AWS Cloud & Big Data Architectures : Project

Jean-Pascal MEWENEMESSE

AUPIAIS--BERTHY Elvin
BLANC Monica-Pauline
JAMINON Hugo
../07/2023

Architecture Design Explanation

The project aims to deploy a PHP application on an Amazon EC2 instance and utilize Amazon RDS to create a private MySQL database from an SQL dump file. The website is for a fictional nonprofit organization called Example Social Research Organization, which provides global development statistics to researchers. The current hosting provider lacks responsiveness and security, prompting the organization to explore AWS.

Within the VPC (Virtual Private Cloud) with an IP address range of 10.0.0.0/24, there is a public subnet with the IP range of 10.0.0.0/25 and a private subnet with two IP ranges: 10.0.1.128/26 and 10.0.0.1.192/24 :

- Public subnet : It contains a security group that includes the EC2 instance (with the IP address 3.233.234.44) running Cloud9.
- Private subnets : They have their own security group and one of them is associated with the RDS (running MariaDB). This security group ensures that only the eC2 instances within the public subnet can access the database.

Additionally, a route table is set up to manage and control the routing of traffic within each subnet (public and private).

To establish internet connectivity for the VPC, an internet gateway is placed at the border of the VPC : it allows inbound and outbound traffic between the VPC and the internet. The arrow that connects the public subnet to the internet gateway indicates the connection between the VPC and internet.

Administrators can connect to the database securely from their local machines using EC2 Instance Connect. Web users have anonymous access to the website. The website runs on a t2.micro EC2 instance, and SSH access for administrators is provided through EC2 Instance Connect, eliminating the need for an AWS Key Pair. The infrastructure design includes an API Gateway endpoint in the VPC, allowing connections from the root user and the IAM Group.

IAM permissions are implemented with the principle of least privilege to ensure secure access. Database connection information, including endpoint, username, password, and database name, are stored securely in the AWS Systems Manager Parameter Store.

.

Answers to the two quiz

A. Network Quiz

Question 1 : Which definition describes a VPC ? **Option 3**

A Virtual Private Cloud created using AWS cloud allows the user to logically isolate and control the network environment for the user's AWS resources. When the user uses a VPC, it can easily define its own IP address range, subnets, routes…

Question 2 : Which subnets addressing scheme meets the requirements and follows AWS best practice ? **Option 3**

In order to choose the one which meets the requirements, we have to be sure that it will support 100 usable addresses now and a potential growth up to a max of 254 usable addresses per subnets. The subnet addressing scheme that meets the requirements and follow AWS best practice is :

- Subnet A: 172.16.0.0/23 (512 addresses)
- Subnet B : 172.16.2.0/23 (512 addresses)

because it allows 512 usable addresses in each subnet, accommodating the 100 usable addresses, leaving space for the 254 usable addresses for the future.

Question 3 : Which combination of actions enable direct internet access for IPv4 hosts in a VPC ? **Option 1 & Option 3 & Option 6**

- **Option 1 :** By creating a route for 0.0.0.0/0, it ensures that all traffic destined for the internet is directed to the internet gateway
- **Option 3 :** Configuring hosts in order to have or obtain an internet-routable address will allow the hosts to communicate directly with the internet (as we have to configured either public or private IP addresses within the VPC in order to be later translated to public IP addresses using NAT)
- **Option 6 :** By configuring security groups and network access control lists to permit internet traffic allow inbound but also outbound internet traffic

Question 4 : How should the instances launch ? **Option 4**

In order to launch EC2 instances in a way that can download updates from the internet but without being accessible from the internet, they have to be launched without public IP addresses, in a subnet with a default route to a NAT gateway.

Why ? Launching it without public IP addresses prevents the instances from being accessible from the internet. Nevertheless, instances have to communicate with the internet in order to download updates so a NAT gateway has to be used. Indeed, the subnet should have a default route pointing to the NAT gateway in order to allow the instances to access to the internet while their own traffic seemed to come from the NAT gateway's IP address.

B. IAM Quiz

a) Folder IAM Quizz

Question 1 : Which statements describe AWS Identity and Access Management (IAM) users ? **Option 3**

In IAM, each user created within an AWS account must have a unique name which ensures that each IAM user can be uniquely identified and managed.

Question 2 : How can you grant the same level of permissions to multiple users within an account ? **Option 1**

An IAM group is used in order to group several users and manage them easily. So, by creating a group and creating a policy for this group, you can grant the same level of permissions to the several users that are in this group.

Question 3 : Which statements describe IAM roles ? **Option 3 & Option 4**

- **Option 3 :** As you can see below in the documentation of IAM roles, IAM roles can be assumed by various entities as individuals, applications or services.

> Vous pouvez utiliser des rôles pour déléguer l'accès à des utilisateurs, des applications ou des services qui n'ont normalement pas accès à vos ressources AWS.

- **Option 4 :** As you can see below in the documentation of IAM roles, a role doesn't have an associated key access or standard identification information so a role provide temporary security credentials

utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle.

Question 4 : Which statement describes a ressources-based policy ? **Option 1**

A ressources-based policy can be applied to any AWS resources, it allows the user to define some permissions and access control (keyword allow or deny) for a specific resource it is attached to.

Question 5 : How does AWS IAM evaluate a policy ? **Option 2**

When an IAM policy is evaluated, it first checks if there is any deny statement : if there is, the access is immediately denied regardless of any allowed statement after. If there isn't, IAM will check if there is an explicit allow statement, if there is, the access is allowed. If there isn't, the access is denied by default.

Question 6 : How can you use AWS IAM to enable access to them ? **Option 3**

By creating an IAM user for each developer and then putting them all in a group and attaching the required IAM policies to the group will ensure that each developer has a unique identity and they can manage individually while providing a common permissions for each developer of the team. Moreover, putting them all in a group facilitates the management of their permissions.

Question 7 : How does identity federations increase security for an application that is built in AWS ? **Option 1**

Identity Federation enables users to use their existing authenticated identities in order to be able to access the AWS resources and applications. Instead of creating users and passwords for each application, users can use SSO to access the application through their existing authenticated identity.

b) IAM Policy in the subject

Question: What actions are allowed for EC2 instances and S3 objects based on this policy? What specific resources are included?

Based on the code, here is the actions allowed for EC2 instances and S3 objects :

- **EC2 instances :** `"ec2:RunInstances"` (creation of EC2 instances) & `"ec2:TerminateInstances"` (terminate the instances)
- **S3 objects :** `"s3:GetObject"` (retrieve S3 object) & `"s3:PutObject"` (Upload S3 objects)

In addition, it also include some ressources :

- EC2 instances - `"arn:aws:ec2:us-east-1:123456789012:instance/*"` which allow actions on all EC2 instances in us-east-1 region belonging to AWS account 123456789012
- S3 object - `"arn:aws:s3:::example-bucket/*"` which allow actions on all objects within the S3 bucket named “example-bucket”

Question: Under what condition does this policy allow access to VPC-related information? Which AWS region is specified?

The condition is that the requested AWS region corresponds to us-west-2, we can see it with the condition that checks if the string of the requested region (`"aws:RequestedRegion"`)key is equal to “us-west-2”. If the requested matches, then policy will allow access to the VPC-related information.

Question: What actions are allowed on the "example-bucket" and its objects based on this policy? What specific prefixes are specified in the condition?

Based on this policy, here is the actions that are allowed on the “example-bucket” :

- `s3:GetObject` : Retrieve S3 Object
- `"s3:PutObject"` : Upload S3 Object

- `"s3:ListBucket"` : List of objects within the “example-bucket”

The specific prefixes are :

- `"documents/*"`
- `"images/*”`

Objects in the “example-bucket” with these prefixes are allowed to be accessed or modified.

Question: What actions are allowed for IAM users based on this policy? How are the resource ARNs constructed?

Based on this policy, here is the action allowed for the IAM users :

- `"iam:CreateUser"` : allowing creating IAM users
- `"iam:DeleteUser"` : allowing deleting IAM users

The ARNs ressources are constructed dynamically using `${aws:username}` which represents the username of the user making the request.
The ressource `"arn:aws:iam::123456789012:user/${aws:username}"` allow specific IAM users identified by their username to be created or deleted.

Questions:

Which AWS service does this policy grant you access to?

This policy grant access to all resources (with *) performing read-only operations within the IAM service. The read-only operation are specified in the policy in the actions array (`"iam:Get*"` & `"iam:List*"`)

Does it allow you to create an IAM user, group, policy, or role?

It does not allow to create an IAM user, group, policy, or role because the actions specified are only (`"iam:Get*"` & `"iam:List*"`) which means you can only retrieve information (read-only operations) and it does not include actions that can allow creating or modifying IAM entities.

Go to https://docs.aws.amazon.com/IAM/latest/UserGuide/ and in the left navigation expand Reference > Policy Reference > Actions, Resources, and Condition Keys. Choose Identity And Access Management. Scroll to the Actions Defined by Identity And Access Management list.Name at least three specific actions that the iam:Get action allows.*

We have several actions, here is three of them :

- **iam:GetGroup :** Grants permission to retrieve a list of IAM users in the specified IAM group
- **iam:GetRole :** Grants permission to retrieve information about the specified role, including the role's path, GUID, ARN, and the role's trust policy
- **iam:GetPolicy :** Grants permission to retrieve information about the specified managed policy, including the policy's default version and the total number of identities to which the policy is attached

Questions: What actions does the policy allow?

The policy allows any actions specified in the Action field because it provides a Deny effect.

Questions : Say that the policy included an additional statement object. How would the policy restrict the access granted to you by this additional statement?

The additional statement allow all action with “*” for the EC2 services. So, the user can perform any actions related to EC2 instances and resources. Nevertheless, we have a Deny effect so the Allow statement does not modify the restrictions imposed by the Deny statement. So, even with the Allow statement permitting all actions for EC2 instances, the Deny statement conditions restrict specific launch types as t2.micro and t2.small.

Questions: If the policy included both the statement on the left and the statement in question 2, could you terminate an m3.xlarge instance that existed in the account?

We say earlier that the deny policy denies specified launch types. Since the m3.xlarge instance does not fall into the denied instances type, the policy will allow it to terminate it.