AWS Academy Cloud Architecting 2.x - Capstone Project

2023, S2 version

Project overview

This project provides you with an opportunity to use the solution design and implementation skills that you have developed throughout this course. You will do this for the customer scenario described below.

To implement this project, use the non-destructive AWS Academy Learner Lab facility provided to you. This Learner Lab facility comes with $100 student credit, and a lab environment that does not destroy resource even after lab timer expiry. *However, the Learner Lab will suspend some resource during lab timeout, and will attempt to reactivate that resource when you return to the Learner Lab (e.g.: this may happen to EC2)*. This is all to help you save costs.

More information on AWS Learner Lab is available here.

You are required to apply cloud architectural design principles, and implementation skills to:

- Deploy a PHP application that runs on an Amazon Elastic Compute Cloud (Amazon EC2) instance.
- Create a database instance that the PHP application can query.
- Create a MySQL database from a structured query language (SQL) dump file.
- Update application parameters in an AWS Systems Manager Parameter Store.
- Secure the application to prevent public access to backend systems.
- **Challenge**: Extend the network "Data Tier" through a VPN (virtual private networks) Tunnel to create a Hybrid Network, then migrate a copy of the database to an On-Premises Database-engine. (i.e.: we are creating an on-site backup and bringing it in-service).

Some resources are listed at the end of this document to help with this implementation project. You may also need to refer to previous BCCS355 course labs on database and other topics, to be able to complete this project – particularly you may want to revisit "Module 5 Challenge Lab: RDS Migrate" and associated demo video.

Customer Scenario: Example Social Research

Example Social Research is a (fictitious) non-profit organization that provides a website for social science researchers to obtain global development statistics. For example, visitors to the site can look up various data, such as the life expectancy for any country in the world over the past 10 years.

Shirley Rodriguez, a researcher at the organization, developed the website. She thought it would be valuable to share the data that she had gathered with other researchers.

History of Customer Scenario (Setting up "As-Found" State)

Shirley stored the data in a MySQL database and made the data available through a PHP website she built. She initially published the site through a commercial hosting company that provides limited support for technical issues and security.

Over the past year, Shirley's website has grown in popularity. As a result of increased traffic, she started receiving complaints that the site is not as responsive as it used to be. She also experienced an attempted ransomware security breach. The security breach was unsuccessful, but her supervisor, Mateo Jackson, suggested that Shirley investigate new ways to host the website.

As-Found

Shirley heard about Amazon Web Services (AWS), and initially moved her website and database to an EC2 instance that runs in a public subnet. The database now runs on a MySQL engine installed *on* the same EC2 instance as the web front-end – i.e.: data has not yet been decoupled.

AWS Capstone Project ACAv2 (extended version)

As you know we have extended the AWS Capstone Project to ensure you have a challenge that fits with NZQA Level 7. We have extended the lab in two ways:

1. you are expected to implement Shirley's "As-found" state – i.e.: an EC2 that hosts web front-end AND the database engine. (i.e.: Your AWS Learner Lab environment will not automatically set up "as-found" state).
2. You will implement a VPN Tunnel to create a Hybrid network.

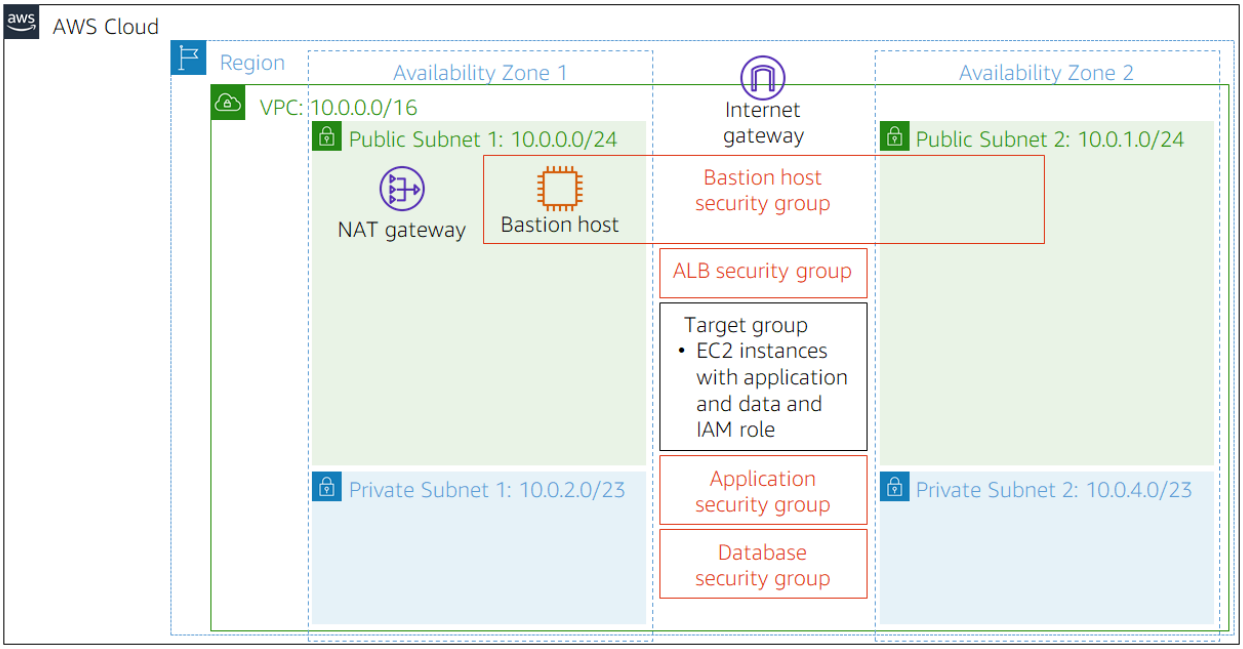
Below you will find some tips on how to set up the "as-found" state.

Shirley's Request for Cloud Architecting Services

After you have set up "as-found" state, move on with the scenario:

Shirley approached *your cloud architecting company* to make sure that her current "as-found" design follows best practices. She wants to make sure that she has a robust and secure website. *One of your colleagues started the process of migrating the site to a more secure implementation (part of "as-found"), but they were reassigned to another project*.

Your need to move on from as-found to make sure that the website is secure and to confirm that the website returns data from the query page. The following summary lists the solution requirements for completion and provides a diagram of the current "as-found" environment.



Solution requirements

Setup:
You will be using the AWS Academy Learner Lab, so unlike other labs in the course the "As-found" state is NOT set-up. As mentioned, you need to start by creating this “as-found state” described above.

Information to do this is contained in this tips Moodle sub-page.

After you have set up “as found state”, move on to do the following tasks:

- Provide secure hosting of the MySQL database on a decouple data-tier using an AWS managed service.
- Provide secure access for an administrative user
- Provide anonymous access to web users
- Run the website on a t2.small (or t3.small) EC2 instance, and provide Secure Shell (SSH) access to administrators
- Provide high availability to the website through a load balancer
- Store database connection information in the AWS Systems Manager Parameter Store
- Provide automatic scaling that uses a launch template
- Extend the Data Tier through VPN Tunnel, to create a Hybrid Network,
- Copy a backup of the Database sqldump file to on-premise
- Advanced:
    - Implement an On-Premise database engine, and import the copied sqldump file
    - By changing connection information in the Parameter Store – prove that the Web Tier now connects successfully through the VPN Tunnel to the On-Premise database

The following parameters are used by the PHP application to connect to the database. It will need to refer to the AWS Systems Manager Parameter Store. (*You should remember a similar approach was used in your previous database lab*):

- /example/endpoint
- /example/username
- /example/password
- /example/database

These parameter values are case sensitive.

Project deliverables

To complete this assignment, you must:

- Deploy a PHP application (in a separate data tier) that meets the system requirements outlined above
- Deploy a VPN Tunnel to achieve a Hybrid Network with On-Premise
- Backup database file to On-Premise
- Advanced: Deploy dB into on-premise mySQL engine, and change AWS Parameter Store and routes such that the cloud front-end connects to the on-premise dB (through VPN).

  Refer to the marking rubric appendix.

Design Document and Implementation Evidence Video

There are two major parts to your submission:

Part One: Submit a Design Document:

- A written summary of the design decisions that you made to achieve the result.
- A topology diagram that illustrates your solution

Part Two: Submit an Implementation Evidence Video:

- Screen-capture video and commentary evidence of your working solution, including:
  - Proof that the mysqldump database file has been migrated to an AWS RDS Server and is working*
  - Proof that the web-tier front end is working and interacting with the database (sql lookups).
  - Proof the Auto-Scaling is working (find a method of stress testing to do this)
  - Proof of Hybrid Network configuration; evidence tunnel is up, and proof of connectivity.
  - Evidence that database has been backed up to On-Premise.
  - Extended Challenge:
    - Implement an on-premise mysql engine.
    - Evidence that web-tier can be redirected to use on-premise database, by updating AWS Systems Manager Parameter Store

It is a good idea to start your video showing your topology diagram design.
In terms of style of video – you could choose to show all the setups steps, or you could give an after-setup tour.
Either way **your video must show all the technical elements that create your solution and prove that it is working, PLUS prove that it your own work** (e.g.: unique identifiers such as AWS account ID).

Help on Creating an Evidence Video:

A Moodle page has been set up outlining how to install Panopto Screen Capture and Video Editing software. A demo video showing how to use Panopto is included.
Some people may prefer to use other software such as OBS Studio and OpenShot editor. Other options: Kdenlive (questions to Flynn).

Note: You are developing customer presentation skills by making a video. This is desirable, because many IT employers want to hire employees that have good customer skills (HR people call this soft skills).

Support Assets for setup of As-Found

Support resources for various elements including for setting up “as-found” condition.

- User-data script for web-tier
- Launch Template for Auto-Scaler
- A second Tips document on VPN Implementation is also available

Support Assets for completing the project

You can use the following assets for this project:

- A SQL dump file that contains sample data
- A .zip file that contains the PHP and image files for the Example Social Research Organization website

Access to AWS Parameter Store - IAM Role

If you are using the AWS Learner Lab (with its US$100 credit) for completing this implementation project, you will be aware it restricts resources you have access to. There should be enough resource permissions to complete this project.

Launched instances need to have a suitable IAM Instance Profile (IAM Role) applied. In the Learner Lab use **LabRole**. It will give permission to retrieve the Systems Manager Parameter Store vales to connect to the RDS Database.

But if you are using your own private AWS account you can create your own IAM Role for this. See the special tip at the end of this page (follow link) to see a suitable role and policy definition.

Marking Rubric 2023

Categories	Seq	Marking Elements	Maximum points for element	Sub-Total for Category
1) VPC & Networking	a	Subnets are suitable & Public /Private Tiers	1.67	
1) VPC & Networking	b	Separate Routing Tables (to achieve public and private tiers)	1.67	
1) VPC & Networking	c	Internet Gateway	1.67	
1) VPC & Networking	d	Application Load Balancer	1.67	
1) VPC & Networking	e	NAT Gateway implemented	1.67	
1) VPC & Networking	f	Private Route Table has default route to NAT Gateway	1.67	10
2) Elasticity	a	Auto-Scaling of Web /App Tier	3.33	
2) Elasticity	b	AS Launch Template & user-data script appropriate	3.33	
2) Elasticity	c	App Instances become part of ALB targets	3.33	10
3) Security	a	IAM Role for Parameter Store access for EC2 (Web-Tier)	2.5	
3) Security	b	Security Groups Data Tier	2.5	
3) Security	c	Security Groups Web /App Tier	2.5	
3) Security	d	Secure Bastion Host for management access implemented	2.5	10
4) Web /php	a	Website /php is functional	10	10
5) Database	a	AWS Systems Manager Parameter Store: Parameters are appropriate for RDS connectivity	2.5	
5) Database	b	mySQL database dump file successfully copied to RDS	2.5	
5) Database	c	Proven that Web site can query the RDS database successfully	2.5	
5) Database	d	Database located in private subnets (subnet groups)	2.5	10
6) VPN /Hybrid Network	a	Private Route Table also has on-premise route to VPG	3.33	
6) VPN /Hybrid Network	b	Proven VPN can carry payload traffic	3.33	
6) VPN /Hybrid Network	c	VPN Tunnel is up	3.33	10
7) Advanced	a	Backup: Send a copy of sql dump file through VPN to on-premise	2.5	
7) Advanced	b	Backup: Implement an on-premise dB engine, and import the sql dump file.	2.5	
7) Advanced	c	System Fail-over: Update AWS Systems Manager Parameter Store to point to the backup engine	2.5	
7) Advanced	d	System Fail-over: Prove that AWS Php front end can query this on-premise backup database - in effect, through VPN networking.	2.5	10
8) Design and Video Evidence	a	Topology Diagram that illustrates your solution	5	
8) Design and Video Evidence	b	Written summary of the design decisions that led to achieving the solution requirements	5	
8) Design and Video Evidence	c	Video submission showing implementation evidence	5	20

8) Design and Video Evidence	d	**Soft Skills /Customer Skills**: Quality of commentary - are the solution elements clearly described?	5	
9) Evidence Quality	a	Quality of functional evidence? i.e.: Video-Evidence Must include proof that this is student's own implementation (eg: Unqiue IDs for Account; VPC; subnet; RDS etc) Note: Any reasonable suspicion of plagiarism will bring a demerit across the entire project.		10
Grand Total				100