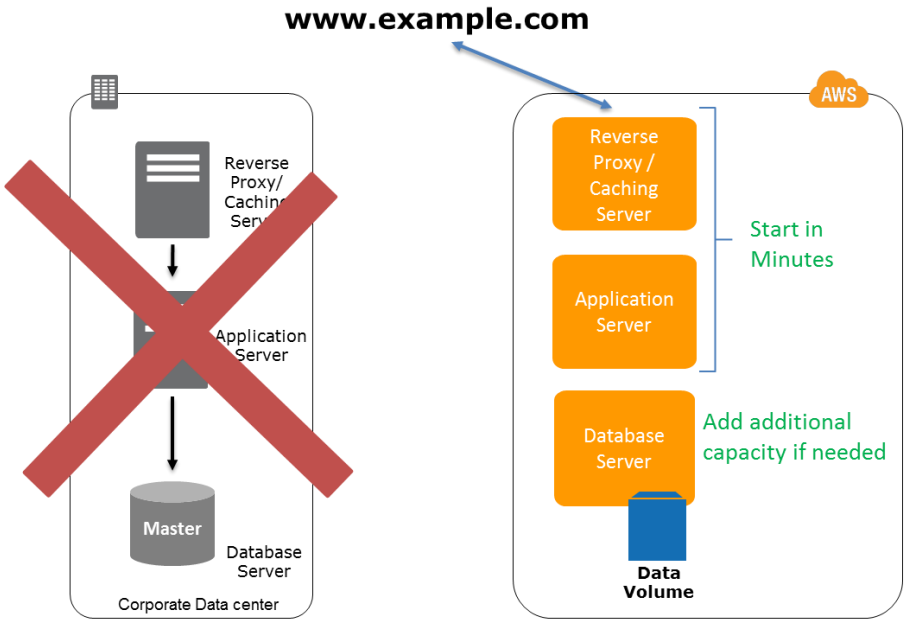


*Ilustración 4: La fase de recuperación del escenario de la luz piloto.*

Puntos clave de la fase de recuperación:

- Inicie las instancias de EC2 de la aplicación a partir de las AMI personalizadas.
- Adapte el tamaño o escale las bases de datos o las instancias de almacén de datos, según proceda.
- Cambie el DNS para mostrar los servidores de EC2.
- Instale y configure cualquier sistema que no esté basado en las AMI, a ser posible, de manera automática.

## Solución de estado de espera semiactiva en AWS

Una solución de estado de espera semiactiva amplía los elementos de la luz piloto y la fase de preparación. Reduce aún más el tiempo de recuperación porque, en este caso, algunos servicios están siempre en ejecución. Mediante la identificación de sistemas de vital importancia para el negocio, podría duplicar totalmente estos sistemas en AWS de forma que estos siempre estén activos.

Estos servidores se pueden ejecutar en un tamaño mínimo de instancias de EC2 con los tamaños más reducidos posibles. Esta solución no se escala para soportar una carga de producción total, pero es totalmente funcional. Se puede utilizar para tareas no productivas, como las pruebas, los controles de calidad, el uso interno, etc.

En un desastre, se amplía el sistema rápidamente para gestionar la carga de producción. En AWS, esto se puede realizar añadiendo más instancias al equilibrador de carga y ajustando el tamaño de los servidores de poca capacidad para ejecutar tipos de instancias más grandes de EC2. Como se ha mencionado anteriormente, si es posible, se prefiere el escalado horizontal con respecto al vertical.

**Fase de preparación:**

En el siguiente diagrama se muestra la fase de preparación para una solución de espera semiactiva, en la que se ejecuta una solución local y de AWS de forma paralela.

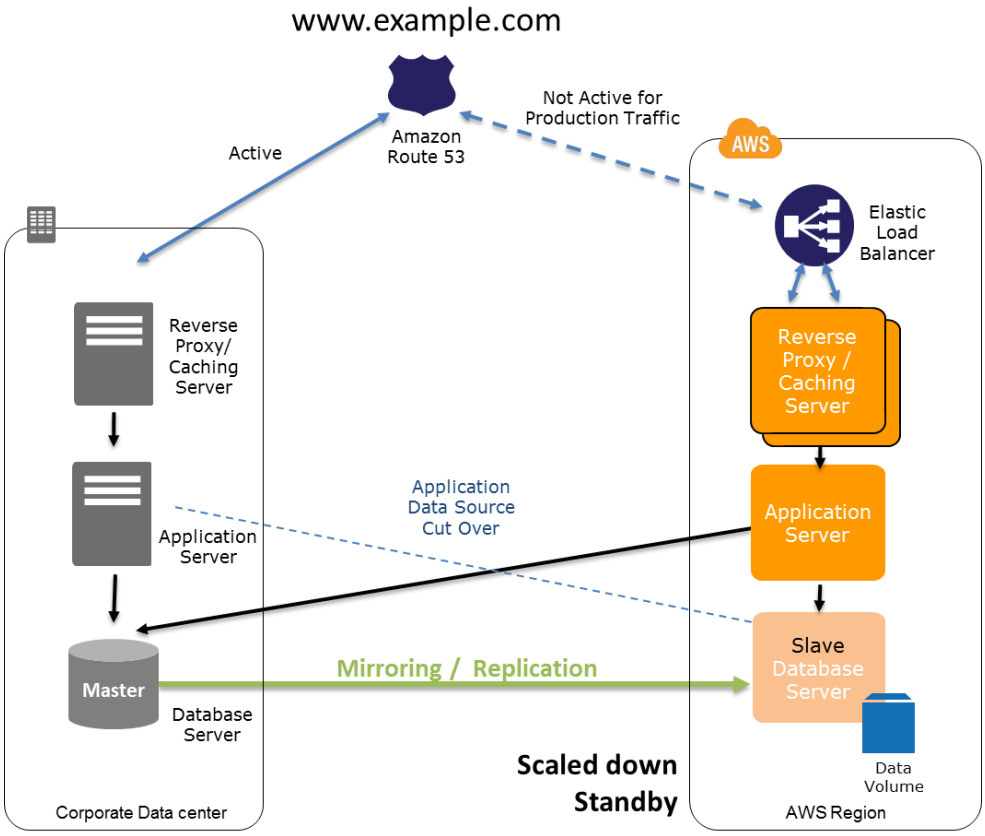


*Ilustración 5: La fase de preparación del escenario de "espera semiactiva".*

Puntos clave de la fase de preparación:

- Configure las instancias de EC2 para replicar o realizar una copia en espejo de los datos.
- Cree y mantenga las imágenes de máquina de Amazon (AMI).
- Ejecute la aplicación usando una huella mínima de instancias de EC2 o la infraestructura de AWS.
- Revise y actualice los archivos de software y configuración en consonancia con el entorno activo.

**Fase de recuperación:**

En caso de que falle el sistema de producción, se aumentará el entorno de espera para la carga de producción y los registros de DNS se cambiarán para dirigir todo el tráfico a AWS.

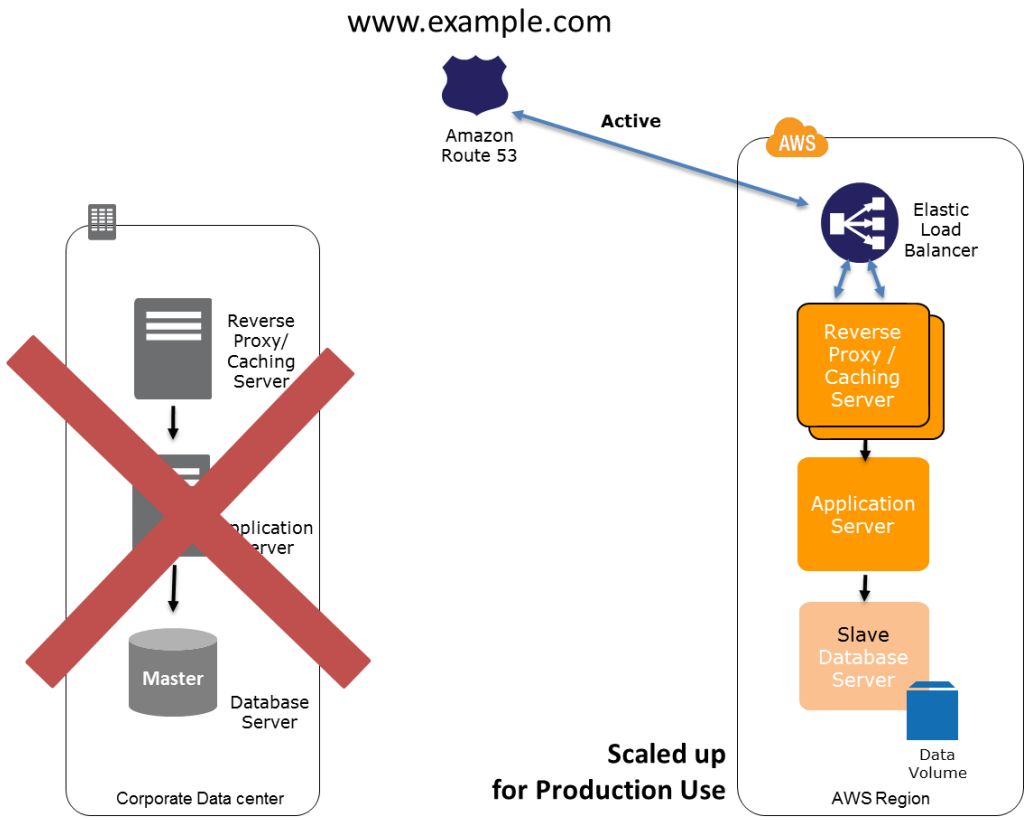


*Ilustración 6: La fase de recuperación del escenario de "espera semiactiva".*

Puntos clave de la fase de recuperación:

- Inicie las aplicaciones en tipos de instancias más grandes de EC2, según proceda (escalado vertical).
- Aumente el tamaño de los grupos de EC2 del servicio con el equilibrador de carga Load Balancer (escalado horizontal).
- Cambie los registros DNS para que todo el tráfico se dirija al entorno de AWS.
- Considere la posibilidad de utilizar Auto Scaling para dar el tamaño adecuado al grupo o para acomodar el aumento de la carga.

## Solución multisitio implementada en AWS y a nivel local

Una solución multisitio se ejecuta en AWS y en la infraestructura local existente con una configuración activo/activo. El método de replicación que utilice se determinará en función del punto de recuperación que elija (consulte el apartado anterior sobre el RPO). Existen varios métodos de replicación (consulte la información que se facilita a continuación).

Se utiliza un servicio DNS ponderado, como Amazon Route 53, para dirigir el tráfico de producción a los diferentes sitios. Una parte del tráfico se dirigirá a la infraestructura de AWS y el resto se dirigirá a la infraestructura local.

En una situación de desastre a nivel local, puede ajustar la ponderación de DNS y enviar todo el tráfico a los servidores de AWS. La capacidad del servicio de AWS puede aumentarse rápidamente para gestionar la carga total de producción. EC2 Auto Scaling puede utilizarse para automatizar este proceso. Es posible que necesite alguna lógica de aplicación para detectar fallos de los servicios de base de datos principales y cortar en los servicios de base de datos paralelos que se ejecutan en AWS.

El coste de este escenario se determina en función de la cantidad de tráfico de producción que AWS gestiona en condiciones operativas normales. En la fase de recuperación, solo debe pagar por los recursos adicionales que utilice y por la duración que se requiera para el entorno de DR con escala total. Puede reducir aún más el coste mediante la adquisición de instancias reservadas para los servidores de AWS que estén siempre activos.

**Fase de preparación:**

En la ilustración siguiente, observamos el uso de DNS para dirigir una parte del tráfico al sitio de AWS. La aplicación de AWS puede acceder a las fuentes de datos en el sistema de producción local. Los datos se replican o reflejan en la infraestructura de AWS.

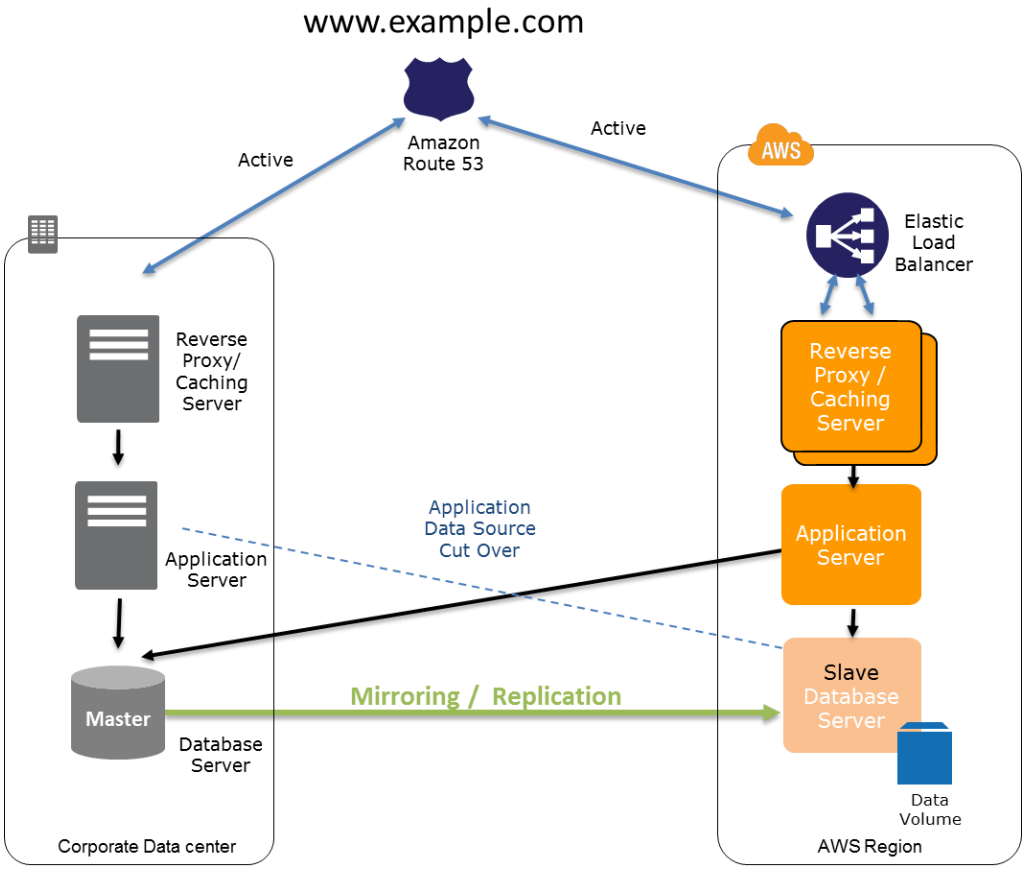


*Ilustración 7: La fase de preparación del escenario "multisitio".*

Puntos clave de la fase de preparación:

- Configure el entorno de AWS para duplicar el entorno de producción.
- Configure la ponderación de DNS o una tecnología similar para distribuir las solicitudes entrantes a ambos sitios.

**Fase de recuperación:**

En la ilustración siguiente se muestra lo que ocurre cuando se produce un desastre a nivel local. El tráfico se corta en la infraestructura de AWS mediante la actualización de DNS.

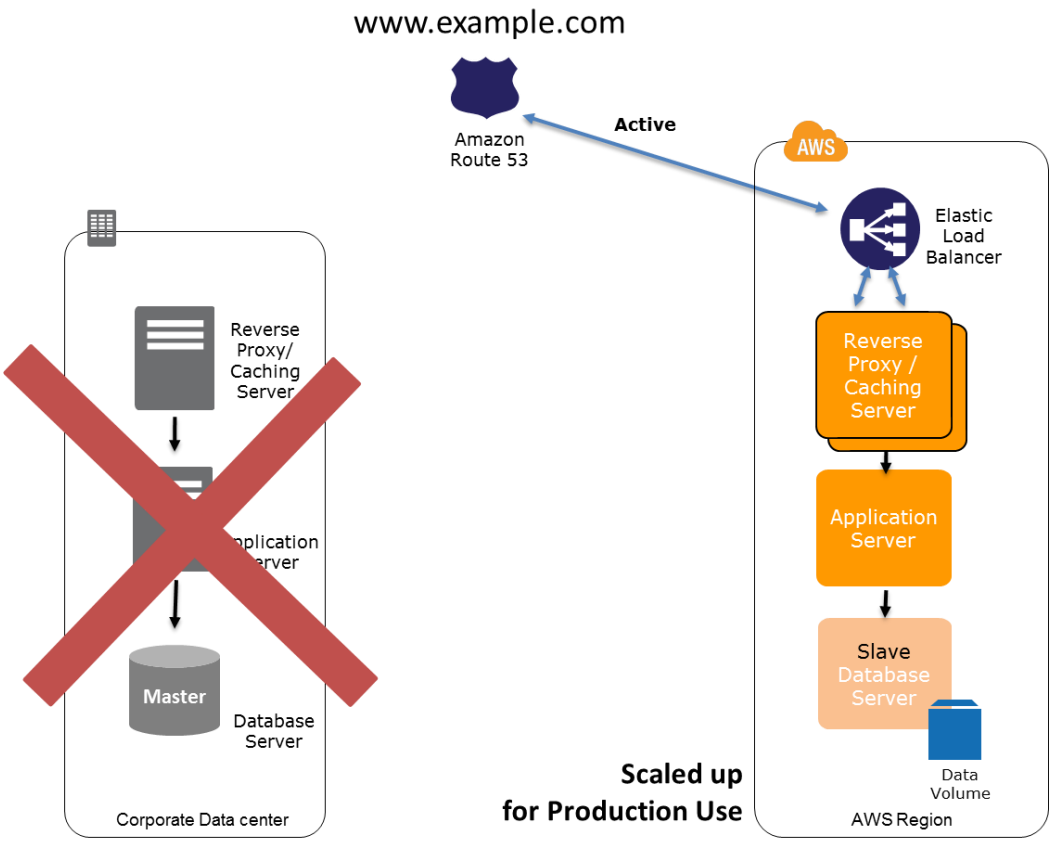


*Ilustración 8: La fase de recuperación del escenario "multisitio" abarca la infraestructura local y la de AWS.*

Puntos clave de la fase de recuperación:

- Cambie la ponderación de DNS para que todas las solicitudes se envíen al sitio de AWS.
- Debe disponer de una lógica de aplicación para la conmutación de error a fin de utilizar los servidores de base de datos locales de AWS.
- Considere la opción de utilizar Auto Scaling para ajustar automáticamente el tamaño del grupo de AWS.

Puede aumentar aún más la disponibilidad de la solución multisitio mediante el diseño de arquitecturas en zonas de disponibilidad múltiples (Multi-AZ). Para obtener información adicional sobre cómo diseñar aplicaciones que se distribuyan por varias zonas de disponibilidad, consulte el documento técnico Creación de aplicaciones tolerantes a fallos en AWS.

# Replicación de datos

Para replicar datos en una ubicación remota, es preciso tener en cuenta una serie de factores.

- Distancia entre los sitios: las distancias más largas normalmente están sujetas a más latencia o vibración.
- Ancho de banda disponible: ¿qué amplitud y variabilidad tienen las interconexiones?
- Volumen de datos que requieren las aplicaciones: el volumen de datos debe ser inferior al ancho de banda disponible.
- La tecnología de replicación debe ser paralela (para que la red se pueda utilizar de forma eficaz).

Existen otros dos enfoques principales que cabe tener en cuenta para replicar datos, es decir, la replicación asincrónica y sincrónica.

### Replicación sincrónica

Los datos se actualizan automáticamente en varias ubicaciones. Esto crea una dependencia del rendimiento y de la disponibilidad de la red.

### Replicación asincrónica

Los datos no se actualizan automáticamente en varias ubicaciones. Se transfieren según permitan el rendimiento y la disponibilidad de la red, y la aplicación continúa grabando datos que, sin embargo, pueden no estar totalmente replicados.

Muchos sistemas de base de datos admiten la replicación asincrónica de los datos. La réplica de la base de datos se puede alojar de forma remota y esta no ha de estar totalmente sincronizada con el servidor de base de datos principal. Esto se admite en muchos escenarios, por ejemplo, como un origen de copia de seguridad o como casos prácticos de generación de informes o de solo lectura.

Recomendamos a los clientes que conozcan la tecnología de replicación que utiliza su solución de software. El análisis detallado de la tecnología de replicación no recae en el ámbito de este documento.

En AWS, las zonas de disponibilidad de una región están bien conectadas, aunque están separadas físicamente. Por ejemplo, cuando la implementación se realiza en el modo "Multi-AZ", Amazon Relational Database Service utiliza la replicación sincrónica para duplicar datos en una segunda zona de disponibilidad. Esto garantiza que los datos no se pierdan en caso de que la zona de disponibilidad principal deje de estar disponible.

Las regiones de AWS son totalmente independientes entre sí, pero no hay diferencias en relación con las formas en que se accede a ellas y en cómo se usan. Esto permite que los clientes creen procesos de recuperación ante desastres que lleguen a abarcar distancias continentales, sin los desafíos ni los costes en los que incurrirían normalmente. Los clientes pueden realizar copias de seguridad de los datos y los sistemas en dos o más regiones de AWS que permitan la restauración del servicio incluso en caso de que se produzcan desastres a gran escala. Los clientes pueden utilizar las regiones de AWS para que asistan a sus clientes finales en todo el mundo con una complejidad relativamente baja para sus procesos operativos.

# Mejora del plan de DR

Es necesario seguir algunos pasos importantes a fin de contar con un plan sólido de recuperación ante desastres. En esta sección se describen algunos de los pasos principales.

### Pruebas

Después de contar con la solución de DR, es necesario que la pruebe. "Día de partido" se corresponde con un escenario en el que el cliente aplica una conmutación por error en el entorno de DR, garantizando la disponibilidad de la documentación suficiente para que el proceso resulte lo más sencillo posible en caso de que se produzca el evento real. Poner en marcha un entorno duplicado para comprobar que los escenarios "Día de partido" es un proceso rápido y rentable en AWS, y normalmente no es preciso que altere el entorno de producción. Puede utilizar AWS CloudFormation para implementar entornos completos en AWS. Este método utiliza una plantilla para describir los recursos de AWS y cualquier dependencia asociada o parámetro de tiempo de ejecución necesarios para crear un entorno completo.

La diferenciación de las pruebas es clave para garantizar que cuente con protección frente a una gran variedad de desastres. A continuación, se describen ejemplos de escenarios "Día de partido":

- Pérdida de potencia en un sitio o en un conjunto de máquinas
- Pérdida de la conexión del ISP con un único sitio
- Virus que repercuten en servicios empresariales principales que afectan a varios sitios
- Los errores de los usuarios que causen la pérdida de datos y que precisen de una recuperación en un punto en el tiempo

### Supervisión y alertas

Debe disponer de una solución para hacer comprobaciones regulares y realizar una supervisión suficiente para notificarle si el entorno de DR se ha visto afectado por el fallo del servidor, los problemas de conectividad y los problemas de la aplicación. Amazon CloudWatch ofrece acceso a métricas sobre los recursos de AWS. Las alarmas se pueden configurar en función de umbrales definidos en cualquiera de las métricas y cuando se puedan enviar los mensajes del servicio de notificación simple de Amazon necesarios para advertir en caso de que se produzca un comportamiento no esperado. Puede utilizar cualquier solución de supervisión en AWS.

También puede seguir utilizando las herramientas de supervisión y alertas existentes que su empresa utiliza para controlar las métricas de las instancias, así como las estadísticas del SO invitado y el estado de la aplicación.

### Copias de seguridad

Cuando haya cambiado a su entorno de DR, debe seguir realizando copias de seguridad regulares. Las pruebas regulares de copia de seguridad y restablecimiento son esenciales a fin de que sirvan como una solución de reversión.

AWS le proporciona la flexibilidad necesaria para realizar pruebas de DR frecuentes y económicas sin que resulte necesario que la infraestructura de DR esté siempre activa.

### Acceso de usuarios

Puede garantizar el acceso a los recursos en el entorno de DR mediante la utilización de Identity and AWS Access Management (IAM). De esta forma puede crear políticas de seguridad basadas en funciones y usuarios que individualizan las responsabilidades de los usuarios mientras trabajan en el entorno de DR.

### Automatización

Puede automatizar la implementación de aplicaciones en los servidores basados en AWS y en los servidores in situ mediante la utilización de software de orquestación o gestión de la configuración. Esto le permitirá gestionar con facilidad los cambios de configuración y aplicación en ambos entornos. Hay varias opciones de software de orquestación conocidas disponibles y, además, puede encontrar los posibles proveedores de soluciones en nuestra página de proveedores de soluciones[4]. AWS CloudFormation funciona junto con varias herramientas para ofrecer servicios de infraestructura de manera automática. Los datos de usuario se pueden transferir a la instancia la primera vez que se inicia y pueden manipularse con una herramienta de gestión de la configuración para determinar el tipo o la función de la instancia, a fin de garantizar la implementación del software y la configuración adecuados. El objetivo general debe basarse en que las instancias acaben con el estado definitivo en el que las necesita de la forma más automática posible.

Auto Scaling se puede utilizar para garantizar que el grupo de instancias tenga el tamaño adecuado para satisfacer la demanda en función de las métricas que especifique en CloudWatch. Esto significa que, en una situación de DR, a medida que la base de usuarios empieza a utilizar más el entorno, la solución puede aumentar de forma dinámica para satisfacer el aumento de la demanda. Después de que se produzca el evento y de que disminuya potencialmente el uso, es posible que se vuelva a reducir la solución a un nivel mínimo de servidores.

## Licencias de software y DR

Asegurarse de que dispone de la licencia adecuada para el entorno de AWS es tan importante como disponer de a licencia adecuada para cualquier otro entorno. Amazon ofrece una serie de modelos para que pueda gestionar las licencias de forma más sencilla. Por ejemplo, el modelo “Bring Your Own License” se puede utilizar para varios componentes de software o para varios sistemas operativos. De forma alternativa, hay un conjunto de software para el que se incluye el coste en la tarifa por hora. Este modelo se conoce como “License included”.

“Bring your Own License” le permite beneficiarse de sus inversiones de software existentes durante un desastre. “License included” minimiza los costes de licencia anticipados para un sitio de recuperación ante desastres que no se usa diariamente como, por ejemplo, durante la prueba de una recuperación ante desastres.

Si en alguna fase tiene dudas acerca de las licencias y sobre su aplicación en AWS, póngase en contacto con el proveedor de su licencia.

## Conclusión

Existen muchas opciones y variaciones en el caso de la recuperación ante desastres; no obstante, en este documento se destacan algunos de los modelos comunes, partiendo de copias de seguridad y restablecimiento sencillos hasta soluciones multisitio tolerantes a fallos. AWS le ofrece un control específico y muchos bloques de compilación para crear la solución adecuada de DR, en función de los objetivos de DR (RTO y RPO) y del presupuesto. Los servicios de AWS se encuentran disponibles bajo demanda y solo debe pagar por lo que utilice. Se trata una ventaja clave para la recuperación ante desastres, donde se precisa con rapidez de la infraestructura importante, pero solo en el caso de un desastre.

En este documento se ha descrito cómo AWS ofrece soluciones de infraestructuras rentables y flexibles, que le permiten disponer de un plan más eficaz de recuperación ante desastres.

[4] Se pueden encontrar proveedores de soluciones en http://aws.amazon.com/solutions/solution-providers/

# Más documentación

- S3 Getting Started Guide, disponible en http://docs.amazonwebservices.com/AmazonS3/latest/gsg/
- EC2 Getting Started Guide, disponible en http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide/
- Find an AWS Solution Provider, disponible en http://aws.amazon.com/solutions/solution-providers/
- Documento técnico Creación de aplicaciones tolerantes a fallos en AWS, disponible en http://aws.amazon.com/whitepapers/
- Centro de seguridad y conformidad legal de AWS, disponible en http://aws.amazon.com/security/
- Centro de arquitectura de AWS, disponible en http://aws.amazon.com/architecture
- Documentos técnicos de AWS, disponibles en http://aws.amazon.com/whitepapers