CSAA Practice Test 3

Completed on 21-October-2020

Attempt
03

Marks Obtained
0 / 65

Your score
0.0%

Time Taken
N/A

Result
Failed

Domains wise Quiz Performance Report

No	1
Domain	Design Cost-Optimized Architectures
Total Question	6
Correct	0
Incorrect	0
Unattempted	6
Marked for review	0

No	2
Domain	Design High-Performing Architectures
Total Question	34
Correct	0
Incorrect	0
Unattempted	34
Marked for review	0
No	3
Domain	Design Secure Applications and Architectures
Total Question	13
Correct	0
Incorrect	0
Unattempted	13
Marked for review	0
No	4
Domain	Design Resilient Architectures
Total Question	12
Correct	0
Incorrect	0
Unattempted	12
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	65
Correct	0
Incorrect	0
Unattempted	65
Marked for review	0

Review the Answers

Sorting by All

Question 1 Unattempted

Domain :Design Cost-Optimized Architectures

A start-up firm has created a cloud storage application that gives users the ability to store any amount of personal data & share with their contacts. For this, they are using Amazon S3 buckets to store user data. During the last quarter, the costing team has observed a surge in storage cost for the S3 bucket. Further checking observed that there are many 100 GB files that are uploaded by users & are in a partially completed state. As an AWS consultant, the IT Team is requesting you for deleting all such files which are uploaded before the current quarter. Which of the following actions can be taken to meet this requirement in a cost-effective way with the least effort?

A. **Create an S3 lifecycle Configuration to abort incomplete multipart uploads.**

B. **Manually delete incomplete multipart uploads from the S3 bucket.**

C. **Use Cron tool to identify incomplete uploads & delete those files.**

D. **All Incomplete uploads are automatically deleted every three months by Amazon S3.**

Explanation:

Correct Answer – A

Amazon S3 Lifecycle rules can be configured to abort all multipart uploads which are failing to complete in a specific time period. For all files from size 5 MB to 5GB, the multipart upload can be used.

Option B is incorrect as this will need additional manual efforts

Option C is incorrect as this incurs additional cost & admin work to use Cron tools.

Option D is incorrect as this is incorrect incomplete uploads are not automatically deleted.

For more information on using S3 Lifecycle policies, refer to the following URL,

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-configuration-examples.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 2 Unattempted

Domain :Design High-Performing Architectures

You are developing a new mobile application which is expected to be used by thousands of customers. You are considering to store user preferences in AWS, and need a data store to save the same. Each data item is expected to be 20KB in size. The solution needs to be cost-effective, highly available, scalable, and secure. How would you design the data layer?

A. Create a new Amazon RDS instance and store the user data there.

B. Create a Amazon DynamoDB table with the required Read and Write capacity and use it as the data layer.

C. Use Amazon Glacier to store the user data.

D. Use an Amazon Redshift Cluster for managing the user preferences.

Explanation:

Correct Answer – B

In this case, since each data item is 20KB and given the fact that DynamoDB is an ideal data layer for storing user preferences, this would be the ideal choice. Also, DynamoDB is a highly scalable and available service.

For more information on AWS DynamoDB, please refer to the URL given below:

https://aws.amazon.com/dynamodb/

Try now labs related to this question

Introduction to AWS DynamoDB

This lab walks you through to Amazon DynamoDB features. In this lab, we will create a table in Amazon DynamoDB to store information and then query that information from the DynamoDB table.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 3 Unattempted

Domain :Design High-Performing Architectures

Your Operations department is using an incident-based application hosted on a set of EC2 Instances. These instances are placed behind an Auto Scaling Group to ensure that the right number of instances are in place to support the application. The Operations department has expressed dissatisfaction with regard to poor application performance every day at 9:00 AM. However, it is also noted that the system performance returns to optimal at 9:45 AM.
What could be done to fix this issue?

A. Create another Dynamic Scaling Policy to ensure that the scaling happens at 9:00 AM.

B. Add another Auto Scaling group to support the current one.

C. Change the Cool Down Timers for the existing Auto Scaling Group.

D. Add a Scheduled Scaling Policy at 8:30 AM.

Explanation:

Correct Answer - D

Scheduled Scaling can be used to ensure that the capacity is peaked before 9:00 AM every day.

AWS Documentation further mentions the following on Scheduled Scaling:

Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.

Option A is incorrect because a scheduled scaling should be used as per the requirements of the question instead of dynamic scaling

Option B is incorrect because adding another autoscaling group will not solve the problem.

Option C is incorrect because changing the cooldown timers of the existing autoscaling group will not meet the requirements of the question.

For more information on Scheduled Scaling, please refer to the URL below:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Try now labs related to this question

Introduction to Amazon Auto Scaling

AWS Auto Scaling will automatically scale resources as needed to align to your selected scaling strategy, This lab walks you through to use Auto Scaling to automatically launch or terminate EC2's instances based on user defined policies, schedules and health checks.

Credit Needed 10 Time 0 : 55 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 4 Unattempted

Domain :Design High-Performing Architectures

A database hosted in AWS is currently encountering an extended number of write operations and is not able to handle the load. What should be done to the architecture to ensure that the write operations are not lost under any circumstances?

A. **Add more IOPS to the existing EBS Volume used by the database.**

B. **Consider using DynamoDB instead of AWS RDS.**

C. **Use SQS FIFO to queue the database writes.**

D. **Use SNS to send notification on missed database writes and then add them manually at a later stage.**

Explanation:

Correct Answer – C

SQS Queues can be used to store the pending database writes, and these writes can then be added to the database. It is the perfect queuing system for such architecture.

Note that adding more IOPS may help the situation but will not totally eliminate the chances of losing database writes.

For more information on AWS SQS, please refer to the URL below:

https://aws.amazon.com/sqs/faqs/

Note:

The scenario in the question is that the database is unable to handle the write operations and the requirement is that without losing any data, we need to perform data writes to the database.

FIFO queues support up to 3,000 messages per second with batching and a single Amazon SQS message queue can contain an unlimited number of messages. However, there is a limit of 120,000 counts for the number of inflight messages for a standard queue and 20,000 counts for a FIFO queue.

Messages are inflight after they have been received from the queue by a consuming component, but have not yet been deleted from the queue.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 5 Unattempted

Domain :Design Secure Applications and Architectures

You have created an AWS Lambda function that will write data to a DynamoDB table. Which of the following must be in place to ensure that the Lambda function can interact with the DynamoDB table?

A. **Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges.**

B. **Ensure an IAM User is attached to the Lambda function which has the required DynamoDB privileges.**

C. **Ensure the Access keys are embedded in the AWS Lambda function.**

D. **Ensure the IAM user password is embedded in the AWS Lambda function.**

Explanation:

Correct Answer – A

AWS Documentation mentions the following to support this requirement:

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

For more information on the Permission Role model for AWS Lambda, please refer to the URL below.

https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html

Ask our Experts

Rate this Question?

View Queries open

Question 6 Unattempted

Domain :Design Cost-Optimized Architectures

A Media firm is saving all its old videos in S3 Glacier Deep Archive. Due to shortage of new video footage, the channel has decided to reuse all these old videos. Since these are old videos, the channel is not sure of its popularity & response from users. Channel Head wants to make sure that these huge size files do not shoot up their budget & for this as an AWS consultant you advise them to use S3 intelligent storage class. The Operations Team is concerned for moving these files to S3 Intelligent-Tiering storage class. Which of the following actions can be taken to move objects in Amazon S3 Glacier Deep Archive to S3 Intelligent-Tiering storage class?

A. **Use Amazon S3 Console to copy these objects from S3 Glacier Deep Archive to required S3 Intelligent-Tiering storage class.**

B. **Use Amazon S3 Glacier Console to restore objects from S3 Glacier Deep Archive & then copy these objects to required S3 Intelligent-Tiering storage class.**

C. **Use Amazon S3 console to restore objects from S3 Glacier Deep Archive & then copy these objects to required S3 Intelligent-Tiering storage class.**

D. **Use Amazon S3 Glacier console to copy these objects to the required S3 Intelligent-Tiering storage class.**

Explanation:

Correct Answer – C

To move objects from Glacier Deep Archive to different storage classes, first need to restore to original locations using Amazon S3 Glacier console & then use lifecycle policy to move objects to required S3 Intelligent-Tiering storage class.

Option A & D are incorrect as Objects in Glacier Deep Archive cannot be directly moved to another storage class. These need to be restored first & then copied to desired storage class.

Option B is incorrect as Amazon S3 Glacier console can be used to access only the vaults and objects in them.

For more information on moving objects between S3 storage classes refer to following URLs,

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

Ask our Experts

Rate this Question?

View Queries open

Question 7 Unattempted

Domain :Design High-Performing Architectures

A large retail firm is saving its global sales reports in S3 bucket & are using S3 Lifecycle rules to move this data from Standard_IA storage class to AWS S3 Glacier post 180 days. Due to the financial year end, the Finance team is looking for a sales report for only Europe region where there is mismatch reported in sales figure. Which of the following is a recommended way to fetch this data with least efforts?

A. **Retrieve this data from Amazon Glacier to S3 bucket & use Amazon S3 select to query specific continent data using simple SQL.**

B. **Retrieve this data from Amazon Glacier to S3 bucket & use Amazon Athena to query specific continent data using SQL.**

C. **Use Amazon S3 Glacier Select to query specific continent data which is restored to S3 bucket from AWS S3 Glacier.**

D. **Use Amazon S3 Glacier Select to query specific continent data directly from Amazon S3 Glacier using simple SQL.**

Explanation:

Correct Answer – D

Amazon S3 Glacier Select can be used to query specific data from Amazon S3 Glacier instead of querying whole data. Amazon S3 Glacier Select can directly query data from Amazon S3 Glacier & restoration of data to S3 bucket is not required for querying this data.

Option A is incorrect as for data stored in Amazon S3 Glacier, it's not necessary to restore data to S3 bucket.

Option B is incorrect as for data stored in Amazon S3 Glacier, it's not necessary to restore data to S3 bucket. Also, Amazon Athena is an interactive query tool to analyse data with S3 bucket.

Option C is incorrect as for using Amazon S3 Glacier Select, there is no restore data in S3 bucket.

For more information on using Amazon S3 Glacier Select, refer to the following URL,

https://aws.amazon.com/glacier/features/#amazon-glacier-select

Ask our Experts

Rate this Question?

View Queries open

Question 8 Unattempted

Domain :Design High-Performing Architectures

A large educational institute is using Amazon S3 buckets to save data for its all graduation streams. During annual external audits from local government bodies, institutes need to fetch data of specific streams to get it audited from auditors. A large amount of data is saved in these S3 buckets which makes it cumbersome to download whole data & retrieve only a small amount of information from it. The IT Team is looking for your consultation for this issue without incurring additional cost or compromising on security. Which of the following actions is recommended for resolution?

A. **Store objects in CSV format compressing it with Snappy using server-side encryption. Use Amazon S3 Select to retrieve a subset of data.**

B. **Store objects in JSON format compressing it with GZIP using server-side encryption. Use Amazon S3 Select to retrieve a subset of data.**

C. **Store objects in Apache Parquet format compressing the whole object with GZIP using server-side encryption. Use Amazon S3 Select to retrieve a subset of data.**

D. **Store objects in CSV format compressing it with BZIP2 without any encryption. Use Amazon S3 Select to retrieve a subset of data.**

Explanation:

Correct Answer – B

Amazon S3 Select can be used to query a subset of data from the objects stored in the S3 bucket using simple SQL. For using this, objects need to be stored in an S3 bucket with CSV, JSON, or Apache Parquet format. GZIP & BZIP2 compression is supported with CSV or JSON format with server-side encryption.

Option A is incorrect as with Amazon S3 Select, only GZIP & BZIP2 compression is supported with CSV format.

Option C is incorrect as Apache Parquet format with GZIP compression is not supported with S3 Select.

Option D is incorrect as although this will work, saving objects in S3 without encryption will risk the security of objects.

For more information on using S3 Select, refer to the following URL,

https://docs.aws.amazon.com/AmazonS3/latest/dev/selecting-content-from-objects.html

Ask our Experts

Rate this Question?

View Queries open

Question 9 Unattempted

Domain :Design High-Performing Architectures

A legal consultant firm is using version enabled S3 buckets to save all its legal documents. To avoid any deletion/ modification of these documents, they have locked these files with a retention period of 6 months. In some of the cases, these legal documents are getting updated with new information that the firm requires to set a different retention period than the original object. Which of the following actions will meet this requirement with the least efforts?

A. **Create another version with the same name as that of the object & have a separate retention period than the current object.**

B. **Create another bucket & place new objects with different retention periods.**

C. **Delete existing objects first & then place an object in the same bucket with different retention periods.**

D. **Modify name & version of object & have separate retention period than the current object.**

Explanation:

Correct Answer – A

With version enabled S3 buckets, each version of an object can have a different retention period.

Option B is incorrect as the creation of different buckets & placing an object in that bucket will work but this is not required as the same can be done using the existing S3 bucket.

Option C is incorrect as the deletion of existing objects is not required.

Option D is incorrect as a different name of the same object is not required which will increase additional complexity.

For more information on using Amazon S3 object lock, refer to the following URL,

https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock-overview.html

Ask our Experts

Rate this Question?

View Queries open

Question 10 Unattempted

Domain :Design High-Performing Architectures

You manage the IT users for a large organization that is moving many services to AWS. You want a seamless way for your employees to log in and use cloud services. You also want to use AWS Managed Microsoft AD and have been asked if users will be able to access services in the on-premises environment. What would you respond?

A. AWS Managed Microsoft AD requires data synchronization and replication to work properly

B. AWS Managed Microsoft AD can only be used for cloud or on-premises environments, not both

C. AWS Managed Microsoft AD can be used as the Active Directory over VPN or Direct Connect

D. **AWS Managed Microsoft AD is 100% the same as Active Directory running on separate EC2 instance**

Explanation:

Correct Answer: C

Option C is correct. Because you want to use AWS Managed Microsoft AD, you want to be certain that your users can use the AWS cloud resources as well as services in your on-premise environment. In order to make your company have connectivity for AWS services, once you implement VPN or Direct Connect, your AWS Managed Microsoft AD can be used for both cloud services and on-premises services.

Option A is incorrect. When data can be synchronized from on-premises to the cloud, it is not required.

Option B is incorrect. AWS Managed Microsoft AD can be used for both, it's not one or the other.

Option D is incorrect. AWS Managed Microsoft AD. being a managed service limits some capabilities versus running Active Directory by itself on EC2 instances

For more information, please visit the URLs below:

https://aws.amazon.com/directoryservice/

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 11 Unattempted

Domain :Design High-Performing Architectures

Your company is planning to use Route 53 as the DNS provider. There is a need to ensure that the company's domain name points to an existing CloudFront distribution. How could this be achieved?

A. Create an Alias record which points to the CloudFront distribution.

B. Create a host record which points to the CloudFront distribution.

C. Create a CNAME record which points to the CloudFront distribution.

D. Create a Non-Alias Record which points to the CloudFront distribution.

Explanation:

Correct Answer - A

AWS Documentation mentions the following:

While ordinary Amazon Route 53 records are standard DNS records, *alias records* provide a Route 53–specific extension to the DNS functionality. Instead of an IP address or a domain name, an alias record contains a pointer to a CloudFront distribution, an Elastic Beanstalk environment, an ELB Classic, Application, or Network Load Balancer, an Amazon S3 bucket that is configured as a static website, or another Route 53 record in the same hosted zone. 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.

For more information on Route 53 Alias records, please visit the following URL:

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

Note:

Route 53 uses "Alias Name" to connect to the CloudFront as Alias Record is a Route 53 extension to DNS. Also, Alias record is similar to a CNAME record, but the main difference is - you can create Alias record for both root domain & subdomain, whereas CNAME record can be created only to subdomain. Check the below link to get more information:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

Ask our Experts

Rate this Question?

View Queries open

Question 12 Unattempted

Domain :Design High-Performing Architectures

A company needs to extend its storage infrastructure to the AWS Cloud. The storage needs to be available as iSCSI devices for on-premises application servers. What should be done to fulfill this requirement?

A. **Create a Glacier vault. Use a Glacier Connector and mount it as an iSCSI device.**

B. **Create an S3 bucket. Use an S3 Connector and mount it as an iSCSI device.**

C. **Use the EFS file service and mount the different file systems to the on-premises servers.**

D. **Use the AWS Storage Gateway-cached volumes service.**

Explanation:

Correct Answer - D

AWS Documentation mentions the following:

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TB in size and attach iSCSI devices to them from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3, retains recently read data in your on-premises storage gateway's cache, and upload buffer storage.

For more information on AWS Storage Gateways, please visit the following URL:

https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html

Ask our Experts

Rate this Question?

View Queries open

Question 13 Unattempted

Domain :Design High-Performing Architectures

A global infrastructure firm is saving all its architectural drawing & project files in a S3 Glacier. These files will be randomly accessed by third-party vendors while performing Structural Audits. You need to ensure that only legitimate users will be able to read the contents of these files & no users should be able to delete these files for 3 years under any circumstances. Access to third-party vendors should be reviewed often as per security SOP. Which of the following can be done to meet this requirement?

A. Use Vault Access Policy to deny delete permission for 3 years updating this policy every 6 months & use Vault Lock Policy to permit read access to third -party vendors updating this policy every 6 months.

B. Use Vault Lock Policy to deny delete permission for 3 years updating policy once initially & use Vault Access Policy to permit read access to third -party vendors updating this policy monthly.

C. Use Vault Lock Policy to deny delete permission for 3 years updating this policy every 6 months & use Vault Access Policy to permit read access to third -party vendors updating this policy monthly.

D. Use Vault Access Policy to deny delete permission for 3 years updating this policy once initially & use Vault Lock Policy to permit read access to third -party vendors updating this policy only once initially.

Explanation:

Correct Answer – B

Vault Lock Policy can be used to lock users from performing specific action on archives stored in S3 Glaciers. Vault Access policy is used to grant permission to access these files in S3 Glacier. To meet the requirement, Vault Lock Policy can be used which can be updated only initially & post that no modifications can be done to this policy. Vault Access Policy can be used to grant standard permission & this policy can be modified as per user requirement.

Option A & D are incorrect as Vault Access policy need to be used to grant permission for access control while Vault Lock Policy need to be used to lock the policy to deny deletion of objects for compliance purpose.

Option C is incorrect as Vault Lock Policy can be modified only once & not every 6 months.

For more information on using Vault Access Policy & Vault Lock Policy, refer to following URL,

https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock.html

Ask our Experts

Rate this Question?

View Queries open

Question 14 Unattempted

Domain :Design Secure Applications and Architectures

Your current setup in AWS consists of the following architecture: 2 public subnets, one subnet which has web servers accessed by users across the Internet and another subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in this setup?

A. Consider moving the web server to a private subnet.

B. Create a private subnet and move the database server to a private subnet.

C. Consider moving both the web and database servers to a private subnet.

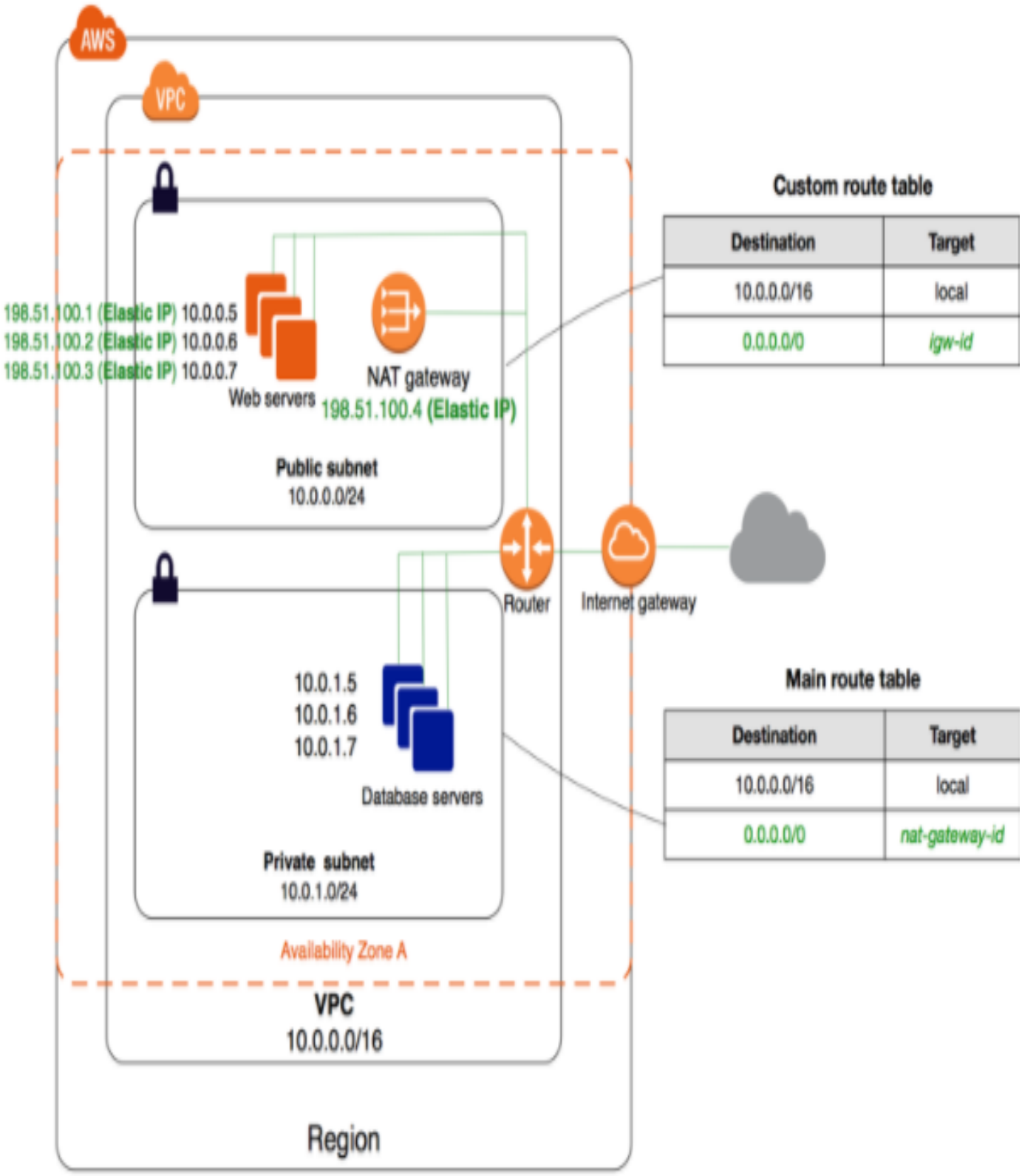
D. Consider creating a private subnet and adding a NAT Instance to that subnet.

Explanation:

Correct Answer – B

The ideal setup is to host the web server in the public subnet so that it can be accessed by users on the Internet. The database server can be hosted in the private subnet.

The below diagram from AWS Documentation shows the set up:



Try now labs related to this question

View Queries open

Question 15 Unattempted

Domain :Design Resilient Architectures

Your company has a set of applications that make use of Docker containers. There is a need to move these containers to AWS. Which option below is the BEST way to set up these Docker containers in a separate AWS environment?

A. **Create EC2 Instances, install Docker, and then upload the containers.**

B. **Create EC2 Container registries, install Docker, and then upload the containers.**

C. **Create an Elastic Beanstalk environment with the necessary Docker containers.**

D. **Create EBS Optimized EC2 Instances, install Docker, and then upload the containers.**

Explanation:

Correct Answer - C

The Elastic Beanstalk service can be used to host Docker containers.

AWS Documentation mentions the following:

Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that

aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run.

For more information on using Elastic Beanstalk for Docker containers, please visit the following URL:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html

Option B is incorrect because just creating the EC2 Container registries would not be sufficient. We need to incorporate some automated mechanism to take care of the function of the docker container if it fails in-between. An ElasticBeanStalk would be used for this purpose.

Note:

Option A could be partially correct as we need to install docker on EC2 instance. In addition to this, you need to create an ECS Task definition which details the docker image that we need to use for containers and how many containers to be used as well as the resource allocation for each container.

But with Option C, we have this added advantage:

If a Docker container running in an Elastic Beanstalk environment is crashed or killed for any reason, Elastic Beanstalk **restarts it automatically**.

In the given question, we have been asked about the best method to set up docker containers, hence Option C seems to be the most appropriate.

For more information, please check the URLs below:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html

https://aws.amazon.com/getting-started/tutorials/deploy-docker-containers/

Try now labs related to this question

Introduction to AWS Elastic Beanstalk

This lab walks you through to AWS Elastic Beanstalk. In this lab, you will quickly deploy and manage a Java application in the AWS Cloud without worrying about the infrastructure that runs those applications.

Credit Needed 10 Time 0 : 45 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 16 Unattempted

Domain :Design High-Performing Architectures

Instances in your private subnet hosted in AWS, need access to important documents in S3. Due to the confidential nature of these documents, you have to ensure that the traffic does not traverse through the internet. As an architect, how would you implement this solution?

A. **Consider using a VPC Endpoint.**

B. **Consider using an EC2 Endpoint.**

C. **Move the instances to a public subnet.**

D. **Create a VPN connection and access the S3 resources from the EC2 Instance.**

Explanation:

Correct Answer – A

AWS documentation mentions the following:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other services does not leave the Amazon network.

For more information on VPC Endpoints, please visit the following URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html

Try now labs related to this question

How to Create Virtual Private Cloud (VPC) with AWS CloudFormation

This lab walks you through how to create a VPC using AWS CloudFormation Stack. In this lab we will launch a AWS CloudFormation template to create a four-subnet Amazon VPC that spans two Availability Zones and a NAT that allows servers in the private subnets to communicate with the Internet in order to download packages and updates.

Credit Needed 10 Time 0 : 55 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 17 Unattempted

Domain :Design Resilient Architectures

The Developers Team is working on a new application for which they will be launching a large number of EC2 Instances. To decrease time in launching all these EC2 instances they want you to pre-warm these instances & keep ready for launching with all required patches & software. Which of the following can be done to meet this requirement?

A. Launch an Amazon EC2 instance with the Auto-Scaling group & enable Hibernate on each instance with the Auto-Scaling group.

B. Launch an Amazon EC2 instance with instance root volume & enable Hibernate.

C. Launch an Amazon EC2 instance with Amazon EBS root volume & enable Hibernate.

D. Launch an Amazon EC2 instance with Auto-Scaling group & enable Hibernate only on EC2 instance which will be hibernating.

Explanation:

Correct Answer – C

To pre-warm EC2 instance, EC2 Hibernate can be used. For this Amazon EC2 needs to be launched with Amazon EBS root volumes & also Auto-Scaling group is not supported with these EC2 instances.

Options A & D are incorrect as EC2 hibernate is not supported with EC2 instance in the Auto-Scaling group.

Option B is incorrect as EC2 hibernate is not supported on Instance store volume, it requires root volumes as Amazon EBS.

For more information on using Amazon EC2 instance, refer to the following URL,

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html

Ask our Experts

Rate this Question?

View Queries open

Question 18 Unattempted

Domain :Design High-Performing Architectures

A company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use EC2 worker instances to pull transcoding jobs from SQS. Why is SQS an appropriate service for this scenario?

A. **SQS guarantees the order of the messages.**

B. **SQS synchronously provides transcoding output.**

C. **SQS checks the health of the worker instances.**

D. **SQS helps to facilitate horizontal scaling of EC2 worker instances when the queue grows.**

Explanation:

Correct Answer - D

Even though SQS guarantees the order of messages for FIFO queues, the main reason for using it is because it helps in horizontal scaling of AWS resources and is used for decoupling systems.

SQS can neither be used for transcoding output nor for checking the health of worker instances. The health of worker instances can be checked via ELB or CloudWatch.

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

https://aws.amazon.com/sqs/faqs/

Ask our Experts

Rate this Question?

View Queries open

Question 19 Unattempted

Domain :Design High-Performing Architectures

You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point, you find out that other sites have been linking to the photos on your site, causing loss to your business. What would be an effective method to mitigate this?

A. **Remove public read access and use signed URLs with expiry dates.**

B. **Use CloudFront 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:

Correct Answer – A

Option B is incorrect because CloudFront is only used for the distribution of content across edge or region locations, and not for restricting access to content.

Option C is not feasible. Because of their dynamic nature, blocking IPs is challenging and you will not know which sites are accessing your main site.

Option D is incorrect since storing photos on an EBS Volume is neither good practice nor an ideal architectural approach for an AWS Solutions Architect.

For more information on Pre-Signed URLs, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html

Try now labs related to this question

Introduction to Amazon Simple Storage Service (S3)

This lab walks you through to Amazon Simple Storage Service. Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. In this lab we will demonstrate AWS S3 by creating a sample S3 bucket, uploading an object to S3 bucket and setting up bucket permission and policy.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 20 Unattempted

Domain :Design Secure Applications and Architectures

An IT firm has deployed a new application on a fleet of EC2 instances in an AWS Cloud Infrastructure. These EC2 instances are monitored by a legacy monitoring tool from on-premise. Some of these EC2 instances are hibernated based upon the response from users. Operations Team is concerned about the IP address retention for EC2 instance post hibernation so that they will modify on-premise monitoring tools accordingly. Which of the following is TRUE with respect to EC2 hibernation?

A. EC2 instance retains public IPv4 address & Elastic IP address assigned to this instance but releases a private IPv4 address associated with it.

B. EC2 instance retains private & public IP address along with Elastic IP address assigned to this instance.

C. EC2 instance retains private IPv4 address & Elastic IP address assigned to this instance but releases public IPv4 address associated with it.

D. EC2 instance releases private & public IP address along with the Elastic IP address assigned to this instance.

Explanation:

Correct Answer – C

Post EC2 hibernation, public IP address are released while Private IP address, as well as Elastic IP address associated with this EC2 instance, are retained.

Option A is incorrect as EC2 retains private & Elastic IP addresses and releases public IP addresses.

Option B is incorrect as the Public IP address allocated to EC2 instance is released post hibernation.

Option D is incorrect as Private IP address & Elastic IP address are retained post EC2 hibernation.

For more information on EC2 hibernation, refer to the following link,

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 21 Unattempted

Domain :Design High-Performing Architectures

A company currently hosts its architecture in the US region. They now need to duplicate this architecture to the Europe region and extend the application hosted on this architecture to the new region. In order to ensure that users across the globe get the same seamless experience, what should be done?

A. Create a Classic Elastic Load Balancer setup to route traffic to both locations.

B. Create a weighted Route 53 policy to route the policy based on the weightage for each location.

C. Create an Application Elastic Load Balancer setup to route traffic to both locations.

D. Create a Geolocation Route 53 Policy to route the traffic based on the location.

Explanation:

Correct Answer - D

AWS Documentation mentions the following with respect to this requirement:

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, which means the location that DNS queries originate from.

For more information on AWS Route 53 Routing Policies, please visit the following URL:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Ask our Experts

Rate this Question?

View Queries open

Question 22 Unattempted

Domain :Design Resilient Architectures

You have a set of EC2 Instances that support an application. They are currently hosted in the US Region. In the event of a disaster, you need a way to ensure that you can quickly provision the resources in another region. How could this be accomplished? (SELECT TWO)

A. **Copy the underlying EBS Volumes to the destination region.**

B. **Create EBS Snapshots and then copy them to the destination region.**

C. **Create AMIs for the underlying instances and copy them to the destination region.**

D. **Copy the metadata for the EC2 Instances to S3.**

Explanation:

Correct Answers – B and C

Snapshots can be used to create a AMI or template of the underlying instance. You can then copy the AMI to another region. You can also make snapshots of the volumes and then copy them to the destination region.

For more information on AMIs and EBS Snapshots, please visit the following URLs:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Try now labs related to this question

Creating New EC2 Instance using Snapshot

This lab walks you through creation of a snapshot of EC2 instance and launch a new EC2 instance using AMI of that snapshot.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 23 Unattempted

Domain :Design Secure Applications and Architectures

A start-up firm has deployed project files in the Amazon S3 bucket. This is accessed globally by intranet users for which they are using Amazon CloudFront. Last few days it was observed that these objects are being altered by unauthorized users directly from the S3 bucket. The Security Team wants to control access to these objects & make sure only authorized users are able to access these files only in a particular time period. You are working to find a resolution for the same. Which of the following actions can remediate this issue in a timely manner?

A. **Create an HTTP cookie for multiple objects in an S3 bucket using a Canned policy specifying start & end time for users to access video files.**

B. **Create an HTTP cookie for each object in an S3 bucket using a Canned policy specifying start & end time for users to access video files.**

C. Create an HTTP cookie for each object in an S3 bucket using Custom policy specifying start & end time for users to access video files.

D. Create an HTTP cookie for multiple objects in an S3 bucket using Custom policy specifying start & end time for users to access video files

Explanation:

Correct Answer – D

Custom policy statements wildcard characters can be used with Custom policy to allow multiple files.

Options A & B are incorrect as with Canned Policy start time & multiple files cannot be specified

Option C is incorrect as for each file there is no need to create a separate Custom policy.

For more information on using restricting access using Amazon CloudFront, refer to the following URLs,

https://aws.amazon.com/blogs/aws/new-amazon-cloudfront-signed-cookies-for-private-content/

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 24 Unattempted

Domain :Design Cost-Optimized Architectures

You are building an automated transcription service in which Amazon EC2 worker instances process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. You do not know about the storage capacity requirements. Which storage option would be both cost-efficient and scalable in this situation?

A. Multiple Amazon EBS Volume with snapshots

B. A single Amazon Glacier Vault

C. A single Amazon S3 bucket

D. Multiple instance stores

Explanation:

Correct Answer – C

Amazon S3 is the perfect storage solution for audio and text files. It is a highly available and durable storage device.

For more information on Amazon S3, please visit the following URL:

https://aws.amazon.com/s3/

Try now labs related to this question

Introduction to Amazon Simple Storage Service (S3)

This lab walks you through to Amazon Simple Storage Service. Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. In this lab we will demonstrate AWS S3 by creating a sample S3 bucket, uploading an object to S3 bucket and setting up bucket permission and policy.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 25 Unattempted

Domain :Design High-Performing Architectures

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the instance have been created with the default settings for the Network Access Control Lists. An IT

Administrator needs to be provided secure access to the underlying instance. How could this be accomplished?

A. **Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation.**

B. **Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation.**

C. **Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation.**

D. **Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation.**

Explanation:

Correct Answer - C

Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation. Since Security groups are stateful, we do not have to configure outbound traffic. What enters the inbound traffic is allowed in the outbound traffic too.

Note: The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated. Since the question does not mention that it is a custom VPC we would assume it to be the default one.

Based on this, Option C is the correct answer.

Since the IT administrator needs to be provided ssh access to the instance. The traffic would be inbound to the instance. Security group being stateful means that return response to the allowed inbound request will be allowed and vice-versa.

Allowing the outbound traffic would mean that instance would ssh into the IT admin's server and this server will send the response to the instance but it does not mean that IT admin would also be able to ssh into instance. SSh does not work like that.

To allow ssh, you need to allow inbound ssh access over port 22. For more information, please refer to the URL below:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html

Prerequisites for ssh

Before you connect to your Linux instance, complete the following prerequisites:

Install an SSH client

Your Linux computer most likely includes an SSH client by default. You can check for an SSH client by typing **ssh** at the command line. If your computer doesn't recognize the command, the OpenSSH project provides a free implementation of the full suite of SSH tools.

For more information, please refer to the URL below:

http://www.openssh.com.

Install the AWS CLI Tools (Optional)

If you're using a public AMI from a third party, you can use the command line tools to verify the fingerprint.

For more information about installing the AWS CLI, see Getting Set Up in the *AWS Command Line Interface User Guide*.

Get the ID of the instance

You can get the ID of your instance using the Amazon EC2 console (from the **Instance ID** column). If you prefer, you can use the describe-instances (AWS CLI) or Get-EC2Instance (AWS Tools for Windows PowerShell) command.

Get the public DNS name of the instance

You can get the public DNS for your instance using the Amazon EC2 console. Check the **Public DNS (IPv4)** column. If this column is hidden, choose the **Show/Hide** icon and select **Public DNS (IPv4)**. If you prefer, you can use the describe-instances (AWS CLI) or Get-EC2Instance (AWS Tools for Windows PowerShell) command.

Get the IPv6 address of the instance (IPv6 only)

If you've assigned an IPv6 address to your instance, you can optionally connect to the instance using its IPv6 address instead of a public IPv4 address or public IPv4 DNS hostname. Your local computer must have an IPv6 address and must be configured to use IPv6. You can get the IPv6 address of your instance using the Amazon EC2 console. Check the **IPv6 IPs field**. If you prefer, you can use the describe-instances (AWS CLI) or Get-EC2Instance (AWS Tools for Windows PowerShell) command.

For more information on IPv6, you can check IPv6 Addresses.

Locate the private key and verify permissions

Get the fully-qualified path to the location of the .pem file on your computer for the key pair that you specified when you launched the instance. Verify that the .pem file has permissions of

0400, not 0777.

For more information, please check Error: Unprotected Private Key File.

Get the default user name for the AMI that you used to launch your instance

For Amazon Linux 2 or the Amazon Linux AMI, the user name is `ec2-user`.

For a Centos AMI, the user name is `centos`.

For a Debian AMI, the user name is `admin` or `root`.

For a Fedora AMI, the user name is `ec2-user` or `fedora`.

For an RHEL AMI, the user name is `ec2-user` or `root`.

For a SUSE AMI, the user name is `ec2-user` or `root`.

For an Ubuntu AMI, the user name is `ubuntu`.

If `ec2-user` and `root` don't work, check with the AMI provider.

Enable inbound SSH traffic from your IP address to your instance

Ensure that the security group associated with your instance allows incoming SSH traffic from your IP address. The default security group for the VPC does not allow incoming SSH traffic by default. The security group created by the launch wizard enables SSH traffic by default.

For more information, please check Authorizing Inbound Traffic for Your Linux Instances.

Try now labs related to this question

Creating AMI From EC2 Instance

This lab walks you through the steps to create AMI from Amazon EC2 Instance. You will practice using Amazon Machine Images to launch Amazon EC2 Instance and Create AMI of that EC2 Instance.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 26 Unattempted

Domain :Design High-Performing Architectures

A company has an on-premises infrastructure which they want to extend to the AWS Cloud. There is a need to ensure that communication across both environments is possible over the Internet when initiated from on-premises. What should be set up on the on-premise side?

A. Create a VPC peering connection between the on-premises and the AWS Environment.

B. Create an AWS Direct connection between the on-premises and the AWS Environment.

C. Create a VPN connection between the on-premises and the AWS Environment.

D. Create a Virtual private gateway connection between the on-premises and the AWS Environment.

Explanation:

Correct Answer - C

AWS Documentation mentions the following:

One can create a Virtual private connection to establish communication across both environments over the Internet.

For more information on Virtual private connection, please visit the following URL:

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

Option A is invalid because 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. It is not used for connection between on-premises environment and AWS.

Option D is invalid because a virtual private gateway is the Amazon VPC side of a VPN connection. For

the communication to take place between the on-premise servers to AWS EC2 instances within the VPC, we need to set up the customer gateway at the on-premise location.

Note: The question says that "There is a need to ensure that communication across both environments is possible **over the Internet.**" AWS Direct Connect does not involve the Internet.

A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. **AWS Direct Connect does not involve the Internet;** instead, it uses dedicated, private network connections between your intranet and Amazon VPC.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 27 Unattempted

Domain :Design Resilient Architectures

A company wants to build a brand new application on the AWS Cloud. They want to ensure that this application follows the Microservices architecture. Which of the following services can be used to build this type of architecture? (SELECT THREE)

A. AWS Lambda

B. AWS ECS

C. AWS API Gateway

D. AWS Config

Explanation:

Correct Answers – A, B, and C

AWS Lambda is a serverless compute service that allows you to build independent services.

The Elastic Container Service (ECS) can be used to manage containers.

The API Gateway is a serverless component for managing access to APIs.

For more information about Microservices on AWS, please visit the following URL:

https://aws.amazon.com/microservices/

Try now labs related to this question

Introduction to Amazon Lambda

This lab walks you through creation and usage of AWS Serverless service called AWS Lambda. In this lab, we will create a sample lambda function which is triggered on S3 Object upload event and makes a copy of that object on another S3 Bucket.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 28 Unattempted

Domain :Design High-Performing Architectures

You are deploying an application to track the GPS coordinates of delivery trucks in the United States. Coordinates are transmitted from each delivery truck once every three seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. Which service should you use to implement data ingestion?

A. Amazon Kinesis

B. AWS Data Pipeline

C. Amazon AppStream

D. Amazon Simple Queue Service

Explanation:

Correct Answer - A

AWS documentation mentions the following:

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to process streaming data cost-effectively at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.

With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and responds instantly instead of waiting until all your data is collected before the processing can begin.

For more information on Amazon Kinesis, please visit the following URL:

https://aws.amazon.com/kinesis/

Ask our Experts

Rate this Question?

View Queries open

Question 29 Unattempted

Domain :Design High-Performing Architectures

Your company authenticates users in a very disconnected network requiring each user to have several username/password combinations for different applications. You have been assigned a task of consolidating and migrating services to the cloud and reducing the number of usernames and passwords, employees need to use. What would you recommend?

A. AWS Directory Service allows users to sign in with their existing corporate credentials – reducing the need for additional credentials.

B. Create two Active Directories – one for the cloud and one for on-premises – reducing username/password combinations to two

C. Require users to use third-party identity providers to log-in for all services

D. Build out Active Directory on EC2 instances to gain more control over user profiles

Explanation:

Correct Answer: A

Option A is correct. AWS Directory Service enables your end-users to use their existing corporate credentials while accessing AWS applications. Once you've been able to consolidate services to AWS, you won't have to create new credentials. Instead, you'll be able to allow the users to use their existing username/password.

Option B is incorrect. One Active Directory can be used for both on-premises and the cloud; this isn't the best option provided.

C. This won't always reduce the number of username/passwords combinations.

D. This requires more effort and additional management than using a managed service

For more information, please refer to the URLs below:

https://aws.amazon.com/directoryservice/faqs

https://aws.amazon.com/directoryservice/

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

Ask our Experts

Rate this Question?

View Queries open

Question 30 Unattempted

Domain :Design Cost-Optimized Architectures

A company is planning to use the AWS Redshift service. The Redshift service and data on it would be used continuously for the next 3 years as per the current business plan. What would be the most cost-effective solution in this scenario?

A. **Consider using On-demand instances for the Redshift Cluster.**

B. **Enable Automated backup.**

C. **Consider using Reserved Instances for the Redshift Cluster.**

D. **Consider not using a cluster for the Redshift nodes.**

Explanation:

Correct Answer - C

AWS documentation mentions the following:

If you intend to keep your Amazon Redshift cluster running continuously for a prolonged period, you should consider purchasing reserved node offerings. These offerings provide significant savings over on-demand pricing, but they require you to reserve compute nodes and commit to paying for those nodes for either a one-year or three-year duration.

For more information on Reserved Nodes in Redshift, please visit the following URL:

https://docs.aws.amazon.com/redshift/latest/mgmt/purchase-reserved-node-instance.html

Ask our Experts

Rate this Question? 

View Queries open

Question 31 Unattempted

Domain :Design High-Performing Architectures

A company is planning to run a number of admin-related scripts using the AWS Lambda service. There is a need to detect errors that occur while these scripts run. How could this be accomplished in

the most effective manner?

A. Use CloudWatch Metrics and Logs to detect the errors.

B. Use CloudTrail to monitor the errors

C. Use the AWS Config service to monitor the errors

D. Use the AWS Inspector service to monitor the errors

Explanation:

Correct Answer – A

AWS Documentation mentions the following:

AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function, Lambda logs all the requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.

For more information on Monitoring Lambda functions, please visit the following URL:

https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html

Try now labs related to this question

Creating Events in CloudWatch

This lab walks you through the Creating Rules in the Events Section of Cloudwatch and adding a SNS target. It will tested using EC2 Instance state events

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 32 Unattempted

Domain :Design Secure Applications and Architectures

Your organization is using a CloudFront distribution to distribute content from an S3 bucket. It is required that only a particular set of users get access to certain content. How could this be accomplished?

A. **Create IAM Users for each user and then provide access to the S3 bucket content.**

B. **Create IAM Group for each set of users and then provide each Group access of the S3 bucket**

C. **Create CloudFront signed URLs and then distribute these URLs to the users.**

D. **Use IAM Polices for the underlying S3 buckets to restrict content.**

Explanation:

Correct Answer - C

AWS Documentation mentions the following:

Many companies that distribute content via the internet, want to restrict access to documents, business data, media streams, or content that is intended for the selected users, for example, users who have paid a fee. To securely serve this private content using CloudFront, you can do the following:

Require that your users access your private content by using special CloudFront signed URLs or signed cookies.

Require that your users access your Amazon S3 content using CloudFront URLs, not Amazon S3 URLs. Requiring CloudFront URLs isn't required, but we recommend it to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies.

For more information on serving private content via CloudFront, please visit the following URL:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html#

Try now labs related to this question

Introduction to Amazon CloudFront

This lab walks you through to Amazon CloudFront creation and working. In this lab you will create an Amazon CloudFront distribution. It will distribute a publicly accessible image file stored in an Amazon S3 bucket.

Credit Needed 10 Time 1 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 33 Unattempted

Domain :Design Resilient Architectures

A financial institute is using a web-based application for its customers. They are planning to migrate to a serverless application for reducing cost & providing a better user experience with less latency. Since this is a critical application, any downtime will incur losses to this institute. For this Programme Director wants to have proper testing of application & post-deployment during the initial period traffic should be shared with existing & new serverless applications. As an AWS consultant which of the following is recommended to meet this requirement with the least cost & efforts?

A. **Test the application locally invoking Lambda function locally using AWS SAM. Post testing deploys application gradually using a separate CodeDeploy resource.**

B. **Test the application locally invoking Lambda function locally using AWS SAM. Post testing deploys application gradually using built-in CodeDeploy resources.**

C. **Test the application by creating a new VPC & test lambda function using AWS SAM. Post testing deploys application gradually using built-in CodeDeploy resources.**

D. **Test the application by creating a new VPC & test lambda function using AWS SAM. Post testing deploys application gradually using a separate CodeDeploy resource.**

Explanation:

Correct Answer – B

With AWS SAM, the application can be tested locally by invoking the Lambda function & event sources locally. Using these SAM templates, the application can be tested thoroughly before deploying in the AWS cloud. Also, CodeDeploy is built with AWS SAM which can help to deploy gradually within Cloud along with the existing applications which can minimize risks.

Option A is incorrect as a separate CodeDeploy resource does not need to be created with AWS SAM, it's inbuilt with AWS SAM.

Options C & D are incorrect as creating a new VPC & a test Lambda function will incur additional admin work & cost, instead of that AWS SAM can be used to invoke the Lambda function locally.

For more information on testing & gradual deployment with AWS SAM, refer to the following URLs,

https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-test-and-debug.html

https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-deploying.html

Ask our Experts

Rate this Question?

View Queries open

Question 34 Unattempted

Domain :Design High-Performing Architectures

You have a small company, running on Windows OS, that leveraging cloud resources like AWS Workspaces and AWS Workmail. You want a fully managed solution to set policies and provide user management. Which of the minimum required AWS Directory Service would you recommend?

A. AWS Managed Microsoft AD for its full-blown AD features and capabilities

B. AD Connector to be used with on-premises applications

C. AWS Cognito for its scalability and customization

D. Simple AD for limited functionality and compatibility with desired applications

Explanation:

Correct Answer: D

Option D - Simple AD for limited functionality and compatibility with desired applications is the correct answer. Simple AD is a Microsoft Active Directory–compatible directory from AWS Directory

Service. You can use Simple AD as a standalone directory in the cloud to support Windows workloads that need basic AD features or compatible AWS applications. It can also be used to support Linux workloads that need LDAP service.

Option A is incorrect. This is more functionality and feature-rich than you need, given the desired applications

Option B is incorrect. You don't have on-premises applications, so AD Connector is not needed.

Option C is incorrect. This is more functionality and feature-rich than you need, given the desired applications

For more information, please check the URLs below:

https://aws.amazon.com/directoryservice/

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

Ask our Experts

Rate this Question?

View Queries open

Question 35 Unattempted

Domain :Design Secure Applications and Architectures

You manage multiple AWS accounts in an AWS Organization. The AWS accounts of the development department are located in an Organizational Unit (OU). To reduce cost, the instance type of all EC2 instances created in these AWS accounts should be t2.micro. You attach a Service Control Policy (SCP) in the OU in order to restrict the instance type. Which of the following SCP is correct?

A.
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictInstanceType",
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals":{
          "ec2:InstanceType":"t2.micro"
        }
      }
    }
  ]
}
```

B.
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RestrictInstanceType",
   "Effect": "Deny",
   "Action": "ec2:RunInstances",
   "Resource": "arn:aws:ec2:*:*:instance/*",
   "Condition": {
    "StringNotEquals":{
     "ec2:InstanceType":"t2.micro"
    }
   }
  }
 ]
}
```

C.
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictInstanceType",
      "Effect": "Deny",
      "Action": "ec2:LaunchInstances",
      "Resource": "*",
      "Condition": {
        "StringEquals":{
          "ec2:InstanceType":"t2.micro"
        }
      }
    }
  ]
}
```

D. SCP cannot meet the requirement.

Explanation:

Correct Answer – B

About how SCP works, please refer to the reference in https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html. In this scenario, the EC2 instance is not allowed to be launched if the instance type is not t2.micro. Option B is the correct answer.

Option A is incorrect: Because other instance types may be allowed as well since by default an AWS Organization has an SCP that allows full AWS access.

Option B is CORRECT: Because the policy has the correct condition to check the instance type and denies the action if it is not t2.micro.

Option C is incorrect: Because the StringEquals condition in the policy is incorrect. With the policy, a t2.micro instance cannot be launched.

Option D is incorrect: Check the above explanations.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 36 Unattempted

Domain :Design High-Performing Architectures

Your company requires a Stack-based model for its resources in AWS. There is a need to have different stacks for the Development and Production environments. Which of the following can be used for this?

A. **Use EC2 tags to define different stack layers for your resources.**

B. **Define the metadata for the different layers in DynamoDB.**

C. **Use AWS OpsWorks to define the different layers for your application.**

D. **Use AWS Config to define the different layers for your application.**

Explanation:

Correct Answer - C

The requirement can be fulfilled via the OpsWorks service. The AWS Documentation given below supports this requirement:

AWS OpsWorks Stacks lets you manage applications and servers on AWS and on-premises. With OpsWorks Stacks, you can model your application as a stack containing different layers, such as load balancing, database, and application server. You can deploy and configure Amazon EC2 instances in each layer or connect other resources such as Amazon RDS databases.

For more information on OpsWorks stacks, please visit the following URL:

https://aws.amazon.com/opsworks/stacks/

A stack is basically a collection of instances that are managed together for serving a common task.

Consider a sample stack whose purpose is to serve web applications. It will be comprised of the following instances.

A set of application server instances, each of which handles a portion of the incoming traffic.

A load balancer instance, which takes incoming traffic and distributes it across the application servers.

A database instance, which serves as a back-end data store for the application servers.

A common practice is to have multiple stacks that represent different environments. A typical set of stacks consists of:

A development stack to be used by developers to add features, fix bugs, and perform other development and maintenance tasks.

A staging stack to verify updates or fixes before exposing them publicly.

A production stack, which is the public-facing version that handles incoming requests from users.

For more information, please see the link given below:

https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 37 Unattempted

Domain :Design High-Performing Architectures

Your company has been hosting a static website in an S3 bucket for several months and gets a fair amount of traffic. Now you want your registered .com domain to serve content from the bucket. Your domain is reached via https://www.myfavoritedomain.com. However, any traffic requested through https://www.myfavorite.com is not getting through. What could be the most likely cause of this disruption?

A. The new domain name is not registered in CloudWatch monitoring

B. The S3 bucket has not been configured to allow Cross-Origin Resource Sharing (CORS)

C. The S3 bucket was not created in the correct region

D. https://www.myfavoritedomain.com wasn't registered with AWS Route 53 and therefore won't work

Explanation:

Correct Answer: B

Option B is correct. The S3 bucket has not been configured to allow Cross-Origin Resource Sharing (CORS). In order to keep your content safe, your web browser implements something called the same-origin policy.

The default policy ensures that scripts and other active content loaded from one site or domain cannot interfere or interact with content from another location without an explicit indication that this is the desired behavior.

Option A is incorrect. Enabling Cloudwatch doesn't affect Cross-Origin Resource Sharing (CORS)

Option C is incorrect. S3 buckets are not region-specific.

Option D is incorrect. The domain can be registered with any online registrar, not just AWS Route53.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html

https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html

https://aws.amazon.com/blogs/aws/amazon-S3-cross-origin-resource-sharing/

Ask our Experts

Rate this Question?

View Queries open

Question 38 Unattempted

Domain :Design Secure Applications and Architectures

An AWS Organization has below the hierarchy of Organizational Units (OUs):
Root -> Project_OU -> Dev_OU
The Root is attached to the default Service Control Policy (SCP).
Project_OU is attached to an SCP that prevents users from deleting VPC Flow Logs.
Dev_OU has an SCP that allows the action of "ec2: DeleteFlowLogs".
Are the IAM users/roles in Dev_OU AWS accounts allowed to delete VPC Flow Logs?

A. **It is permitted because the SCP in Dev_OU allows it.**

B. **It is allowed because the Root has the default SCP that allows all actions.**

C. **It is not allowed as the SCP in Project_OU restricts the action.**

D. **It is not allowed as the default SCP in Root denies the action.**

Explanation:

Correct Answer – C

Check https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html for how SCPs work in an AWS Organization.

Option A is incorrect: Because if any parent OU has an SCP to deny the action, the final result is Deny.

Option B is incorrect: Although the default SCP allows the action, the parent OU (Project_OU) denies it.

Option C is CORRECT: Because an explicit Deny statement in Project_OU overrides any Allow.

Option D is incorrect: Because the default SCP is FullAWSAccess which allows all actions and all services.

Ask our Experts

Rate this Question?

View Queries open

Question 39 Unattempted

Domain :Design Secure Applications and Architectures

One AWS Organization owns several AWS accounts. Recently, due to a change of company organizations, one member account needs to be moved from this AWS Organization to another one. How can you achieve this?

A. **In the AWS console, drag and drop this account from one Organization to another.**

B. **In the AWS console, select the member account and migrate it to the destination AWS Organization.**

C. **Delete the old AWS Organization. Send an invite from the new Organization and accept the invite for the member account.**

D. **Remove the account in the old Organization. Send an invite from the new Organization and accept the invite from the member account.**

Explanation:

Correct Answer – D

About how to move accounts between AWS Organizations, please refer to https://aws.amazon.com/premiumsupport/knowledge-center/organizations-move-accounts/.

Option A is incorrect: This operation cannot be performed.

Option B is incorrect: Because a member account cannot be migrated to another AWS Organization directly.

Option C is incorrect: Because there is no need to delete the old Organization.

Option D is CORRECT: The account needs to be removed from the old Organization and then accept the invitation from the new Organization. The option describes the correct method.

Ask our Experts

Rate this Question?

View Queries open

Question 40 Unattempted

Domain :Design Secure Applications and Architectures

While managing permissions for the API Gateway, what could be used to ensure that the right level of permissions is given to Developers, IT Admins, and users? Also, the permissions should be easily managed.

A. **Use the secure token service to manage the permissions for different users.**

B. **Use IAM Policies to create different policies for different types of users.**

C. **Use the AWS Config tool to manage the permissions for different users.**

D. **Use IAM Access Keys to create sets of keys for different types of users.**

Explanation:

Correct Answer – B

AWS Documentation mentions the following:

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.

To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

For more information on permissions with the API Gateway, please visit the following URL:

https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html

Try now labs related to this question

Introduction to AWS Identity Access Management(IAM)

This lab walks you through the steps on how to create IAM Users, IAM Groups and adding IAM User to the IAM Group in AWS IAM service

Credit Needed 0 Time 0 : 20 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 41 Unattempted

Domain :Design High-Performing Architectures

Your Development team wants to use EC2 Instances to host their Application and Web servers. In the automation space, they want the Instances to always download the latest version of the Web and Application servers when they are launched. As an architect, what would you recommend for this scenario?

A. Ask the Development team to create scripts which can be added to the User Data section when the instance is launched.

B. Ask the Development team to create scripts which can be added to the Meta Data section when the instance is launched.

C. Use Auto Scaling Groups to install the Web and Application servers when the instances are launched.

D. Use EC2 Config to install the Web and Application servers when the instances are launched.

Explanation:

Correct Answer - A

AWS Documentation mentions the following:

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts.

You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. You can also pass this data into the launch wizard as plain text, as a file (this is useful for launching instances using the command line tools) or as base64-encoded text (for API calls).

For more information on User Data, please visit the following URL:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 42 Unattempted

Domain :Design High-Performing Architectures

Your company has an application that takes care of uploading, processing, and publishing videos, posted by users. The current architecture for this application includes the following:
a) A set of EC2 Instances to transfer user-uploaded videos to S3 buckets
b) A set of EC2 worker processes to process and publish the videos
c) An Auto Scaling Group for the EC2 worker processes
Which of the following can be added to the architecture to make it more reliable?

A. Amazon SQS

B. Amazon SNS

C. Amazon CloudFront

D. Amazon SES

Explanation:

Correct Answer - A

Amazon SQS is used to decouple systems. It can store requests to process videos, to be picked up by the worker processes.

AWS Documentation mentions the following:

Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable, hosted queue for storing messages as they travel between applications or microservices. It moves data between distributed application components and helps you decouple these components.

For more information on AWS SQS, please visit the following URL:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/Welcome.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 43 Unattempted

Domain :Design High-Performing Architectures

There is an urgent requirement to monitor some database metrics for a database hosted on AWS and send notifications. Which AWS services can accomplish this? (Select Two)

A. Amazon Simple Email Service

B. Amazon CloudWatch

C. Amazon Simple Queue Service

D. Amazon Route 53

E. Amazon Simple Notification Service

Explanation:

Correct Answer – B and E

Amazon CloudWatch will be used to monitor the IOPS metrics from the RDS Instance and Amazon Simple Notification Service will be used to send the notification if an alarm is triggered.

For more information on CloudWatch and SNS, please visit the URLs below.

https://aws.amazon.com/cloudwatch/

https://aws.amazon.com/sns/

Try now labs related to this question

Creating Events in CloudWatch

This lab walks you through the Creating Rules in the Events Section of Cloudwatch and adding a SNS target. It will tested using EC2 Instance state events

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 44 Unattempted

Domain :Design Resilient Architectures

You have a business-critical two-tier web application, currently deployed in 2 Availability Zones in a single region, using Elastic Load Balancing and Auto Scaling. The app depends on synchronous replication at the database layer. The application needs to remain fully available even if one application AZ goes offline or Auto Scaling cannot launch new instances in the remaining AZ. How could the current Elastic Load Balancing be enhanced to ensure this?

A. **Deploy in 2 regions using Weighted Round Robin with Auto Scaling set at a minimum 50% peak load per region.**

B. **Deploy in 3 AZ with Auto Scaling, set to handle a minimum of 33 percent peak load per zone.**

C. **Deploy in 3 AZ with Auto Scaling, set to handle a minimum 50 percent peak load per zone.**

D. **Deploy in 2 regions using Weighted Round Robin with Auto Scaling, set at minimum 100% peak load per region.**

Explanation:

Correct Answer – C

Since the requirement states that the application should never go down even if an AZ is not available, we need to maintain 100% availability.

Options A and D are incorrect because region deployment is not possible for ELB. ELBs can manage traffic within a region, not between regions.

Option B is incorrect because even if one AZ goes down, we would be operating at only 66% and not the required 100%.

For more information on Auto Scaling, please visit the URL below:

https://aws.amazon.com/autoscaling/

NOTE:

In the question, it is clearly mentioned that "The application needs to remain fully available even if one application AZ goes offline and if Auto Scaling cannot launch new instances in the remaining AZ".

Here you need to maintain 100% availability.

In option B, when you create 3 AZs with minimum 33% load on each, If any failure occurs in one AZ then

$$33\% + 33\% = 66\% .$$

Here you can handle only 66% and the remaining 34% of load, not handling.

But when you select option C, when you create 3 AZs with minimum 50% load on each, If any failure occurs in one AZ then

50% + 50% =100% .

Here you can handle full load i.e 100%.

Try now labs related to this question

Introduction to Amazon Auto Scaling

AWS Auto Scaling will automatically scale resources as needed to align to your selected scaling strategy, This lab walks you through to use Auto Scaling to automatically launch or terminate EC2's instances based on user defined policies, schedules and health checks.

Credit Needed 10 Time 0 : 55 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 45 Unattempted

Domain :Design Resilient Architectures

You have been asked to create a VPC network topology for your company. The VPC network must support both internet-facing applications and internal-facing applications accessed only over VPN. Both Internet-facing and internal-facing applications must be able to leverage at least 3 AZs for high availability. How many subnets must you create within your VPC to accommodate these requirements?

A. 2

B. 3

C. 4

D. 6

Explanation:

Correct Answer - D

Since each subnet corresponds to one Availability Zone and you need 3 AZs for both the internet and intranet applications, you will need 6 subnets.

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

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

Ask our Experts

Rate this Question?

View Queries open

Question 46 Unattempted

Domain :Design High-Performing Architectures

You have the following architecture deployed in AWS:
a) A set of EC2 Instances which sit behind an ELB
b) A database hosted in Amazon RDS
Of late, the performance on the database has been slacking due to a high number of read requests.
Which of the following can be added to the architecture to alleviate the performance issue? **(Select Two)**

A. **Add read replica to the primary database to offload read traffic.**

B. **Use ElastiCache in front of the database.**

C. **Use AWS CloudFront in front of the database.**

D. **Use Amazon DynamoDB to offload all the reads. Populate the common read items in a separate table.**

Explanation:

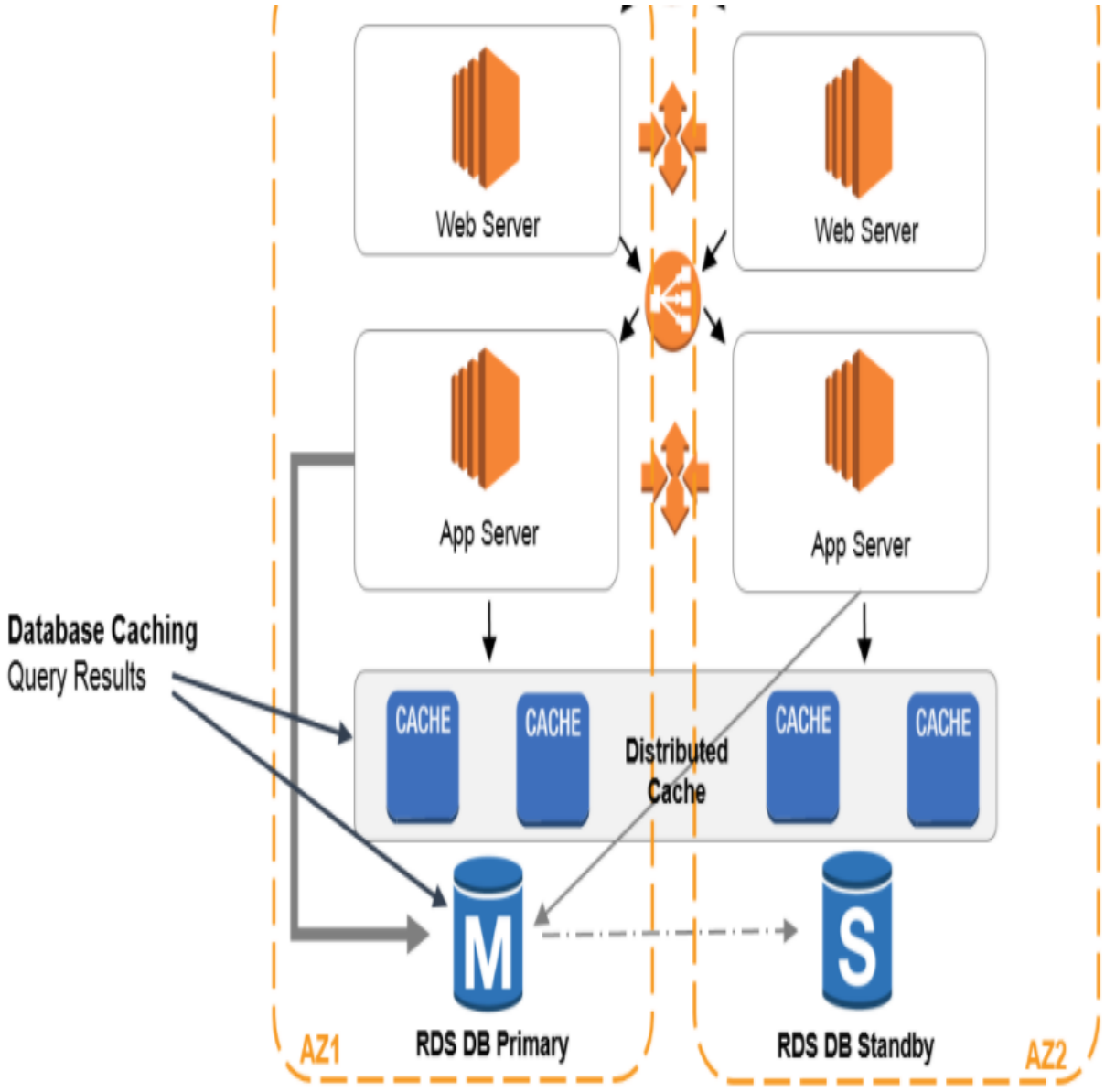
Correct Answer - A and B

Option A is correct.

AWS says "Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. **This 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."

Amazon ElastiCache is an in-memory cache which can be used to cache common read requests.

The below diagram shows how caching can be added to an existing architecture:



For more information on database caching, please visit the URL below:

https://aws.amazon.com/caching/database-caching/

Note:

Option C is incorrect because CloudFront is a valuable component of scaling a website, especially for

geo-location workloads and queries; more advanced for the given architecture.

Option D is incorrect because it will have latency and additional changes as well.

Ask our Experts

Rate this Question?

View Queries open

Question 47 Unattempted

Domain :Design Secure Applications and Architectures

You have two AWS Organizations. All the AWS accounts in Organization A need to be moved to Organization B. You have already moved all the member accounts and now you need to migrate the master account. Which of the following options should you choose?

A. **Delete Organization A and invite the master account to join Organization B.**

B. **Remove the master account from Organization A and send an invitation to the account to join Organization B.**

C. **Send an invitation to the master account. Accept the invitation to move the account from Organization A to Organization B.**

D. **The master account in one Organization cannot join another one.**

Explanation:

Correct Answer – A

The reference can be found in https://aws.amazon.com/premiumsupport/knowledge-center/organizations-move-accounts/.

Option A is CORRECT: For the master account, the Organization needs to be deleted before the account accepts an invitation to join another one.

Option B is incorrect: Because the master account cannot be removed from an AWS Organization.

Option C is incorrect: Because the master account in one AWS Organization cannot accept an invitation to join another one.

Option D is incorrect: Check the above explanations in option A.

Ask our Experts

Rate this Question?

View Queries open

Question 48 Unattempted

Domain :Design High-Performing Architectures

A customer wants to import the existing virtual machines to the cloud. Which service should they use for this purpose?

A. VM Import/Export

B. AWS Import/Export

C. AWS Storage Gateway

D. DB Migration Service

Explanation:

Correct Answer – A

VM Import/Export enables customers to import Virtual Machine (VM) images in order to create Amazon EC2 instances. Customers can also export previously imported EC2 instances to create VMs. Customers can use VM Import/Export to leverage their previous investments in building VMs by migrating their VMs to Amazon EC2.

For more information on AWS VM Import, please visit the URL below:

https://aws.amazon.com/ec2/vm-import/

Few strategies used for migration are:
1. Forklift migration strategy
2. Hybrid migration strategy
3. Creating AMIs

AWS Import/Export - It is a data transport service used to move large amounts of data in and out of the Amazon Web Services public cloud using portable storage devices for transport.

https://aws.amazon.com/about-aws/whats-new/2009/05/20/AWS-Import-Export/

AWS Storage Gateway - It connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure. The gateway provides access to objects in S3 as files or file share mount points.

https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

DB Migration Service - It can migrate your data to and from most of the widely used commercial and open-source databases. It supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora.

For more information, please check the URL below:

https://aws.amazon.com/dms/

Ask our Experts

Rate this Question?

View Queries open

Question 49 Unattempted

Domain :Design Resilient Architectures

A company website is set to launch in the upcoming weeks. There is a probability that the traffic will be quite high during the initial weeks. In the event of a load failure, how is it possible to set up DNS failover to a static website?

A. Duplicate the exact application architecture in another region and configure DNS Weight-based routing.

B. Enable failover to an on-premises data center to the application hosted there.

C. Use Route 53 with the failover option, to failover to a static S3 website bucket or CloudFront distribution.

D. Add more servers in case the application fails.

Explanation:

Correct Answer – C

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources.

If you have multiple resources that perform the same function, you can configure DNS failover so that Amazon Route 53 will route your traffic from an unhealthy resource to a healthy resource. For example, if you have two web servers and one web server becomes unhealthy, Amazon Route 53 can route traffic to the other web server. So you can route traffic to a website hosted on S3 or to a CloudFront distribution.

For more information on DNS failover using Route 53, please refer to the link below.

http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html

Ask our Experts

Rate this Question?

View Queries open

Question 50 Unattempted

Domain :Design Resilient Architectures

A company is running three production web server reserved EC2 Instances with EBS-backed root volumes. These instances have a consistent CPU load of 80%. Traffic is being distributed to these instances by an Elastic Load Balancer. They also have production and development Multi-AZ RDS MySQL databases. What recommendation would you make to reduce cost in this environment without affecting the availability of mission-critical systems? Choose the correct answer from the options given below.

A. **Consider using On-demand instances instead of Reserved EC2 instances.**

B. **Consider not using a Multi-AZ RDS deployment for the development database.**

C. **Consider using Spot instances instead of Reserved EC2 instances.**

D. **Consider removing the Elastic Load Balancer.**

Explanation:

Correct Answer – B

Multi-AZ databases are better for production environments rather than for development environments, so you can reduce costs by not using these for development environments.

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. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

For more information on Multi-AZ RDS, please refer to the link below.

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

Note:

Mission Critical system refers to production Instances and Databases. However, if you notice, they have Multi-AZ RDS also on the Development environment which is not necessary. Because management is always concerned about production, the environment should be perfect.

In order to reduce the cost, we can disable the Multi-AZ RDS for Development environment and keep it only for the Production environment.

Try now labs related to this question

Introduction to AWS Relational Database Service

This lab walks you through to the creation and testing of an Amazon Relational Database Service (Amazon RDS) database. We will create an RDS MySql Database and test the connection using MySQL Workbench.

Credit Needed 10 Time 0 : 50 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 51 Unattempted

Domain :Design Cost-Optimized Architectures

In order to manage a large number of AWS accounts in a better way, you create a new AWS Organization and invite these accounts. You only enable the “Consolidated billing” feature set in the organization. Which of the below features does the AWS Organization have?

A. Apply SCPs to restrict the services that IAM users can access.

B. Configure tag policies to maintain consistent tags for resources in the organization's accounts.

C. Configure a policy to prevent IAM users in the organization from disabling AWS CloudTrail.

D. Combine the usage across all accounts to share the volume pricing discounts.

Explanation:

Correct Answer – D

Refer to https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#feature-set-cb-only for the differences between "Consolidated billing" and "All features".

Option A is incorrect: Because SCP is part of the advanced features which belong to "All features".

Option B is incorrect: Because tag policies can be applied under the feature set of "All features".

Option C is incorrect: This is implemented using SCP which is not supported in "Consolidated billing".

Option D is CORRECT: This is supported in "Consolidated billing" according to

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html.

Ask our Experts

Rate this Question?

View Queries open

Question 52 Unattempted

Domain :Design Resilient Architectures

You are designing an architecture on AWS with disaster recovery in mind. Currently, the architecture consists of an ELB and underlying EC2 Instances lie in a primary and secondary region. How could you establish a switchover in case of failure in the primary region?

A. Use Route 53 Health Checks and then do a failover.

B. Use CloudWatch metrics to detect the failure and then do a failover.

C. Use scripts to scan CloudWatch logs to detect the failure and then do a failover.

D. Use CloudTrail to detect the failure and then do a failover.

Explanation:

Correct Answer - A

AWS Documentation mentions the following:

If you have multiple resources that perform the same function, you can configure DNS failover so that Route 53 will route your traffic from an unhealthy resource to a healthy resource. For example, if you have two web servers and one web server becomes unhealthy, Route 53 can route traffic to the other web server.

For more information on configuring DNS failover using Route 53, please refer to the below link:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html

Ask our Experts

Rate this Question?

View Queries open

Question 53 Unattempted

Domain :Design Resilient Architectures

You are working as an AWS Architect for an IT Company. Your Company is using EC2 instances in multiple VPCs spanning Availability Zones in (US-EAST-1) Region. The Development Team has deployed a new Intranet application that needs to be accessed via VPC. You have been asked to establish connectivity between all the VPCs and to make sure the solution is highly scalable and secure. Which of the following solution would you recommend?

A. **Attach an Internet Gateway to all the VPCs at the "US-EAST-1" region and allow all users to access this application over the internet.**

B. **Deploy Network Load Balancers along with VPC endpoint service (AWS PrivateLink) to establish connectivity between the VPC's in the "US-EAST-1" region.**

C. **Use VPC Peering between all the VPCs at the "US-EAST-1" region to provide connectivity between users & servers.**

D. **Create a VPN between instances at the various VPCs in "US-EAST-1" region to establish connectivity**

Explanation:

Correct Answer – B

AWS PrivateLink provides secure private connectivity for services between separate VPC's. For this, Network Load Balancers can be used in service provider while Elastic Network Interface is created in service, consuming VPC. Using DNS, service provider service is resolved to the local IP address assigned to Elastic Network Interface which will forward all traffic to the Network Load Balancer in the provider network. Network Load Balancer will perform a source NAT for all traffic & forward it to the provider instance.

Option A is incorrect. Using the Internet to establish connectivity between users & servers will not be a highly secure solution.

Option C is incorrect. With VPC peering, all resources in each VPC will have access to resources in other VPC. Also, since only one client will be initiating a request to servers, VPC peering will not be an ideal solution.

Option D is incorrect as VPN connectivity between the instance of various VPCs will not be a scalable solution.

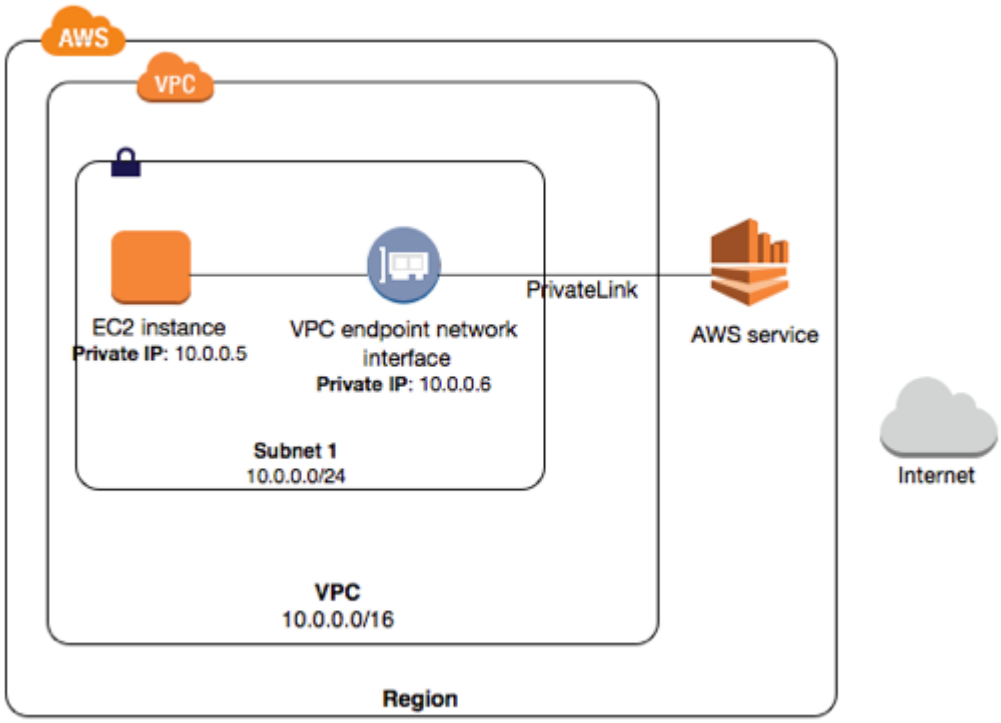
For more information on AWS PrivateLink, refer to the following URL:

https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html

Accessing Services Through AWS Private Links:

AWS PrivateLink is a highly available, scalable technology that enables you to privately connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services. You do not require an internet gateway, NAT device, public IP address, AWS Direct Connect connection, or AWS Site-to-Site VPN connection to communicate with the service. The traffic between your VPC and the service does not leave the Amazon network.

To use AWS PrivateLink, create an interface VPC endpoint for a service in your VPC. This creates an elastic network interface in your subnet with a private IP address that serves as an entry point for the traffic, destined to the service. For more information, see VPC Endpoints.



You can create your own AWS PrivateLink-powered service (endpoint service) and enable other AWS customers to access your service. For more information, see VPC Endpoint Services (AWS PrivateLink).

For more information, refer to the following URLs:

https://aws.amazon.com/privatelink/

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html#what-is-privatelink

Ask our Experts

Rate this Question?

View Queries open

Question 54 Unattempted

Domain :Design High-Performing Architectures

You want to host a static website on AWS. As a Solutions architect, you have been given a task to establish a serverless architecture for the website. Which of the following could be included in the proposed architecture? **(Select Two)**

A. **Use DynamoDB to store data in tables.**

B. **Use EC2 to host data on EBS Volumes.**

C. **Use the Simple Storage Service to store data.**

D. **Use AWS RDS to store data.**

Explanation:

Correct Answer – A and C

Both the Simple Storage Service and DynamoDB are complete serverless offerings from AWS for which you don't need to maintain servers, and your applications have the automated high availability.

For more information on S3 and DynamoDB, please refer to the links below.

https://aws.amazon.com/s3/

https://aws.amazon.com/dynamodb/

https://aws.amazon.com/serverless/

https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/

Try now labs related to this question

View Queries open

Question 55 Unattempted

Domain :Design High-Performing Architectures

Currently, you're responsible for the design and architect of a highly available application. After building the initial environment, you discover that a part of your application does not work correctly until port 443 is added to the security group. After adding port 443 to the appropriate security group, how much time will it take for the application to work correctly?

A. Generally, it takes 2-5 minutes for the rules to propagate.

B. Immediately after a reboot of the EC2 Instances, belonging to that security group.

C. Changes apply instantly to the security group, and the application should be able to respond to 443 requests.

D. It will take 60 seconds for the rules to apply to all Availability Zones within the region.

Explanation:

Correct Answer – C

This is given in the AWS Documentation:

"Some systems for setting up firewalls let you filter on source ports. Security groups let you filter only on destination ports.

When you add or remove rules, they are automatically applied to all instances associated with the security group".

For more information on Security Groups, please refer to the below link:

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

Ask our Experts

Rate this Question?

View Queries open

Question 56 Unattempted

Domain :Design Secure Applications and Architectures

You work in a large organization. Your team creates AWS resources such as Amazon EC2 dedicated hosts and reserved capacities that need to be shared by other AWS accounts. You need an AWS service to centrally manage these resources so that you can easily specify which accounts or Organizations can access the resources. Which AWS service would you choose to meet this requirement?

A. IAM

B. Resource Access Manager

C. Service Catalog

D. AWS Single Sign-On

Explanation:

Correct Answer – B

AWS Resource Access Manager (AWS RAM) helps users to share resources with other AWS accounts or Organizations. Refer to https://docs.aws.amazon.com/ram/latest/userguide/what-is.html.

Option A is incorrect: Because IAM cannot be used to manage and share these resources.

Option B is CORRECT: EC2 dedicated hosts and reserved capacities are shareable resources that are supported by Resource Access Manager. Check https://docs.aws.amazon.com/ram/latest/userguide/shareable.html.

Option C is incorrect: Because Service Catalog is used to manage catalogs and cannot share resources with others.

Option D is incorrect: Because AWS Single Sign-On is used for SSO access and does not share the mentioned resources.

Ask our Experts

Rate this Question?

View Queries open

Question 57 Unattempted

Domain :Design High-Performing Architectures

Your company wants to use an S3 bucket for web hosting but have several different domains to perform operations on the S3 content. In the CORS configuration, you have added CORSRule AllowedOrigin for the following Domains: http://www.domainnamea.com, https://www.secure.domainnamea.com, and http://www.domainnameb.com. Following Domains, https://www.domainnameb.com and http://www.domainnameb.com:80, are not allowed to access the S3 bucket.
What could be the most likely cause behind it?

A. **Both request https:// domainnameb.com and http://www.domainnameb.com:80 don't match the allowed in configuration.**

B. **HTTPS must contain a specific port in the request, e.g. https:// domainnameb.com:443**

C. **There's a limit of two origin sites per S3 bucket allowed**

D. **Adding CORS automatically removes the S3 ACL and bucket policies**

Explanation:

Correct Answer: A

Option A is correct. The origin was configured as http://www.domainnameb.com and request was sent for https://www.domainnameb.com and http://www.domainnameb.com:80 instead of http://www.domainnameb.com. The exact syntax must be matched. In some cases, wildcards can be used to help the origin URLs.

Option B is incorrect. This is not required to allow an origin domain to be included; although it can be.

Option C is incorrect. The limit is 100.

Option D is incorrect. The ACLs and policies continue to apply when you enable CORS on the bucket.

Verify that the Origin header in your request matches at least one of the AllowedOrigin elements in the specified CORSRule.

The scheme, the host, and the port values in the Origin request header must match the AllowedOrigin elements in the CORSRule. For example, if you set the CORSRule to allow the origin http://www.example.com, then both https://www.example.com and http://www.example.com:80 origins in your request don't match the allowed origin in your configuration.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html

https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html

https://aws.amazon.com/blogs/aws/amazon-S3-cross-origin-resource-sharing/

Try now labs related to this question

How to Create a static website using Amazon S3

This lab walks you through how to create a static HTML webstie using aws S3 and make it global to the internet.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 58 Unattempted

Domain :Design High-Performing Architectures

Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of Spot EC2 Instances. Files submitted by your premium customers must be transformed at the highest priority. How would you implement such a system?

A. Use a DynamoDB table with an attribute defining the priority level. Transformation instances will scan the table for tasks, sorting the results by priority level.

B. Use Route 53 latency-based routing to send high priority tasks to the closest transformation instances.

C. Use two SQS queues, one for high priority messages and the other for default priority. Transformation instances will first poll the high priority queue; if there is no message, they will poll the default priority queue.

D. Use a single SQS queue. Each message contains the priority level. Transformation instances poll high-priority messages first.

Explanation:

Correct Answer – C

The best way is to use two SQS queues. Each queue can be polled separately. The high priority queue can be polled first.

For more information on AWS SQS, please refer to the link below:

https://aws.amazon.com/sqs/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 59 Unattempted

Domain :Design High-Performing Architectures

A VPC has been set up with a subnet and an internet gateway. The EC2 instance is set up with a public IP but you are still not able to connect to it via the Internet. The security groups are also in place. What should you do to connect to the EC2 Instance from the Internet?

A. Set an Elastic IP Address to the EC2 Instance.

B. Set a Secondary Private IP Address to the EC2 Instance.

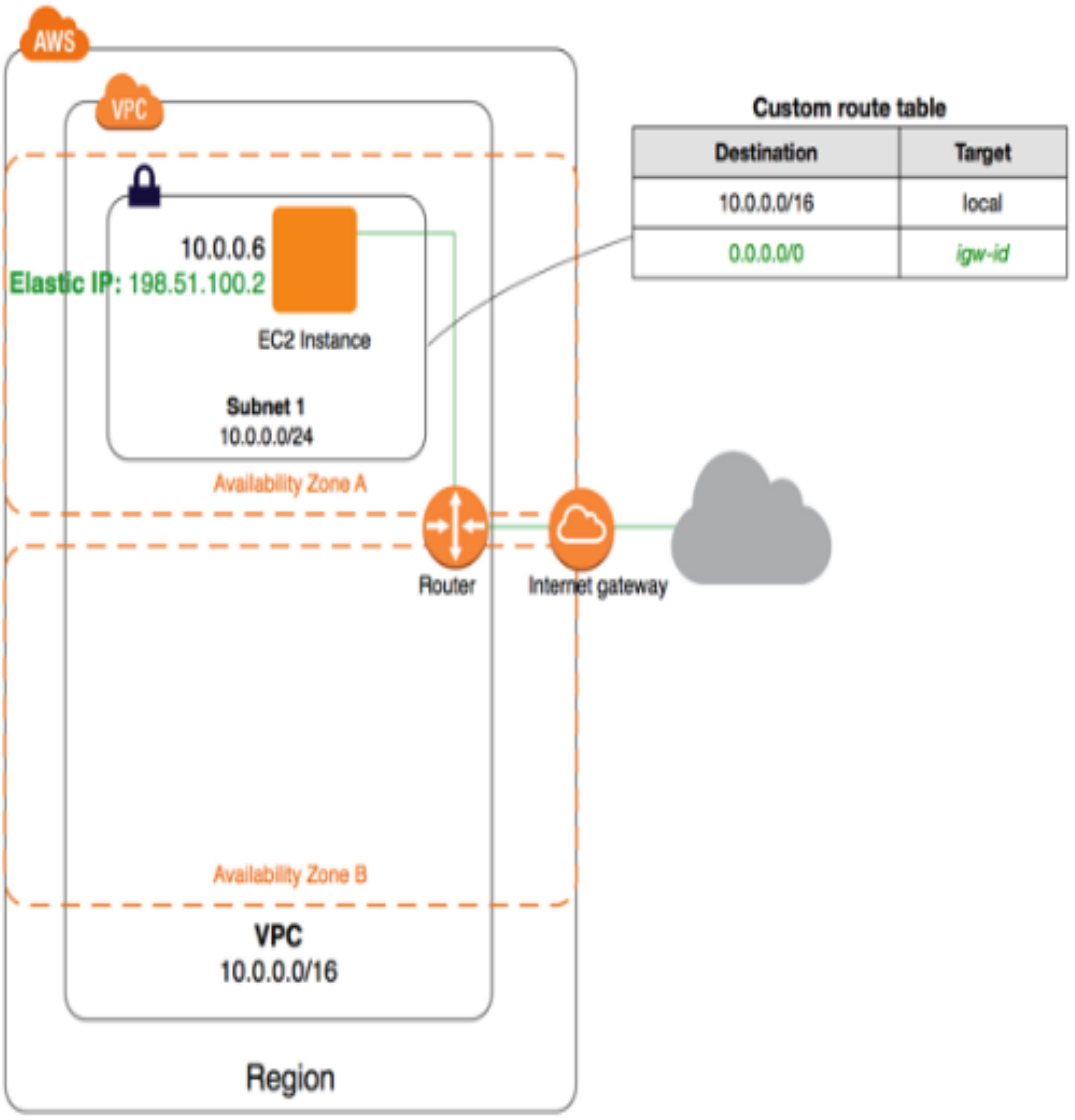
C. Ensure that the right route entry is there in the Route table.

D. There must be some issue in the EC2 Instance. Check the system logs.

Explanation:

Correct Answer – C

You have to ensure that the Route table has an entry to the Internet Gateway because this is required for instances to communicate over the Internet. The diagram shows the configuration of the public subnet in a VPC:



Option A is incorrect. Since you already have a public IP assigned to the instance, this should have been enough to connect to the Internet.
Option B is incorrect. Private IPs cannot be accessed from the Internet.
Option D is incorrect. The Route table is causing the issue and not the system.

For more information on AWS public subnet, please visit the link below.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

Try now labs related to this question

Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.

2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.

3. This will give an in-depth understanding of internal components of VPC and subnets.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 60 Unattempted

Domain :Design High-Performing Architectures

A customer has a single 3 TB volume on-premises that is used to hold a large repository of images and print layout files. This repository is growing at 500 GB a year and must be presented as a single logical volume. The customer is becoming increasingly constrained with their local storage and wants to utilize the cloud to store the data, but the customer is concerned about latency while trying to access most frequent data from the cloud. Which AWS Storage Gateway configuration would meet the customer requirements?

A. Gateway-Cached Volumes with snapshots scheduled to Amazon S3

B. Gateway-Stored Volumes with snapshots scheduled to Amazon S3

C. Gateway-Virtual Tape Library with snapshots to Amazon S3

D. Gateway-Virtual Tape Library with snapshots to Amazon Glacier

Explanation:

Correct Answer - A

Gateway-cached volumes let you use Amazon Simple Storage Service (Amazon S3) as your primary data storage while retaining frequently accessed data locally in your storage gateway. Gateway-

cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TB in size and attach them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.

For more information on Storage Gateways, please visit the link below:

http://docs.aws.amazon.com/storagegateway/latest/userguide/storage-gateway-cached-concepts.html

Note:

The two requirements of the question are low latency access to frequently accessed data and an offsite back up of the data.

Option A is correct because your primary data is written to S3 while retaining your frequently accessed data locally in a cache for low-latency access.

Option B is incorrect because it is storing the primary data locally (but we have a storage constraint hence this is not a viable solution) and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

Options C & D are incorrect as they cannot provide low latency access to frequently accessed data.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 61 Unattempted

Domain :Design Cost-Optimized Architectures

A company is planning to use the AWS ECS service to work with containers in "us-east-1" region. There is a need for the least amount of administrative overhead while launching containers. How could this be achieved?

A. **Use the Fargate launch type in AWS ECS.**

B. Use the EC2 launch type in AWS ECS.

C. Use the Auto Scaling launch type in AWS ECS.

D. Use the ELB launch type in AWS ECS.

Explanation:

Correct Answer - A

AWS Documentation mentions the following:

The Fargate launch type allows you to run your containerized applications without the need to provision and manage the backend infrastructure. Just register your task definition and Fargate launches the container for you.

For more information on the different launch types, please visit the links below:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/launch_types.html

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 62 Unattempted

Domain :Design Resilient Architectures

You currently manage a set of web servers hosted on EC2 Servers with public IP addresses. These IP addresses are mapped to domain names. There was an urgent maintenance activity that had to be carried out on the servers and the servers had to be stopped and restarted. Now the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier. Which of the following could be a reason for this?

A. The Route 53 hosted zone needs to be restarted.

B. The network interfaces need to initialized again.

C. The public IP addresses need to be associated with the ENI again.

D. The public IP addresses have changed after the instance was stopped and started again.

Explanation:

Correct Answer – D

By default, the public IP address of an EC2 Instance is released after the instance is stopped and started. Hence, the earlier IP address which was mapped to the domain names would have become invalid now.

For more information on public IP address, please visit the URL below:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses

Note:

This only applies to IPv4 public addresses, IPv6 public address isn't disassociated after an instance is stopped.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 63 Unattempted

Domain :Design Secure Applications and Architectures

You are responsible for deploying a critical application to AWS. It is required to ensure that the controls set for this application meet PCI compliance. Also, there is a need to monitor web application logs to identify any malicious activity. Which of the following services could be used to fulfill this requirement? **(Select Three)**

A. Amazon CloudWatch Logs

B. Amazon VPC Flow Logs

C. Amazon Trusted Advisor

D. Amazon CloudTrail

Explanation:

Correct Answers – A, B, and D

AWS Documentation mentions the following about these services:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

For more information on CloudTrail, please refer to following URL:

https://aws.amazon.com/cloudtrail/

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

For more information on CloudWatch logs, please refer to the URL below:

Please refer to the "PCI" tab on the following link to check for services that are "PCI Compliant"

https://aws.amazon.com/compliance/services-in-scope/

Please check for the column "PCI" with a tick mark for the services that are "PCI Compliant"

Flow logs enable you to track and analyze the IP address traffic going to and from network interfaces in your VPC. For example, if you have a content delivery platform, flow logs can profile, analyze, and predict customer patterns of the content access, and track down top talkers and malicious calls. Taking the above definition into consideration, VPC Flow Logs is a correct option.

Option C is incorrect because AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It is not required as per the requirement.

To know more, please check the URL below:

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/

https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

Ask our Experts

Rate this Question?

View Queries open

Question 64 Unattempted

Domain :Design High-Performing Architectures

There is a requirement to host a database server. The server should be able to connect to the Internet while downloading the required database patches, but the ingress traffic to the instances are not allowed. Which of the following solutions would satisfy all the above requirements at best?

A. Setup the database in a private subnet with a security group that only allows outbound traffic.

B. Setup the database in a public subnet with a security group that only allows inbound traffic.

C. Setup the database in a local data center and use a private gateway to connect the application to the database.

D. Setup the database in a private subnet which connects to the Internet via a NAT Instance.

Explanation:

Correct Answer – D

This setup coincides with Scenario 2 of setting up a VPC as per AWS documentation:

Scenario 2: VPC with Public and Private Subnets (NAT)

The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application while maintaining backend servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.

For more information on the VPC Scenario for public and private subnets, please see the below link:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

Try now labs related to this question

Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.
2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.
3. This will give an in-depth understanding of internal components of VPC and subnets.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 65 Unattempted

Domain :Design Secure Applications and Architectures

You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Which of the following would be the best way to accomplish this using policies?

A. **Launch the development and production instances in separate VPCs and use VPC Peering.**

B. Create an IAM group with a condition that allows access to only those instances which are used for production or development.

C. Launch the development and production instances in different Availability Zones and use Multi-Factor Authentication.

D. Define the tags on the Development and production servers and add a condition to the IAM Policy which allows access to specific tags.

Explanation:

Correct Answer – D

You can easily add tags to define which instances are the production instances and which ones are development instances. These tags can then be used while controlling access via an IAM Policy.

For more information on tagging your resources, please refer to the link below.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

Note:

It can be done with the help of option B as well. However, the question is looking for the "best way to fulfill the requirement using policies".

By using the option D, you can reduce the usage of different IAM Policies on each instance.

Try now labs related to this question

Introduction to AWS Identity Access Management(IAM)

This lab walks you through the steps on how to create IAM Users, IAM Groups and adding IAM User to the IAM Group in AWS IAM service

Credit Needed 0 Time 0 : 20 Try Now

Ask our Experts

Rate this Question?

View Queries open

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Become Our Instructor

Support

Discussions

Blog

Business

Support

Contact Us

Help Topics

Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!

Follow us