Arquitecturas de nube con AWS

Ing. Fernando Lichtschein
Ing. Mora Villa Abrille

16. Planeamiento para desastres

UNIVERSIDAD AUSTRAL

Objetivos

Identificar estrategias de planificación de actividades ante desastres, incluyendo los *recovery point objective* (RPO) y los *recovery time objective* (RTO) sobre la base de los requerimientos de negocio.

Identificar las categorías de servicios de planeamiento para desastres de AWS.

Describir los patrones comunes para la recuperación ante desastres y cómo implementarlos.

Aplicar los principios del AWS Well-Architected Framework al diseño de un plan de recuperación ante desastres.

Objetivos

De un arquitecto de nube

Diseñar arquitecturas que mitigan el riesgo ante desastres y permiten una recuperación oportuna cuando suceden, para contribuir a minimizar el impacto de un desastre en el negocio.

Considerar las necesidades de negocio para aplicar patrones de recuperación ante desastres que balanceen el costo, la pérdida de datos y el tiempo de recuperación.

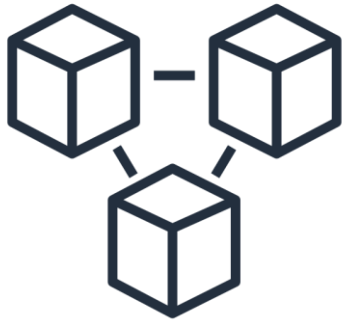
Estrategias de recuperación

UNIVERSIDAD AUSTRAL

Escala de eventos

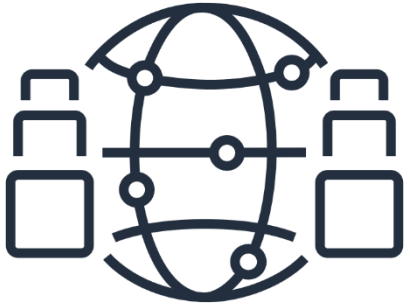
Eventos de menor escala

Caída de servidor



Eventos a gran escala

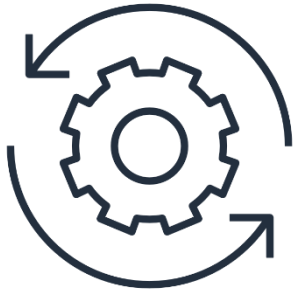
Múltiples recursos no disponibles en una Availability Zone.



Evento global

Falla generalizada que afecta a múltiples usuarios y sistemas.

Estrategias de continuidad



Fault tolerance	Backup	Disaster recovery
Minimizar la frecuencia de situaciones que dejan los datos no disponibles.	Asegurar la existencia de un plan de backup para gestionar los datos ante desastres.	Recuperar los datos y reestablecer las aplicaciones después de un desastre.

Estrategias de continuidad

Dependencia del tiempo

¿Con qué velocidad debemos recuperar los servicios para minimizar el impacto?

Pérdida de datos

¿Qué cantidad de datos toleramos perder? ¿Qué tipos de datos podemos perder?

Ubicación geográfica

¿Tiene impacto en varias regiones?

¿Las distintas regiones requieren medidas de recuperación distintas?

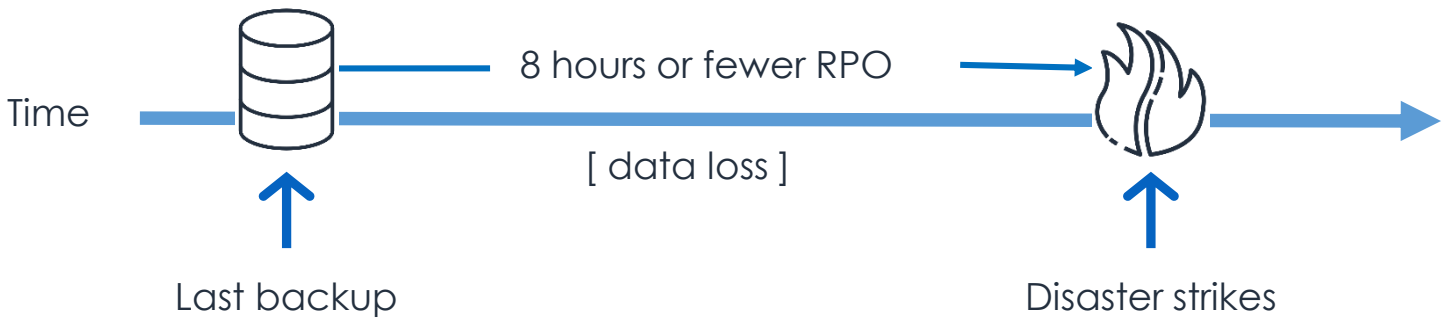
Costo

¿El nivel de costos es acorde al impacto en el negocio y a los riesgos?

Determinación del RPO

Es la pérdida de datos máxima que resulta aceptable, medida en tiempo.

¿Con qué frecuencia debemos resguardar los datos?



Determinación del RPO

Determinar que una pérdida máxima de 800 registros es aceptable para tu aplicación.

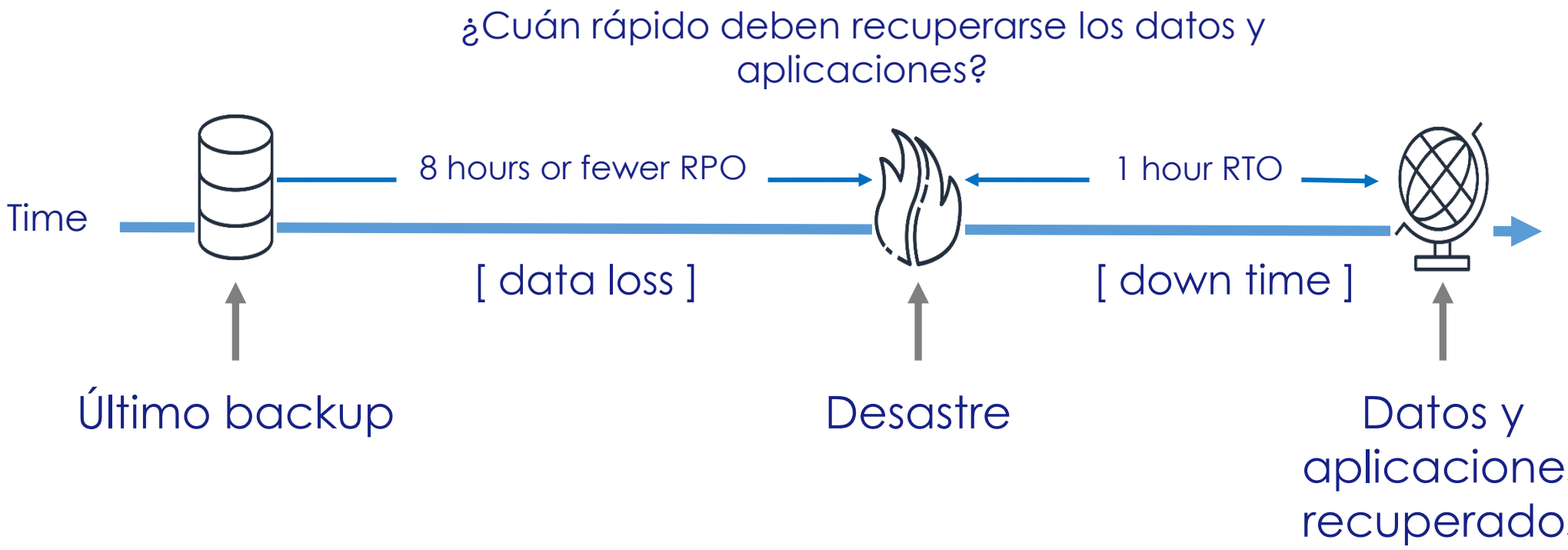
Usar los patrones existentes para determinar que no se crean más de 100 registros por hora.

Calcular el RPO aceptable de 8 horas.

Con esta información, podemos ver que, si a las 10 pm se produce un desastre, el sistema debería poder recuperar toda la información que estaba en el sistema **antes** de las 2pm

Determinación del RTO

RTO es el tiempo máximo de indisponibilidad de un proceso después de que se produce un desastre.



Determinación del RTO

Determinar que un servicio de tickets para un show musical se debe restaurar dentro de dos horas.

El negocio calcula que después de 2 horas de caída, comenzará a perder ganancias por ventas perdidas.

Calcular un RTO aceptable de 2 horas.

Sobre la base de esta información, si un desastre ocurre a las 9 p.m., el Sistema se debería poder recuperar antes de las 11 pm.

Preparación para el BCP

Un plan de continuidad de negocios (BCP) es un Sistema para la prevención y la recuperación respecto de amenazas potenciales para una compañía.

Un BCP está conformado por:

- Business Impact Analysis
- Evaluación de riesgos
- Disaster Recovery Plan
- RPO y RTO evaluados y definidos

Resumen

Puede haber fallas en cualquier momento y en cualquier escala.

Un plan de recuperación contribuye a reducir el impacto de un desastre sobre el negocio y los clientes.

El RPO es la pérdida de datos máxima aceptable luego de un incidente de pérdida de datos.

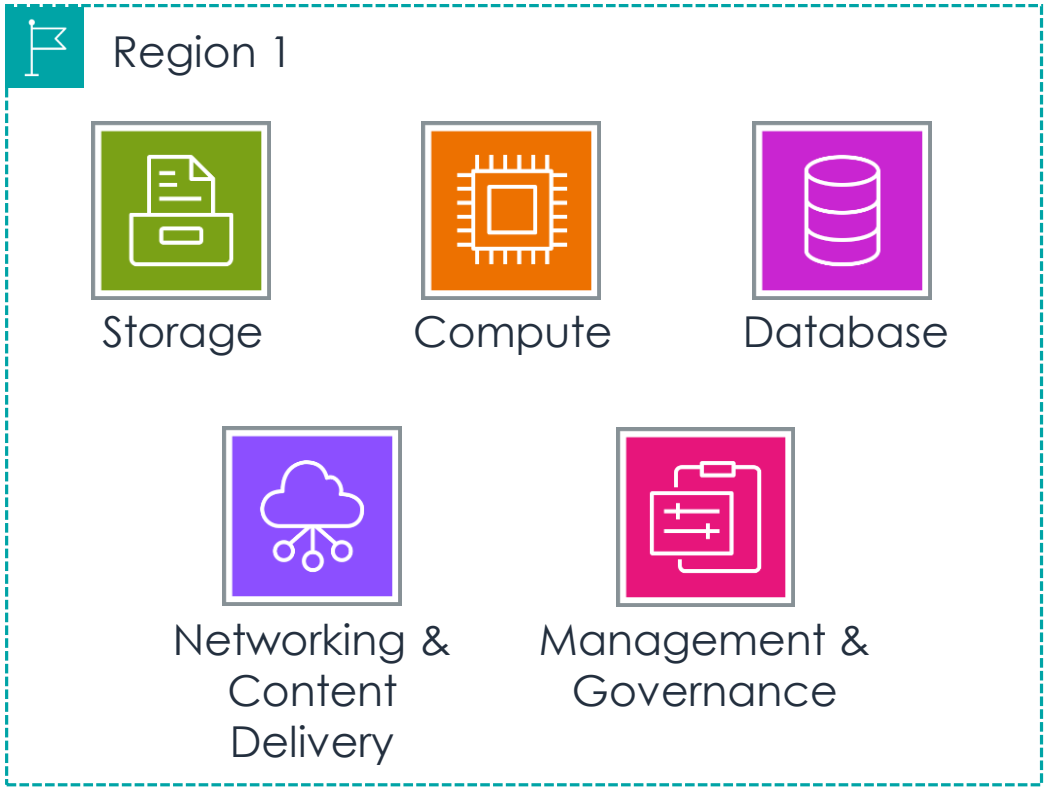
El RTO es el tiempo que una aplicación, sistema o proceso puede estar caído sin provocar un daño significativo al negocio.

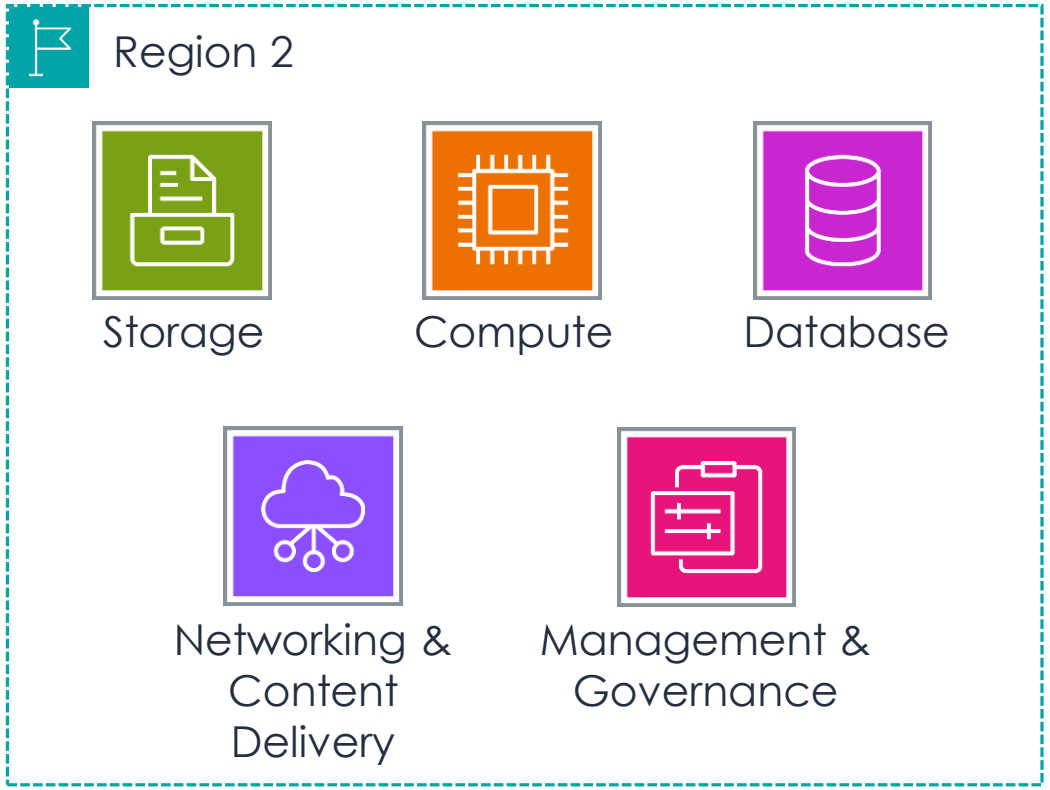
Un BCP permite prevenir y recuperar incidentes potenciales.

AWS Disaster Recovery Planning

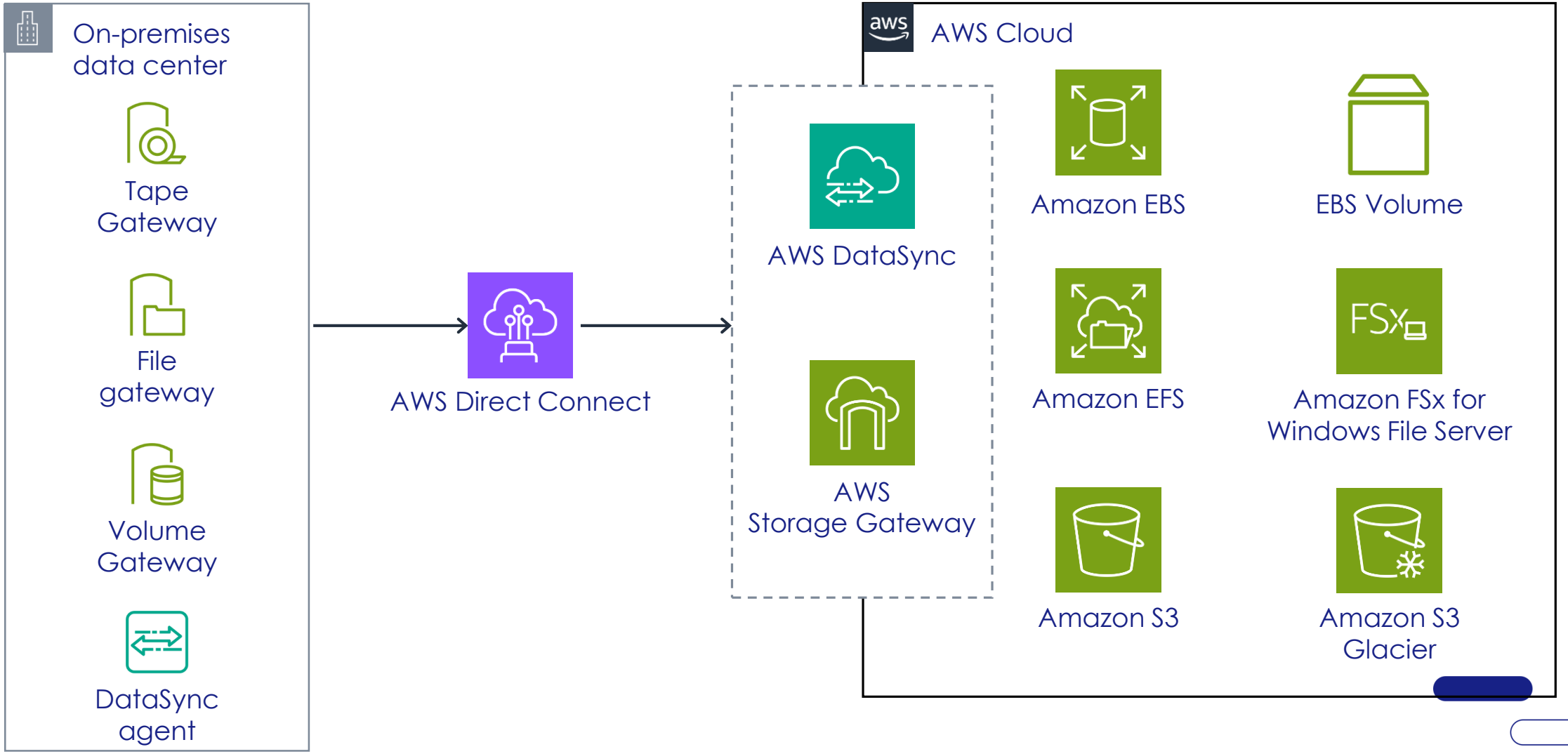
UNIVERSIDAD AUSTRAL

DRP en más de una región

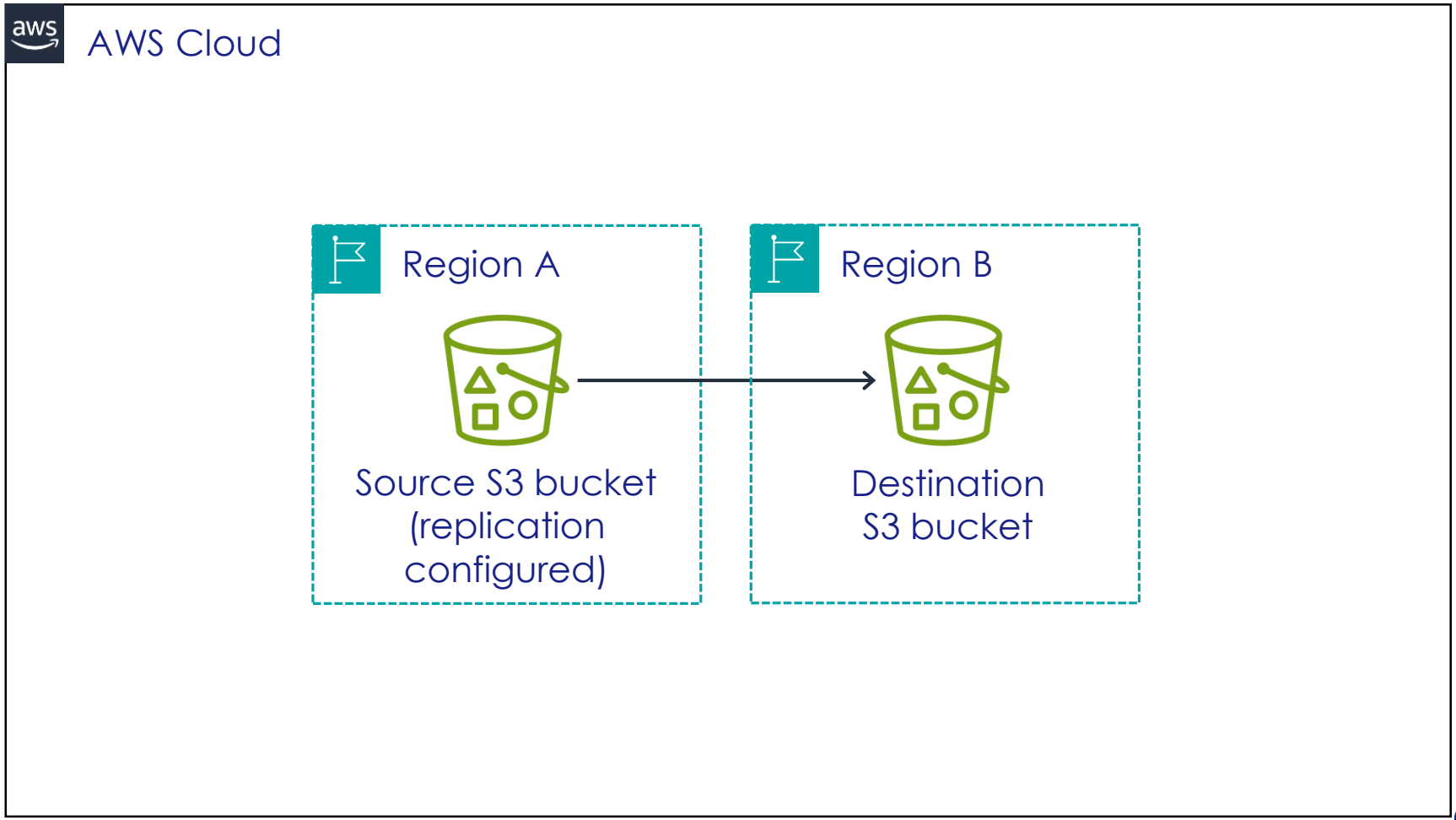




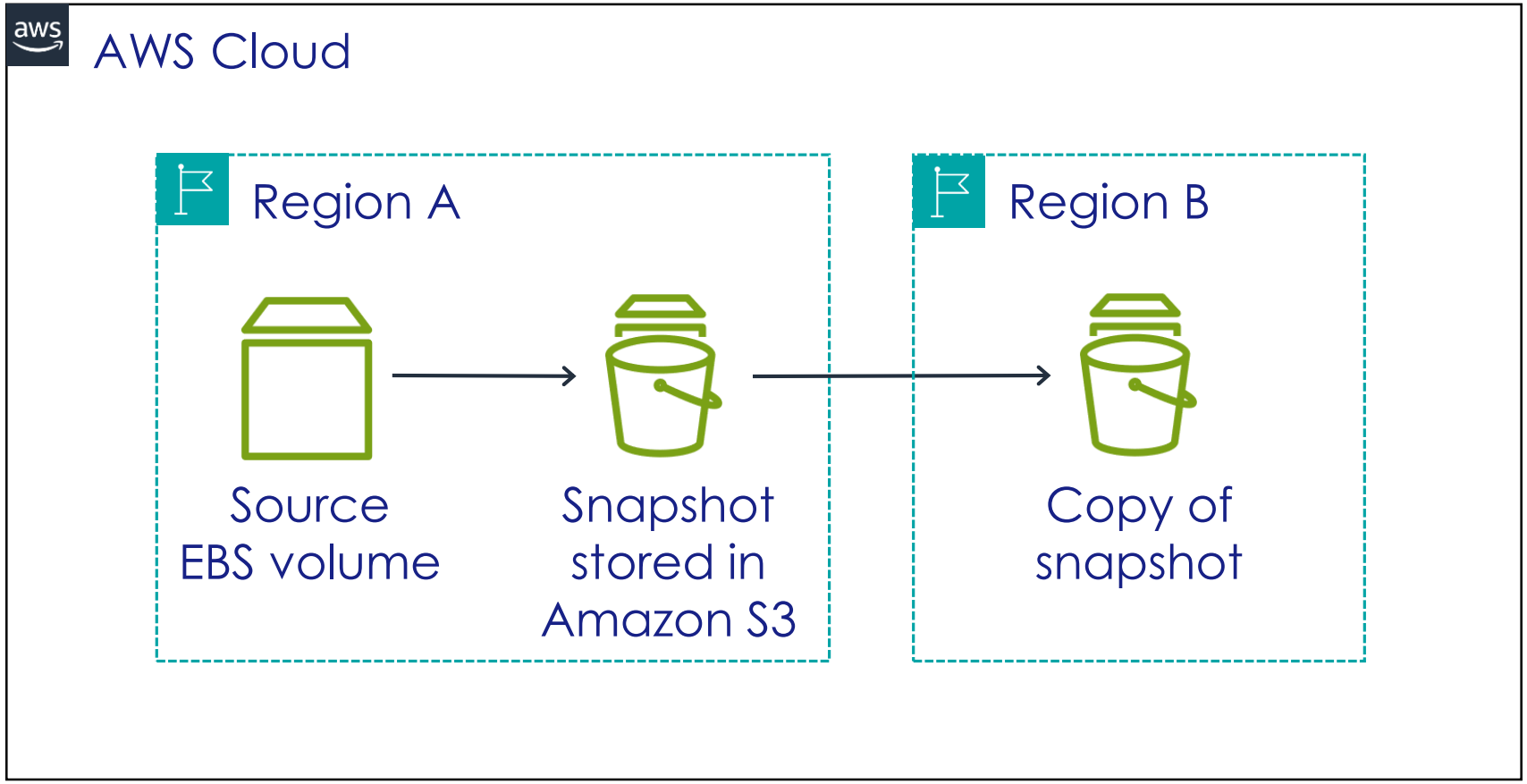
Almacenamiento y backups



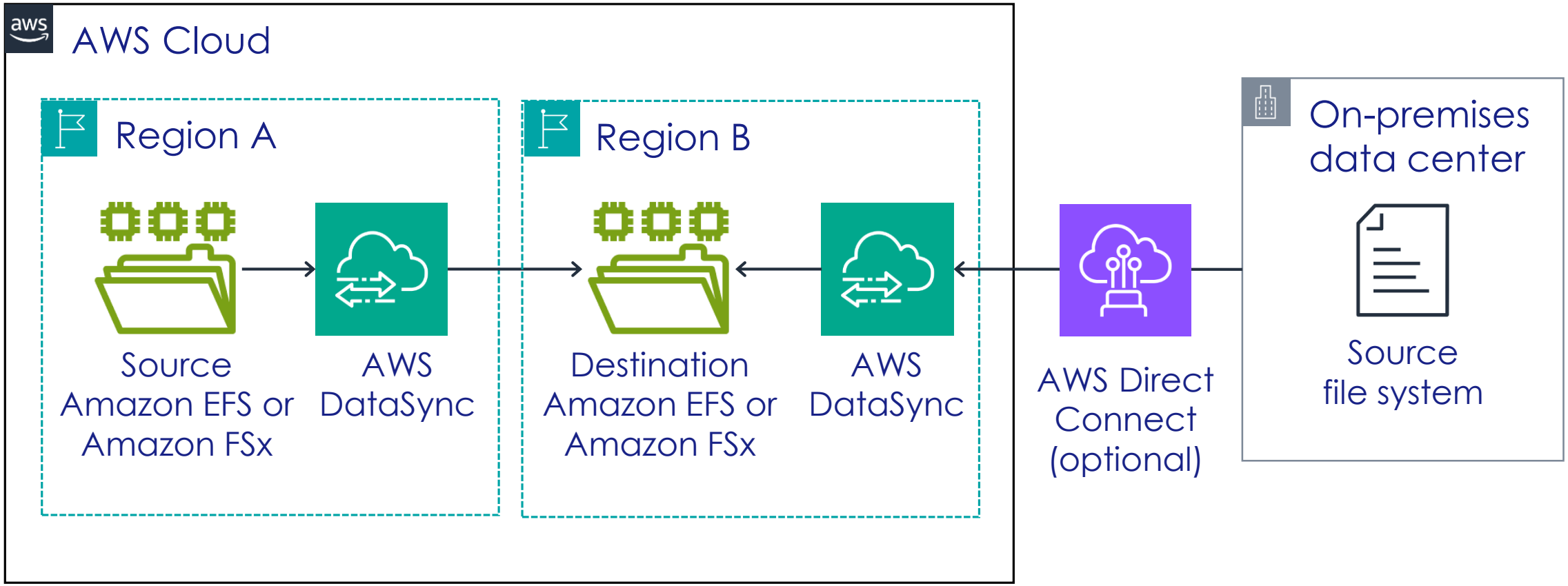
Réplica entre regiones



Snapshots de volúmenes de EBS

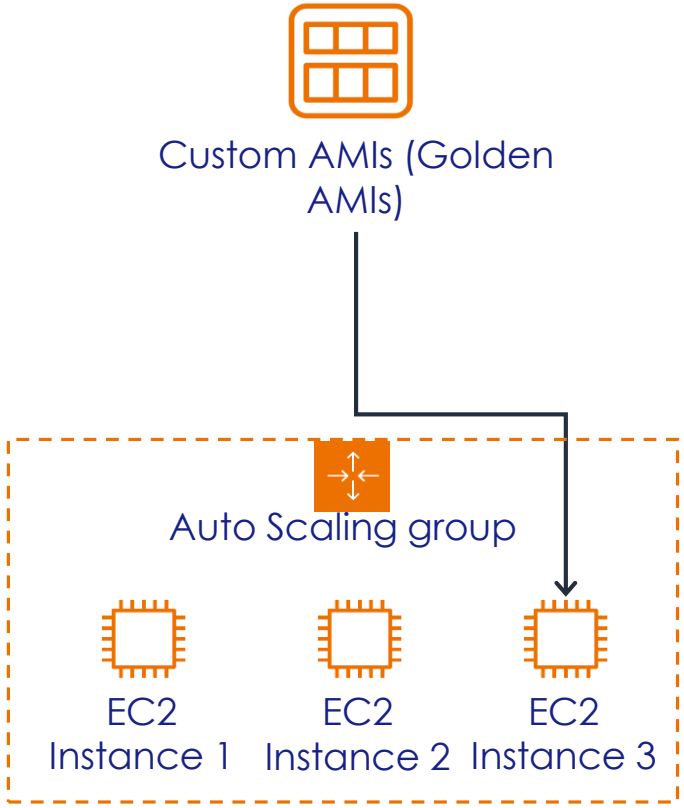


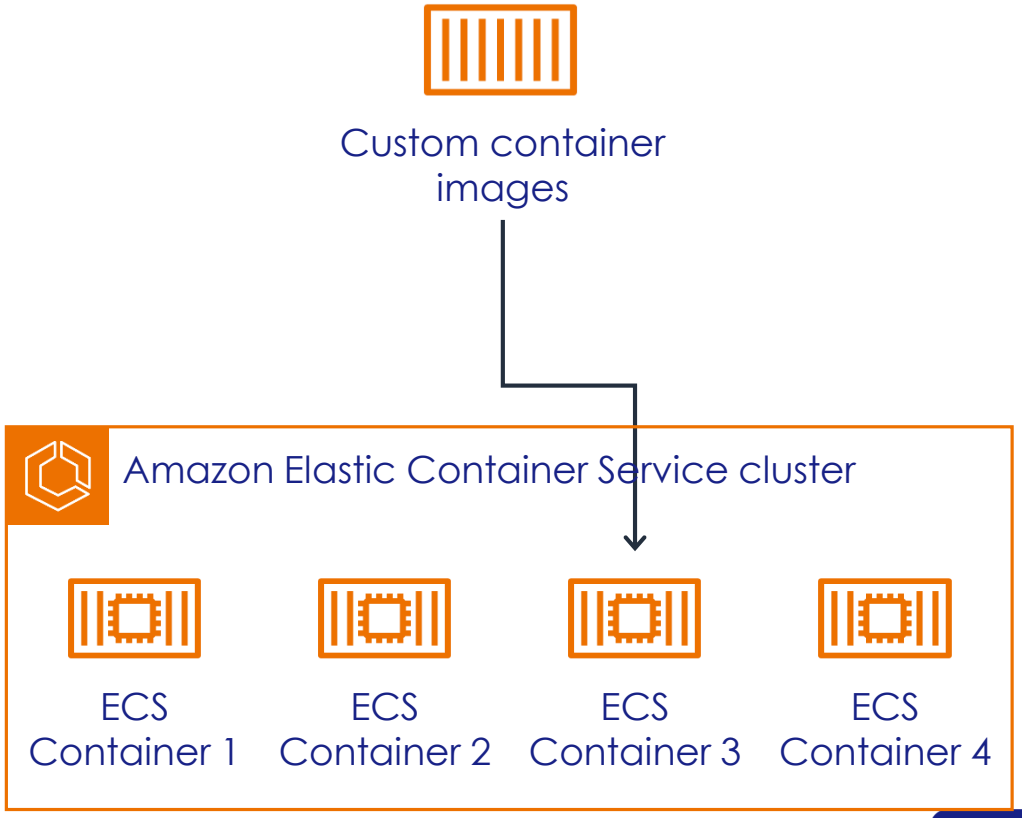
Réplica de *file servers*



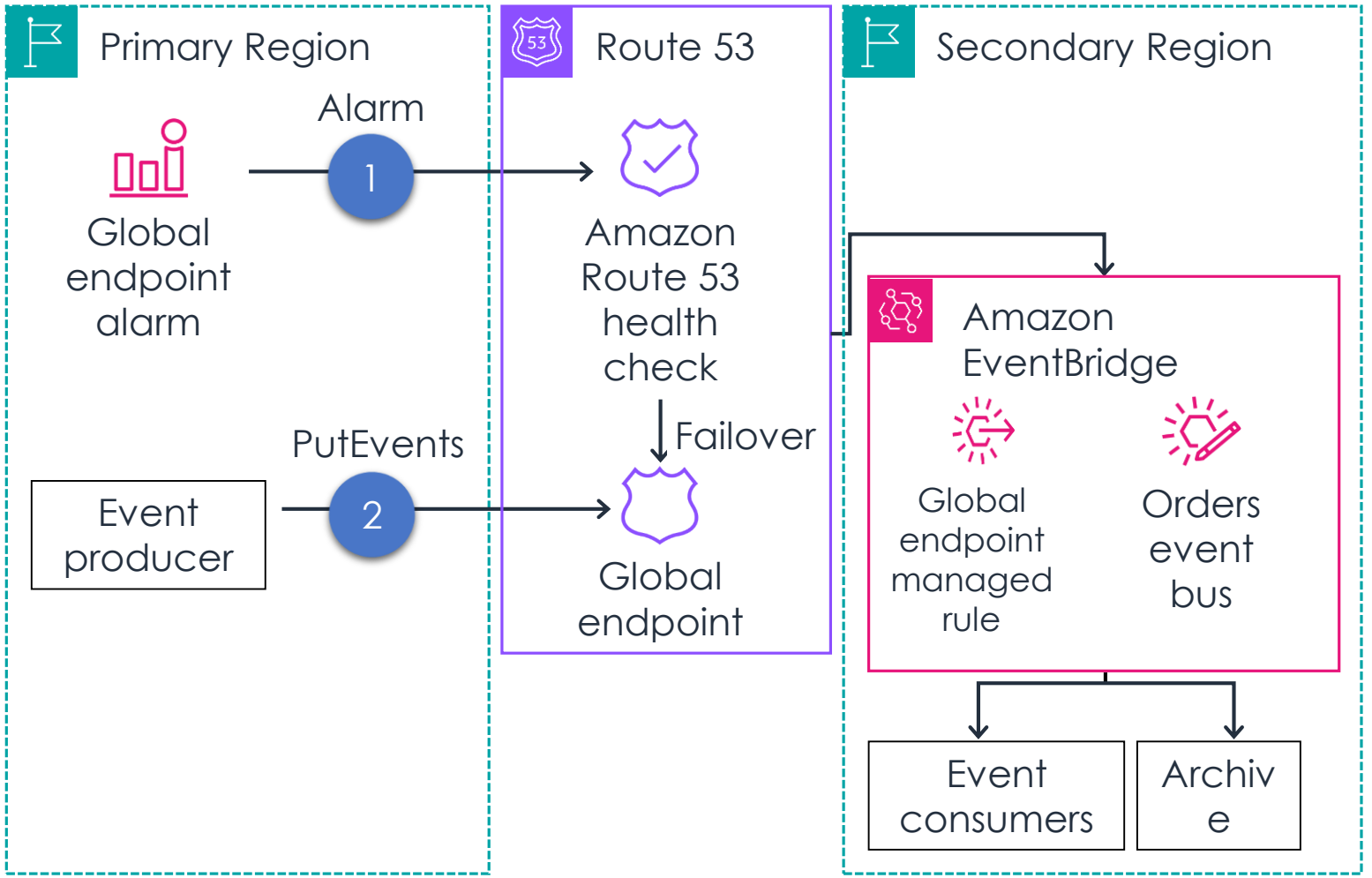
Recuperación de infraestructura

Es posible obtener e iniciar nuevas instancias y contenedores en pocos minutos





Uso de EventBridge para *failover*



Diseño para la resiliencia y recuperación

Route 53

Balanceo de carga basado en DNS

Brinda *failover* básico entre los *endpoints* o los sitios de S3

ELB

Provee distribución de tráfico

Facilita la implementación de recuperación ante desastres

Amazon VPN

Provee acceso seguro a la red *on-premise* desde la VPC de Amazon a través de una VPN

AWS Direct Connect

Conexión dedicada que no depende de internet

Recuperación de bases de datos

Amazon RDS

Guardar un *snapshot* en una región separada.

Usar *read replicas* e implementaciones Multi-AZ.

Retener *backups* automáticos.

DynamoDB

Hacer *backups* de tablas completas.

Usar *point-in-time-recovery* para restaurar tablas.

Crear backups.

Usar tablas globales para construir una base de datos multi-región.

Réplicas y reinstalaciones

CloudFormation

Usar *templates* para implementar colecciones de recursos rápidamente según la necesidad.

Duplicar los ambientes de producción en una nueva región o VPC más rápidamente.

Réplicas y reinstalaciones

Backup and restore

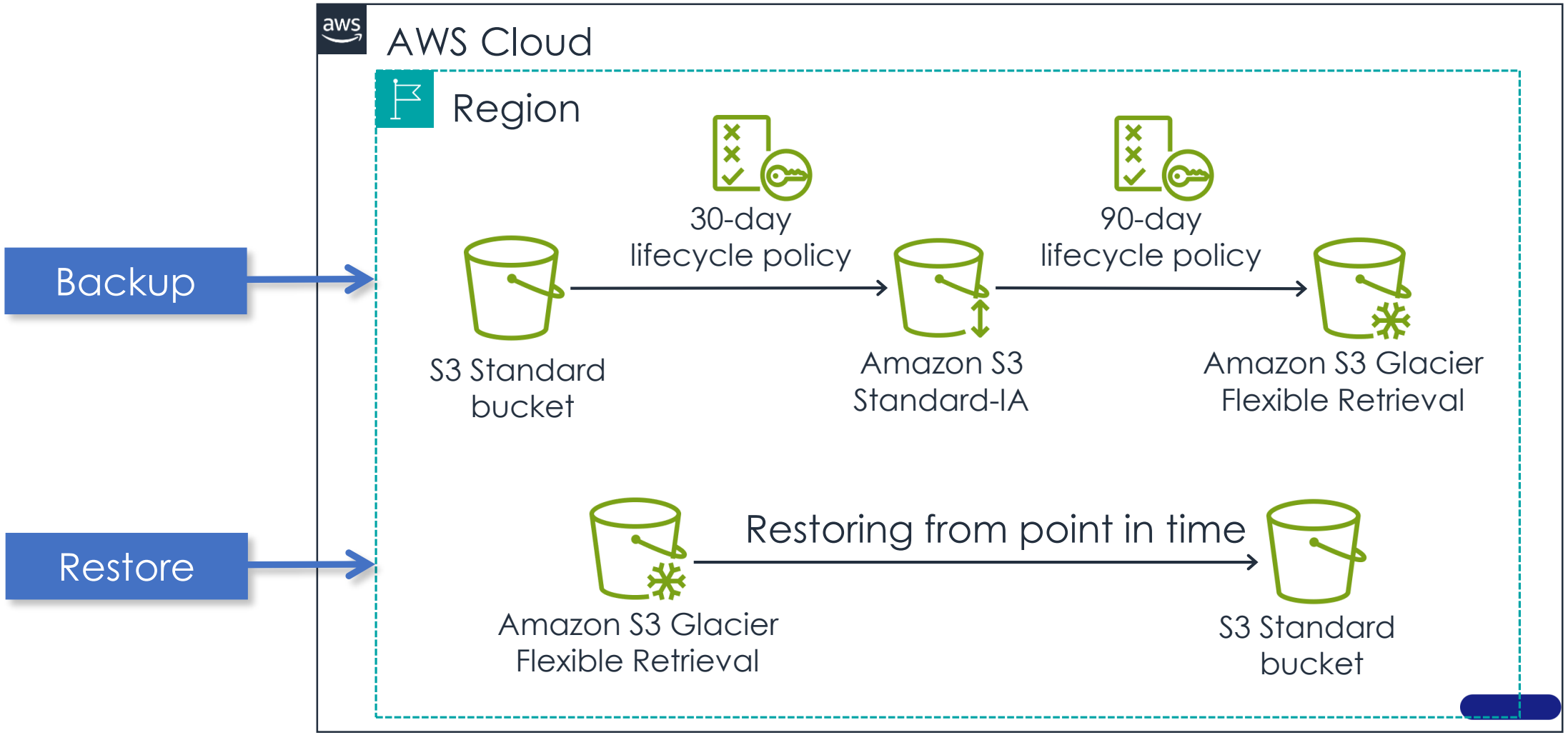
Pilot light

Warm standby

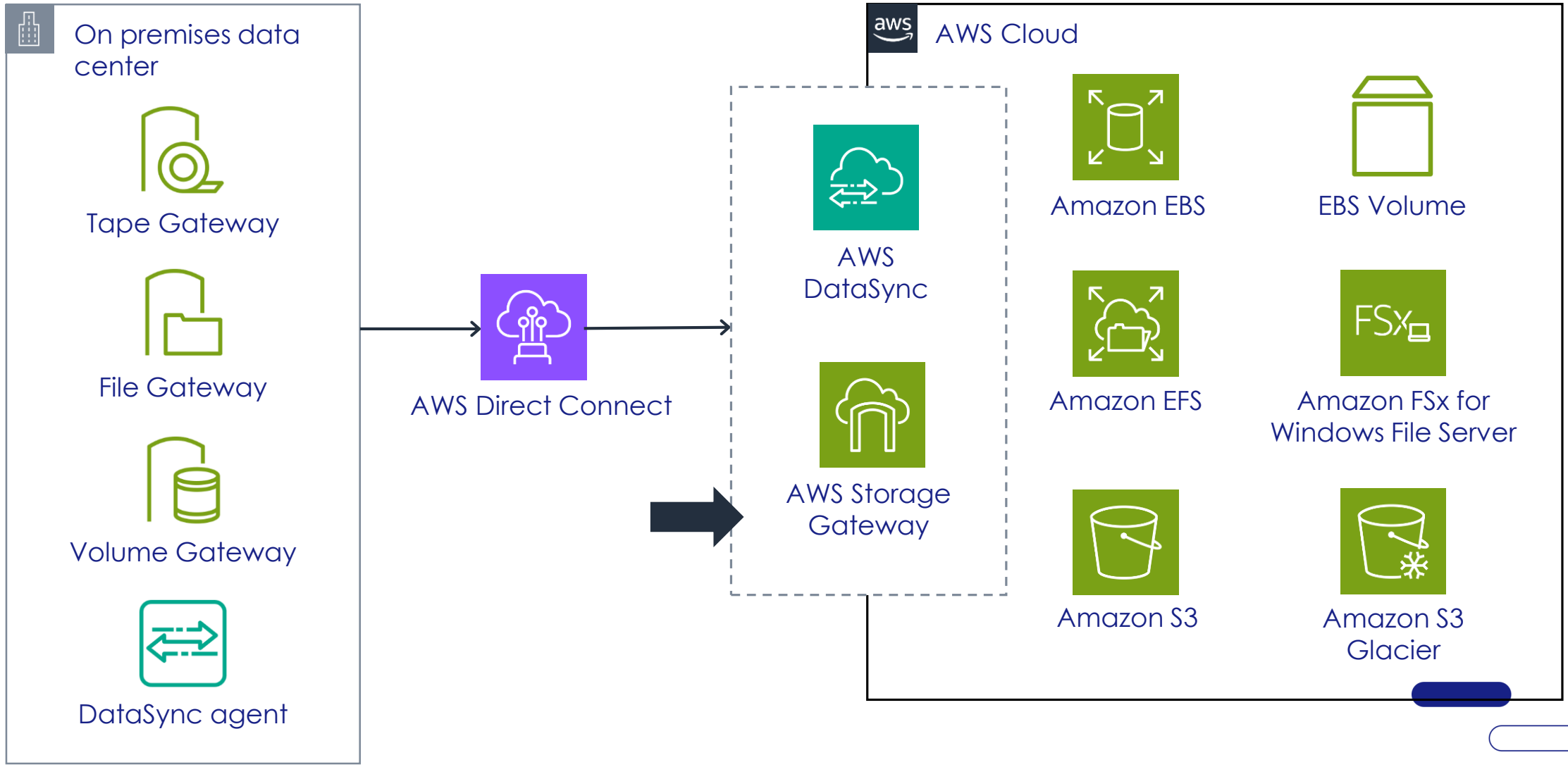
Multi-site

Cada patrón se aplica a un escenario diferente (RPO, RTO y costos).

Backup & restore



AWS Storage Gateway



AWS Storage Gateway

Preparación

Crear backups de los sistemas actuales.

Almacenar los resguardos en Amazon S3.

Documentar los procedimientos de restauración.

En caso de desastre

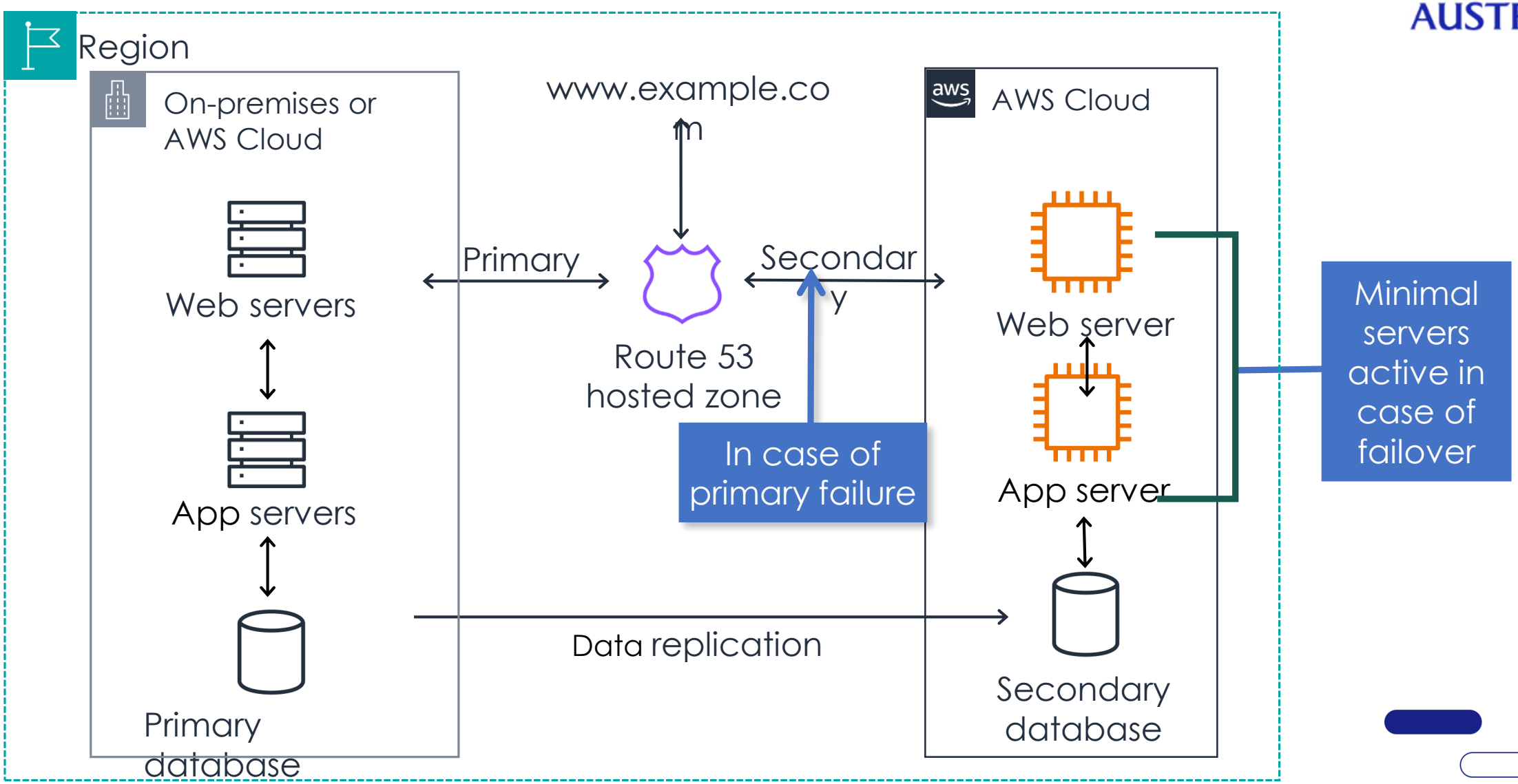
Recuperar las copias de seguridad de S3.

Restaurar la infraestructura necesaria.

Recuperar los sistemas a partir de los backups.

Redirigir el tráfico al nuevo sistema.

Luz piloto


Region
On-premises or AWS Cloud
Web servers
App servers
Primary database
www.example.com
Route 53 hosted zone
Primary
Secondary
In case of primary failure
Data replication
AWS Cloud
Web server
App server
Secondary database
Minimal servers active in case of failover

Luz piloto

Fase de preparación

Se configuran instancias de EC2 para replica los servicios.

Se crean y mantienen AMIs de los servidores más importantes, que necesitan recuperación rápida.

Se ejecutan, prueban y actualizan regularmente esos servidores.

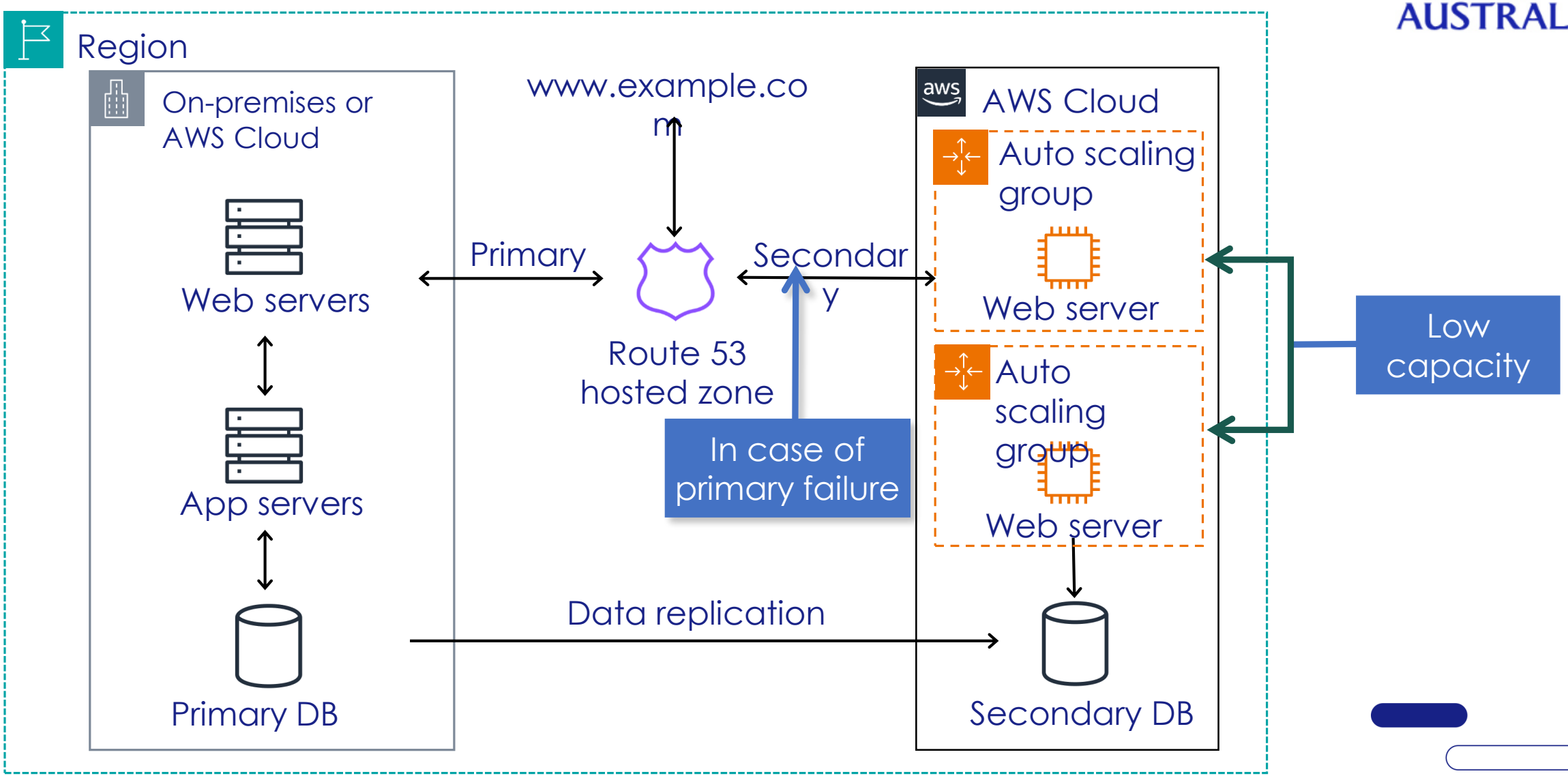
En caso de desastre

Habilite los recursos necesarios para el conjunto de datos principal replicado.

A continuación, escale el sistema según sea necesario para gestionar el tráfico de producción actual.

Cambie al nuevo sistema.

Warm stand by



Warm stand by

Preparación

Similar al piloto.

Tiene todos los componentes necesarios funcionando 24/7, pero no están escalados el tráfico de producción.

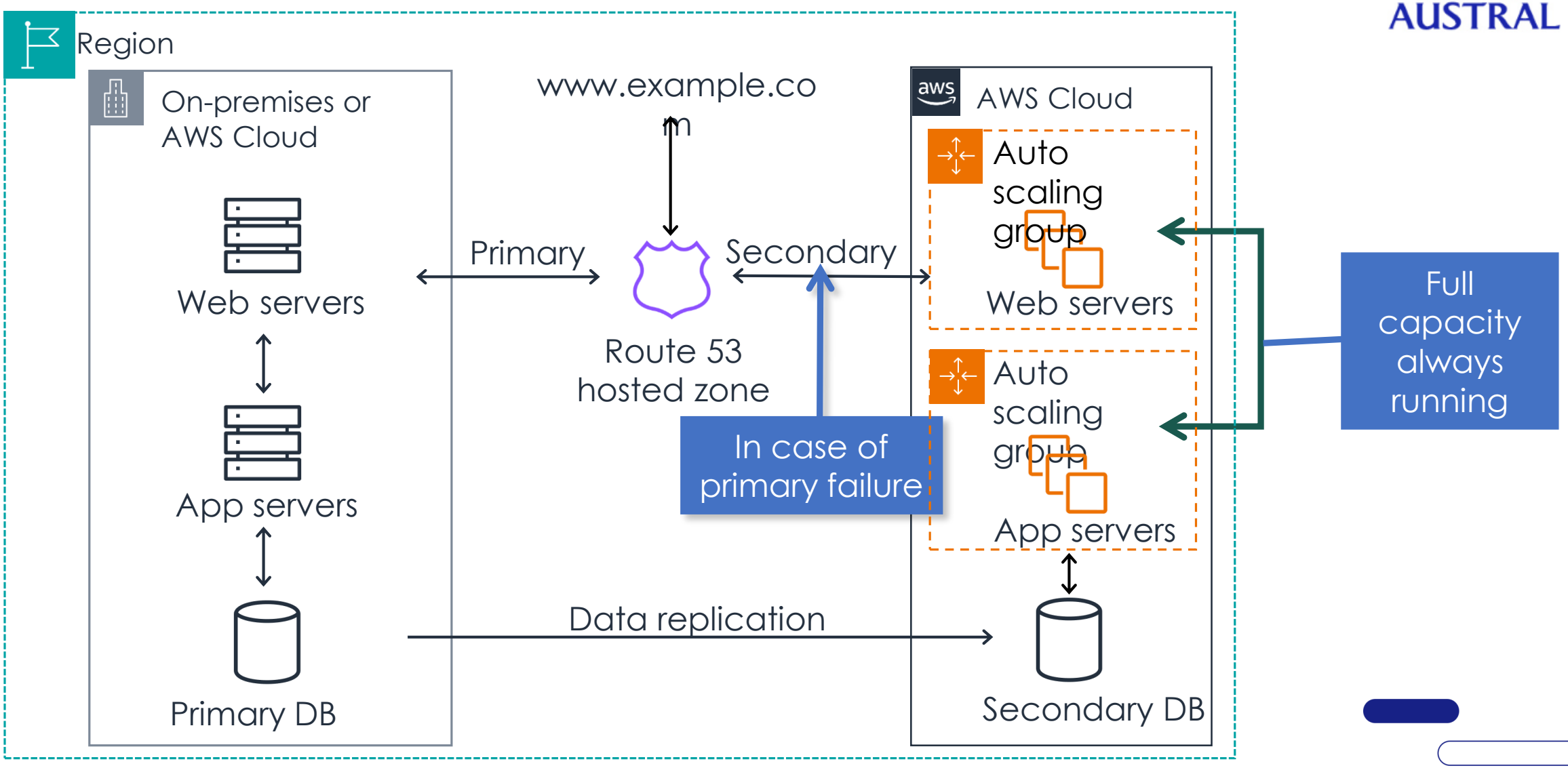
Se deben realizar pruebas continuas de los componentes.

En caso de desastre

La carga más crítica de producción se carga inmediatamente.

Escalar el sistema para administrar toda la carga de producción (automáticamente)

Patrones multisitio



Patrones multisitio

Preparación

Similar al *warm standby*.

Está configurado para escalar automáticamente para soportar las cargas de producción.

Hay que evaluar los costos de este tipo de implementación en función de la criticidad del sistema.

En caso de desastre

Failover inmediato de toda la carga de producción.

Patrones de recuperación ante desastres

Backup and restore	Pilot light	Warm standby	Multi-site

Costo

Soluciones con RTO/RPO en lapsos de horas

Casos de uso de menor prioridad

Soluciones: Amazon S3, Storage Gateway

Soluciones que requieren RTO y RPO en el orden de decenas de minutos

Servicios principales

Escalamiento de recursos de AWS

Soluciones que requieren RTO y RPO en el orden de minutos

Servicios críticos para el negocio

Soluciones que requieren RTO and RPO prácticamente en tiempo real.

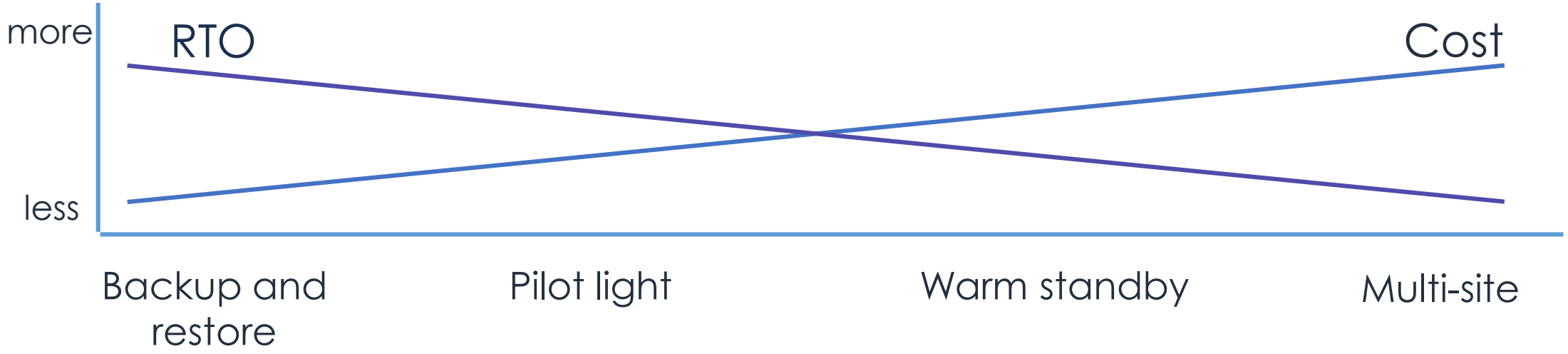
Failover automático a un duplicado que está en ejecución.

Prácticas y ejercicios de continuidad

Asegurar que los resguardos, snapshots y AMIs están siendo creados y que se pueden usar para recuperar los datos.

Controlar el Sistema de monitoreo.

Establecer RTO y RPO, y trabajar para mejorar la performance cuando sea posible.



AWS Well-Architected Framework

Aplicado a la continuidad de negocio

UNIVERSIDAD AUSTRAL

Well-Architected Framework

Reliability

Operational Excellence

Security

Planificación de *failover*

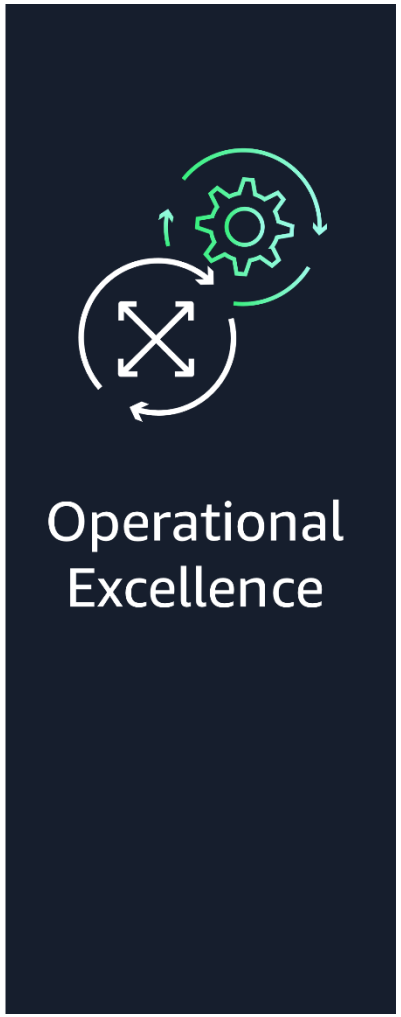
Buena práctica

Definir los objetivos de recuperación, en términos de caída y pérdida de datos.

Usar estrategias de recuperación definidas para cumplir los objetivos de recuperación.

Probar la implementación de recuperación ante desastres para validar la implementación.

Gestión de incidentes



Buena práctica

Definir un plan de comunicación a los clientes para las caídas.

Gestión de accesos

Buena práctica

Establecer un proceso de acceso en emergencia.

Resumen

Identificar estrategias de planificación de continuidad, incluyendo el RPO y RTO sobre la base de los requerimientos de negocio.

Reconocer la planificación de desastre para categorías de servicio de AWS.

Describir patrones comunes para la aplicación de una estrategia de backup y recuperación y cómo implementarlas.

Usar los principos del AWS Well-Architected Framework para diseñar un plan de recuperación ante desastres.

Módulo 16

Pregunta de práctica

A solutions architect must create a disaster recovery (DR) solution for a company's business-critical applications. The maximum acceptable amount of data loss is 7 minutes. The DR solution also requires the deployment of a completely functional version of the applications to handle the majority of traffic immediately, and then scale up to full capacity over time. Which disaster recovery pattern would provide the most cost-effective solution?

Identifiquemos las palabras o frases clave:

The following are the key words and phrases:

- Business-critical
- Functional version of the applications
- Handle the majority of traffic immediately
- Cost-effective

Módulo 16

Pregunta de práctica

A solutions architect must create a disaster recovery (DR) solution for a company's **business-critical** applications. The maximum acceptable amount of data loss is 7 minutes. The DR solution also requires the deployment of a completely **functional version of the applications to handle the majority of traffic immediately**, and then scale up to full capacity over time. Which disaster recovery pattern would provide the most **cost-effective** solution?

Choice	Response
A	Backup and restore
B	Pilot light
C	Warm standby
D	Multi-site

Módulo 16

Pregunta de práctica

A solutions architect must create a disaster recovery (DR) solution for a company's **business-critical** applications. The maximum acceptable amount of data loss is 7 minutes. The DR solution also requires the deployment of a completely **functional version of the applications to handle the majority of traffic immediately**, and then scale up to full capacity over time. Which disaster recovery pattern would provide the most **cost-effective** solution?

Choice	Response

C Warm standby

Muchas gracias.

www.austral.edu.ar

UNIVERSIDAD AUSTRAL