**Cloud Computing CA 2**

**Jianyu He**

**D17124591**

**VPC Details**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VPC** | **Region** | **Purpose** | **Subnets** | **AZs** |
|  |  |  |  |  |
| 1 | EUROPE | Test/Dev | 8 | 2 |
| 2 | South America | Test/Dev | 8 | 2 |
| 3 | Southern California | Production | 8 | 2 |

Production VPC

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **VPC** | **Subnet type (Public/private)** | **AZ** |
|  |  |  |  |
| Public1 | 1 | Public | A |
| Public2 | 1 | Public | B |
| Web1 | 1 | Private | A |
| Web2 | 1 | Private | B |
| App1 | 1 | Private | A |
| App2 | 1 | Private | B |
| Database1 | 1 | Private | A |
|  |  |  |  |
| Database2 | 1 | Private | B |

TEST VPC

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **VPC** | **Subnet type (Public/private)** | **AZ** |
|  |  |  |  |
| Public1 | 2 | Public | A |
| Public2 | 2 | Public | B |
| Web1 | 2 | Private | A |
| Web2 | 2 | Private | B |
| App1 | 2 | Private | A |
| App2 | 2 | Private | B |
| Database1 | 2 | Private | A |
|  |  |  |  |
| Database2 | 2 | Private | B |

TEST VPC

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **VPC** | **Subnet type (Public/private)** | **AZ** |
|  |  |  |  |
| Public1 | 3 | Public | A |
| Public2 | 3 | Public | B |
| Web1 | 3 | Private | A |
| Web2 | 3 | Private | B |
| App1 | 3 | Private | A |
| App2 | 3 | Private | B |
| Database1 | 3 | Private | A |
|  |  |  |  |
| Database2 | 3 | Private | B |

**Security Details**

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Group** | **SG Name** | **Rule** | **Source** |
|  |  |  |  |
| ELB load balancer | Elb-sg | Allow 443 | 0.0.0.0/0 |
| Web Tier | Web-sg | Allow HTTP (80) | ELB |
| App Tier | App-sg | Allow 80 | Web-tier |
| Database Tier | Db-sg | Allow 1433 | App-tier |

|  |  |
| --- | --- |
| **Other Security Options** | **Justification** |
|  |  |
| AWS Certificate Manager | Use to Encryption data in transit |
| AWS Firewall Manager | makes easier to centrally configure and manage AWS WAF rules across your accounts and applications |
| AWS Key Management Service | create and control the encryption keys used to encrypt your data. |
| AWS WAF | helps protect your web applications from common web exploits |

**Encryption Options**

Based on the requirements, list your encryption options:

|  |  |
| --- | --- |
| **Requirement** | **Solution** |
|  |  |
| Encryption option for  **data at rest** | Use AWS KMS to create and control the encryption keys for encryption data at rest |
| Encryption option for  **data in transit** | Use AWS Certificate Manager to encryption data in transit |

**Instance Details**

Describe the type, size, and justification for the instances you will use for each tier.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tier** | **AMI** | **Tag** | **Type** | **Size** | **Justification** | **# of instances** |
|  |  |  |  |  |  |  |
| Web | SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type | **Key: Name** | t2 | medium | Six virtual machines (Two vCPUs/4-GB memory) | 6 |
|  |  | **Value: app-tier** |  |  |  |  |
|  |  |  |  |  |  |  |
| App | SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type | **Key: Name** | r5a | xlarge | Five virtual machines (Four vCPUs/32-GB memory) | 6 |
|  |  | **Value: web-tier** |  |  |  |  |
|  |  |  |  |  |  |  |
| DB | SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type | **N/A** | Db.p3 | 2xlarge | Two virtual machines (Eight vCPUs/48-GB memory /5.5-TB storage) | 2 |
|  |  |  |  |  |  |  |

**RPO Options**

**Q.** How would you achieve a Recovery Point Objective (RPO) offour hours?

Use Amazon Redshift Utils module to helps manage the Snapshots, then use aws Lambda to ensure cluster snapshots as frequently 4 hours.

**Document Storage**

How would you design document storage based on the requirements?

|  |  |
| --- | --- |
| **Storage/Archive** | **Detail** |
| **Option** |  |
|  |  |
| S3 | In first 3 months, the document and picture store in S3, after 3 month the document and picture move to aws Glacier, then delete those data from s3. |
| Aws Glacier | The data will keep 5 years, first 3 months will store in s3, after 3 months will store in aws glacier, if time expire then delete all data. |

**Web Tier Requirements**

|  |  |
| --- | --- |
| **Requirement** | **Solution** |
|  |  |
|  |  |
| Architecture must be flexible and handle  any peak in traffic or performance. | Web server design must create auto scaling to allow service handle any peak in traffic. |
| The overall acceptable incoming network  bandwidth is between 300 Mbps and 750  Mbps. | Use auto scaling and cloudwatch to ensure network brandwidth is between 300 mbps and 750 mbps. |
| Application administrators want to be  notified by email if there are more than  100 “400 HTTP errors” per minute in the  application. | Create web log set into cloudwatch, then use an alarm: when 100 errors web happens per minute in the application then send email to administration. |

**App Tier Requirements**

|  |  |
| --- | --- |
| **Requirement** | **Solution** |
|  |  |
| Architecture must be flexible and | application server design must create auto scaling to allow service handle any peak in traffic. |
| handle any peak in traffic or |  |
| performance. |  |
|  |  |
| Overall memory and CPU |  |
| utilization should not go above | Use auto scaling and cloudwatch to ensure overall memory between 80% and 30%, and CPU utilization between 75% and 30%。 |
| 80% and 75% respectively or |  |
| below 30% for either. |  |
|  |  |
| Internet access is required for |  |
| patching and updates without | The vpc must set with nat gateway. |
| exposing the servers. |  |
|  |  |

**Database Tier Requirements**

|  |  |
| --- | --- |
| **Requirement** | **Solution** |
|  |  |
| Database needs consistent storage |  |
| performance at 21,000 IOPS. | Create RDS use SSD volumes, and this volumes have performance at 21000 IOPS. |
|  |  |
|  |  |
| High availability is a requirement |  |
|  | Use Amazon Relational Database Service to ensuring high availability for database tier. |
|  |  |
|  |  |
|  |  |
|  |  |
| No change to the database  schema can be made at this time. | When create aws RDS set a seamless migration option. |
|  |  |
|  |  |

**Additional Services**

List any additional AWS services that you would use for your solution and why?

AWS IAM service

Create IAM service ensure security for different designer.

