CSAA PRACTICE TEST 6

Attempt	17
Marks Obtained	58 / 65
Your score is	89.23%
Completed on	Thursday , 31 January 2019 , 03:31 PM
Time Taken	00 H 15 M 36 S
Result	Pass

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Define Performant Architectures	20	19	1	0
2	Design Resilient Architectures	11	11	0	0
3	Specify Secure Applications and Architectures	14	9	5	0
4	Define Operationally-Excellent Architectures	14	13	1	0
5	Design Cost-Optimized Architectures	5	5	0	0
6	Other	1	1	0	0

65 Questions	**58** Correct	**7** Incorrect	**0** Unattempted

Show Answers

All

QUESTION 1 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your company is planning on hosting a set of EC2 Instances in AWS. The Instances would be divided into subnets, one for the web tier and the other for the database tier. The web tier would be exposed to the Internet via the Internet gateway. As an architect , which of the following would be needed to ensure that traffic can flow between the Instances in each subnet.

- A. Ensure that the route tables have the desired routing between the subnets
- B. Ensure that the Security Groups have the required rules defined to allow traffic ✔
- C. Ensure that all instances have a public IP for communication
- D. Ensure that all subnets are defined as public subnets

Explanation :

Answer – B
The AWS Documentation mentions the following
A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC
Option A is invalid since the route tables would already have the required rules to route traffic between subnets in a VPC
Option C is invalid since the instances would communicate with each other on the private IP
Option D is invalid since the database should be in the private subnet and not the public subnet
For more information on Security Groups, please visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Ask our Experts

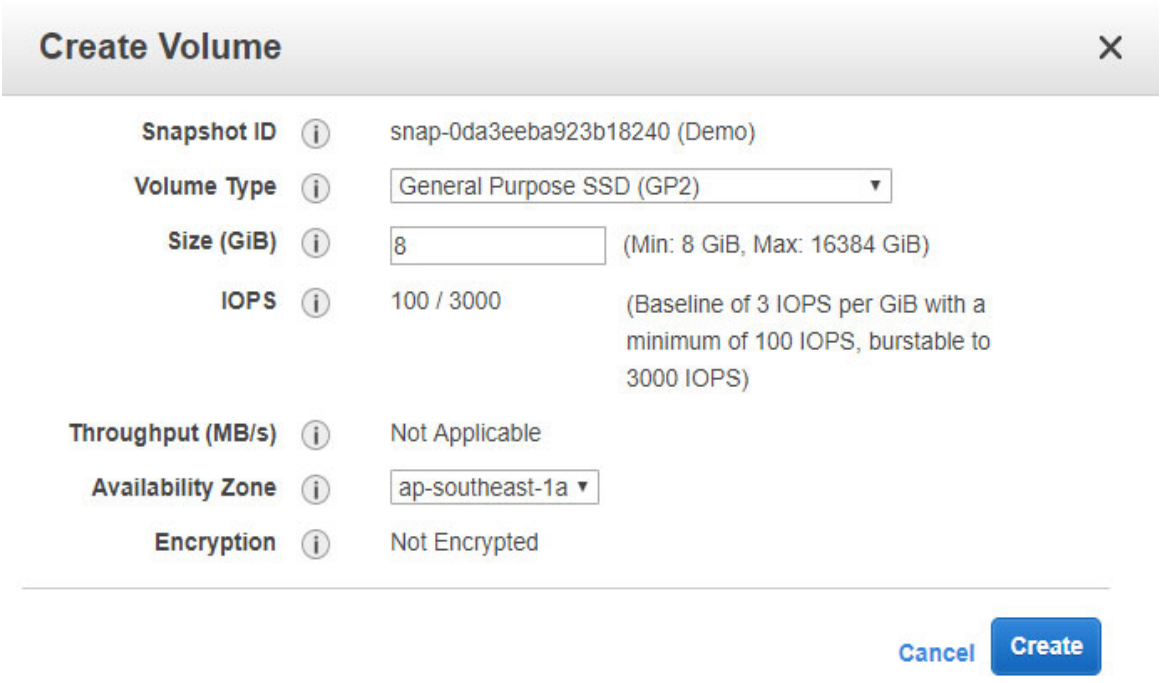
QUESTION 2 CORRECT DESIGN RESILIENT ARCHITECTURES

You work for a company that has a set of EC2 Instances. There is an internal requirement to create another instance in another availability zone. One of the EBS volumes from the current instance needs to be moved from one of the older instances to the new instance. How can you achieve this?

- **A.** Detach the volume and attach to an EC2 instance in another AZ.
- **B.** Create a new volume in the other AZ and specify the current volume as the source.
- **C.** Create a snapshot of the volume and then create a volume from the snapshot in the other AZ ✔
- **D.** Create a new volume in the AZ and do a disk copy of contents from one volume to another.

Explanation :

Answer – C
In order for a volume to be available in another availability zone, you need to first create a snapshot from the volume. Then in the snapshot from creating a volume from the snapshot , you can then specify the new availability zone accordingly.



Option A is invalid, because the Instance and Volume have to be in the same AZ in order for it to be attached to the instance
Option B is invalid , because there is no way to specify a volume as a source
Option D is invalid , because the Diskcopy would just be a tedious process.

For more information on snapshots, please visit the below URL

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

Ask our Experts

QUESTION 3 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your team has developed an application and now needs to deploy that application onto an EC2 Instance. This application interacts with a DynamoDB table. Which of the following is the correct and MOST SECURE way to ensure that the application interacts with the DynamoDB table

- **A.** Create a role which has the necessary permissions and can be assumed by the EC2 instance ✔
- **B.** Use the API credentials from an EC2 instance. Ensure the environment variables areupdated with the API access keys.
- **C.** Use the API credentials from a bastion host. Make the application on the EC2 Instance send requests via the bastion host.
- **D.** Use the API credentials from a NAT Instance. Make the application on the EC2 Instance send requests via the NAT Instance

Explanation :

Answer – A
IAM roles are designed in such a way so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.
Option B,C and D are invalid because it is not secure to use API credentials from any EC2 instance. The API credentials can be tampered with and hence is not the ideal secure way to make API calls.
For more information on IAM roles for EC2, please visit the below URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html)

Ask our Experts

QUESTION 4 CORRECT DESIGN RESILIENT ARCHITECTURES

You are planning to use the MySQL RDS in AWS. You have a requirement to ensure that you are able to recover from a database crash. As an architect which of the following can you use to recover from a database crash. Choose 2 answers from the options given below

- [x] **A.** Ensure that automated backups are enabled for the RDS ✔
- [ ] **B.** Ensure that the database is encrypted at rest
- [ ] **C.** Ensure that you define multiple endpoints for the database
- [x] **D.** Use the Multi-AZ feature for the database ✔

Explanation :

Answer - A and D
The AWS Documentation mentions the following
Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.
Amazon RDS creates and saves automated backups of your DB instance. Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases.
Option B is incorrect since this has to do with security and not high availability
Option C is incorrect since you cannot define endpoints of the database , this is generated by the AWS service
For more information on AWS RDS Automated backups, please visit the below URL:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html)

For more information on AWS RDS Multi-AZ, please visit the below URL:

- https://aws.amazon.com/rds/details/multi-az/ (https://aws.amazon.com/rds/details/multi-az/)

Ask our Experts

QUESTION 5 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company is big on building container-based applications. Currently they use Kubernetes for their on-premises docker based orchestration. They want to move to AWS and preferably not have to manage the infrastructure for the underlying orchestration service. Which of the following could be used for this purpose?

- A. AWS DynamoDB
- B. AWS ECS ✔
- C. AWS EC2 with Kubernetes installed
- D. AWS Elastic beanstalk

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container (https://aws.amazon.com/containers/) orchestration service that supports Docker (https://aws.amazon.com/docker/) containers and allows you to easily run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.
Option A is incorrect since this is a fully managed NoSQL database
Option C is incorrect since this would add maintenance overhead for the company and the question mentions that the company does not want to manage the infrastructure
Option D is incorrect since this is used to deploy applications but will not provide a managed orchestration service
For more information on AWS ECS service, please visit the below URL:

- https://aws.amazon.com/ecs/ (https://aws.amazon.com/ecs/)

Ask our Experts

QUESTION 6 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your company is looking at decreasing the amount of time it takes to build servers which are deployed as EC2 Instances. These Instances always have the same type of software installed as per the security standards. As an architect what would you recommend in decreasing the server build time.

- A. Look at creating snapshots of EBS Volumes
- B. Create the same master copy of the EBS volume
- C. Create a base AMI ✔
- D. Create a base profile

Explanation :

Answer – C
The AWS Documentation mentions the following
An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify a source AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.
Options A and B are incorrect since these cannot be used to create a master copy of the instance
Option D is incorrect because creating a profile will not assist
For more information on AMI's, please visit the below URL:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html)

Ask our Experts

QUESTION 7 CORRECT DEFINE PERFORMANT ARCHITECTURES

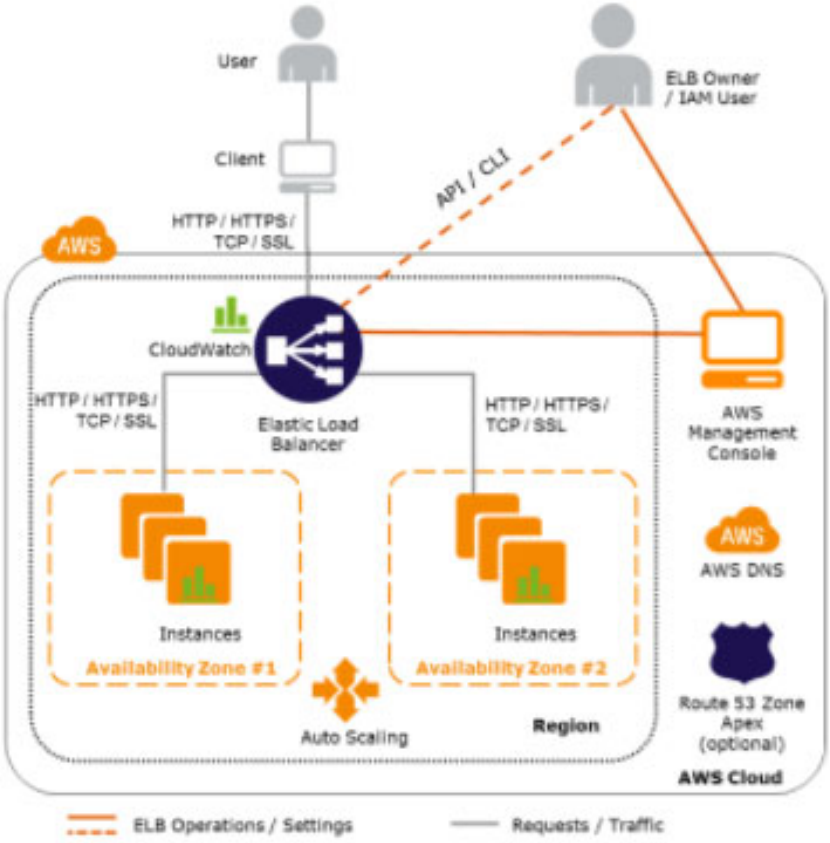
As an architect you have been told to construct the deployment design for an application. You need to ensure that the application is fault tolerant. When using the following AWS services, which elements of the application needs more attention for deploying high availability solutions? Choose 2 answers from the options below.

- [ ] **A.** Amazon DynamoDB
- [x] **B.** Amazon Elastic Compute Cloud (EC2) ✔
- [x] **C.** Amazon Elastic Load Balancing ✔
- [ ] **D.** Amazon Simple Storage Service (S3)

Explanation :

Answer - B and C

The below snapshot shows how the ELB and EC2 instances get setup for high availability. You have the ELB placed in front of the instances. The instances are placed in different AZ's.



Option A is wrong because the service runs across Amazon's proven, high-availability data centers. The service replicates data across three facilities in an AWS Region to provide fault tolerance in the event of a server failure or Availability Zone outage.

Option D is wrong because Amazon S3 Standard and Standard - IA redundantly stores your objects on multiple devices across multiple facilities in an Amazon S3 Region. The service is designed to sustain concurrent device failures by quickly detecting and repairing any lost redundancy
For more information on the Elastic Load Balancer, please visit the below URL:

- https://aws.amazon.com/elasticloadbalancing/ (https://aws.amazon.com/elasticloadbalancing/)

Ask our Experts

QUESTION 8 CORRECT DEFINE PERFORMANT ARCHITECTURES

You are designing the following application in AWS. Users will use the application to upload videos and images. The files will then be picked up by a worker process for further processing. Which of the below services should be used in the design of the application. Choose 2 answers from the options given below

- [x] **A.** AWS Simple storage service for storing the videos and images ✔
- [ ] **B.** AWS Glacier for storing the videos and images
- [ ] **C.** AWS SNS for distributed processing of messages by the worker process
- [x] **D.** AWS SQS for distributed processing of messages by the worker process ✔

Explanation :

Answer - A and D
The AWS Documentation mentions the following
Amazon Simple Storage Service is storage for the Internet. It is designed to make web-scale computing easier for developers.
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and

empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.
Option B is incorrect since this is used for archive storage
Option C is incorrect since this is used as a notification service
For more information on S3, please visit the below URL:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html)

For more information on SQS, please visit the below URL:

- https://aws.amazon.com/sqs/ (https://aws.amazon.com/sqs/)

Ask our Experts

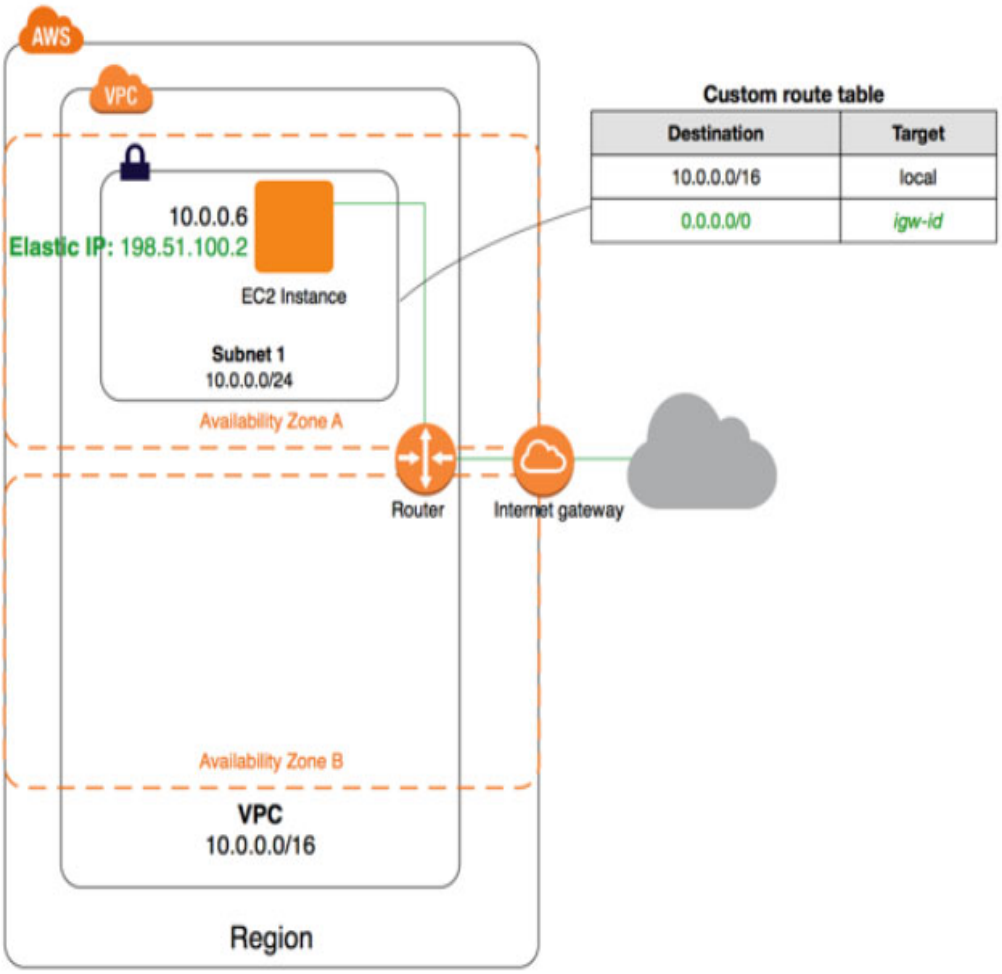
QUESTION 9 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your development team has created a web application that needs to be tested on VPC. You need to advise the IT admin team on how they should implement the VPC to ensure the application can be accessed from the Internet. Which of the following components would be part of the design. Choose 3 answers from the options given below

- [x] **A.** An Internet gateway attached to the VPC. ✔
- [ ] **B.** A NAT gateway attached to the VPC.
- [x] **C.** Route table entry added for the Internet gateway ✔
- [x] **D.** All instances launched with a public IP ✔

Explanation :

Answer - A, C and D
The below diagram from the AWS Documentation shows the design of a public subnet



Option B is incorrect since this should be used for communication of instances in the private subnet to the Internet

For more information on public subnets and the VPC, please visit the below URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

Ask our Experts

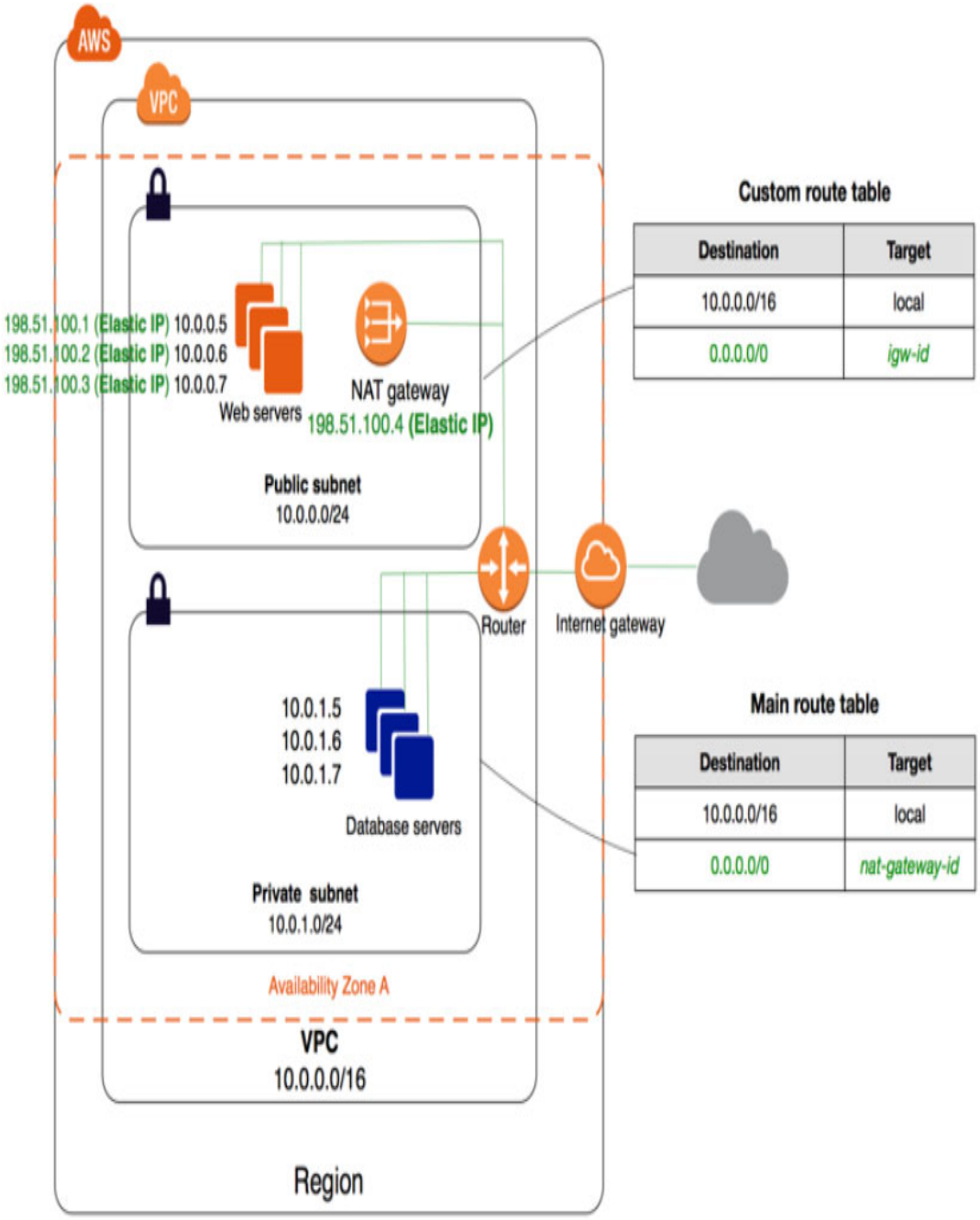
QUESTION 10 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your company is planning on deploying an application which will consist of a web and database tier. The database tier should not be accessible from the Internet. How would you design the networking part of the application? Choose 2 answers from the options below

- [x] **A.** A public subnet for the web tier ✔
- [ ] **B.** A private subnet for the web tier
- [ ] **C.** A public subnet for the database tier
- [x] **D.** A private subnet for the database tier ✔

Explanation :

Answer - A and D
The below diagram from the AWS Documentation shows the design of a web and database tier



Option B is incorrect since users will not be able to access the web application if it placed in a private subnet

Option C is incorrect since the question mentions that the database should not be accessible from the internet

For more information on private and public subnets and the VPC, please visit the below URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts

QUESTION 11 CORRECT DESIGN RESILIENT ARCHITECTURES

You are creating a number of EBS Volumes for the EC2 Instances hosted in your company's AWS account. The company has asked you to ensure that the EBS volumes are available even in the event of a disaster. How would you accomplish this? Choose 2 answers from the options given below

- [ ] **A.** Configure Amazon Storage Gateway with EBS volumes as the data source and store the backups on premise through the storage gateway
- [x] **B.** Create snapshots of the EBS Volumes. ✔
- [ ] **C.** Ensure the snapshots are made available in another availability zone
- [x] **D.** Ensure the snapshots are made available in another region ✔

Explanation :

Answer - B and D
The AWS Documentation mentions the following
You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.
Option A is incorrect since you have to make use of EBS snapshots
Option C is incorrect since the snapshots need to be made available in another region for disaster recovery purposes.
For more information on EBS snapshots, please visit the below URL:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

Ask our Experts

QUESTION 12 CORRECT DEFINE PERFORMANT ARCHITECTURES

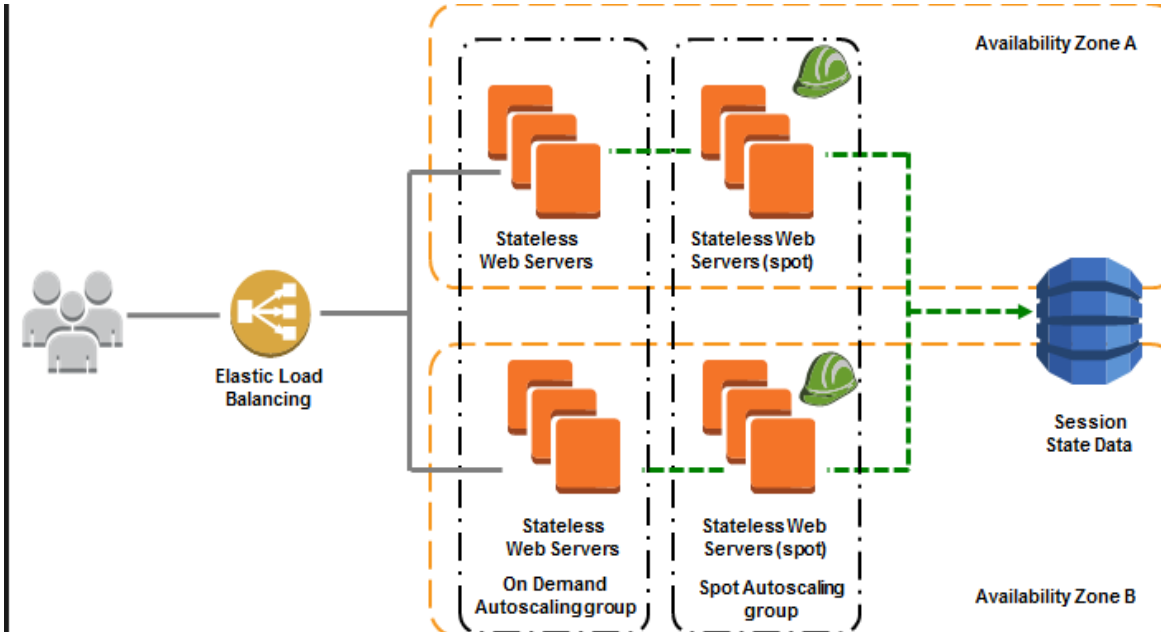
You are planning on hosting a static website on an EC2 Instance. You need to ensure that the environment is highly available and scalable to meet demand. Which of the below aspects can be used to create a highly available environment. Choose 3 answers from the options given below.

- [x] **A.** An auto scaling group to recover from EC2 instance failures ✔
- [x] **B.** Elastic Load Balancer ✔
- [ ] **C.** An SQS queue
- [x] **D.** Multiple Availability Zones ✔

Explanation :

Answer - A,B and D

The diagram below shows an example of a high available architecture for hosting EC2 Instances



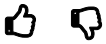
Here you have the

1) ELB which is placed in front of the users which helps in directing the traffic to the EC2 Instances.
2) The EC2 Instances which are placed as part of an AutoScaling Group
3) And then you have multiple subnets which are mapped to multiple availability zones

For a static web site, the SQS is not required to build such an environment. If you have a system such as an order processing systems, which has that sort of queuing of requests, then that could be a candidate for using SQS Queues.
For more information on high availability, please visit the below URL:

- https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf (https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf)

Ask our Experts



QUESTION 13 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company is hosting a set of crucial documents in an S3 bucket. There is a requirement to ensure that documents are also available in the event of a disaster. How can you achieve this?

- A. Use the AWS CLI to copy the objects from the S3 bucket to an EBS volume
- B. Use the AWS CLI to copy the objects from the S3 bucket to another availability zone
- C. Enable Cross Region Replication for the underlying bucket ✔
- D. Enable Multi-AZ Replication for the underlying bucket

Explanation :

Answer – C
Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions. We refer to these buckets as *source* bucket and *destination* bucket. These buckets can be owned by different AWS accounts.
Option A is incorrect since using EBS volumes is not the right approach for disaster recovery of the objects in the S3 bucket
Options B and D is incorrect since the objects need to be copied across regions and there is no option to copy objects across availability zones
For more information on cross region replication, please visit the below URL:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)

Ask our Experts

QUESTION 14 CORRECT DESIGN RESILIENT ARCHITECTURES

You have a requirement to host a web based application. You need to enable high availability for the application, so you create an Elastic Load Balancer and place the EC2 Instances behind the Elastic Load Balancer. You need to ensure that users only access the application via the DNS name of the load balancer. How would you design the network part of the application? Choose 2 answers from the options below

- [x] **A.** Create 2 public subnets for the Elastic Load Balancer ✔
- [ ] **B.** Create 2 private subnets for the Elastic Load Balancer
- [ ] **C.** Create 2 public subnets for the backend instances
- [x] **D.** Create 2 private subnets for the backend instances ✔

Explanation :

Answer - A and D
The AWS Documentation mentions the following
You must create public subnets in the same Availability Zones as the private subnets that are used by your private instances. Then associate these public subnets to the internet-facing load balancer.
Option B is incorrect since the ELB needs to be placed in the public subnet to allow access from the Internet
Option C is incorrect based on security issues. Private subnet gives us the better security from the attacks.
For more information on an example to use the Load balancer , please visit the below URL:

- https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/ (https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/)

Ask our Experts

QUESTION 15 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company has a large set of resources hosted on AWS. Your company wants to keep a check on the Active Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?

- A. AWS Cloudwatch
- B. AWS EC2
- C. AWS Trusted Advisor ✔
- D. AWS SNS

Explanation :

Answer – C
An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.
Below is a snapshot of the service limits it can monitor

Service	Limits
Amazon Elastic Compute Cloud (Amazon EC2)	Elastic IP addresses (EIPs) Reserved Instances - purchase limit (monthly)
Amazon Elastic Block Store (Amazon EBS)	Active volumes Active snapshots General Purpose (SSD) volume storage (GiB) Provisioned IOPS Provisioned IOPS (SSD) volume storage (GiB) Magnetic volume storage (GiB)
Amazon Kinesis Streams	Shards

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.
Option B is invalid because this is the Elastic Compute cloud service
Option D is invalid because it can be sent notification but not check on service limits
For more information on the Trusted Advisor monitoring, please visit the below URL:

- https://aws.amazon.com/premiumsupport/ta-faqs/ (https://aws.amazon.com/premiumsupport/ta-faqs/)

Ask our Experts

QUESTION 16 CORRECT DEFINE PERFORMANT ARCHITECTURES

You work as an architect for a consulting company. The consulting company normally creates the same set of resources for their clients. They want some way of building templates, which can then be used to deploy the resources to the AWS accounts for the various clients. Which of the following service can help fulfil this requirement?

- A. AWS Elastic Beanstalk
- B. AWS SQS
- C. AWS Cloudformation ✔
- D. AWS SNS

Explanation :

Answer – C
The AWS Documentation mentions the following
AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.
Option A is invalid because this is good to get a certain set of defined resources up and running. But It cannot be used to duplicate infrastructure as code.
Option B is invalid because this is the Simple Queue Service which is used for sending messages.
Option D is invalid because this is the Simple Notification service that is used for sending notifications.
For more information on Cloudformation, please visit the below URL:

- http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html (http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html)

Ask our Experts

QUESTION 17 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You work as an architect for a company. An application is going to be deployed on a set of EC2 instances in a VPC. You need to ensure that IT administrators can securely administer the instances in the VPC. How can you accomplish this?

- **A.** Create a NAT gateway, ensure SSH access is provided to the NAT gateway. Access the Instances via the NAT gateway.
- **B.** Create a NAT instance in a public subnet, ensure SSH access is provided to the NAT instance. Access the Instances via the NAT instance.
- **C.** Create a bastion host in the private subnet. Make IT admin staff use this as a jump server to the backend instances.
- **D.** Create a bastion host in the public subnet. Make IT admin staff use this as a jump server to the backend instances. ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration. For example, you can use a bastion host to mitigate the risk of allowing SSH connections from an external network to the Linux instances launched in a private subnet of your Amazon Virtual Private Cloud (VPC).
Options A and B are invalid because you would not route access via the NAT instance or the NAT gateway
Option C is incorrect since the bastion host needs to be in the public subnet
For more information on bastion hosts please visit the below URL:

- https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/ (https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/)

Ask our Experts

QUESTION 18 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You work as an architect for a company. An application is going to be deployed on a set of EC2 instances in a VPC. The Instances will be hosting a web application. You need to design the security group to ensure that users have the ability connect from the Internet via HTTPS. Which of the following needs to be configured for the security group

- **A.** Allow Inbound access on port 443 for 0.0.0.0/0 ✔
- **B.** Allow Outbound access on port 443 for 0.0.0.0/0
- **C.** Allow Inbound access on port 80 for 0.0.0.0/0
- **D.** Allow Outbound access on port 80 for 0.0.0.0/0

Explanation :

Answer – A
The AWS Documentation mentions the following
A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.
Option B is incorrect since security groups are stateful, you don't need to define the rule for outbound traffic
Options C and D are incorrect since you need to only ensure access for HTTPS , hence you should not configure rules for port 80
For more information on security groups, please visit the below URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Ask our Experts

QUESTION 19 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company runs an automobile reselling company that has a popular online store on AWS. The application sits behind an Auto Scaling group and requires new instances of the Auto Scaling group to identify their public and private IP addresses. You need to inform the development team on how they can achieve this. Which of the following advice would you give to the development team?

- **A.** By using Ipconfig for windows or Ifconfig for Linux.
- **B.** By using a cloud watch metric.
- **C.** Using a Curl or Get Command to get the latest meta-data from http://169.254.169.254/latest/meta-data/ ✔
- **D.** Using a Curl or Get Command to get the latest user-data from http://169.254.169.254/latest/user-data/

Explanation :

Answer – C
To get the private and public IP addresses, you can run the following commands on the running instance

- http://169.254.169.254/latest/meta-data/local-ipv4 (http://169.254.169.254/latest/meta-data/local-ipv4)
- http://169.254.169.254/latest/meta-data/public-ipv4 (http://169.254.169.254/latest/meta-data/public-ipv4)

Option A is partially correct, but is an overhead when you already have the service running in AWS.
Option B is incorrect, because you cannot get the IP address from the cloudwatch metric.
Option D is incorrect, because user-data cannot get the IP addresses
For more information on instance metadata, please refer to the below URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html)

Ask our Experts

You have been designing a CloudFormation template that creates one elastic load balancer fronting two EC2 instances. Which section of the template should you edit so that the DNS of the load balancer is returned upon creation of the stack?

- A. Resources
- B. Parameters
- C. Outputs ✔
- D. Mappings

Explanation :

Answer – C
The below example shows a simple CloudFormation template. It creates an EC2 instance based on the AMI - ami-d6f32ab5. When the instance is created, it will output the AZ in which it is created.

```
{
  "Resources": {
    "MyEC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "ImageId": "ami-d6f32ab5"
      }
    }
  },
  "Outputs": {
    "Availability": {
      "Description": "The Instance ID",
      "Value":
      { "Fn::GetAtt" : [ "MyEC2Instance", "AvailabilityZone" ]}
    }
  }
}
```

Option A is incorrect because this is used to define the main resources in the template
Option B is incorrect because this is used to define parameters which can taken in during template deployment
Option D is incorrect because this used to map key value pairs in a template
To understand more on CloudFormation, please visit the url

- https://aws.amazon.com/cloudformation/ (https://aws.amazon.com/cloudformation/)

Ask our Experts

QUESTION 21 INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company has a set of VPC's defined in AWS. They need to connect this to their on-premises network. They need to ensure that all data is encrypted in transit. Which of the following would you use to connect the VPC's to the on-premises networks?

- A. VPC Peering
- B. VPN connections ✔
- C. AWS Direct Connect ✖
- D. Placement Groups

Explanation :

Answer – B
The AWS Documentation mentions the following
By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.
Option A is incorrect because this is used to connect multiple VPC's together.
Option C is incorrect because this does not encrypt traffic in connections between AWS VPC's and the On-premises network
Option D is incorrect because this is used for low latency access between EC2 Instances
For more information on AWS Managed VPN connections , please visit the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts

QUESTION 22 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company wants to host a selection of MongoDB instances. They are expecting a high load and want to have as low latency as possible. As an architect, you need to ensure that the right storage is used to host the MongoDB database. Which of the following would you incorporate as the underlying storage layer?

- A. Provisioned IOPS ✔
- B. General Purpose SSD
- C. Throughput Optimized HDD
- D. Cold HDD

Explanation :

Answer – A
The below snapshot from the AWS Documentation shows the different volume types and why Provisioned IOPS is the most ideal for this requirement

Amazon EBS Volume Types

The following table shows use cases and performance characteristics of current generation EBS volumes:

	Solid State Drives (SSD)		Hard Disk Drives (HDD)	
Volume Type	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Short Description	Highest performance SSD volume designed for latency-sensitive transactional workloads	General Purpose SSD volume that balances price performance for a wide variety of transactional workloads	Low cost HDD volume designed for frequently accessed, throughput intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads

Because of what is mentioned in the documentation as the ideal storage type , the other options are invalid.

For more information on the different EBS volume types , please visit the below URL

- https://aws.amazon.com/ebs/details/ (https://aws.amazon.com/ebs/details/)

Ask our Experts

QUESTION 23 INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A customer needs corporate IT governance and cost oversight of all AWS resources consumed by its divisions. Each division has their own AWS account and there is a need to ensure that the security policies are kept in place at the Account Level. How can you achieve this? Choose 2 answers from the options given below

- [x] **A.** Use AWS organizations ✔
- [ ] **B.** Club all divisions under a single account instead
- [x] **C.** Use IAM Policies to segregate access ✖
- [ ] **D.** Use Service control policies ✔

Explanation :

Answer - A and D
With AWS Organizations, you can centrally manage policies across multiple AWS accounts without having to use custom scripts and manual processes. For example, you can apply service control policies (SCPs) across multiple AWS accounts that are members of an organization. SCPs allow you to define which AWS service APIs can and cannot be executed by AWS Identity and Access Management (IAM) entities (such as IAM users and roles) in your organization's member AWS accounts. SCPs are created and applied from the master account, which is the AWS account that you used when you created your organization.
Option B is incorrect since the question mentions that you need to use separate AWS accounts
Option C is incorrect since you need to use service control policies
For more information on how to use service control policies , please visit the below URL

- https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-in-aws-organizations/ (https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-in-aws-organizations/)

Ask our Experts

QUESTION 24 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company has a set of EC2 Instances hosted on the AWS Cloud. As an architect you have been told to ensure that if the status of any of instances is related to a failure, then the instances are automatically restarted. How can you achieve this in the MOST efficient way possible?

- **A.** Create CloudWatch alarms that stop and start the instance based off of status check alarms ✔
- **B.** Write a script that queries the EC2 API for each instance status check
- **C.** Write a script that periodically shuts down and starts instances based on certain stats.
- **D.** Implement a third-party monitoring tool.

Explanation :

Answer – A
Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.
All other options are possible , but would just be an extra maintenance overhead
For more information on using alarm actions, please refer to the below link

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html)

Ask our Experts

QUESTION 25 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company is planning on migrating their infrastructure to AWS. For the data stores , the company does not want to manage the underlying infrastructure. Which of the following would be ideal for this scenario? Choose 2 answers from the options give below

- [x] **A.** AWS S3 ✔
- [ ] **B.** AWS EBS Volumes
- [x] **C.** AWS DynamoDB ✔
- [ ] **D.** AWS EC2

Explanation :

Answer - A and C
AWS S3 is object level storage that is completely managed by AWS.
Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling.
Option B is incorrect since you need to manage EBS volumes
Option D is incorrect since this is a compute service
For more information on DynamoDB, please refer to the below link

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)

For more information on Simple Storage Service, please refer to the below link

- https://aws.amazon.com/s3/ (https://aws.amazon.com/s3/)

Ask our Experts

QUESTION 26 INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your company has a set of resources defined in AWS. These resources consist of applications hosted on EC2 Instances. Data is stored on EBS volumes and S3. The company mandates that all data should be encrypted at rest. How can you achieve this? Choose 2 answers from the options below

- [x] **A.** Enable SSL with the underlying EBS volumes ✖
- [ ] **B.** Enable EBS Encryption ✔
- [ ] **C.** Make sure that data is transmitted from S3 via HTTPS
- [x] **D.** Enable S3 server-side Encryption ✔

Explanation :

Answer - B and D
The AWS Documentation mentions the following
Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption.
Options A and C are incorrect since these have to do with encryption of data in transit and not encryption of data at rest
For more information on EBS Encryption, please refer to the below link

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

For more information on S3 server-side encryption, please refer to the below link

- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html)

Ask our Experts

QUESTION 27 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your company has a web application hosted in AWS that makes use of an Application Load Balancer. You need to ensure that the web application is protected from web-based attacks such as cross site scripting etc.

Which of the following implementation steps can help protect web applications from common security threats from the outside world?

- **A.** Place a NAT instance in front of the web application to protect against attacks
- **B.** Use the WAF service in front of the web application ✔
- **C.** Place a NAT gateway in front of the web application to protect against attacks
- **D.** Place the web application in front of a CDN service instead

Explanation :

Answer – B
The AWS Documentation mentions the following
AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.
Options A and C are incorrect because these are used to allow instances in your private subnet to communicate with the internet
Option D is incorrect since this is ideal for content distribution and good when you have DDos attacks , but the WAF should be used for concentrated types of web attacks
For more information on AWS WAF, please refer to the below link

- https://aws.amazon.com/waf/ (https://aws.amazon.com/waf/)

Ask our Experts

QUESTION 28 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your supervisor asks you to create a decoupled application whose process includes dependencies on EC2 instances and servers located in your company's on-premises data center. Which of the following would you include in the architecture?

- **A.** An SQS queue as the messaging component between the Instances and servers ✔
- **B.** An SNS topic as the messaging component between the Instances and servers
- **C.** An Elastic Load balancer to distribute requests to your EC2 Instance
- **D.** Route 53 resource records to route requests based on failure

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.
Option B is incorrect since this is a notification service
Option C is incorrect since there is no mention in the question on adding any fault tolerance
Option D is incorrect since there is no mention in the question on adding any failure detection
For more information on AWS SQS, please refer to the below link

- https://aws.amazon.com/sqs/ (https://aws.amazon.com/sqs/)

Ask our Experts

QUESTION 29 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company has a set of VPC's. There is now a requirement to establish communication across the Instances in the VPC's. Your supervisor has asked you to implement the VPC peering connection. Which of the following considerations would you keep in mind for VPC peering. Choose 2 answers from the options below

- [x] **A.** Ensuring that the VPC's don't have overlapping CIDR blocks ✔
- [x] **B.** Ensuring that no on-premises communication is required via transitive routing ✔
- [ ] **C.** Ensuring that the VPC's only have public subnets for communication
- [ ] **D.** Ensuring that the VPC's are created in the same region

Explanation :

Answer - A and B

The AWS Documentation mentions the following with restrictions for VPC peering

Overlapping CIDR Blocks

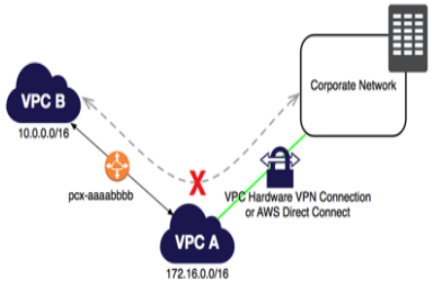
You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.

Example: Edge to Edge Routing Through a VPN Connection or an AWS Direct Connect Connection

You have a VPC peering connection between VPC A and VPC B (*pcx-aaaabbbb*). VPC A also has a VPN connection or an AWS Direct Connect connection to a corporate network. Edge to edge routing is not supported; you cannot use VPC A to extend the peering relationship to exist between VPC B and the corporate network. For example, traffic from the corporate network can't directly access VPC B by using the VPN connection or the AWS Direct Connect connection to VPC A.

Example: Edge to Edge Routing Through a VPN Connection or an AWS Direct Connect Connection

You have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb). VPC A also has a VPN connection or an AWS Direct Connect connection to a corporate network. Edge to edge routing is not supported; you cannot use VPC A to extend the peering relationship to exist between VPC B and the corporate network. For example, traffic from the corporate network can't directly access VPC B by using the VPN connection or the AWS Direct Connect connection to VPC A.



Option C is incorrect since it is not necessary that the VPC's only contain public subnets
Option D is incorrect since it is not necessary that the VPC's are created in the same region
For more information on Invalid peering configurations, please refer to the below link

- https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html (https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html)

Note: AWS now supports VPC Peering across different regions. Please check below AWS Docs for more details:

- https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/ (https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/)
- https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html (https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html)

Ask our Experts

QUESTION 30 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You have been instructed to establish a successful site-to-site VPN connection from your on-premises network to the VPC (Virtual Private Cloud). As an architect , which of the following pre-requisites should you ensure are in place for establishing the site-to-site VPN connection. Choose 2 answers from the options given below

- [ ] **A.** The main route table to route traffic through a NAT instance
- [x] **B.** A public IP address on the customer gateway for the on-premises network ✔
- [x] **C.** A virtual private gateway attached to the VPC ✔
- [ ] **D.** An Elastic IP address to the Virtual Private Gateway

Explanation :

Answer - B and C
This is mentioned in the AWS Documentation

Virtual Private Gateway

A *virtual private gateway* is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection.

When you create a virtual private gateway, you can specify the private Autonomous System Number (ASN) for the Amazon side of the gateway. If you don't specify an ASN, the virtual private gateway is created with the default ASN (64512). You cannot change the ASN after you've created the virtual private gateway. To check the ASN for your virtual private gateway, view its details in the **Virtual Private Gateways** screen in the Amazon VPC console, or use the describe-vpn-gateways AWS CLI command.

> **Note**
>
> If you create your virtual private gateway before 2018-06-30, the default ASN is 17493 in the Asia Pacific (Singapore) region, 10124 in the Asia Pacific (Tokyo) region, 9059 in the EU (Ireland) region, and 7224 in all other regions.

Customer Gateway

A *customer gateway* is a physical device or software application on your side of the VPN connection.

To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. The following table describes the information you'll need to create a customer gateway resource.

Item	Description
Internet-routable IP address (static) of the customer gateway's external interface.	The public IP address value must be static. If your customer gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device, and adjust your firewall rules to unblock UDP port 4500.

Option A is incorrect since NAT instance is not required to route traffic via the VPN connection

Option D is incorrect the Virtual Private Gateway is managed by AWS
For more information on VPN connections, please refer to the below link

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts

QUESTION 31 INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your company wants to enable encryption of services such as S3 and EBS volumes so that the data it maintains is encrypted at rest. They want to have complete control over the keys and the entire lifecycle around the keys. How can you accomplish this?

- A. Use the HSM Module ✔
- B. Use the KMS service ✖
- C. Enable S3 server-side encryption
- D. Enable EBS Encryption with the default KMS keys

Explanation :

Answer – A
This is mentioned in the AWS Documentation
AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs
Options B,C and D are incorrect since here the keys are maintained by AWS
For more information on cloud HSM, please refer to the below link

- https://aws.amazon.com/cloudhsm/ (https://aws.amazon.com/cloudhsm/)

Ask our Experts

QUESTION 32 CORRECT DEFINE PERFORMANT ARCHITECTURES

A company wants to implement a data store in AWS. The data store needs to have the following requirements

1) Completely managed by AWS

2) Ability to store JSON objects efficiently

3) Scale based on demand

Which of the following would you use as the data store?

- A. AWS Redshift
- B. AWS DynamoDB ✔
- C. AWS Aurora
- D. AWS Glacier

Explanation :

Answer – B
Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling. It is ideal for storing JSON based objects
Option A is incorrect since this is normally used to host a data warehousing solution
Option C is incorrect since this is used to host a MySQL database
Option D is incorrect since this is used for archive storage
For more information on DynamoDB, please refer to the below link

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)

Ask our Experts

QUESTION 33 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company has setup some EC2 Instances in a VPC with the default Security group and NACL settings. They want to ensure that IT admin staff can connect to the EC2 Instance via SSH. As an architect what would you ask the IT admin team to do to ensure that they can connect to the EC2 Instance from the Internet. Choose 2 answers from the options below

- [x] **A.** Ensure that the Instance has a Public or Elastic IP ✔
- [ ] **B.** Ensure that the Instance has a Private IP
- [x] **C.** Ensure to modify the Security groups ✔
- [ ] **D.** Ensure to modify the NACL rules

Explanation :

Answer - A and C
The AWS Documentation mentions the following
To enable access to or from the internet for instances in a VPC subnet, you must do the following:

- Attach an internet gateway to your VPC.
- Ensure that your subnet's route table points to the internet gateway.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

Option B is incorrect since the Private IP will always be created, and would not be used to connect from the internet
Option D is incorrect since the default NACL rules will allow all traffic
For more information on exposing VPC resources to the Internet please refer to the below link

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html)

Ask our Experts

QUESTION 34 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company has a set of EBS volumes and a set of adjoining EBS snapshots. They want to minimize the costs for the underlying EBS snapshots. Which of the following approaches provides the lowest cost for Amazon Elastic Block Store snapshots while giving you the ability to fully restore data?

- **A.** Maintain two snapshots: the original snapshot and the latest incremental snapshot.
- **B.** Maintain a volume snapshot; subsequent snapshots will overwrite one another
- **C.** Maintain a single snapshot the latest snapshot is both Incremental and complete. ✔
- **D.** Maintain the most current snapshot, archive the original and incremental to Amazon Glacier.

Explanation :

Answer – C
The AWS Documentation mentions the following
You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.
For more information on EBS Snapshots, please refer to the below link

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

Ask our Experts

QUESTION 35 CORRECT DEFINE PERFORMANT ARCHITECTURES

You are using an m1.small EC2 Instance with one 300GB EBS General purpose SSD volume to host a relational database. You determined that write throughput to the database needs to be increased. Which of the following approaches can help achieve this? Choose 2 answers from the options given below

- [x] **A.** Use a larger EC2 Instance ✔
- [ ] **B.** Enable Multi-AZ feature for the database.
- [x] **C.** Consider using Provisioned IOPS Volumes. ✔
- [ ] **D.** Put the database behind an Elastic Load Balancer.

Explanation :

Answer - A and C
The below snapshot from the AWS Documentation shows the different volume types and why Provisioned IOPS is the most ideal for this requirement

Amazon EBS Volume Types

The following table shows use cases and performance characteristics of current generation EBS volumes:

	Solid State Drives (SSD)		Hard Disk Drives (HDD)	
Volume Type	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Short Description	Highest performance SSD volume designed for latency-sensitive transactional workloads	General Purpose SSD volume that balances price performance for a wide variety of transactional workloads	Low cost HDD volume designed for frequently accessed, throughput intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads

Also consider using a larger instance size for better processing capabilities

Option B is incorrect since the Multi-AZ feature is only for high availability
Option D is incorrect since this would not alleviate the high number of writes to the database

For more information on the different EBS volume types , please visit the below URL

- https://aws.amazon.com/ebs/details/ (https://aws.amazon.com/ebs/details/)

Ask our Experts

QUESTION 36 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company has a set of AWS RDS Instances. Your management has asked you to disable Automated backups to save on cost. When you disable automated backups for AWS RDS, what are you compromising on?

- **A.** Nothing,you are actually saving resources on aws
- **B.** You are disabling the point-in-time recovery. ✔
- **C.** Nothing really, you can still take manual backups.
- **D.** You cannot disable automated backups in RDS.

Explanation :

Answer – B
Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. You can set the backup retention period when you create a DB instance. If you don't set the backup retention period, Amazon RDS uses a default period retention period of one day. You can modify the backup retention period; valid values are 0 (for no backup retention) to a maximum of 35 days
You will also specifically see AWS mentioning the risk of not allowing automated backups.
Important
We highly discourage disabling automated backups because it disables point-in-time recovery.If you disable and then re-enable automated backups, you are only able to restore starting from the time you re-enabled automated backups.
Because of the risk which is clearly mentioned in the AWS Documentation, all other options are incorrect.
For more information on Automated backups, please visit

- http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html (http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html)

Ask our Experts

QUESTION 37 CORRECT DEFINE PERFORMANT ARCHITECTURES

A company is planning on setting up a web-based application. They need to ensure that users across the world have the ability to view the pages from the web site with the least amount of latency. How can you accomplish this?

- A. Use Route 53 with latency-based routing
- B. Place a cloudfront distribution in front of the web application ✔
- C. Place an Elastic Load balancer in front of the web application
- D. Place an Elastic Cache in front of the web application

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon CloudFront is a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to your viewers with low latency and high transfer speeds. CloudFront is integrated with AWS – including physical locations that are directly connected to the AWS global infrastructure, as well as software that works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code close to your viewers.
Option A is incorrect since this is used for multiple sites and latency baed routing between the sites
Option C is incorrect since this is used for fault tolerance for the web application
Option D is incorrect since this is used for caching requests in front of a database layer
For more information on AWS Cloudfront, please visit

- https://aws.amazon.com/cloudfront/ (https://aws.amazon.com/cloudfront/)

Ask our Experts

QUESTION 38 INCORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The customer also uses Amazon Route 53 to manage their public DNS. How should Route 53 be configured to ensure the custom domain is made to point to the load balancer? Choose 2 answers from the options below.

- [x] **A.** Create an A record pointing to the IP address of the load balancer ✖
- [ ] **B.** Create a CNAME record pointing to the load balancer DNS name.
- [x] **C.** Create an alias for a CNAME record to the load balancer DNS name. ✔
- [ ] **D.** Ensure that a hosted zone is in place ✔

Explanation :

Answer - C and D
The AWS Documentation mentions the following
While ordinary Amazon Route 53 records are standard DNS records, *alias records* provide a Route 53 –specific extension to DNS functionality. Instead of an IP address or a domain name, an alias record contains a pointer to an AWS resource such as a CloudFront distribution or an Amazon S3 bucket. When Route 53 receives a DNS query that matches the name and type in an alias record, Route 53 follows the pointer and responds with the applicable value:

- An alternate domain name for a CloudFront distribution – Route 53 responds as if the query had asked for the CloudFront distribution by using the CloudFront domain name, such as d111111abcdef8.cloudfront.net.
- An Elastic Beanstalk environment – Route 53 responds to each query with one or more IP addresses for the environment.
- An ELB load balancer – Route 53 responds to each query with one or more IP addresses for the load balancer.
- An Amazon S3 bucket that is configured as a static website – Route 53 responds to each query with one IP address for the Amazon S3 bucket.

- Option D is correct. Hosted Zone - is a container for records, and records contain information about how you want to route traffic for a specific domain, such as example.com, and its subdomains (vpc.example.com, elb.example.com). A hosted zone and the corresponding domain have the same name, and we have 2 types of hosted zones;

- Public Hosted Zone - contain records that specify how you want to route traffic on the internet.
- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHZWorkingWith.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHZWorkingWith.html)

- Private Hosted Zone - contain records that specify how you want to route traffic in an Amazon VPC.
- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html)
- Options A and B are incorrect since you need to use ALIAS names for this.

For more information on ALIAS records, please visit

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html)

Note:
Wordings for Option C "**create an alias record for a CNAME record**" is mentioned in below AWS Docs:

- https://aws.amazon.com/premiumsupport/knowledge-center/route-53-create-alias-records/ (https://aws.amazon.com/premiumsupport/knowledge-center/route-53-create-alias-records/)

They mentioned that " **CNAME support:** Route 53 follows the pointer in an alias record only if the record type also matches. **To create an alias record for a CNAME record,** the alias target must also resolve to a CNAME value."

Ask our Experts

QUESTION 39 CORRECT DEFINE PERFORMANT ARCHITECTURES

A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The web application interfaces with a AWS RDS database. It has been noticed that a set of similar types of queries is causing a performance bottleneck at the database layer. Which of the following architecture additions can help alleviate this issue?

- A. Deploy ElastiCache in front of the web servers
- B. Deploy ElastiCache in front of the database servers ✔
- C. Deploy Elastic Load balancer in front of the web servers
- D. Enable Multi-AZ for the database

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon ElastiCache offers fully managed Redis (https://aws.amazon.com/redis/) and Memcached (https://aws.amazon.com/memcached/). Seamlessly deploy, operate, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores
Option A is incorrect since the database is having issues hence you need to ensure that ElastiCache is placed in front of the database servers
Option C is incorrect since there is an issue with the database servers, so we don't need to add anything for the web servers
Option D is incorrect since this is used for high availability of the database
For more information on ElastiCache, please visit

- https://aws.amazon.com/elasticache/ (https://aws.amazon.com/elasticache/)

Ask our Experts

QUESTION 40 CORRECT DESIGN RESILIENT ARCHITECTURES

A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The web application interfaces with a AWS RDS database. The management has specified that the database be available in case of a hardware failure on the primary database. The secondary needs to be made available in the least amount of time. Which of the following would you opt for?

- A. Made a snapshot of the database
- B. Enabled Multi-AZ failover ✔
- C. Increased the database instance size
- D. Created a read replica

Explanation :

Answer – B
The AWS Documentation mentions the following

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.
Options A and D are incorrect since even though they can be used to recover a database, it would just take more time than just enabling Multi-AZ
Option C is incorrect since this will not help the cause
For more information on Multi-AZ, please visit

- https://aws.amazon.com/rds/details/multi-az/ (https://aws.amazon.com/rds/details/multi-az/)

Ask our Experts

QUESTION 41 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company is planning on launching a set of EC2 Instances for hosting their production-based web application. As an architect you have to instruct the operations department on which service they can use for the monitoring purposes. Which of the following would you recommend?

- A. AWS Cloudtrail
- B. AWS Cloudwatch ✔
- C. AWS SQS
- D. AWS SNS

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes,

optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications and services that run on AWS, and on-premises servers.
Option A is incorrect since this is used for API monitoring
Option C is incorrect since this is used to working with messages in the queue
Option D is incorrect since this is used for sending notifications
For more information on AWS Cloudwatch, please visit the below URL

- https://aws.amazon.com/cloudwatch/ (https://aws.amazon.com/cloudwatch/)

Ask our Experts

QUESTION 42 CORRECT DEFINE PERFORMANT ARCHITECTURES

A company is planning on storing their files from their on-premises location onto the Simple Storage service. After a period of 3 months, they want to archive the files, since they would be rarely used. Which of the following would be the right way to service this requirement?

- **A.** Use an EC2 instance with EBS volumes. After a period of 3 months, keep on taking snapshots of the data.
- **B.** Store the data on S3 and then use Lifecycle policies to transfer the data to Amazon Glacier ✔
- **C.** Store the data on Amazon Glacier and then use Lifecycle policies to transfer the data to Amazon S3
- **D.** Use an EC2 instance with EBS volumes. After a period of 3 months , keep on taking copies of the volume using Cold HDD volume type.

Explanation :

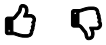
Answer – B
The AWS Documentation mentions the following
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- Transition actions—Define when objects transition to another storage class. For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.
- Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

Options A and D are incorrect since using EBS volumes is not the right storage option for this sort of requirement
Option C is incorrect since the files should be initially stored in S3.
For more information on AWS S3 Lifecycle policies, please visit the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html)

Ask our Experts



QUESTION 43 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company has a workflow that sends video files from their on-premises system to AWS for transcoding. They use EC2 worker instances that pull transcoding jobs from SQS. As an architect you need to design how the SQS service would be used in this architecture. Which of the following is the ideal way in which the SQS service should be used?

- **A.** SQS should be used to guarantee the order of the messages.
- **B.** SQS should be used to synchronously manage the transcoding output.
- **C.** SQS should be used to check the health of the worker instances.
- **D.** SQS should be used to facilitate horizontal scaling of encoding tasks. ✔

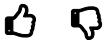
Explanation :

Answer – D
The AWS Documentation mentions the following
Amazon Simple Queue Service (Amazon SQS) offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components.
Option A is incorrect since there is no mention in the question for the order of the messages to be guaranteed
Options B and C are incorrect since these are not the responsibility of the SQS queue

For more information on AWS SQS queues, please visit the below URL

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html)

Ask our Experts



QUESTION 44 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You're an architect for your company. Your IT admin staff needs access to newly created EC2 Instances for administrative purposes. Which of the following needs to be done to ensure that the IT admin staff can successfully connect via port 22 on to the EC2 Instances

- A. Adjust Security Group to permit egress traffic over TCP port 443 from your IP.
- B. Configure the IAM role to permit changes to security group settings.
- C. Modify the instance security group to allow ingress of ICMP packets from your IP.
- D. Adjust the instance's Security Group to permit ingress traffic over port 22. ✔
- E. Apply the most recently released Operating System security patches.

Explanation :

Answer - D
A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances.
For connecting via SSH on EC2, you need to ensure that port 22 is open on the security group for the EC2 instance.
Option A is wrong, because port 443 is for HTTPS and not for SSH.
Option B is wrong because IAM role is not pertinent to security groups
Option C is wrong because this is relevant to ICMP and not SSH
Option E is wrong because it does not matter what patches are there on the system
For more information on EC2 Security groups, please visit the url

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html)

Ask our Experts

QUESTION 45 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company is running a photo sharing website. Currently all the photos are stored in S3. At some point the company finds out that other sites have been linking to the photos on your site, causing loss to your business. You need to implement a solution for the company to mitigate this issue. Which of the following would you look at implementing?

- **A.** Remove public read access and use signed URLs with expiry dates. ✔
- **B.** Use Cloud Front distributions for static content.
- **C.** Block the IPs of the offending websites in Security Groups.
- **D.** Store photos on an EBS volume of the web server.

Explanation :

Answer - A
The AWS Documentation mentions the following
A pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permissions to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.
Option B is incorrect since Cloud front is only used for distribution of content across edge or region locations. It is not used for restricting access to content
Option C is incorrect since Blocking IP's is challenging because they are dynamic in nature and you will not know which sites are accessing your main site
Option D is incorrect since Storing photos on EBS volume is not a good practice or architecture approach for an AWS Solution Architect
For more information on serving private content please visit the url

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

(https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html)

Ask our Experts

QUESTION 46 CORRECT

You have been hired as a consultant for a company to implement their CI/CD processes. They currently use an on-premises deployment of Chef for their configuration management on servers. You need to advise them on what they can use on AWS to leverage their existing capabilities. Which of the following service would you recommend?

- A. Amazon Simple Workflow Service
- B. AWS Elastic Beanstalk
- C. AWS CloudFormation
- D. AWS OpsWorks ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. OpsWorks has three offerings, AWS Opsworks for Chef Automate, AWS OpsWorks for Puppet Enterprise, and AWS OpsWorks Stacks.
All of the other options are incorrect since the only tool which works effectively with the Chef Configuration management tool is AWS OpsWorks.
For more information on AWS Opswork, please visit the url

- https://aws.amazon.com/opsworks/ (https://aws.amazon.com/opsworks/)

Ask our Experts

QUESTION 47 CORRECT DEFINE PERFORMANT ARCHITECTURES

You have been hired as a consultant for a company to implement their CI/CD processes. They have a keen eye to implement the deployment of their infrastructure as code. You need to advise them on what they can use on AWS to fulfil this requirement. Which of the following service would you recommend?

- A. Amazon Simple Workflow Service
- B. AWS Elastic Beanstalk
- C. AWS CloudFormation ✔
- D. AWS OpsWorks

Explanation :

Answer – C
The AWS Documentation mentions the following
AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. You don't need to individually create and configure AWS resources and figure out what's dependent on what; AWS CloudFormation handles all of that.
All of the other options are incorrect since the only tool that works effectively with building templates is Cloudformation.
For more information on AWS Cloudformation, please visit the url

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html)

Ask our Experts

QUESTION 48 CORRECT DEFINE PERFORMANT ARCHITECTURES

You work as an architect for a company. There is a requirement for an application to be deployed on a set of EC2 Instances. These would be part of a compute cluster that requires low inter-node latency. Which of the following would you use for this requirement?

- A. Multiple Availability Zones
- B. AWS Direct Connect
- C. EC2 Dedicated Instances
- D. Cluster placement Groups ✔
- E. VPC private subnets

Explanation :

Answer – D
The AWS Documentation mentions the following
Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both, and if the majority of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking
Because of what is mentioned in the documentation , all other options are incorrect
For more information on AWS placement groups, please visit the url

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html)

Ask our Experts

QUESTION 49 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company stores a large set of files in Amazon S3. They need to ensure that if any new files are added to an S3 bucket, an event notification would be sent to the IT admin staff. Which of the following could be used to fulfil this requirement? Choose 2 answers from the options given below.

- [x] **A.** Create an SNS topic ✔
- [ ] **B.** Create an SQS queue
- [x] **C.** Add an event notification to the S3 bucket ✔
- [ ] **D.** Add an event notification to the S3 object

Explanation :

Answer - A and C
The AWS Documentation mentions the following
The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.
Option B is incorrect since you need to create an SNS topic that could be used to send an email to multiple IT administrators
Option D is incorrect since the event notification needs to be placed on the bucket and not the object
NOTE:
Options C and D are different.
Option C: Add an event notification to the **S3 bucket**
Option D: Add an event notification to the **S3 object**
For more information on AWS S3 notifications, please visit the url

- https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html)

Ask our Experts

QUESTION 50 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company is planning on migrating some code from their on-premises infrastructure onto AWS. They want to ensure to limit the amount of maintenance that would be required for the underlying infrastructure. Which of the following would they choose for hosting the code base?

- [x] **A.** AWS Lambda ✔

- **B.** AWS EC2
- **C.** AWS ECS
- **D.** AWS SQS

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume - there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service - all with zero administration
Option B is incorrect since here you would need to manage the underlying servers
Option C is incorrect since there is no mention of docker containers or the requirement for an orchestration service
Option D is incorrect since this is a messaging service
For more information on AWS Lambda, please visit the url

- https://docs.aws.amazon.com/lambda/latest/dg/welcome.html (https://docs.aws.amazon.com/lambda/latest/dg/welcome.html)

Ask our Experts

QUESTION 51 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. There is a requirement to ensure that instances in the Development and Test VPC can access resources in the Production VPC for a limited amount of time. Which of the following would be the ideal way to get this in place?

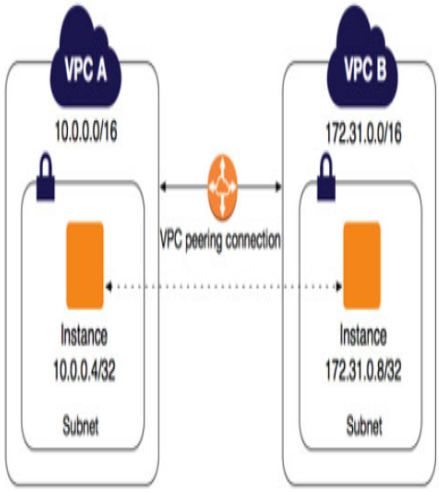
- **A.** Create an AWS Direct Connect connection between the Development, Test VPC to the Production VPC
- **B.** Create a separate VPC peering connection from Development to Production and from Test to the Production VPC ✔

- C. Create a VPN connection between the Development, Test VPC to the Production VPC
- D. Create a VPC peering connection between the Development to the Production VPC and from Development to the Test VPC.

Explanation :

Answer – B
Options A and C are incorrect since this is only required for a short duration of time , hence you need to choose VPC peering
Options D is incorrect since the VPC Perring configuration mentioned would be invalid.
You can peer the VPC's as mentioned in the AWS documentation:
"A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection)."

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an *inter-region* VPC peering connection).



For more information on VPC peering please visit the url

- https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html (https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html)

Ask our Experts

QUESTION 52 INCORRECT DEFINE PERFORMANT ARCHITECTURES

You are designing the application architecture for a company. The architecture is going to consist of a web tier that will be hosted on EC2 Instances placed behind an Elastic Load Balancer. Which of the following would be considered important when considering what should the specification for the components of the application architecture?

Select 2 options:

- [ ] **A.** Determine the required I/O operations ✔
- [x] **B.** Determining the minimum memory requirements for an application ✔
- [ ] **C.** Determining where the client intends to serve most of the traffic
- [x] **D.** Determining the peak expected usage for a client's application ✖

Explanation :

Answer - A and B
You should decide on what are requirements for the underlying EC2 Instance. You can then choose the Instance type for the underlying EC2 Instance
Options C and D are not required. The ELB will take care of the peak usage and distribution of traffic
For more information on EC2 Instance types, please visit the url

- https://aws.amazon.com/ec2/instance-types/ (https://aws.amazon.com/ec2/instance-types/)

Ask our Experts

QUESTION 53 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company has a requirement to host an application in AWS that requires access to a NoSQL database. But there are no human resources available who can take care of the database infrastructure. In addition to this, the database should have the capability to scale automatically based on demand and also have high availability. Which of the following databases would you use for this purpose?

- **A.** DynamoDB ✔
- **B.** ElasticMap Reduce
- **C.** Amazon RDS
- **D.** Amazon Aurora

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon DynamoDB is a nonrelational database that delivers reliable performance at any scale. It's a fully managed, multi-region, multi-master database that provides consistent single-digit millisecond latency, and offers built-in security, backup and restore, and in-memory caching.
Option B is invalid since this is used for Big Data
Option C is invalid since here you still have to partially manage the infrastructure
Option D is invalid since this would allow you to host MySQL compatible databases
For more information on DynamoDB, please visit the url

- https://aws.amazon.com/dynamodb/ (https://aws.amazon.com/dynamodb/)

Ask our Experts

QUESTION 54 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your company is planning on moving to the AWS Cloud. There is a strict compliance policy that mandates that data should be encrypted at rest. As an AWS Solution architect, you have been tasked to put the organization data on the cloud and also ensure that all compliance requirements have been met. Which of the below needs to be part of the implementation plan to ensure compliance with the security requirements. Choose 2 answers from the options given below.

- [x] **A.** Ensure that all EBS volumes are encrypted ✔
- [x] **B.** Ensure that server-side encryption is enabled for S3 buckets ✔
- [ ] **C.** Ensure that SSL is enabled for all load balancers
- [ ] **D.** Ensure that the EC2 Security rules only allow HTTPS traffic

Explanation :

Answer - A and B
The AWS Documentation mentions the following
Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key
Options C and D are invalid since these are used to manage encryption of data in transit
For more information on Encryption of EBS volumes, please visit the url

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

For more information on Encryption of S3 buckets, please visit the url

- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html)

Ask our Experts

QUESTION 55 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company is planning on moving to the AWS Cloud. One of the applications will be launched on a set of EC2 Instances. You need to ensure that the architecture is fault tolerant and highly available. Which of the following would be considered during the design process. Choose 2 answers from the options given below

- [ ] **A.** Enable Multi-AZ for the databases
- [x] **B.** Use a load balancer in front of the EC2 Instances ✔
- [x] **C.** Ensure that the EC2 Instances are spread across multiple availability zones ✔
- [ ] **D.** Ensure that the EC2 Instances are spread across a single availability zone for better maintenance

Explanation :

Answer - B and C
This is clearly mentioned in the AWS Documentation
What Is Elastic Load Balancing?
Elastic Load Balancing distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in multiple Availability Zones. Elastic Load Balancing scales your load balancer as traffic to your application changes over time, and can scale to the vast majority of workloads automatically.
Load Balancer Benefits
A load balancer distributes workloads across multiple compute resources, such as virtual servers. Using a load balancer increases the availability and fault tolerance of your applications.

Option A is invalid because the question does not mention anything around using AWS RDS service
Option D is invalid because you need to ensure that the Instances are spread across multiple availability zones
For more information on what is load balancing, please visit the url

- https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html)

Ask our Experts

A company want to implement a hybrid architecture where it wants to connect VPC's in its account to its on-premises architecture. There are requirements which state that all traffic needs to be encrypted between the on-premises data centres and the AWS VPC's. Which of the following would you recommend to fulfil this requirement?

- A. AWS Direct Connect ✖
- B. AWS VPN ✔
- C. AWS VPC peering
- D. AWS Direct Link

Explanation :

Answer - B
The AWS Documentation mentions the following

VPN connectivity option	Description
AWS managed VPN	You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections, and the Amazon VPC Network Administrator Guide.

IPSec is used for encryption of traffic in the VPN connection
Option A is invalid because here the traffic is not encrypted
Option C is invalid because this is used to link VPC's together
Option D is invalid because this not a valid service
For more information on AWS VPN Connections, please visit the url

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html)

Ask our Experts

QUESTION 57 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company currently has a set of EC2 Instances. Your supervisor has advised that as part of the business continuity requirement that EC2 Instances should be available in another region in case the primary region goes down for any reason. You need to ensure that Instances in the secondary region come up in the shortest possible time frame. Which of the following technique would you implement for this requirement?

- **A.** Create an AMI and copy it to another region ✔
- **B.** Create an EBS Snapshot and then copy it to another region
- **C.** Make a copy of the instance to another region
- **D.** Create a new instance in the new region and then install the required software's

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Machine Images (AMIs) are preconfigured with operating systems, and some preconfigured AMIs might also include application stacks. You can also configure your own AMIs. In the context of DR, we strongly recommend that you configure and identify your own AMIs so that they can launch as part of your recovery procedure. Such AMIs should be preconfigured with your operating system of choice plus appropriate pieces of the application stack.
Option B is invalid because creating the snapshot itself will not result in getting the Instance up and running ASAP
Option C is invalid because this is not a valid option
Option D is invalid because this will result in a long time to recover the instance
For more information on disaster recovery techniques, please visit the url

- http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf (http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf)

Ask our Experts

QUESTION 58 CORRECT DESIGN RESILIENT ARCHITECTURES

As a solutions architect, it is your job to design for high availability and fault tolerance. Company-A is utilizing Amazon S3 to store large amounts of file data. You need to ensure that the files are available in case of a disaster. How can you achieve this?

- **A.** Copy the S3 bucket to an EBS optimized backed EC2 instance
- **B.** Amazon S3 is highly available and fault tolerant by design and requires no additional configuration
- **C.** Enable Cross-Region Replication for the bucket ✔
- **D.** Enable versioning for the bucket

Explanation :

Answer – C
The AWS Documentation mentions the following
Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions. We refer to these buckets as *source* bucket and *destination* bucket. These buckets can be owned by different AWS accounts.
Option A is invalid because this is not the right way to take backups of an S3 bucket
Option B is invalid because yes S3 will ensure objects are available in multiple availability zones but not across regions in case of a disaster
Option D is invalid because versioning can only help from accidental deletion of objects but not from disaster recovery
For more information on cross region replication, please visit the url

- https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)

Ask our Experts

QUESTION 59 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company currently has a set of virtual servers that need to be migrated to the AWS Cloud. These Instances are normally 70% utilized and used throughout most of the year. As a solutions architect which of the following Instance pricing model would you suggest?

- A. Reserved instances ✔
- B. On-demand instances
- C. Spot instances
- D. Regular instances

Explanation :

Answer – A
The AWS Documentation mentions the following on the different instance pricing options
Amazon EC2 provides the following purchasing options to enable you to optimize your costs based on your needs:

- On-Demand Instances – Pay, by the second, for the instances that you launch.
- Reserved Instances – Purchase, at a significant discount, instances that are always available, for a term from one to three years.
- Scheduled Instances – Purchase instances that are always available on the specified recurring schedule, for a one-year term.
- Spot Instances – Request unused EC2 instances, which can lower your Amazon EC2 costs significantly.
- Dedicated Hosts – Pay for a physical host that is fully dedicated to running your instances, and bring your existing per-socket, per-core, or per-VM software licenses to reduce costs.
- Dedicated Instances – Pay, by the hour, for instances that run on single-tenant hardware.

Based on this , all other pricing options are invalid.
For more information on instance pricing options, please visit the url

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html)

Ask our Experts

QUESTION 60 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company currently has a set of EC2 Instances hosted on the AWS Cloud. There is a requirement to ensure the restart of instances if a cloudwatch metric goes beyond a certain threshold. As a solutions architect, how would you ask the IT admin staff to implement this?

- **A.** Look at the Cloudtrail logs for events and then restart the Instance based on the events
- **B.** Create a CloudWatch metric which looks into the instance threshold, and assign this metric against an alarm to reboot the instance. ✔
- **C.** Create a CLI script that restarts the server at certain intervals
- **D.** Use the AWS Config utility on the EC2 Instance to check for metrics and restart the server

Explanation :

Answer – B
The AWS Documentation mentions the following
Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.
Based on what the AWS Documentation mentions , all other options are invalid
For more information on using alarm actions, please visit the url

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html)

Ask our Experts

QUESTION 61 CORRECT DEFINE PERFORMANT ARCHITECTURES

You have a read intensive application hosted in AWS. The application is currently using the MySQL RDS feature in AWS. The cloudwatch metrics is showing high read throughput on the database and is causing performance issues on the database. Which of the following can be used to reduce the read throughput on the MySQL database?

- **A.** Enable the Multi-AZ on the MySQL RDS
- **B.** Use Cold Storage Volumes for the MySQL RDS
- **C.** Enable Read Replica's and offload the reads to the replica's ✔
- **D.** Use SQS to queue up the reads

Explanation :

Answer – C
The AWS documentation mentions the following on Read Replica's
Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.
Option A is invalid since this is used for fault tolerance for the database
Option B is invalid since this is not the ideal storage mechanism to used for databases which require high read throughput
Option D is invalid since SQS is used as a decoupling component and would not be the ideal fit to reduce the reads on the database
For more information on Read Replica's , please visit the below URL:

- https://aws.amazon.com/rds/details/read-replicas/ (https://aws.amazon.com/rds/details/read-replicas/)

Ask our Experts

A company is planning on moving an application which is currently hosted on their on-premises environment onto AWS. The application currently connects to a JSON based data store. They want to choose the right replacement in AWS. They also want to ensure that they avoid the task of maintaining the underlying infrastructure for the database. Which of the following should they choose as the underlying data store?

- A. AWS RDS
- B. AWS DynamoDB ✔
- C. AWS Redshift
- D. AWS Elastic Map Reduce

Explanation :

Answer - B
The AWS Documentation mentions the following
Amazon DynamoDB is a nonrelational database that delivers reliable performance at any scale. It's a fully managed, multi-region, multi-master database that provides consistent single-digit millisecond latency, and offers built-in security, backup and restore, and in-memory caching.
Option A is invalid since this is the not an ideal storage for JSON based data and is not fully managed
Option C is invalid since this is used for data warehousing solutions
Option D is invalid since this is used for Big data solutions
For more information on DynamoDB, please visit the below URL

- https://aws.amazon.com/dynamodb/ (https://aws.amazon.com/dynamodb/)

Ask our Experts

QUESTION 63 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company has started hosting their databases on the AWS Cloud. As an architect, they have requested you to advise the IT admin staff on what they should use to monitor the underlying databases and notifications should be sent to IT admin staff if any issues are detected. Which AWS services can accomplish these requirements? Choose 2 answers from the options given below.

- [ ] **A.** Amazon Simple Email Service
- [x] **B.** Amazon CloudWatch ✔
- [ ] **C.** Amazon Simple Queue Service (SQS)
- [ ] **D.** Amazon Route 53
- [x] **E.** Amazon Simple Notification Service (SNS) ✔

Explanation :

Answer - B and E
The AWS Documentation mentions the following
You can monitor DB instances using Amazon CloudWatch, which collects and processes raw data from Amazon RDS into readable, near real-time metrics. These statistics are recorded for a period of two weeks, so that you can access historical information and gain a better perspective on how your web application or service is performing.
Option A is invalid since this an email service and not a notification service
Option C is invalid since this is a queuing service
Option D is invalid since this is a domain name service
For more information on monitoring databases, please visit the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Monitoring.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Monitoring.html)

Ask our Experts

QUESTION 64 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company has started hosting their data store on AWS by using the Simple Storage service. They are storing files which are downloaded by users on a frequent basis. After a duration of 3 months, the files need to transferred to archive storage since they are not used beyond this point. Which of the following could be used to effectively manage this requirement?

- [ ] **A.** Transfer the files via scripts from S3 to Glacier after a period of 3 months
- [x] **B.** Use Lifecycle policies to transfer the files onto Glacier after a period of 3 months ✔

- **C.** Use Lifecycle policies to transfer the files onto Cold HDD after a period of 3 months
- **D.** Createa snapshot of the files in S3 after a period of 3 months

Explanation :

Answer - B
The AWS Documentation mentions the following
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A *lifecycle configuration* is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- Transition actions—Define when objects transition to another storage class (http://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html). For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.
- Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf. The lifecycle expiration costs depend on when you choose to expire objects.

Option A is invalid since there is already the option of lifecycle policies
Option C is invalid since lifecycle policies are used to transfer to Glacier or S3-Infrequent Access
Option D is invalid since snapshots are used for EBS volumes
For more information on S3 lifecycle policies, please visit the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html)

Ask our Experts

QUESTION 65 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your company is planning on setting up a VPC with private and public subnets and then hosting EC2 Instances in the subnet. It has to be ensured that instances in the private subnet can download updates from the internet. Which of the following needs to be part of the architecture for this requirement?

- **A.** WAF
- **B.** Direct Connect

C. NAT Gateway ✔

D. VPN

Explanation :

Answer – C
The AWS Documentation mentions the following
You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances
Option A is invalid since this is a web application firewall
Options B and D are invalid since this are used to connect on-premises infrastructure to AWS VPC's
For more information on NAT gateway, please visit the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14809)

Mobile App

Android Coming Soon

iOS Coming Soon

Follow us

(https://www.facebook.com/whizlabs.software/)

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

(https://plus.google.com/+WhizlabsSoftware)