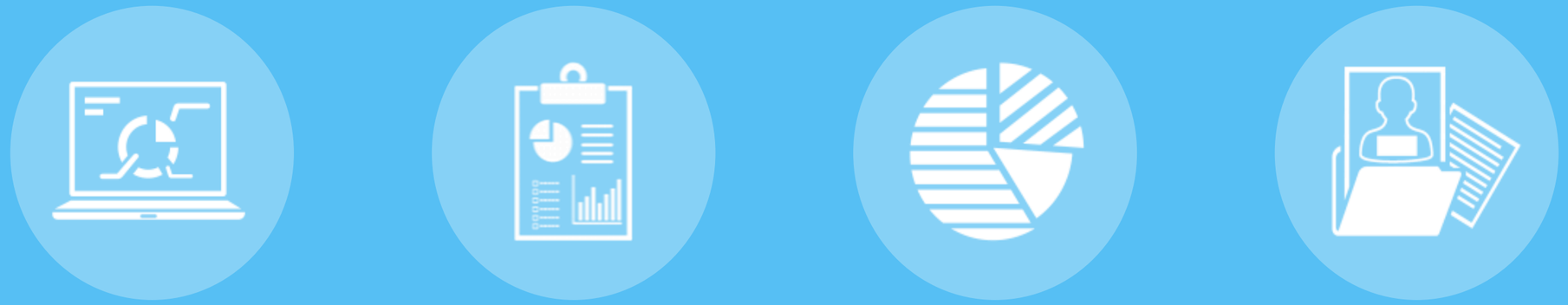
AWS Solutions Architect—Associate Level

Lesson 11: Disaster Recovery



What You'll Learn

- Disaster Recovery and its importance
- Difference between traditional and Cloud Disaster Recovery practices
- Recovery Time Objective and Recovery Point Objective
- DR methodologies

Disaster Recovery Overview

Overview of Disaster Recovery

Disaster Recovery Definition

Disaster Recovery (DR) is the term used to prepare for and recover from a disaster. A disaster can include anything that puts your organization's operations at risk:

- Cyber Attacks
- Equipment Failures
- Natural Disasters
- Terrorist Attacks

Disaster Recovery

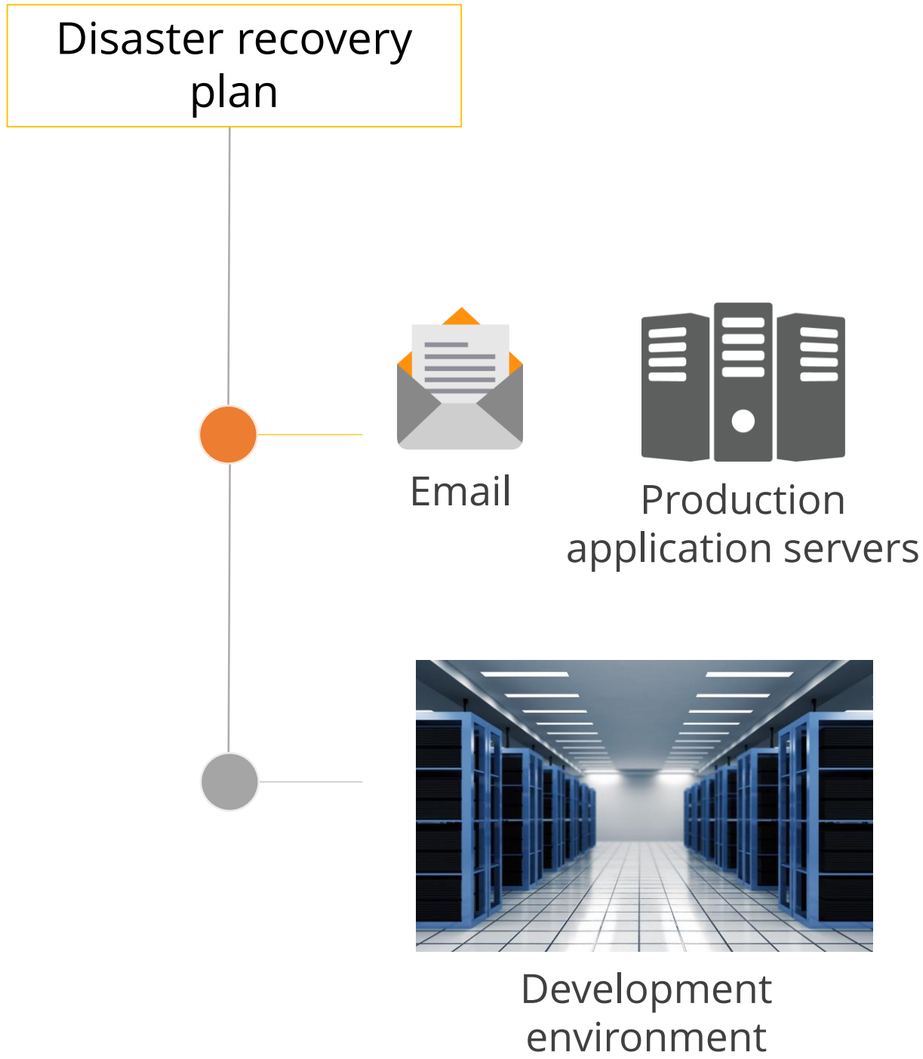
Failure to have a Disaster Recovery plan means that your organization faces significant downtime and financial loss in the event of a disaster.

Significant Downtime

Financial Loss

Disaster Recovery Plans

Disaster recovery plans aim to minimize the impact of a disaster by training employees and documenting the Disaster Recovery process, so it can be executed quickly, efficiently, and safely.



Traditional Disaster Recovery

Following the traditional methods of Disaster Recovery, companies duplicate their environments to another data center in a location remote to the primary site.

The remote data center infrastructure has to be purchased, installed, and maintained so it is ready whenever it is required.

The Disaster Recovery site is often under-utilized or over-provisioned, and is nothing but a wastage of money.

Cloud Disaster Recovery

With AWS you can bring up a Disaster Recovery site in minutes in locations all over the world and pay for it only when you are using it.

- Regions and Availability Zones
- New regions coming soon

Traditional Versus Cloud

The following table lists the differences between traditional and Cloud followed Disaster Recovery methodologies:

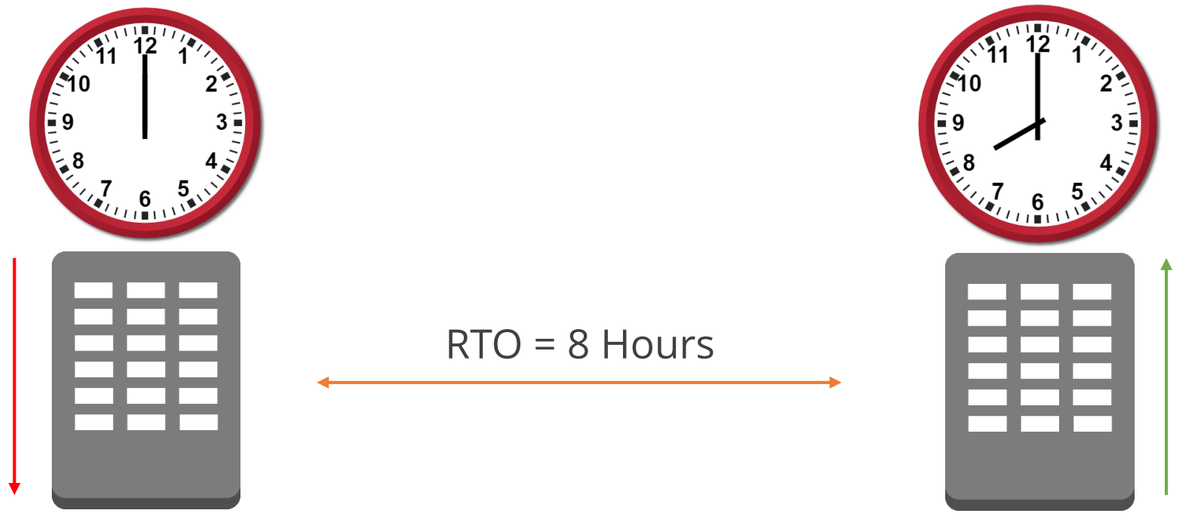
	Traditional	AWS
Facilities: Data centers, power, and cooling, and so on	User responsibility	AWS responsibility
Security to ensure the physical protection of assets	User responsibility	AWS responsibility
Suitable capacity to scale the environment	User responsibility	AWS responsibility
Support for repairing, replacing, and refreshing the infrastructure	User responsibility	AWS responsibility
Internet service provider contracts to provide bandwidth utilization for your environment under full load	User responsibility	AWS responsibility
Network infrastructure such as firewalls, routers, switches, and load balancers	User responsibility	AWS responsibility
Enough server capacity to run mission critical services	User responsibility	AWS responsibility

RTO Versus RPO

Two important considerations with Disaster Recovery are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

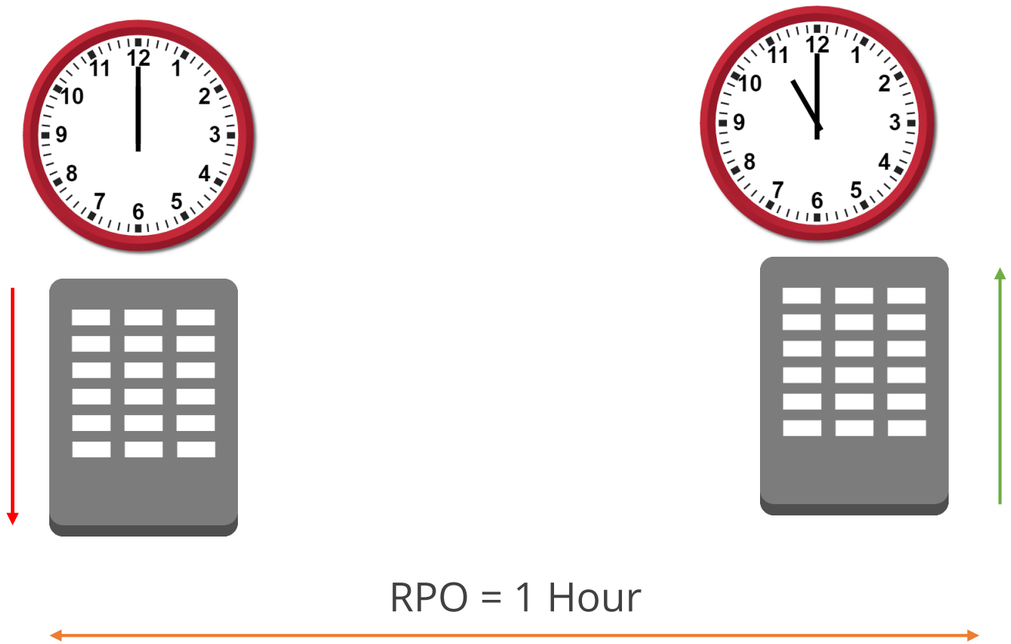
Recovery Time Objective (RTO)

Recovery Time Objective (RTO) is the time it takes after a disruption to restore business processes to its acceptable service level.



Recovery Point Objective (RPO)

Recovery Point Objective (RPO) measures the acceptable amount of data loss measured in time.



Knowledge Check

KNOWLEDGE CHECK	Which of the following statements correctly defines Recovery Point Objective?

a. The time it takes after a disruption to restore a business process to its service level

b. How to prepare for and recover from a disaster

c. The acceptable amount of data loss measured in time

d. The point in the recovery plan that IT needs to start from

KNOWLEDGE CHECK

Which of the following statements correctly defines Recovery Point Objective?

a. The time it takes after a disruption to restore a business process to its service level

b. How to prepare for and recover from a disaster

c. The acceptable amount of data loss measured in time

d. The point in the recovery plan that IT needs to start from

The correct answer is **c**

Recovery Point Objective measures the acceptable amount of data loss measured in time.

Using AWS Products for Disaster Recovery

Details about how AWS products can be used for Disaster Recovery

AWS Products for Disaster Recovery

The AWS products and services involved in Disaster Recovery process are:

Compute

EC2

AMI

ELB

Storage

S3

Glacier

EBS

EFS

Import/Export

Storage Gateway

Databases

RDS

DynamoDB

Redshift

Networking

Route 53

VPC

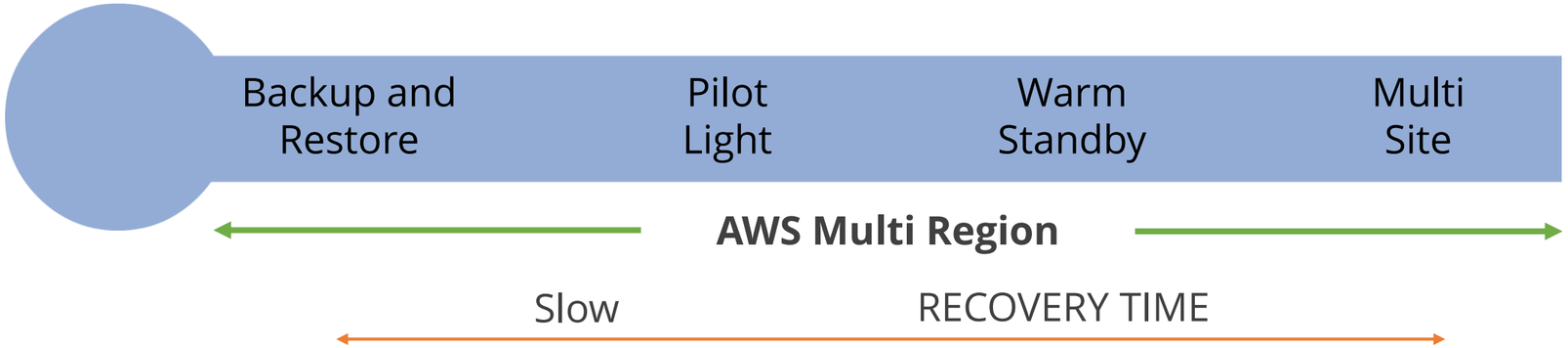
Direct Connect

Deployment

CloudFormation

Disaster Recovery Methodologies

Four DR methodologies of AWS are the following:



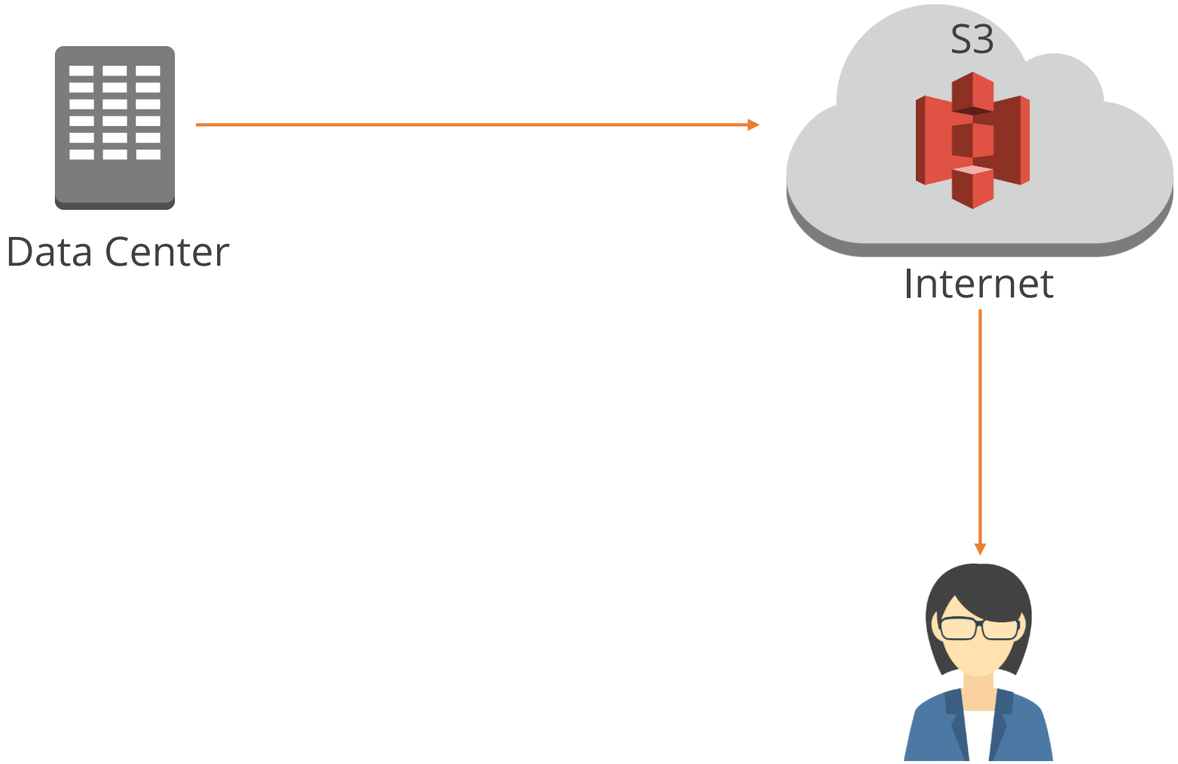
Backup and Restore

Data is backed up using tape, disk, and so on, and sent off-site for storage. It is usually done on a daily basis. In the event of a disaster, data is recovered from the backup tapes and restored; but it can take a long time.

Backup and restore is the most basic recovery technique.

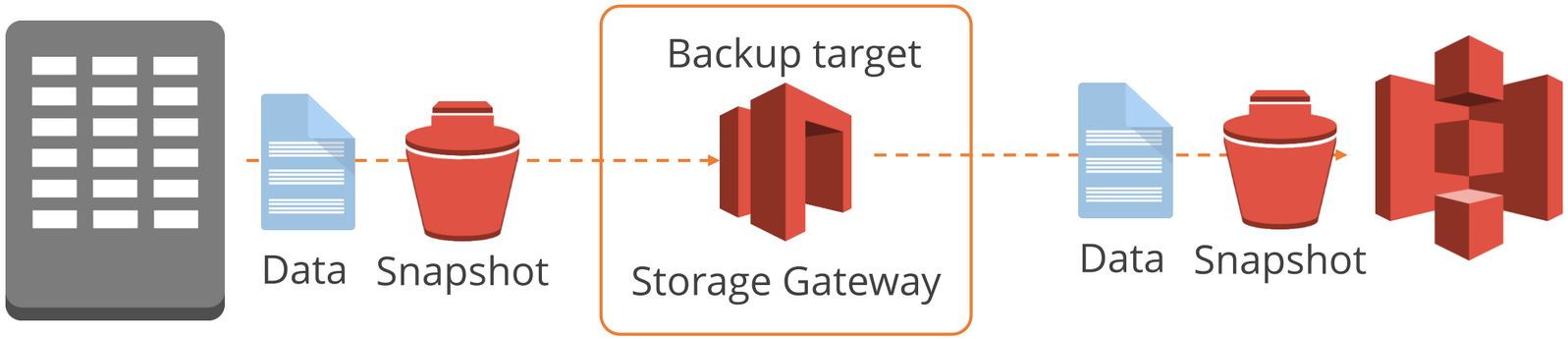
AWS Backup and Restore

With AWS you can back up your data to Amazon S3 rather than to tapes. The back-up data is available whenever required over the Internet.



AWS Backup and Restore (contd.)

AWS Storage Gateway allows you to store important data on Amazon S3. You can copy snapshots of your data volumes to Amazon S3 for safe keeping.



Backup and Restore Key Steps

The key steps to configure backup and restore are as follows:

- Select an appropriate tool or method to back up the data into AWS
- Ensure you have an appropriate retention policy for this data
- Ensure appropriate security measures are in place for this data
- Regularly test the recovery of this data and the restoration of your system

Pilot Light

Pilot light allows you to run a minimal version of your environments in the cloud. In case of a disaster, you can scale up the standby copies of your core systems up to production capacity. In pilot light the RTO is medium and the RPO is low-to-medium depending on the frequency of replication.

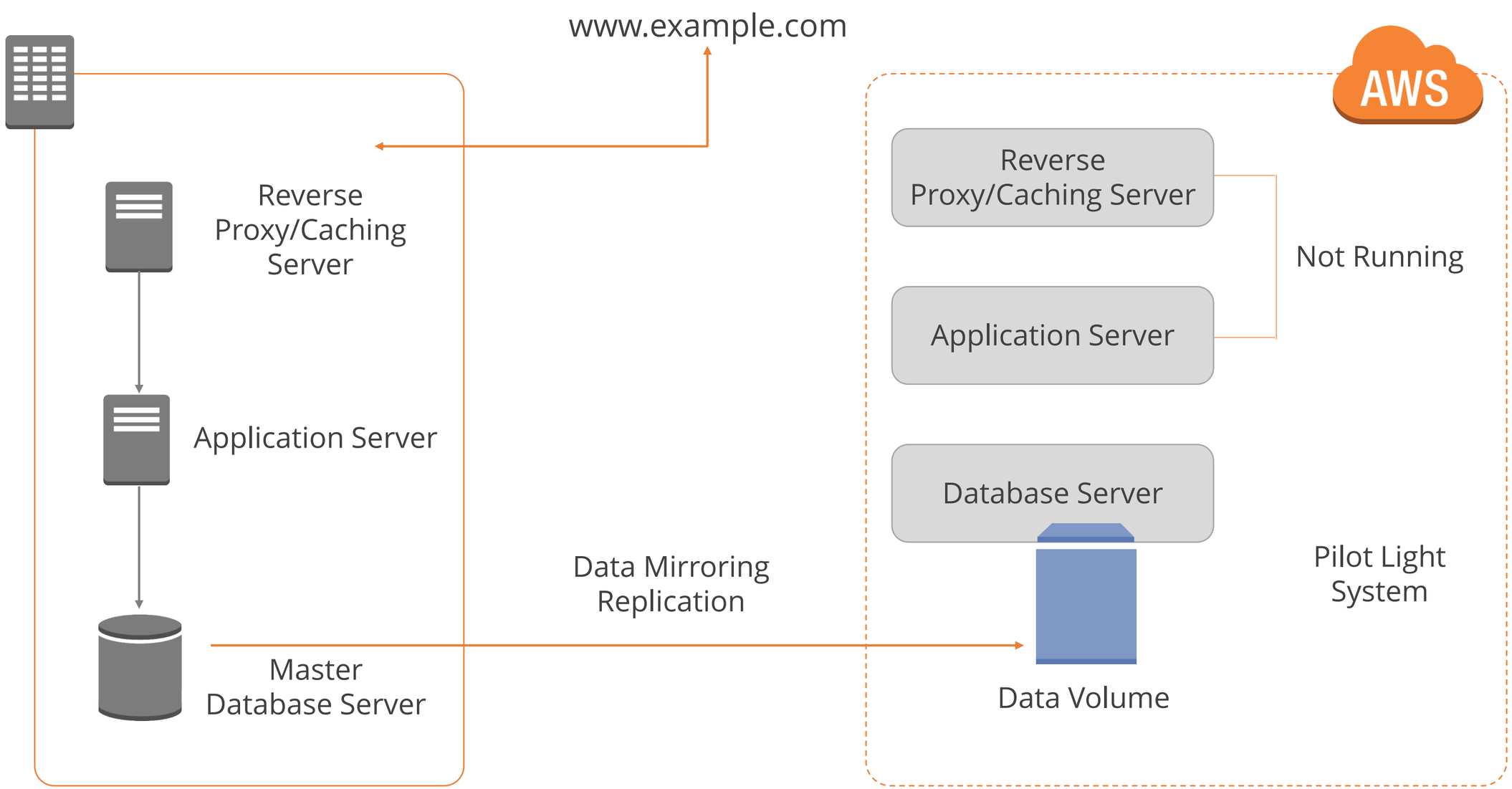
AWS Pilot Light

The products and services that provide pilot light are as follows:

Amazon RDS/EC2	Build replicas of your primary instances on RDS/EC2 instances and replicate data to them via AWS Database Migration Services or Amazon S3 buckets
Amazon Machine Images	Ready-to-deploy AMIs of your business infrastructure that can be quickly and easily brought online
Elastic Load Balancing	Used to point your traffic to the newly created AWS resources via an ELB using DNS

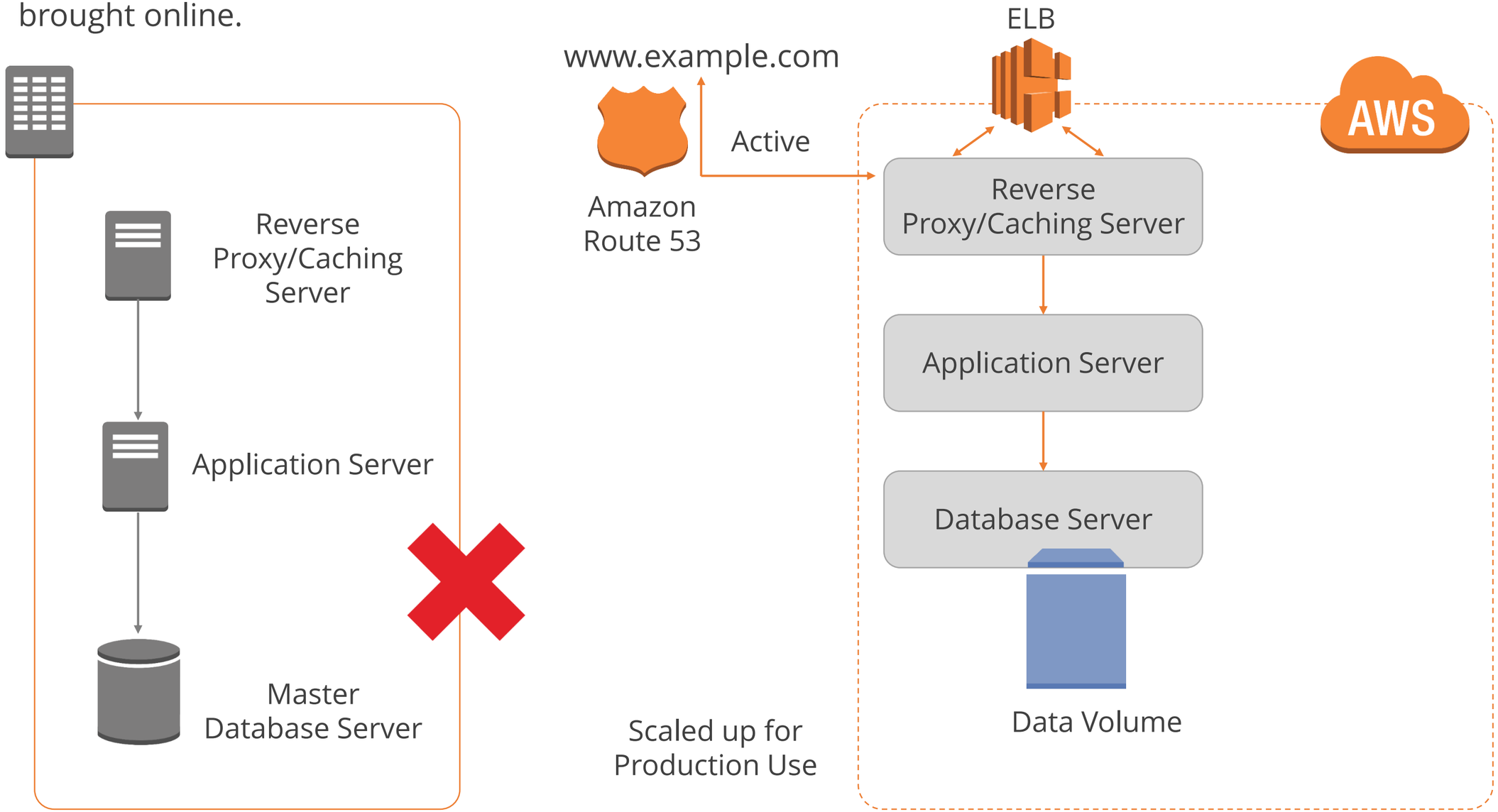
AWS Pilot Light (contd.)

The diagram shows a pilot light configuration of a web server.



AWS Pilot Light Failover

The diagram represents a scenario of a failover in the primary site, the pilot light environment is brought online.



Pilot Light Key Steps

The key steps to configure pilot light are as follows:

- Ensure you have all supporting custom software packages available in AWS
- Create and maintain AMIs of key servers where fast recovery is required
- Regularly run the servers, test them, and apply any software updates and configuration changes
- When using Amazon RDS turn on multi Availability Zones to improve resilience
- Use Route 53 to point traffic at the Amazon EC2 servers

Warm Standby

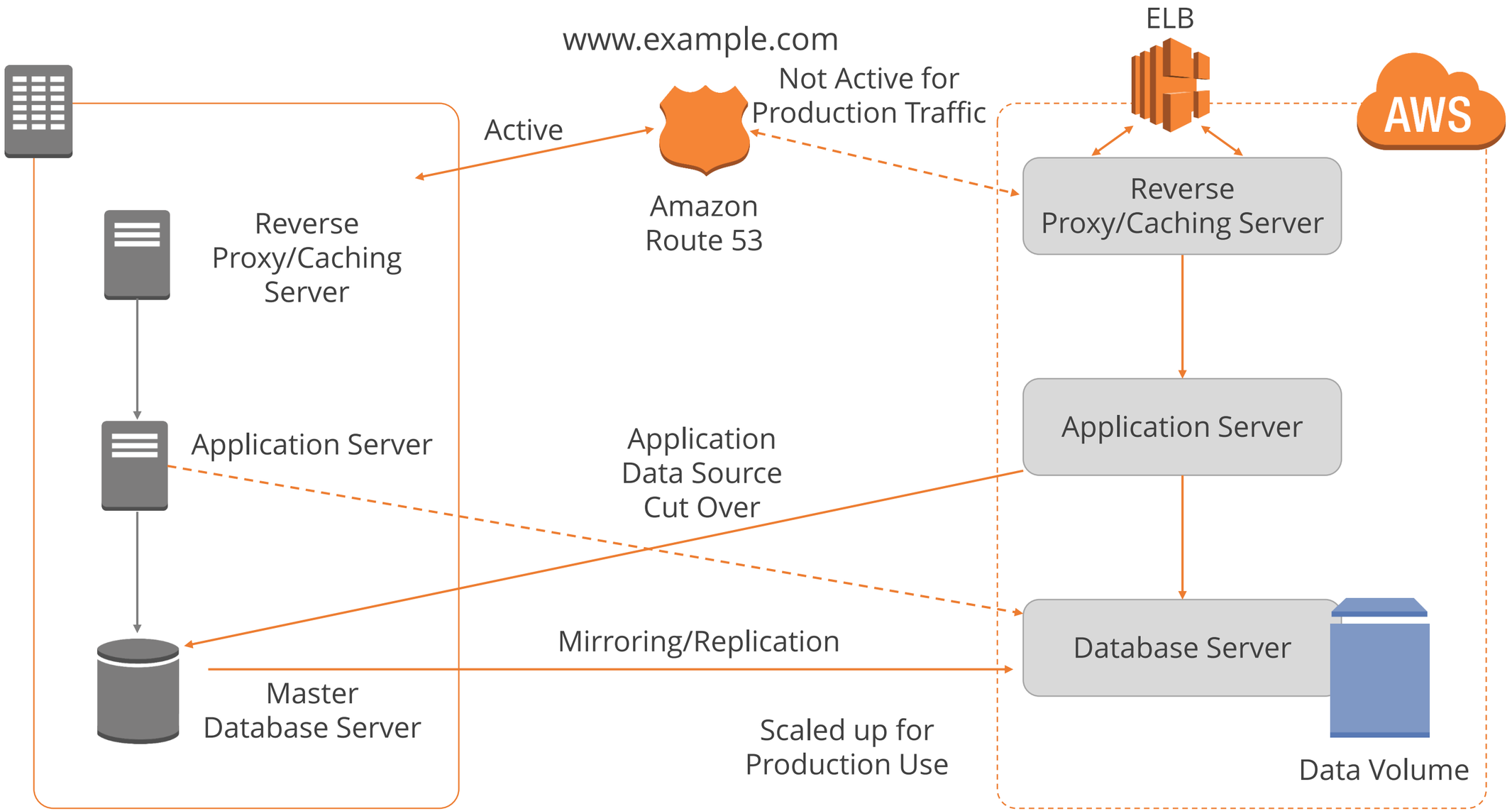
It extends the idea of pilot light by running a scaled down version of a fully functional environment always running in the Cloud.

The method decreases recovery time as the critical systems are already operational. The warm standby site can either be on instances ready for production or on lower sized instances that can be scaled as required.

The RTO is low to medium and the RPO is low.

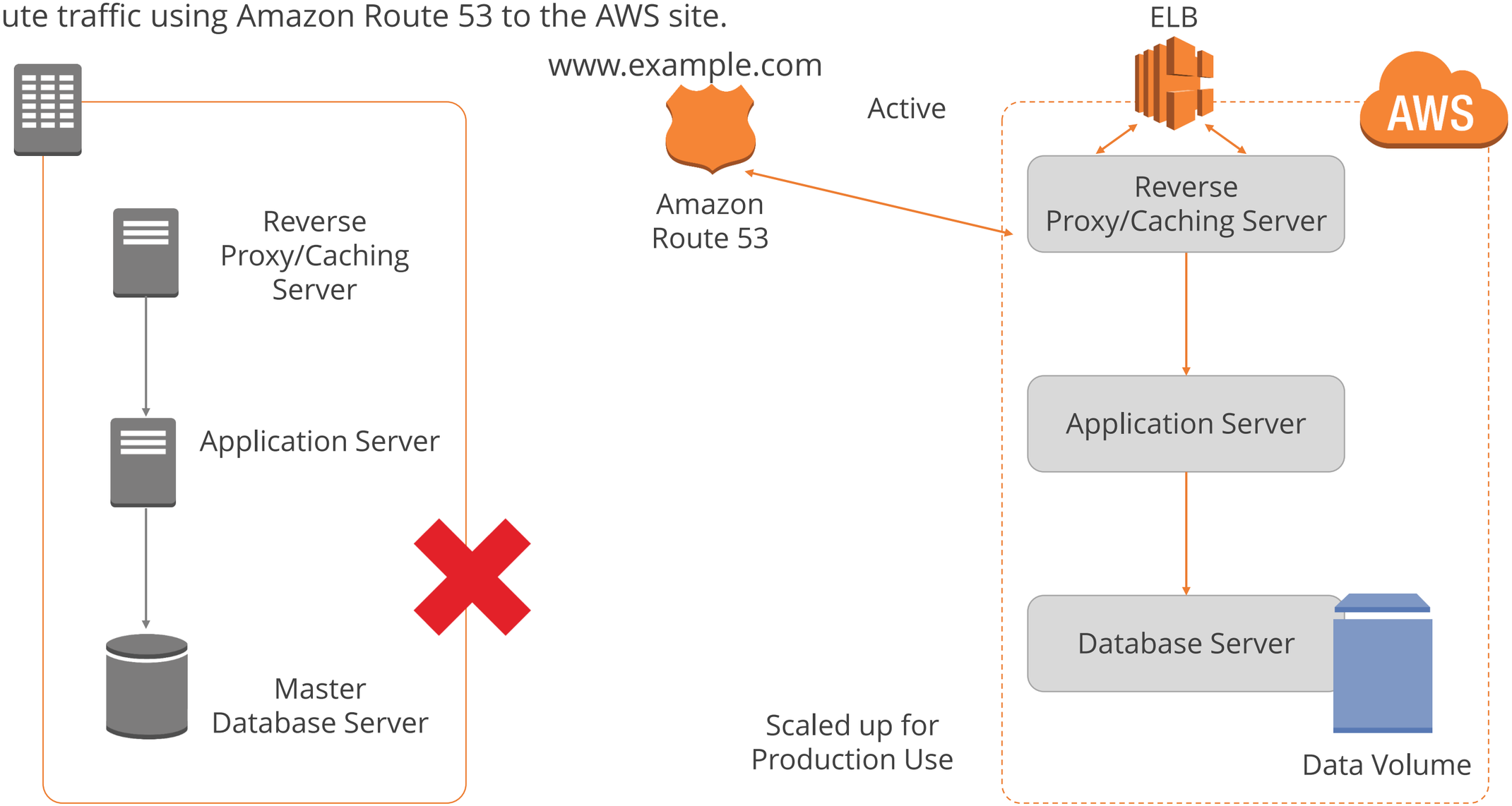
AWS Warm Standby

The diagram represents an AWS warm standby scenario.



AWS Warm Standby Failover

The diagram represents a scenario of a failover. In case of a failover at the primary site you can just simply reroute traffic using Amazon Route 53 to the AWS site.



Warm Standby Key Steps

The key steps to configure warm standby are as follows:

- Set up Amazon EC2 instances to replicate or mirror data
- Run your application using a minimal footprint of AWS infrastructure and scale in a DR situation
- Patch, update, and change configuration files in line with your live environment
- Use Route 53 to point traffic at the Amazon EC2 servers
- Use Auto Scaling to right-size your resources to accommodate the increased load

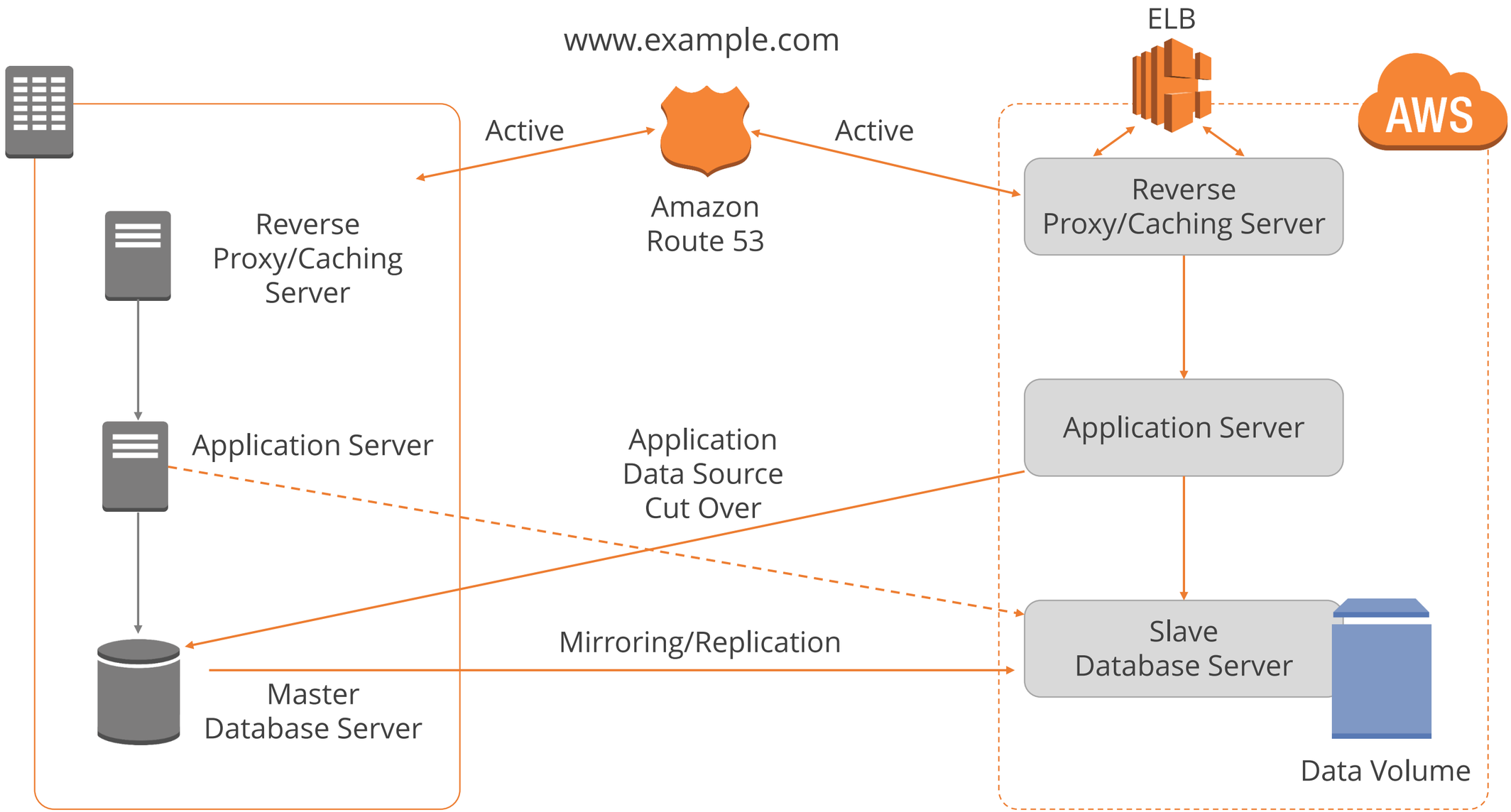
Multi-Site

In the multisite scenario the infrastructure runs both in AWS and in existing on-premise sites in an active-active configuration.

Users can use both sites. You can direct the user traffic via Route 53 weighted routing.
In this case the RTO is short and the RPO is very low.

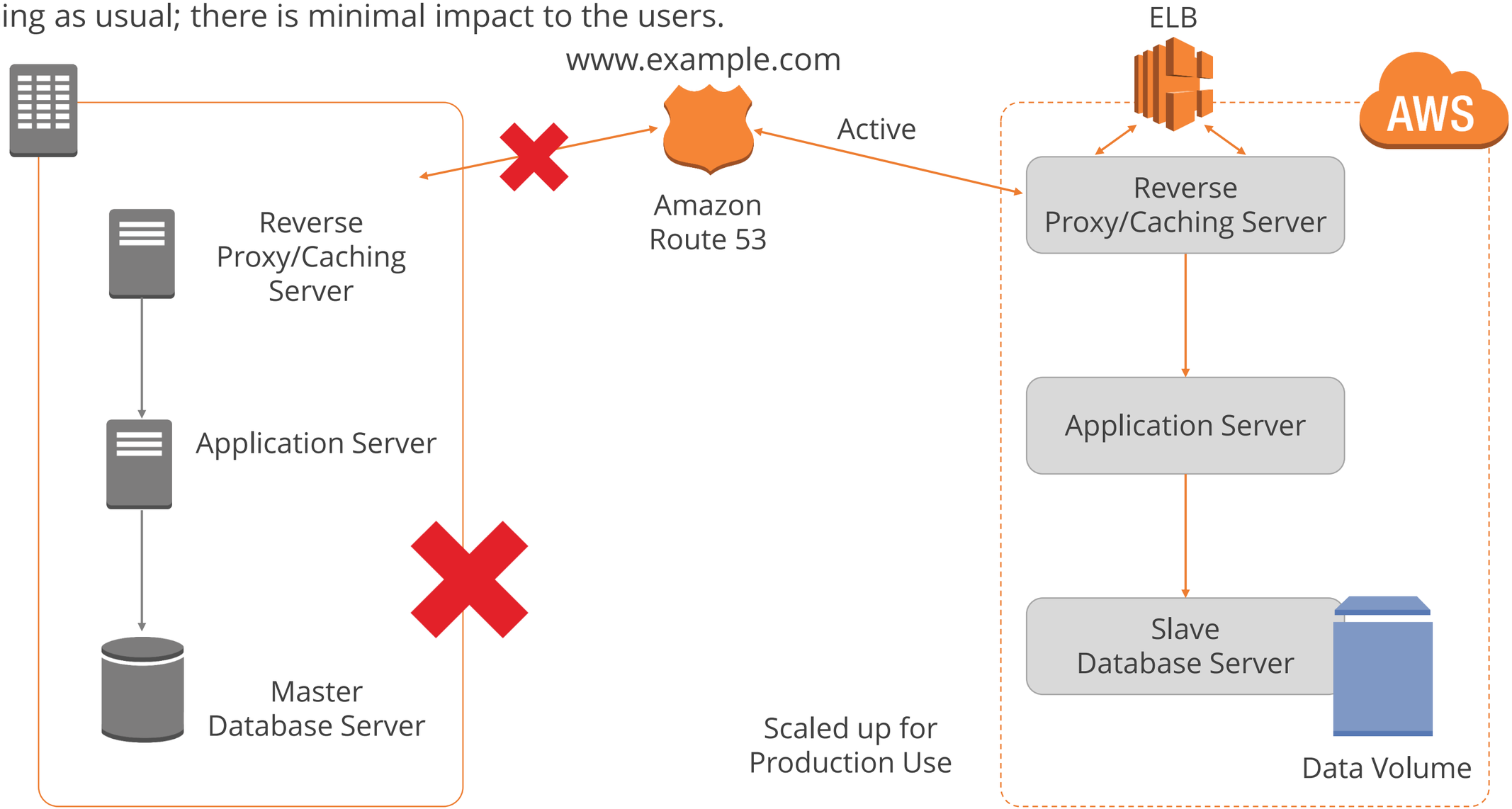
AWS Multi-Site

The diagram presents a multi-site scenario.



AWS Multi-Site Failover

In the event of a DR, Amazon Route 53 blocks traffic to the corporate data center. The AWS site keeps running as usual; there is minimal impact to the users.



Multi-Site Key Steps

The key steps to configure multi-site availability are as follows:

- Configure AWS environment to duplicate your production environment
- Configure DNS weighting to distribute requests to both sites and redirect traffic away from sites in Disaster Recovery situation
- Use failover application logic to use the local AWS database servers for all queries
- Use Auto Scaling to automatically right-size the AWS fleet

AWS to AWS DR

Implementing Disaster Recovery becomes easier if you use AWS for both production and failover sites.

- No need to negotiate contracts with another provider in another region
- Use the same underlying AWS technologies across regions
- Use the same tools or APIs

Improve your DR plan

Testing	AWS allows you to easily test DR scenarios: full site loss, viruses affecting a subset of core services
Monitoring and alerting	Use CloudWatch to monitor thresholds and KPIs to ensure your services are always ready
Backups	Ensure that the backups work by restoring them onto easily created AWS resources and environments.
User Access	Use AWS IAM to ensure that your users have the correct access to your DR environments
Automation	Automate the deployment of your DR environments using tools such as AWS CloudFormation or Auto Scaling

Knowledge Check

KNOWLEDGE CHECK

Which Disaster Recovery methodology offers the lowest RTO?

a. Backup and restore

b. Pilot light

c. Warm standby

d. Multi-site

KNOWLEDGE CHECK

Which Disaster Recovery methodology offers the lowest RTO?

a. Backup and restore

b. Pilot light

c. Warm standby

d. Multi-site

The correct answer is **d**

Multi-site offers the lowest RTO as infrastructure runs both in AWS and in existing on-premise sites in an active-active configuration.

Practice Assignment: Disaster Recovery

Calculate RTO and RPO

Disaster Recovery Assignment

Your company is concerned about the RTO and RPO of their accounting database, which is used to store important accounting data and run reports.

Management wants to have an RTO < 1 hours and RPO < 15 minutes.

You need to calculate the maximum RTO and RPO for the accounting database to see if it meets the proposed SLA and if it doesn't, suggest an infrastructure solution using AWS.

Accounting database backup details:

- Backed up to tape at 10PM each night
- Tapes are rotated at 9AM each morning and taken offsite
- Retrieval time for the tapes is 4 hours
- It takes 2 hours to restore the database from a backup

Key Takeaways

Key Takeaways

- Disaster Recover (DR) is the term used to prepare for and recover from a disaster.
- With traditional Disaster Recovery methodologies the Disaster Recovery site remains often under-utilized or over-provisioned and normally just wastes money.
- Two important considerations with Disaster Recovery are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- Four DR scenarios that showcase how AWS can be used are: Backup and Restore, Pilot light, Warm standby, and Multi-site.

This concludes “Disaster Recovery.”

The next lesson is “Troubleshooting.”