> My Courses > AWS Certified Solutions Architect Associate > CSAA Practice Test 7 > **Report**

Search Courses

CSAA Practice Test 7

Completed on 21-October-2020

Attempt

03

Marks Obtained

0 / 67

Your score

0.0%

Time Taken

N/A

Result

Failed

Domains wise Quiz Performance Report

Join us on Slack community

No	1
Domain	Design Resilient Architectures
Total Question	14
Correct	0
Incorrect	0
Unattempted	14
Marked for review	0

No	2
Domain	Design Secure Applications and Architectures
Total Question	16
Correct	0
Incorrect	0
Unattempted	16
Marked for review	0

No	3
Domain	Design Cost-Optimized Architectures
Total Question	8
Correct	0
Incorrect	0
Unattempted	8
Marked for review	0

No	4
Domain	Design High-Performing Architectures
Total Question	27
Correct	0
Incorrect	0
Unattempted	27
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 Resilient Architectures

Your company is planning on the following architecture for their application

A set of EC2 Instances hosting the web part of the application.

A relational database for the backend

A Load balancer for distribution of traffic

A NAT gateway for routing traffic from the database server to the Internet

Which of the following architecture ensures high availability across all components?

A. **A Load balancer with one public subnet, one private subnet. The EC2 Instances placed in one Availability Zone. RDS with Multi-AZ Enabled. NAT Gateway in one availability zone.**

B. **A Load balancer with 2 public subnets, 2 private subnets. The EC2 Instances placed across 2 Availability Zones. RDS with Multi-AZ Enabled. NAT Gateways in each availability zone**

C. **A Load balancer with 2 public subnets, 2 private subnets. The EC2 Instances placed in 2 Availability Zones. RDS with Multi-AZ Enabled. NAT Gateway in one availability zone**

D. **A Load balancer with 2 public subnets, 2 private subnets. The EC2 Instances placed in one Availability Zone. RDS with Multi-AZ Enabled. NAT Gateway in one availability zone**

Explanation:

Answer: B

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Let’s try to understand the scenario using a few use cases:

Depending upon your appetite for risk, you might configure things differently…

Use Case 1: A load balancer, one public subnet, one private subnet in same AZ, one NAT Gateway, and RDS with Multi-AZ

The NAT Gateway goes into the public subnet

The EC2 Instances go into the private subnet

The Route Table for the private subnet points to the NAT Gateway in the public subnet

Use Case 2: A load balancer, two public subnets, two private subnets, one NAT Gateway, RDS with Multi-AZ

The NAT Gateway goes into one public subnet (Public-Subnet-A)

The EC2 instances are launched in private subnets across two AZs (Private-Subnet-A, Private-Subnet-B) or across same AZ (Private-Subnet-A/Private-Subnet-B)

The Route Table for *both* of the private subnets point to the NAT Gateway

However, if there is a failure with Availability Zone A (rare, but can happen), then the NAT Gateway is not reachable from Private-Subnet-B. Thus, the system may be impacted even though it is running across two AZs or single AZ.

Use Case 3: A load balancer, two public subnets, two private subnets, two NAT Gateways, RDS with Multi-AZ

The NAT Gateway goes into both public subnets (Public-Subnet-A, Public-Subnet-B)

The EC2 instances are launched in private subnets across two AZs (Private-Subnet-A, Private-Subnet-B)

The Route Table Private-Subnet-A points to the NAT Gateway in Public-Subnet-A

The Route Table Private-Subnet-B points to the NAT Gateway in Public-Subnet-B

If one of the AZs should fail, then the EC2 instances in the remaining private subnet will still be able to communicate with the Internet because they have their own NAT Gateway in the same AZ.

Option A) is incorrect because according to Use Case 1, High Availability is not ensured as

When you enable an Availability Zone for your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. If you register targets in an Availability Zone but do not enable the Availability Zone, these registered targets do not receive traffic. Note that your load balancer is most effective if you ensure that each enabled Availability Zone has at least one registered target.

We recommend that you enable multiple Availability Zones. (Note that with an Application Load Balancer, we require you to enable multiple Availability Zones.) With this configuration, if one

Availability Zone becomes unavailable or has no healthy targets, the load balancer can continue to route traffic to the healthy targets in another Availability Zone.

Option B) is Correct because according to Use Case 3, High Availability is ensured.

Option C) and D) are incorrect because according to Use Case 2, High Availability is not ensured as either if we have EC2 in single AZ or in multiple AZ, We have NAT Gateway in single AZ which is a cause for not ensuring High Availability.

For more information on Elastic Load Balancing, Multi-AZ and NAT gateway, please refer to the below URL's

https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 **Time** 0 : 30 Try Now

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 2 Unattempted

Domain :Design Secure Applications and Architectures

Your company has an AWS account and a lot of resources defined in the Frankfurt region. They want to track the changes to the resources in their account. Which of the following should be used for this purpose?

A. **AWS Config**

B. **AWS CloudTrail**

C. **AWS CloudWatch**

D. **AWS Opswork**

Explanation:

Answer: B

Option A is incorrect because AWS Config is a fully managed service that provides you with a resource inventory, configuration history, and configuration change notifications to enable security and governance. Also, you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time.

Option B is correct because this is an API monitoring service and using 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. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts.

Also, CloudTrail records the changes made to AWS Config including who made the change, vice versa may not true.

Option C is invalid because this is a metric and logging service

Option D is invalid because is used to deploy stacks of resources

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

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

CloudWatch and Config serve distinct use cases for monitoring and complements each other from the AWS ecosystem.

Config is typically used for auditing and compliance purposes across organizations to verify whether AWS resource changes being made are per compliance rules.

CloudWatch is designed to provide performance information about AWS resources such as EC2, Lambda, etc. Developers can use information from CloudWatch to identify bottlenecks in applications or workflows.

CloudWatch will help you to send alerts when CPU /Memory utilization reaches a certain threshold and browse metrics associated with CPU/Network to identify operational and security issues.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 3 Unattempted

Domain :Design Resilient Architectures

You are working for a Pharma company having operations in North America. The company has a corporate Data Centre in New York which includes Web Servers & Active Directory. As a part of migrating all services to the cloud, few services will be initially migrated to EC2 instances deployed in VPC at the us-east-1 region. The Pharma Company already has a managed AD server in AWS. You are planning to set up AWS SSO for this purpose so that users can sign in to AWS accounts using on-premise Active Directory credentials. You need to ensure that the proposed solution should consider the future growth of users and all users should be able to reset the password from anywhere.
Also, the highly available solution should be secure, cost-effective and ensure reliable performance with bandwidth requirement up-to 1.2 Gbps. What would be the most appropriate solution to meet this requirement?

A. **Setup a Direct-Connect between the Data Centre and VPC in us-east1. Create a Two-Way Trust relationship with on-premise Active Directory.**

B. **Setup a Direct-Connect between the Data Centre and VPC in us-east1. Create an AD Connector with on-premise Active Directory.**

C. **Setup a VPN connection between the Data Centre and VPC in us-east1. Create a Two-Way Trust relationship with on-premise Active Directory.**

D. **Setup a VPN connection between Data Centre & VPC in us-east1. Create an AD Connector with on-premise Active Directory.**

Explanation:

Correct Answer – C

AWS SSO can connect to On-Premise Active Directory so that users in on-premise Active-Directory can use AWS SSO to access AWS accounts & resources. Since the company is looking for a solution with future growth, there would be a necessity of 1.2 Gbps bandwidth for which VPN connection between Data Centre & VPC will be the most appropriate solution.

> Option A is incorrect because each connection consists of a single dedicated connection between ports on your router and an Amazon router. We recommend establishing a second connection if redundancy is required. When you request multiple ports at the same AWS Direct Connect location, they will be provisioned on redundant Amazon routers. To achieve high availability, we recommend you to have connections at multiple AWS Direct Connect locations. You can refer to the below URL to learn more about achieving highly available network connectivity. Setting up second connection will incur high costs whereas setting up a failover VPN connection will not incur high cost.

https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/

> Option B is incorrect as with AD Connector, users will not be able to reset passwords from AWS SSO, but only from On-Premise Active Directory. With AD Connector, AWS SSO does not cache user information & forward all requests to On-Premise Active Directory.
>
> Option C is correct as because VPN connection is encrypted and high available and have bandwidth up to 1.25 Gbps.

https://aws.amazon.com/vpn/features/

> Option D is incorrect because, With AD Connector, users will not be able to reset passwords from AWS SSO, but only from On-Premise Active Directory. With AD Connector, AWS SSO does not cache user information and forward all requests to On-Premise Active Directory.

A two-way trust relationship is required because when two-way trust relationships are created between AWS Managed Microsoft AD and an on-premises Active Directory, on-premises users can sign in with their corporate credentials to various AWS services and business applications.

For more information on connecting AWS SSO to On-Premise Active Directory, refer to the following URLs:

https://docs.aws.amazon.com/singlesignon/latest/userguide/connectonpremad.html

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries

open ⌄

Question 4

Unattempted

Domain :Design Resilient Architectures

A company is planning on hosting an application with the below architecture

- A lambda function which reads the metadata of objects from an S3 bucket
- The Lambda function then stores the metadata in DynamoDB and AWS RDS - MySQL

Which of the following needs to be in place to ensure the above architecture is high available?

A. **Enable Cross Region Replication for the S3 bucket**

B. **Enable Lambda functions in Multiple Availability Zones**

C. **Enabling Multi-AZ for the MySQL database**

D. **Enable Auto-Scaling for the DynamoDB table**

Explanation:

Answer – C

Option C is correct because In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Option A is invalid because the S3 service is already a highly available service within a particular region. Also, Amazon S3 gives any developer access to the same highly scalable, highly available, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites. The S3 Standard storage class is designed for 99.99% availability, the S3 Standard-IA storage class is designed for 99.9% availability, the S3 One Zone-IA storage class is designed for 99.5% availability, and the S3 Glacier and S3 Glacier Deep Archive class are designed for 99.99% availability and SLA of 99.9%. All of these storage classes are backed by the Amazon S3 Service Level Agreement

Options B is invalid because AWS Lambda already a highly available service in AWS, Refer below document.

https://aws.amazon.com/lambda/features/

Option D is invalid because High Availability is about availability; AS is about performance (usually throughput), also DynamoDB is high available by default. High Availability focuses on maintaining the liveness of the system in the presence of server or network failures whereas Auto Scaling just means adding more resources when demand increases. Refer the below document for DynamoDB reliability.

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

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

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

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 5 Unattempted

Domain :Design Secure Applications and Architectures

A company has a set of EC2 Instances hosting a revenue generating applications. Some of the data on the root EBS volumes are critical to retain. Hence it has to be ensured that even after the instances are terminated, the EBS volumes will still remain intact. Which of the following needs to be done to ensure this requirement can be met?

A. **Enable the DisableApiTermination for the EC2 Instance**

B. **Make the attribute of DeleteOnTermination for the EBS volume to false**

C. **Run the command, (aws ec2 delete-volume –f) in AWS Command Line Interface to disable deletion of volume on terminating Instances.**

D. **Run the command (aws ec2 modify-instance-attribute \ --block-device-mappings 'DeviceName=/dev/sda1,Ebs={DeleteOnTermination-false}) in AWS Command Line Interface to disable deletion of volume on terminating Instances**

Explanation:

Answer – B

The AWS Documentation mentions the following

Option B is correct because When an instance is terminated, Amazon Elastic Compute Cloud (Amazon EC2) uses the value of the DeleteOnTermination attribute for each root EBS volume to determine whether to preserve or delete the volume when the instance is terminated. By default, the DeleteOnTermination attribute for the root volume of an instance is set to true, but it is set to false for all other volume types.

To preserve the root volume when an instance is terminated, change the DeleteOnTermination attribute for the root volume to false.

Option A is invalid since the flag needs to be set on the EBS volume

Option C is invalid because (-f) no such parameter exists as per AWS Documentation and moreover, this command is used to delete the volume, see the below correct syntax to delete a volume using CLI

```
aws ec2 delete-volume --volume-id vol-049df61146cXXXX
```

Option D is invalid because command syntax is not correct, (=) should be used but (-) is used, see the actual syntax below

```
aws ec2 modify-instance-attribute\ --instance-id i-1234567890abcdef0 \ --block-device
```

In AWS Documentation, the format is given in JSON, so if you follow that you have to specify the JSON in a file mapping.json

```
[{\"DeviceName\": \"/dev/sda1\",\"Ebs\":{\"DeleteOnTermination\":false}}]
```

And run the command as below

```
aws ec2 modify-instance-attribute --block-device-mappings file://mapping.json
```

If you don't want to follow this, another syntax provided above is also correct

For more information on the Delete on termination flag, please refer to the below URL https://aws.amazon.com/premiumsupport/knowledge-center/deleteontermination-ebs/

https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-attribute.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 6 Unattempted

Domain :Design Secure Applications and Architectures

A company has a set of EC2 Instances hosted in a VPC. The IT Security department has specified that they need to ensure they get a list of IP addresses for all sources that are making requests to the EC2 Instances. Which one of the following could help achieve this requirement?

A. **AWS VPC Flow Logs**

B. **AWS Cloudwatch**

C. **AWS CloudFormation**

D. **AWS Trusted Advisor**

Explanation:

Answer – A

The AWS Documentation mentions the following

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Option B is invalid since this is a monitoring service which can only give metrics and not the detailed IP address tracing for traffic flowing into EC2 Instances

Option C is invalid since AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS

Option D is invalid since this is only used as a recommendation service

For more information on VPC Flow logs, please refer to the below URL

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 7 Unattempted

Domain :Design Secure Applications and Architectures

You are working as an AWS Architect for a financial company having intranet application hosted on AWS. They are using AWS SSO for granting access to users to AWS resources. During the annual security audit, Auditors have concerns on users sign-in process & prompted non-compliance for the security process when sign-in is observed from users using unknown locations or devices. Auditors are looking for enhancing security controls to be in place for such users. What would you use to improve the security process during user sign-in?

A. **Enable Context-aware MFA with TOTP (time-based one-time passcodes) available in Auth App on MFA Device**

B. **Enable Always-On MFA with TOTP (time-based one-time passcodes) available in Auth App on MFA Device**

C. **Enable Always-On MFA with verification code sent to the user's email address.**

D. **Enable Context-aware MFA with verification code sent to the user's email address.**

Explanation:

Answer – A

Option A is correct because, for additional security, AWS SSO MFA can be enabled. After MFA is enabled, post login with authorized email & password, users are prompted for additional verification code which is generated on Authentication App like Google Auth on MFA Device (MFA Device has to be registered first, Refer below document to see how to register MFA Device).

With Context-aware MFA, AWS SSO analyzes user sign-in context such as browser, location, and devices. If any deviation is observed, only then it asks for the additional second level of verification code. With this, a user does not have to perform MFA repeatedly from the same device.

Option B is incorrect because with Always-on MFA, each time the user logs in to any cloud application, it would prompt for TOTP generated in Authentication App. This is true even if the user logs in from the same device. We need to authenticate only when Sign-In is observed from unknown locations or devices.

Email-based Verification code can be used also by enabling 'Require Them to Provide a One-Time Password Sent by Email' while configuring MFA, this is for the Users not having MFA Device registered. But email-based verification is not that much secure option.

Option C is incorrect as with Always-on MFA, each time the user logs in to any cloud application, it would prompt for MFA verification code. This is true even if the user logs in from the same device.

Option D could be a correct choice but it is not that much secure option.

For more information on enabling MFA on AWS SSO, refer to the following URL:

https://docs.aws.amazon.com/singlesignon/latest/userguide/how-to-register-device.html

https://docs.aws.amazon.com/singlesignon/latest/userguide/enable-mfa.html

https://aws.amazon.com/about-aws/whats-new/2019/10/increase-aws-single-sign-on-security-with-multi-factor-authentication-using-authenticator-apps/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 8 Unattempted

Domain :Design Resilient Architectures

Your company has just started using the AWS RDS service. They have an application making requests to a MySQL instance on this service. Due to the sudden surge of high requests, you need to ensure that the backup activities on the database do not interfere with the normal operation of the database. Which of the following would help in this requirement?

A. **Ensure that the underlying instance type RDS instance is using General Purpose SSD storage. This type of storage will give minimal impact on such operations.**

B. **Ensure that the underlying instance type RDS instance is using Enhanced Networking. This type of setting will give minimal impact on such operations.**

C. **Ensure that the Multi-AZ feature has been enabled for the underlying RDS Instance.**

D. **Ensure that cross-region replication is enabled for the underlying RDS Instance.**

Explanation:

Option C is correct because, In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

We know that during the backups, for instance taking snapshots, there is usually an I/O consumption that takes place. To avoid this when using a multi-AZ enabled RDS database engine, create a backup on the standby instance. With automated backups, I/O activity is no longer suspended on your primary during your preferred backup window, since backups are taken from the standby

Options A and B are incorrect because, by using General Purpose SSD Storage or using Enhanced networking, our backup activities will interfere with normal database operation.

Option D is incorrect, Cross-region replication not required as it is Asynchronous replication.

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

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 9 Unattempted

Domain :Design Cost-Optimized Architectures

A company has an application that needs to be hosted on an EC2 Instance. The general amount of throughput data per volume will be in the range of 400-500 MiB/s from the application. Which of the following should be used as the storage type for the underlying EC2 Instance in a Cost-effective manner?

A. **EBS - General Purpose SSD**

B. **EBS - Provisioned IOPS SSD**

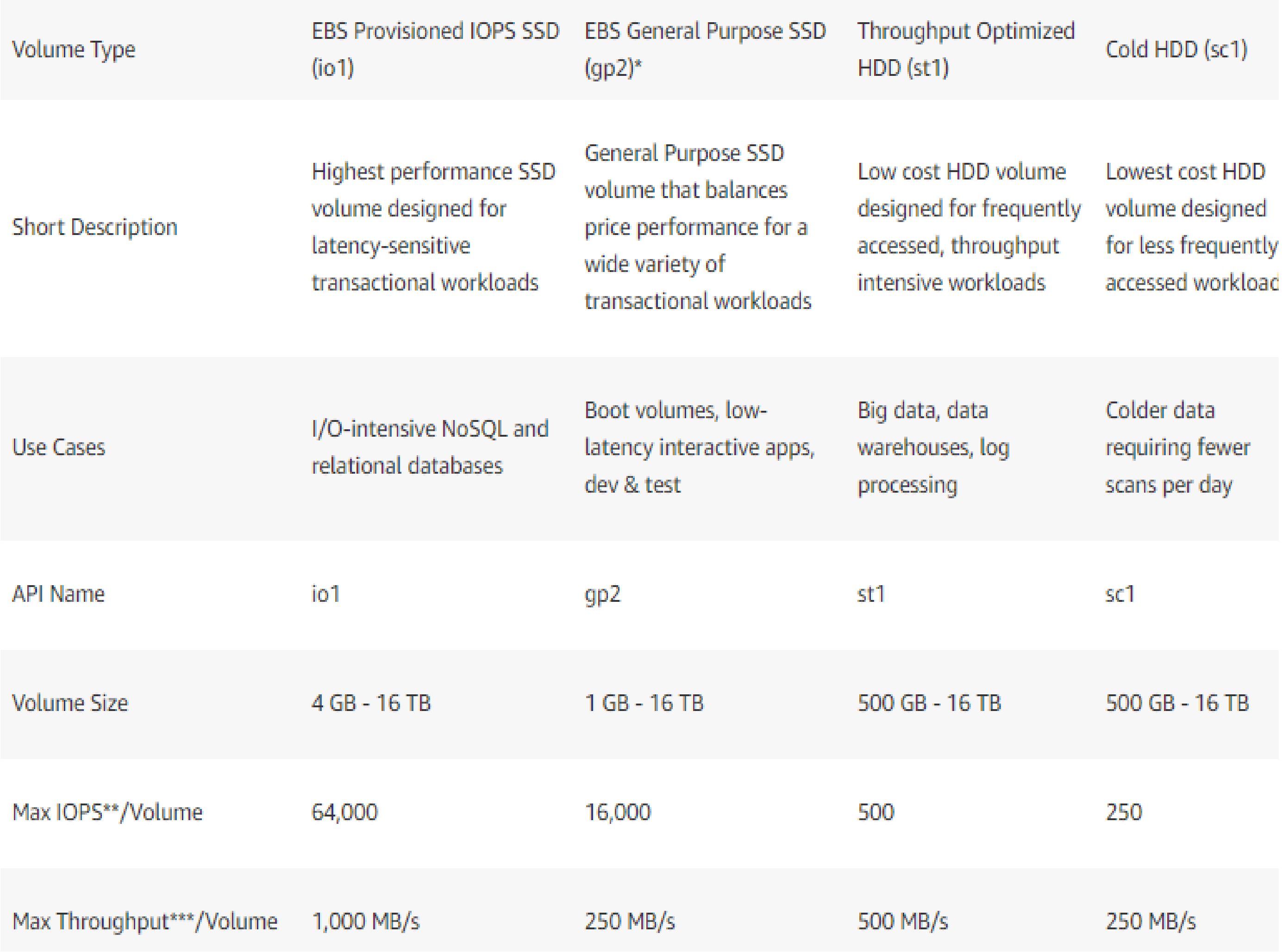
C. **EBS - Throughput Optimized HDD**

D. **EBS - Cold HDD**

Explanation:

Answer – C

When you want high throughput, you should choose using the Throughput Optimized EBS volume. The below snapshot from the AWS Documentation shows the features of the different types of volumes.



Volume Type	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Short Description	Highest performance SSD volume designed for latency-sensitive transactional workloads	General Purpose SSD volume that balances price performance for a wide variety of transactional workloads	Low cost HDD volume designed for frequently accessed, throughput intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloac
Use Cases	I/O-intensive NoSQL and relational databases	Boot volumes, low-latency interactive apps, dev & test	Big data, data warehouses, log processing	Colder data requiring fewer scans per day
API Name	io1	gp2	st1	sc1
Volume Size	4 GB - 16 TB	1 GB - 16 TB	500 GB - 16 TB	500 GB - 16 TB
Max IOPS**/Volume	64,000	16,000	500	250
Max Throughput***/Volume	1,000 MB/s	250 MB/s	500 MB/s	250 MB/s

As per the above document, Option A), B) and D) stands invalid

For more information on the EBS volume types, please refer to the below URL

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 10 Unattempted

Domain :Design High-Performing Architectures

A company has setup their application in AWS. It consists of a web tier hosted on a set of EC2 Instances. These instances interact with a MongoDB database server located in a private subnet. The web tier also interacts with many service-based applications in the private subnet. A NAT Instance is being used to route traffic from the instances in the private subnet to the Internet. The IT Administrative team is now getting Cloudwatch alerts that the NAT Instance is going beyond its threshold value for Network Activity. Which of the following would you advise to increase the performance of this architecture?

A. **Place the database server and application servers in the public subnet.**

B. **Place the NAT instance closer to the database servers by placing them in the private subnet**

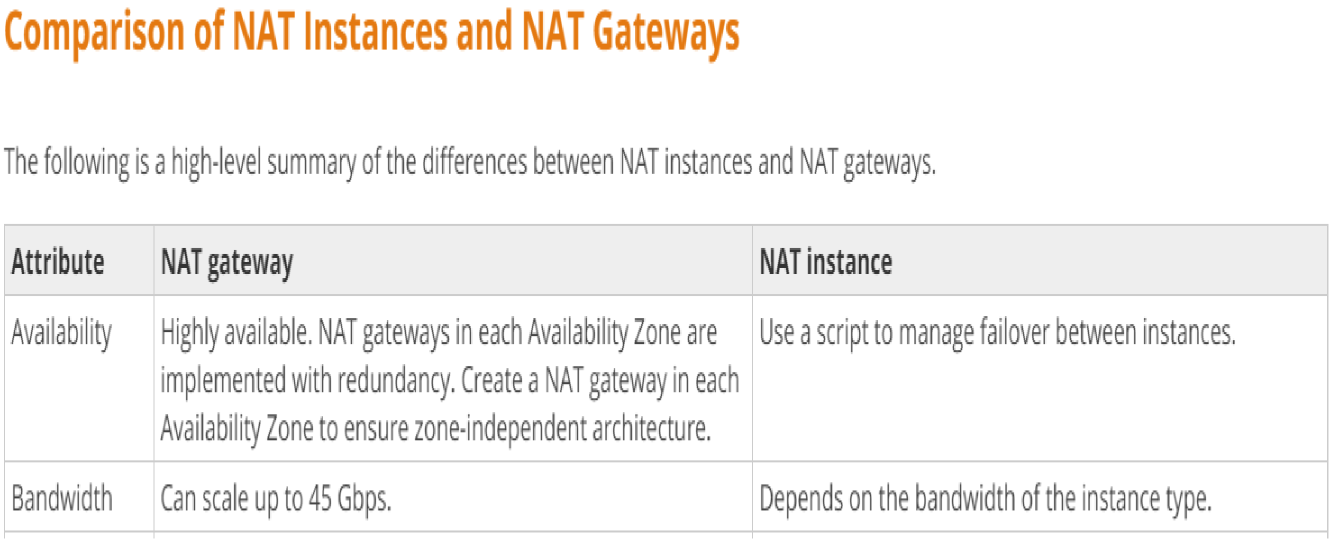
C. **Use the NAT gateway service instead of the NAT Instance**

D. **Use a VPN connection for the Instances in the private subnet**

Explanation:

Answer – C

The below snapshot from the AWS Documentation shows a partial comparison of the NAT Instance and NAT Gateway. You should consider using the NAT gateway for higher bandwidth requirements



Comparison of NAT Instances and NAT Gateways

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.

Option A is incorrect since you should not change the architecture of the database or application servers since this would result in security issues

Option B is incorrect since this would still alleviate the current network issue

Option D is incorrect since the NAT instance should be used to route traffic to the Internet from the Instances in the private subnet

For more information on the comparison between NAT Instances and the NAT gateway, please refer to the below URL

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 11 Unattempted

Domain :Design Cost-Optimized Architectures

Your company is currently hosting a long-running heavy load application on its On-premise environment. The company has developed this application in-house. Consulting companies then use this application via API calls. You now need to consider moving this application to AWS. Which of the following services would best be suited in the architecture design, which would also help deliver a cost-effective solution? Choose 2 answers from the options given below.

A. **AWS Lambda**

B. **AWS API Gateway**

C. **AWS Config**

D. **AWS EC2**

Explanation:

Answer – B and D

Option A might be a valid choice but the question specifies heavy load application which may lead to a need for time-out of API greater than 15min. As per AWS documentation, AWS Lambda can handle max time-out of up to 15 minutes. In this case, the application may take more time to run.

Option B is correct because Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application.

Option C is incorrect since this is a configuration service available from AWS.

Option D is correct because EC2 would fit for using API calls for the application. For more information on AWS EC2 and the API gateway, please refer to the below URL

https://aws.amazon.com/api-gateway/

https://aws.amazon.com/ec2

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 12 Unattempted

Domain :Design Resilient Architectures

Your company is planning on the following architecture for their application

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend
- A Load balancer for distribution of traffic

Due to the critical nature of the data stored on the underlying EBS volumes attached to the EC2 Instances, As a Solutions Architect of the Company, your supervisor has asked you to follow best backup practices to make sure data is available in another region for disaster recovery purposes. Which of the following would you consider complying with this requirement

A. **Create a copy of the volume in another region.**

B. **Create a snapshot of the volume in another region.**

C. **Create a snapshot. Copy the snapshot to the new region.**

D. **Create a copy of the volume. Copy the volume to the new region.**

Explanation:

Answer – C

The AWS Documentation showcases the use cases of EBS snapshots

Use Cases

Geographic expansion: Launch your applications in a new region.

Migration: Move an application to a new region, to enable better availability and to minimize cost.

Disaster recovery: Back up your data and logs across different geographical locations at regular intervals. In case of disaster, you can restore your applications using point-in-time backups stored in the secondary region. This minimizes data loss and recovery time.

Encryption: Encrypt a previously unencrypted snapshot, change the key with which the snapshot is encrypted, or, for encrypted snapshots that have been shared with you, create a copy that you own in order to restore a volume from it.

Data retention and auditing requirements: Copy your encrypted EBS snapshots from one AWS account to another to preserve data logs or other files for auditing or data retention. Using a different account helps prevent accidental snapshot deletions, and protects you if your main AWS account is compromised.

Options A and D are incorrect, since you need to create a snapshot

Option B is incorrect since you cannot directly create a snapshot in another region

For more information on EBS Snapshot copy, please refer to the below URL

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.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 13 Unattempted

Domain :Design Resilient Architectures

An application consists of a fleet of EC2 Instances. These Instances are launched in the Oregon (us-west-2) region which consists of 3 availability zones. This application needs 6 Instances running at all times. As an architect, you need to distribute the instances in such a way that the application could still maintain its capacity if any availability zone goes down. Also, you need to ensure that the cost is kept to a minimum? Which of the following configurations would you consider?

A. **6 Instances running in us-west-2a, 6 Instances running in us-west-2b, 6 Instances running in us-west-2c**

B. **3 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-east-2c**

C. **6 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-west-2c**

D. **3 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-west-2c**

Explanation:

Answer – D

So now let's look at Option A

If any availability zone goes down, we will have a total of 12 instances running. This is an additional 6 over the requirement of the question and will result in a higher cost.

So now let's look at Option B

If the availability zone us-west-2a goes down, then you will have only 3 instances running. Because other 3 instances are running in us-east-2c region

So now let's look at Option C

If either us-west-2b or us-west-2c availability zone goes down, we will have a total of 9 instances running. This is an additional 3 over the requirement of the question and will result in a higher cost.

So now let's look at Option D

If either us-east-2a or us-west-2b or us-west-2c availability zone goes down, there will be a total of 6 instances running, which is what we need

For more information on Regions and Availability zones, please refer to the below URL

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 **Time** 0 : 30 Try Now

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 14 Unattempted

Domain :Design High-Performing Architectures

You have a set of EC2 Instances in a custom VPC. You have installed a web application and need to ensure that only HTTP and HTTPS traffic is allowed into the instance. Which of the following would you consider for this requirement?

A. **Add a security group rule to allow HTTP and HTTPS Traffic**

B. **Add a security group rule to an explicit DENY all traffic and a default allow on HTTP and HTTPS Traffic**

C. **Add a security group rule to deny explicit traffic on HTTP and HTTPS Traffic**

D. **Add a security group rule to allow all traffic**

Explanation:

Answer – A

Option A is correct because we need to specify the allowed traffic in Security group i.e. HTTP and HTTPS Traffic must be allowed from all sources. No inbound traffic is allowed by default. By adding security group rules, you can specify which traffic you want to allow. This is essentially a whitelist.

Options B is incorrect since by default nothing is allowed and in Security group we can't specify what is denied. We don't have any deny option in Security Groups.

Option C is incorrect because in Security group we can specify what is allowed but not what is denied. If you want to deny explicitly, you should use Network Access control list.

Option D is incorrect since this would be a security issue.

For more information on VPC Security groups, please refer to the below URL https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 15 Unattempted

Domain :Design High-Performing Architectures

A company has an application defined with the following architecture

A fleet of EC2 Instances which are used to accept video uploads from users.

A fleet of EC2 Instances which are used to process the video uploads.

Which of the following would help architect an operationally excellent architecture?

A. **Create an SQS queue to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the Memory utilization of the underlying processing servers**

B. **Create an SQS queue to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the size of the queue**

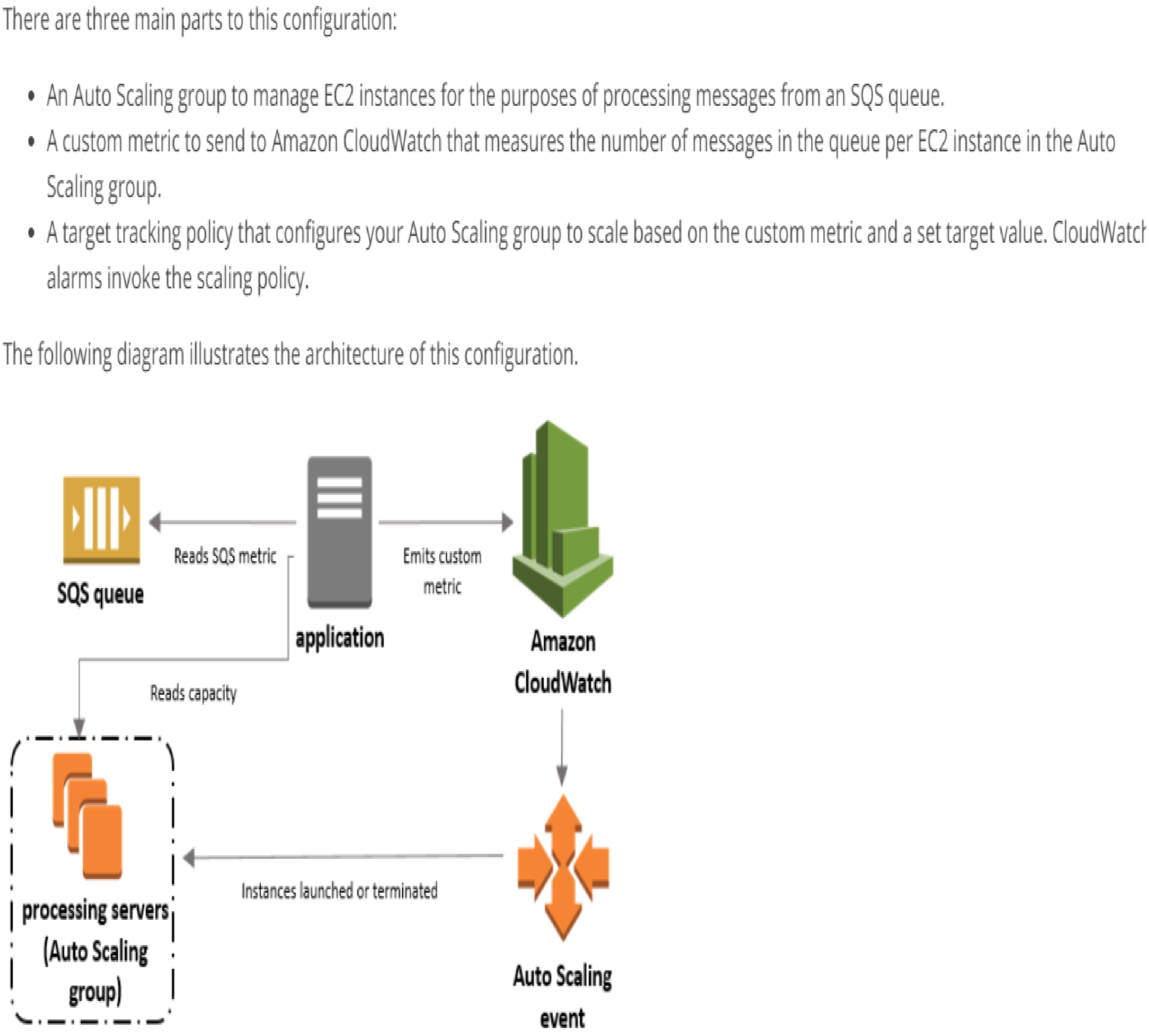
C. **Create an SNS topic to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the Memory utilization of the underlying processing servers**

D. **Create an SNS topic to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the size of the queue messages**

Explanation:

Answer – B

This architecture is also given in the AWS Documentation



There are three main parts to this configuration:

- An Auto Scaling group to manage EC2 instances for the purposes of processing messages from an SQS queue.
- A custom metric to send to Amazon CloudWatch that measures the number of messages in the queue per EC2 instance in the Auto Scaling group.
- A target tracking policy that configures your Auto Scaling group to scale based on the custom metric and a set target value. CloudWatc alarms invoke the scaling policy.

The following diagram illustrates the architecture of this configuration.

Option A is incorrect the ideal approach is to scale the instances based on the size of queue.

Options C and D are incorrect since you should be using SQS queues. SNS topics are used for notification purposes.

For more information on using SQS queues for Autoscaling, please refer to the below URL

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html

As per AWS,
You can use the number of messages stored in an SQS queue as an indicator of the amount of work that is waiting in line for eventual processing within an Auto Scaling Group comprised of a variable number of EC2 instances. Each SQS queue reports a number of metrics to CloudWatch at five minute intervals, including `ApproximateNumberOfMessagesVisible`. If your workload is spikey in nature, you may want to build an application that can respond more quickly to changes in the size of the queue.

Memory utilization metrics is a custom metric. For this, to work, you need to install Cloudwatch agent on the EC2 instances and need to aggregate the dimensions.
However, AWS already has a well-defined architecture based on SQS Queuelength being used for Autoscaling EC2 instances.

For more information please refer:

https://aws.amazon.com/blogs/aws/auto-scaling-with-sqs/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 16 Unattempted

Domain :Design High-Performing Architectures

A company has an application that currently produces a lot of data streams that need to be processed in real-time. They need to do some custom processing for their internal analysis. Which of the following can be used to help fulfill this requirement?

A. **AWS Kinesis Data Firehose**

B. **AWS Kinesis Data Streams**

C. **AWS Athena**

D. **AWS Redshift**

Explanation:

Answer - B

You can use Amazon Kinesis Data Streams to collect and process large streams of data records in real-time. Kinesis data streams are highly customizable and best suited for developers building custom applications or streaming data for specialized needs whereas Firehose handles loading data streams directly into AWS products for processing.

You should use Kinesis Data Streams if you want to do some custom processing with streaming data. With Kinesis Data Firehose you are simply ingesting it into S3, Redshift or ElasticSearch.

Option A is incorrect since Company needs to do customized processing for which data streams are best suited and also data needs to be processed in real-time, Firehose is nearly real-time but not exactly real-time.

Option C is incorrect since is used for getting data via SQL queries from data sources such as S3

Option D is incorrect since is used for petabyte data storage

For more information on AWS Data Streams and Firehose, please refer to the below URL:

https://docs.aws.amazon.com/streams/latest/dev/introduction.html

https://aws.amazon.com/kinesis/data-firehose/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 17 Unattempted

Domain :Design High-Performing Architectures

A company has an Amazon Aurora cluster setup. They have setup a Lambda function which needs to insert records into a DynamoDB table. The Amazon Aurora cluster needs to invoke the Lambda. Which of the following need to be in place for this setup to work. Choose 2 answers from the options given below

A. **Ensure that the Lambda function has an IAM Role assigned to it which can be used to invoke functions on Amazon Aurora**

B. **Ensure that the Amazon Aurora cluster has an IAM Role which allows it to invoke Lambda functions**

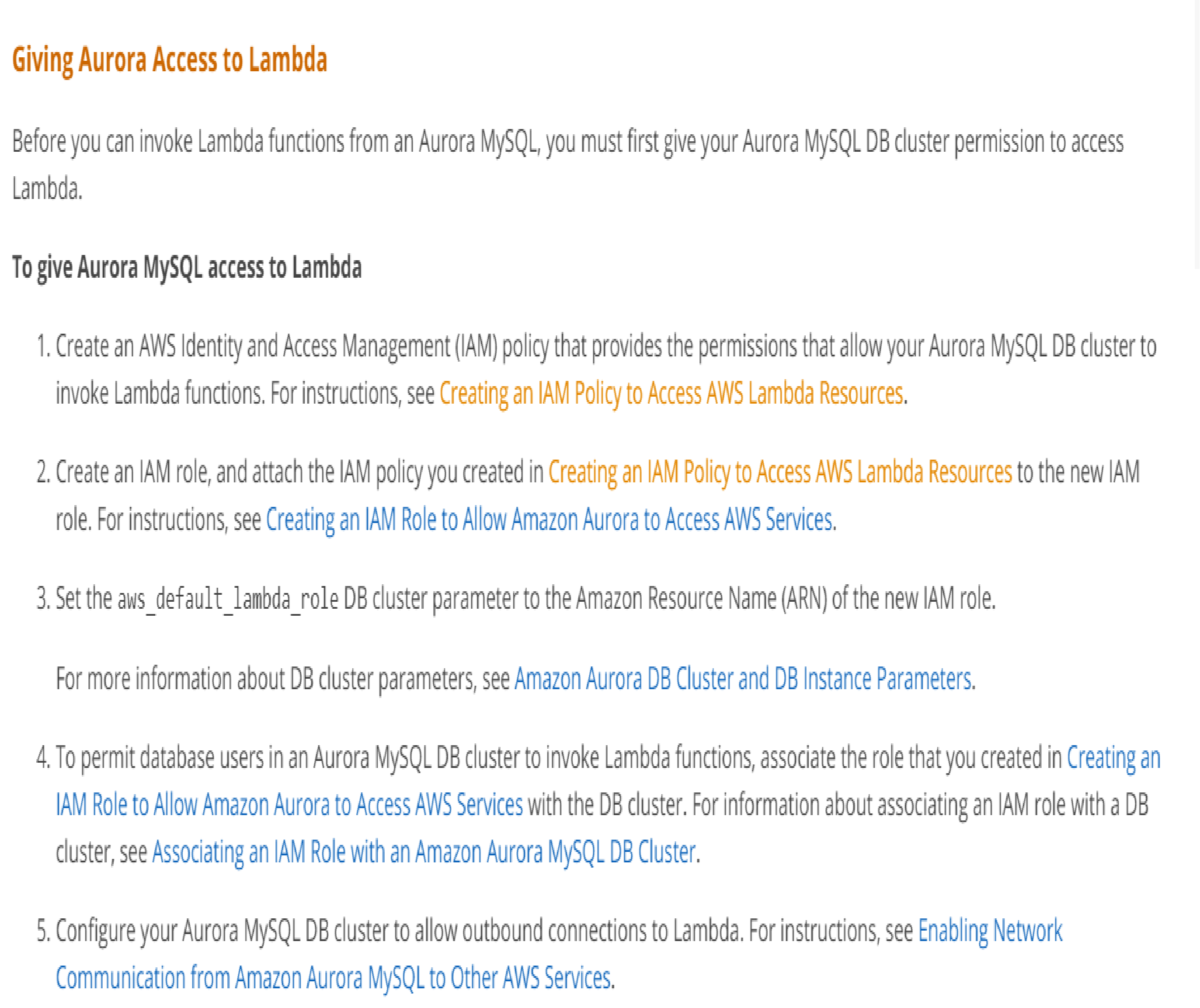
C. **Allow the Lambda function to allow outbound communication to Amazon Aurora**

D. **Allow the Amazon Aurora cluster to allow outbound communication to the Lambda function**

Explanation:

Answer – B and D

The below snapshot from the AWS Documentation shows what are the different steps required to ensure that the Lambda function has access to Amazon Aurora



Giving Aurora Access to Lambda

Before you can invoke Lambda functions from an Aurora MySQL, you must first give your Aurora MySQL DB cluster permission to access Lambda.

To give Aurora MySQL access to Lambda

1. Create an AWS Identity and Access Management (IAM) policy that provides the permissions that allow your Aurora MySQL DB cluster to invoke Lambda functions. For instructions, see Creating an IAM Policy to Access AWS Lambda Resources.
2. Create an IAM role, and attach the IAM policy you created in Creating an IAM Policy to Access AWS Lambda Resources to the new IAM role. For instructions, see Creating an IAM Role to Allow Amazon Aurora to Access AWS Services.
3. Set the `aws_default_lambda_role` DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role.

   For more information about DB cluster parameters, see Amazon Aurora DB Cluster and DB Instance Parameters.
4. To permit database users in an Aurora MySQL DB cluster to invoke Lambda functions, associate the role that you created in Creating an IAM Role to Allow Amazon Aurora to Access AWS Services with the DB cluster. For information about associating an IAM role with a DB cluster, see Associating an IAM Role with an Amazon Aurora MySQL DB Cluster.
5. Configure your Aurora MySQL DB cluster to allow outbound connections to Lambda. For instructions, see Enabling Network Communication from Amazon Aurora MySQL to Other AWS Services.

Options A and C are incorrect since the configurations need to be the other way around

For more information on invoking AWS Lambda using Aurora, please refer to the below URL

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 18 Unattempted

Domain :Design High-Performing Architectures

Your application consists of a set of EC2 Instances that are spun up as part of an Auto scaling group. These Instances need to access objects in an S3 bucket. Which of the following is the ideal approach to ensure this access is set in place?

A. **Ensure that the Access Keys are picked up from another S3 bucket. Access Keys can be embedded in the User data during Instance Launch.**

B. **Ensure that the launch configurations in Auto scaling group have an IAM Role to access S3 Objects**

C. **Ensure that an IAM policy is attached to the S3 bucket which allows access to the S3 buckets.**

D. **Ensure that the launch configurations in Auto scaling group have an IAM user to access S3 Objects.**

Explanation:

Answer – B

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalfs, such as Spot Instances or instances in

Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

A launch configuration is an instance configuration template that an Auto Scaling group uses to launch EC2 instances

For details about launch configurations, please refer below URL

https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-launch-config.html

Option A is incorrect since using Access keys is the least secure option

Option C is incorrect since the IAM policy is not the right option, you have to use IAM Roles instead. Also, attaching IAM role should be a part of Launch Configurations.

Option D is incorrect since you need to use IAM Roles and not IAM Users

To understand the basic difference between IAM Roles and Users:

IAM controls: Who can do What in your AWS account. Who (Authentication) in IAM is defined using users/groups and roles means what (Authorization) defined by policies.

User - End-user think about people

Groups- a set of users under one set of permission(policies)

Roles - are used to grant specific permission to specific users for a set of duration of time.

For more information on IAM Roles for EC2, please refer to the below URL

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 19 Unattempted

Domain :Design High-Performing Architectures

You are an architect for a company that is going to be hosting an application in AWS. They want to load balance the traffic based on which route the user chooses. The 2 possible routes for the application are /customer and /orders. Which of the following would you include in the design?

A. **Application Load Balancer**

B. **EC2 Container service**

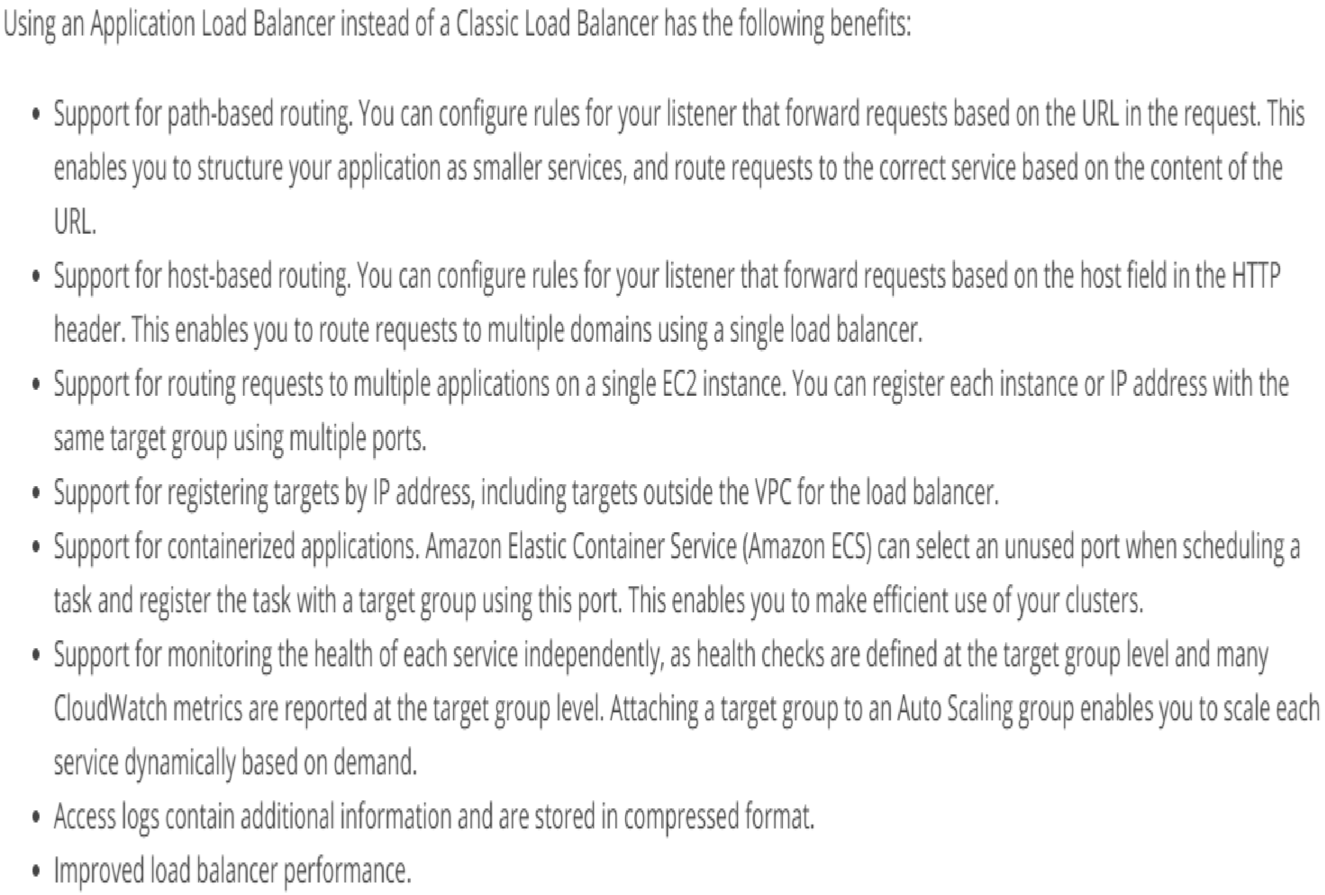
C. **Classic Load Balancer**

D. **Docker containers on EC2 Instances**

Explanation:

Answer – A

The below snapshot from the AWS Documentation shows the benefits of using the Application Load balancer



Using an Application Load Balancer instead of a Classic Load Balancer has the following benefits:

- Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.
- Support for host-based routing. You can configure rules for your listener that forward requests based on the host field in the HTTP header. This enables you to route requests to multiple domains using a single load balancer.
- Support for routing requests to multiple applications on a single EC2 instance. You can register each instance or IP address with the same target group using multiple ports.
- Support for registering targets by IP address, including targets outside the VPC for the load balancer.
- Support for containerized applications. Amazon Elastic Container Service (Amazon ECS) can select an unused port when scheduling a task and register the task with a target group using this port. This enables you to make efficient use of your clusters.
- Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand.
- Access logs contain additional information and are stored in compressed format.
- Improved load balancer performance.

Options B and D are incorrect since we don't have enough information on the question to decide on whether to use Docker containers or not.

Option C is invalid since Classic Load balancers will not fit the requirement for route-based load balancing

For more information on the Application Load Balancer, please refer to the below URL

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 20 Unattempted

Domain :Design Secure Applications and Architectures

Your company is planning on the following architecture for their application

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend using the AWS RDS MySQL service
- A Load balancer for distribution of traffic

There is a requirement to ensure that all data hosted in the database service is encrypted at rest. How can you achieve this requirement in the easiest manner? (Select 2)

A. **Encrypt the underlying EBS volumes for the database**

B. **Use the Encryption feature for RDS**

C. **Use S3 server-side encryption**

D. **Use AWS Key Management Service**

Explanation:

Answer – B and D

The AWS Documentation mentions the following

Option B is correct because, With RDS-encrypted resources, data is encrypted at rest, including the underlying storage for a database (DB) instance, its automated backups, read replicas, and snapshots. This capability uses the open standard AES-256 encryption algorithm to encrypt your data, which is transparent to your database engine.

This encryption option protects against physical exfiltration or access to your data bypassing the DB instances. It is therefore critical to complement encrypted resources with an effective encryption key management and database credential management practice to mitigate any unauthorized access. Otherwise, compromised credentials or insufficiently protected keys might allow unauthorized users to access the plaintext data directly through the database engine.

Encryption key management is provided using the AWS KMS

Option D is correct because Amazon RDS encrypts your databases using keys you manage with the AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. RDS encryption uses the industry-standard AES-256 encryption algorithm to encrypt your data on the server that hosts your RDS instance.

Options C is incorrect because this is used for encryption of objects in S3.

Option A is incorrect since this can be easily achieved using the encryption at rest feature for AWS RDS.

The term 'rest' means when data is resting (not in transition-while data is traveling to database

For more information on Encryption for AWS RDS, please refer to the below URL

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

https://aws.amazon.com/blogs/database/selecting-the-right-encryption-options-for-amazon-rds-and-amazon-aurora-database-engines/

https://aws.amazon.com/rds/features/security/

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 21 Unattempted

Domain :Design High-Performing Architectures

Your company is planning on hosting an application that will be based on Docker containers. They need to setup an orchestration service that would automatically scale based on the load. As much as possible , the company does not want the burden of managing the underlying infrastructure. Which of the following can assist in this scenario?

A. **AWS ECS with service Auto Scaling**

B. **Use an Elastic Load Balancer in front of an EC2 Instance. Use Docker containers on the EC2 Instance.**

C. **Use Auto Scaling with Spot Instances for the Orchestration Service.**

D. **Install and use Kubernetes on the EC2 Instance**

Explanation:

Answer – A

AWS Documentation mentions the following

Your Amazon ECS service can optionally be configured to use Service Auto Scaling to adjust its desired count up or down in response to CloudWatch alarms. Service Auto Scaling leverages the Application Auto Scaling service to provide this functionality. Service Auto Scaling is available in all regions that support Amazon ECS.

Amazon ECS publishes CloudWatch metrics with your service's average CPU and memory usage. You can use these service utilization metrics to scale your service out to deal with high demand at peak times, and to scale your service in to reduce costs during periods of low utilization.

Options B is incorrect because load balancer won't help scale up, but Auto Scaling can be used with a load balancer which is not mentioned in the question. Moreover, if all the things are in place then also this architecture would involve a lot of manual maintenance.

Option D is incorrect since this would involve a lot of manual maintenance

Option C is incorrect since Spot Instances are volatile and should not be used for the orchestration service

For more information on AWS ECS with Auto Scaling, please refer to the below URL

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html

https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 22 Unattempted

Domain :Design High-Performing Architectures

Your team has an application hosted on AWS. This application currently interacts with a DynamoDB table which has the Read capacity set to 10. Based on recent cloudwatch alarms which indicated that throttling was occurring in the requests to the DynamoDB table. Which of the following would help ensure the issue was resolved now and also help ensure the issue does not occur in the future?

A. **Add an Elastic Load Balancer in front of the DynamoDB table.**

B. **Change the Read Capacity for the table to 20.**

C. **Change the Write capacity for the table to offset the Read capacity.**

D. **Enable Autoscaling for the underlying DynamoDB table.**

Explanation:

Answer – D

The AWS Documentation mentions the following

DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.

You can optionally allow DynamoDB Auto-scaling to manage your table's throughput capacity. However, you still must provide initial settings for read and write capacity when you create the table. DynamoDB auto scaling uses these initial settings as a starting point and then adjusts them dynamically in response to your application's requirements.

As your application data and access requirements change, you might need to adjust your table's throughput settings. If you're using DynamoDB Auto-scaling, the throughput settings are automatically adjusted in response to actual workloads. You can also use the `UpdateTable` operation to manually adjust your table's throughput capacity. You might decide to do this if you need to bulk-load data from an existing data store into your new DynamoDB table.

For more details, please refer to below URL:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ProvisionedThroughput.html

https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/

Option A is incorrect since the Elastic Load balancer in front of the DynamoDB table won't help increase the capacity of DynamoDB. Here, We need to scale up and down the capacity automatically based on the requirement.

Option B is incorrect since this would only help in temporarily resolving the situation

Option C is incorrect since provisioning Write capacity would not help in this case

For more information on DynamoDB Autoscaling, please refer to the below URL

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 23 Unattempted

Domain :Design High-Performing Architectures

Your team is developing Lambda functions. These functions would need to interact with databases belonging to different environments. Which of the following is the ideal approach to ensuring that the

Lambda functions are designed in the right way to interact with Databases in multiple environments?

A. **Create a lambda function for each environment**

B. **Create a lambda function for each environment and ensure each has a different programming language**

C. **Make use of environment variables to store the database connecting strings**

D. **Make use of AWS Lambda tags to store the database connecting strings**

Explanation:

Answer – C

The AWS Documentation mentions the following

Environment variables for Lambda functions enable you to dynamically pass settings to your function code and libraries, without making changes to your code. Environment variables are key-value pairs that you create and modify as part of your function configuration, using either the AWS Lambda Console, the AWS Lambda CLI or the AWS Lambda SDK. AWS Lambda then makes these key-value pairs available to your Lambda function code using standard APIs supported by the language, like process.env for Node.js functions.

You can use environment variables to help libraries know what directory to install files in, where to store outputs, store connection and logging settings, and more. By separating these settings from the application logic, you don't need to update your function code when you need to change the function behavior based on different settings.

Option A is invalid since creating a lambda function for each environment will create overhead.

Option B is invalid since creating a lambda function for each environment will create overhead and using different programming languages makes no sense.

Option D is invalid since, you can tag Lambda functions to organize them by owner, project or department. Tags are freeform key-value pairs that are supported across AWS services for use in filtering resources and adding detail to billing reports. It is not used to store such connection strings.

For more information on AWS Lambda environment variables, please refer to the below URL.

https://docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html

https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 24 Unattempted

Domain :Design High-Performing Architectures

Your team has been instructed to develop an application that will make use of a DynamoDB table. During the design stage, you have to provide inputs to ensure that an optimal strategy is employed for a high read and write expectancy on the underlying DynamoDB table. Which of the following would you consider?

A. **Consider a lesser number of partition keys for the underlying table**

B. **Use partition keys with a large number of distinct values for the underlying table**

C. **Use partition keys with a small number of distinct values for the underlying table**

D. **Use partition keys with the number data type only**

Explanation:

Answer – B

The AWS Documentation mentions the following

DynamoDB is optimized for uniform distribution of items across a table's partitions, no matter how many partitions there may be. We recommend that you choose a partition key that can have a large number of distinct values relative to the number of items in the table.

DynamoDB stores data as groups of attributes, known as items. Items are similar to rows or records in other database systems. DynamoDB stores and retrieves each item based on the primary key value which must be unique.

When an Amazon DynamoDB table is created, you can **specify the desired throughput in Reads per second and Writes per second**. The table will then be provisioned across multiple partitions sufficient to provide the requested throughput.

You **do not have visibility** into the number of partitions created -- it is fully managed by DynamoDB. Additional partitions will be created as the quantity of data increases or when the provisioned throughput is increased.

Let's say you have requested 1000 Reads per second and the data has been internally partitioned across 10 partitions. Each partition will provide **100 Reads per second**. If all Read requests are for the same partition key, the throughput will be limited to 100 Reads per second. If the requests are spread over a range of different values, the throughput can be the full **1000 Reads per second**.

If multiple queries are made for the same Partition Key, it may result in a limited available throughput.

Let's try to understand with a real-world example, Think of it as a **bank with lines in front of teller windows**. If everybody lines up at one teller, fewer customers can be served. It is more efficient to distribute customers across many different teller windows. A **good partition key** for distributing customers might be the customer number since it is different for each customer. A **poor partition key** might their zip code because they all live in the same area near the bank.

All other Options are incorrect since option B is the most optimal choice.

For more information on how to choose your partition key wisely, please refer to the below URL

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.Partitions.html

https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/

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 25 Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Architect for an enterprise customer. Users access Amazon S3 buckets to save all project-related documents and also use business applications like Office 365 for daily work activities. These applications need to be accessible from any device for a limited number of hours in the day.
They are using AWS SSO to centrally manage and control access to AWS resources. Users are complaining that after each hour, they are getting logout from console & need to re-login. You need to ensure that the User session is optimum based upon the time required to complete the activity. Which of the following can be set to meet this requirement?

A. **Create a custom Permission Set with session duration as 24 hours**

B. **Use an existing Job Function policy to set session duration as 24 hours**

C. **Create a custom Permission Set with session duration as 6 hours**

D. **Use an existing Job Function policy to set session duration as 6 hours**

Explanation:

Correct Answer – C

Permission sets can control time duration for user login to the AWS Console by setting session duration. The Default Session duration is 1 hour while the maximum can be set to 12 hours. Post this session duration, the user is automatically logout.

AWS Single Sign-On (SSO) enables you to customize the session duration to AWS accounts ranging from 1 hour up to 12 hours. You can configure session duration for each permission set so that you can optimize how long your users can access the AWS Management Console and AWS CLI for your AWS accounts. For example, when your users need to run long-running operations, you can increase the session duration so that your users can complete the operation using a single session.

Option A is incorrect as the maximum Session duration that can be set is 12 hours.

Option B is incorrect. This will use predefined AWS managed policies since the requirement is for customized permission policy for session duration. Also, the maximum Session duration that can be set is 12 hours.

Option D is incorrect. This will use predefined AWS managed policies since the requirement is for customized permission policy for session duration.

For more information on Permission Set properties in AWS SSO, refer to the following URL:

https://aws.amazon.com/about-aws/whats-new/2018/10/aws-single-sign-on-now-enables-you-to-optimize-how-long-you-can-access-aws-accounts/

https://docs.aws.amazon.com/singlesignon/latest/userguide/howtosessionduration.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 26 Unattempted

Domain :Design High-Performing Architectures

Your company has a set of applications hosted on AWS. Currently, the IT Admin is manually checking the database storage to see if it is getting full. Which of the following can be used to automate these checks? (Select 2)

A. **CloudTrail**

B. **Cloudwatch**

C. **VPC Flow Logs**

D. **AWS Trusted Advisor**

Explanation:

Answer – B and D

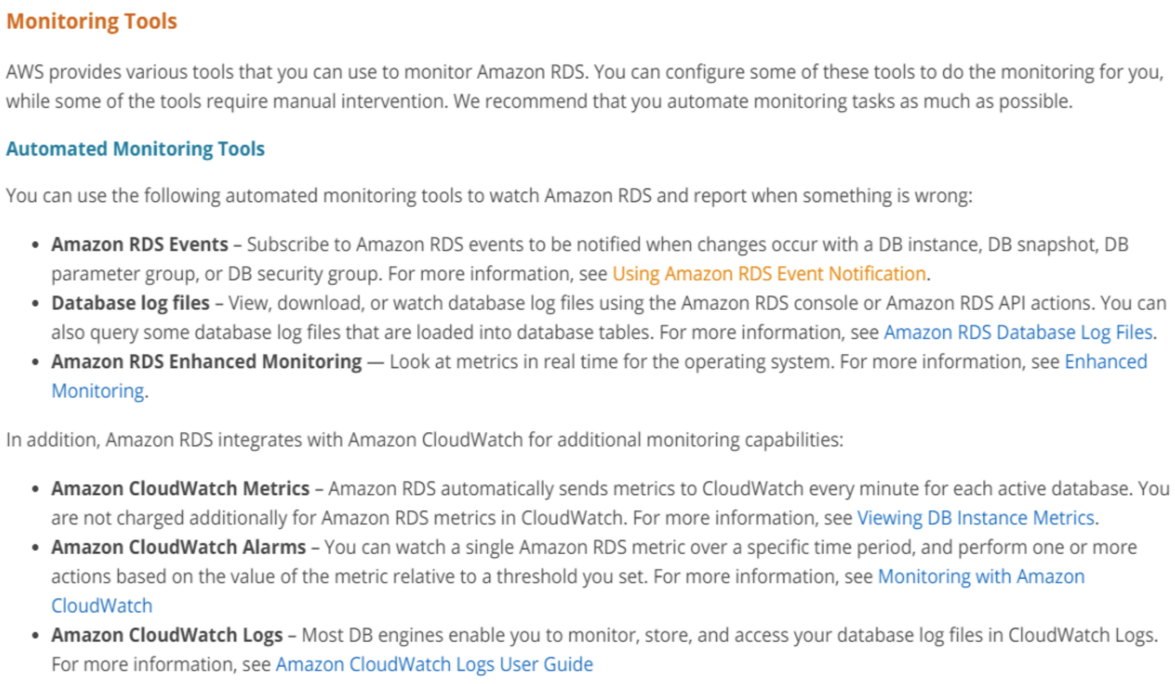
The AWS Documentation mentions the following

CloudWatch – You can watch a single Amazon RDS metric over a specific time period, and perform one or more actions based on the value of the metric relative to a threshold you set.

Option A is incorrect since this is only used for API monitoring

Option C is incorrect since this is used for monitoring network traffic to your EC2 Instances

Option D is correct since AWS Trusted Advisor is an online tool that provides you real-time service limit checks



Monitoring Tools

AWS provides various tools that you can use to monitor Amazon RDS. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.

Automated Monitoring Tools

You can use the following automated monitoring tools to watch Amazon RDS and report when something is wrong:

- **Amazon RDS Events** – Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group. For more information, see Using Amazon RDS Event Notification.
- **Database log files** – View, download, or watch database log files using the Amazon RDS console or Amazon RDS API actions. You can also query some database log files that are loaded into database tables. For more information, see Amazon RDS Database Log Files.
- **Amazon RDS Enhanced Monitoring** — Look at metrics in real time for the operating system. For more information, see Enhanced Monitoring.

In addition, Amazon RDS integrates with Amazon CloudWatch for additional monitoring capabilities:

- **Amazon CloudWatch Metrics** – Amazon RDS automatically sends metrics to CloudWatch every minute for each active database. You are not charged additionally for Amazon RDS metrics in CloudWatch. For more information, see Viewing DB Instance Metrics.
- **Amazon CloudWatch Alarms** – You can watch a single Amazon RDS metric over a specific time period, and perform one or more actions based on the value of the metric relative to a threshold you set. For more information, see Monitoring with Amazon CloudWatch
- **Amazon CloudWatch Logs** – Most DB engines enable you to monitor, store, and access your database log files in CloudWatch Logs. For more information, see Amazon CloudWatch Logs User Guide

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

For more information on monitoring for databases, please refer to the below URL

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.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 27

Unattempted

Domain :Design High-Performing Architectures

Your company has an application hosted in AWS. This application consists of a web tier and database tier. The web tier is hosted on EC2 Instances. The database is hosted in the AWS RDS service and data keeps changing every few hours. Recently performance issues have been encountered in the application and this is due to the high number of read requests. Which of the following can be used to help resolve the issue?

A. **Enable Multi-AZ for the database**

B. **Use Read Replica**

C. **Use Amazon DynamoDB Accelerator (DAX)**

D. **Place an Elastic Cache service in front of the database service**

Explanation:

Answer –B

In terms of load, they have the same goal, but they differ in some areas:

Up-to-dateness of data:

> A read replica will continuously sync from the master. So your results will probably lag 0 - 3s (depending on the load) behind the master.
>
> A cache takes the query result at a specific point in time and stores it for a certain amount of time.

Performance:

> A cache can only return results for queries it has already seen. So if you run the same queries over and over again, it's a good match.
>
> If you have many different, frequently changing, or dynamic queries, a read replica will be a better match.
>
> ElastiCache should be much faster since it's returning values directly from RAM. However, this also limits the number of results you can store.

Option B is correct since the question specifies data keeps changing frequently, as it keeps data up-to-date and read performance is also improved.

ElastiCache can be used to reduce the latency of requests but it is a caching service and according to question data keeps changing every few hours, so Elasticache is not recommended choice.

Option A is incorrect since this is used for high availability for the databases

Option C is incorrect since Amazon DynamoDB Accelerator (DAX) is a Fully managed, in-memory cache for DynamoDB only.

For more information on Read Replica and Elasticache, please refer to the below URL

https://aws.amazon.com/rds/features/read-replicas/

https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.htm

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 28 Unattempted

Domain :Design Resilient Architectures

A Startup company is launching a three-tier application with the Multicontainer Docker platform. This application needs to be integrated with the Amazon RDS database instance. The application will be launched using AWS Elastic Beanstalk. As an AWS consultant for this company, you need to design the environment for blue/green deployment along with decoupled architecture in the production environment. What would you recommend for integrating the Amazon RDS database with AWS Elastic Beanstalk?

A. **Launch Amazon RDS instance within the same AWS Elastic Beanstalk environment, setting connection string to the database in environment properties.**

B. **Launch Amazon RDS instance outside the AWS Elastic Beanstalk environment storing the connection string in the S3 bucket.**

C. **Launch Amazon RDS instance within the same AWS Elastic Beanstalk environment storing the connection string in the S3 bucket.**

D. **Launch Amazon RDS instance outside AWS Elastic Beanstalk environment, setting connection string to the database in environment properties**

Explanation:

Correct Answer – B

AWS Elastic Beanstalk provisions and configures all the AWS resources required to run and support your application. For Amazon RDS database instance to be launched in the production environment, best practice is to launch it outside the AWS Elastic Beanstalk environment. It helps in having multiple environments connecting to a single database, using database types not supported with the integrated database, performing blue/green deployments. Also, the database instance remains up & running when the AWS Elastic Beanstalk environment is terminated.

For a production environment, you can launch a database instance outside of your environment and configure your application to connect to it outside of the functionality provided by Elastic Beanstalk. Using a database instance that is external to your environment requires additional security group and connection string configuration.

Providing connection information to your application with environment properties is a good way to keep passwords out of your code, but it's not a perfect solution. Environment properties are discoverable in the environment management console and can be viewed by any user that has permission to describe configuration settings on your environment. Depending on the platform, environment properties may also appear in instance logs.

You can lock down your connection information by storing it in an Amazon S3 bucket that you control. The basic steps are as follows:

Upload a file that contains your connection string to an Amazon S3 bucket.

Grant the EC2 instance profile permission to read the file.

Configure your application to download the file during deployment.

Read the file in your application code.

Option A is incorrect as launching Amazon RDS in an AWS Elastic Beanstalk environment is suitable for test/development purposes & not for a production environment. If the AWS Elastic Beanstalk environment is terminated, the Amazon RDS database instance is also terminated.

Option C is incorrect as launching Amazon RDS in an AWS Elastic Beanstalk environment is suitable for test/development purposes & not for the production environment.

Option D is incorrect. When Amazon RDS instance is launched outside the AWS Elastic Beanstalk environment, best practice is to save the connection string in the Amazon S3 bucket.

For more information on launching Amazon RDS instance with AWS Elastic Beanstalk and storing the connection string, refer to the following URLs:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.db.html

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

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/rds-external-credentials.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 29 Unattempted

Domain :Design Secure Applications and Architectures

Your company has an application that has been developed and needs to be hosted on an EC2 Instance. The EC2 Instance is located in a private subnet and needs to access AWS Kinesis streams without passing into the Internet. How can you achieve this in the best manner possible?

A. **Attach a NAT gateway to the VPC**

B. **Attach an Internet gateway to the VPC**

C. **Create a VPC Gateway Endpoint that would allow access to Kinesis Streams**

D. **Create a VPC Interface Endpoint that would allow access to Kinesis Streams**

Explanation:

Answer – D

The AWS Documentation mentions the following

You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC

Options A and B are incorrect since it is mentioned in the question that traffic should not go via the Internet

Option C is incorrect since this is mostly used for S3 and DynamoDB access from Instances in the private subnet

For more information on VPC Endpoints Interfaces, please refer to the below URL

https://docs.aws.amazon.com/streams/latest/dev/vpc.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 30 Unattempted

Domain :Design Secure Applications and Architectures

A company is planning to store sensitive documents in an S3 bucket. They want to ensure that documents are encrypted at rest. They want to ensure they manage the underlying keys which are used for encryption but not the encryption/decryption process. Which of the following can be used for this purpose?

A. **Use S3 server-side encryption with Customer keys**

B. **Use S3 client-side encryption**

C. **Use S3 server-side encryption with AWS managed keys**

D. **Use S3 server-side encryption with AWS KMS keys with Key policy document of size 40kb.**

E. **Use S3 server-side encryption with AWS KMS keys with the keys uploaded by the company to KMS**

Explanation:

Answer – A

AWS Documentation mentions the following

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

In short,

SSE-S3 requires that Amazon S3 manage the data and master encryption keys.
SSE-C requires that you manage the encryption key

SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS

For more information, please refer to the following URL.
https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

Option B is incorrect because when you do client-side encryption data goes to s3 in an encrypted format. Again when you download, it is the client who has to decrypt the data. But question specifies customer should not manage the encryption/decryption process.

Options C is incorrect since here you will still not manage the complete lifecycle of the keys.

Options D is incorrect because the maximum key policy document size is 32kb.

https://docs.aws.amazon.com/kms/latest/developerguide/limits.html

https://aws.amazon.com/blogs/aws/new-bring-your-own-keys-with-aws-key-management-service/

For more information on Server-side encryption with customer keys and Client-side encryption, please refer to the below URL

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 31 Unattempted

Domain :Design High-Performing Architectures

Your company currently has the following architecture for its e-commerce application
· EC2 Instances hosting the application
· An Autoscaling group for the EC2 Instances
The users who use the application keep on complaining that the application is slow in the morning from 9:00 – 9:30, after which no issues occur. Which of the following can be done to ensure the issue is not encountered during the morning time?

A. **Ensure that a Simple scaling policy is added to the Auto scaling Group**

B. **Ensure that a step scaling policy is added to the Auto scaling Group**

C. **Ensure that a scheduled scaling policy is added to the Auto scaling Group**

D. **Ensure that a static scaling policy is added to the Auto scaling Group**

Explanation:

Answer – C

The AWS Documentation mentions the following

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 simple scaling increase or decrease the current capacity of the group based on a single scaling adjustment.

Option B is incorrect because Step Scaling increase or decrease the current capacity of the group based on a set of scaling adjustments, known as step adjustments, that vary based on the size of the alarm breach.

Option D is incorrect since Static scaling policy doesn't exist.

For more information on scaling policies for Auto scaling, please refer to the below URL's

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

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html#as-scaling-types

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.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 32 Unattempted

Domain :Design Secure Applications and Architectures

A three-tier web application is running on AWS VPC in two availability zones as shown below. Here are the CIDR ranges for each subnet and the corresponding servers.

Web server
10.16.0.0/25
10.16.0.128/25

Application Server
10.16.1.0/25
10.16.1.128/25

DB Server
10.16.2.0/25
10.16.2.128/25

The DB server is running MySQL, which would run on its default port, should only allow access to Application Server tier and access from the rest of the tiers should be denied.
Which inbound rule of Security Group on the DB server needs to be attached to meets this requirement?

A. **Type : MySQL |**
Protocol: TCP |
Port: 3306 |
Source: 10.16.0.0/24

B. **Type : MySQL |**
Protocol: TCP |
Port: 3306 |
Source: 10.16.2.0/24

C. **Type : MySQL |**
Protocol: TCP |
Port : 3306 |
Source: 10.16.1.0/24

D. Type : MySQL |
Protocol: TCP |
Port : 3306 |
Source: 10.16.3.128/25

Explanation:

Answer: C

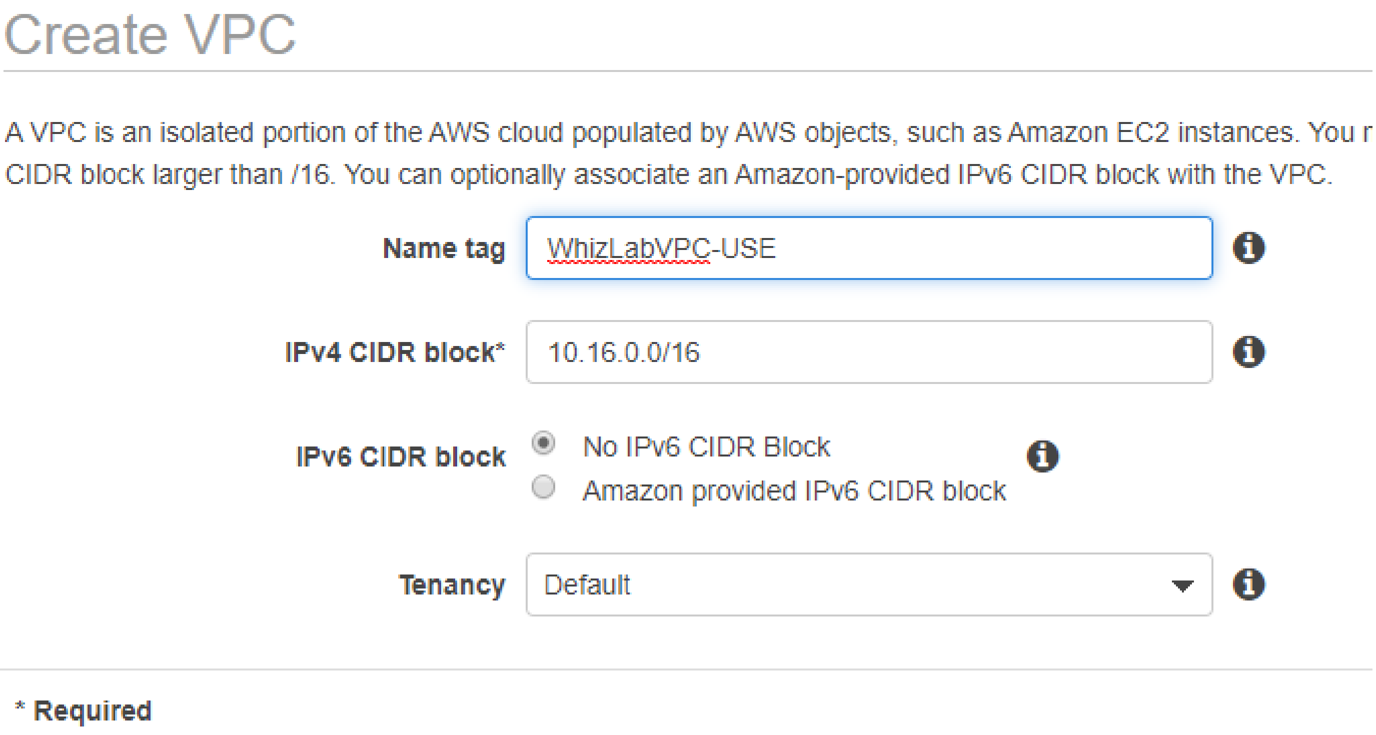
The requirement here is to allow access from Application Tier to DB Tier. The other point to note here is that MySQL would run on its default port. The default port for MySQL is '3306'

Two /25 networks equal a /24 network. Two /27 networks equal a /26 network. Two /26 networks equal a /25 network. And so on, and so on. The notion of combining two smaller networks into a larger one is another benefit of classless networks named supernetting In order to create a supernet the smaller networks must be contiguous. For example, 192.0.2.240/29 and 192.0.2.248/29 can form a supernet 192.0.2.240/28, but 192.0.2.240/29 and 192.0.2.8/29 could not as it must be 192.0.2.248/29 in order to form a supernet

Application Server tier IP's across two subnets are - 10.16.1.0/25 and 10.16.1.128/25 that is from 10.16.1.0 to 10.16.1.255 which is same as 10.16.1.0/24

Action Required here

Create A VPC



Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You r
CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag: WhizLabVPC-USE

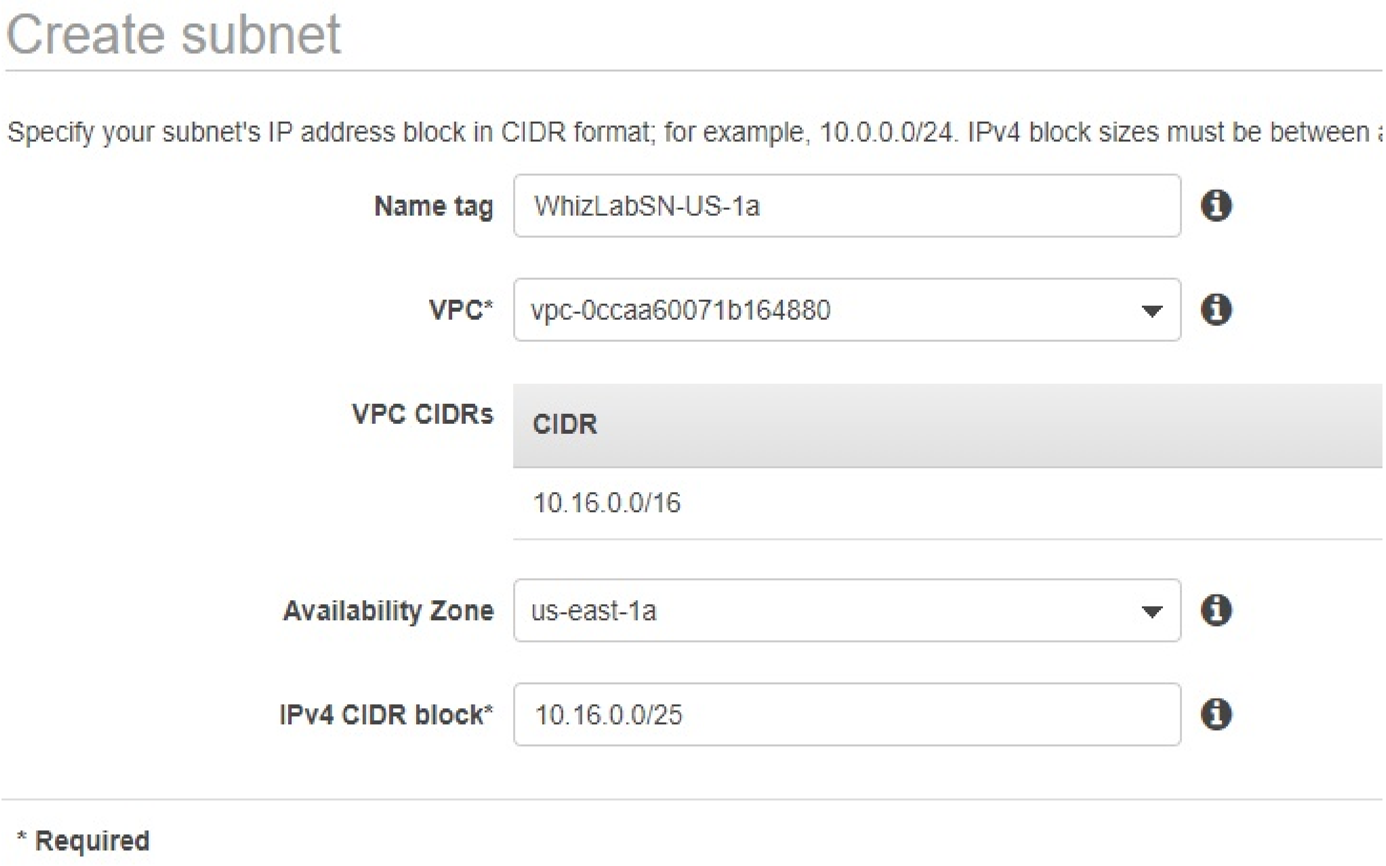
IPv4 CIDR block*: 10.16.0.0/16

IPv6 CIDR block: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block

Tenancy: Default

* Required

Now create 2 subnets inside this VPC

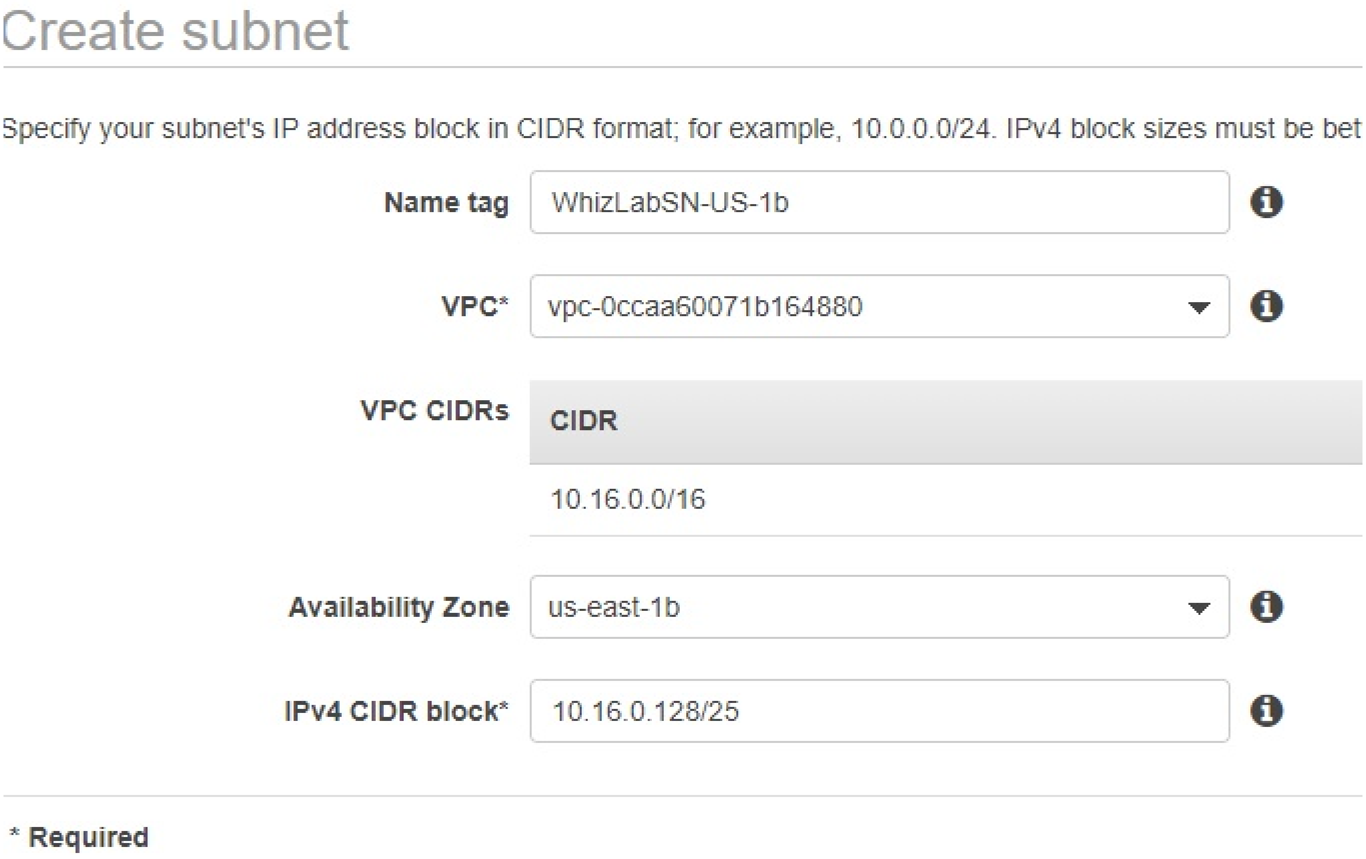


Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between

Name tag	WhizLabSN-US-1a
VPC*	vpc-0ccaa60071b164880
VPC CIDRs	**CIDR** 10.16.0.0/16
Availability Zone	us-east-1a
IPv4 CIDR block*	10.16.0.0/25

*** Required**



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be bet

Name tag	WhizLabSN-US-1b
VPC*	vpc-0ccaa60071b164880
VPC CIDRs	CIDR 10.16.0.0/16
Availability Zone	us-east-1b
IPv4 CIDR block*	10.16.0.128/25

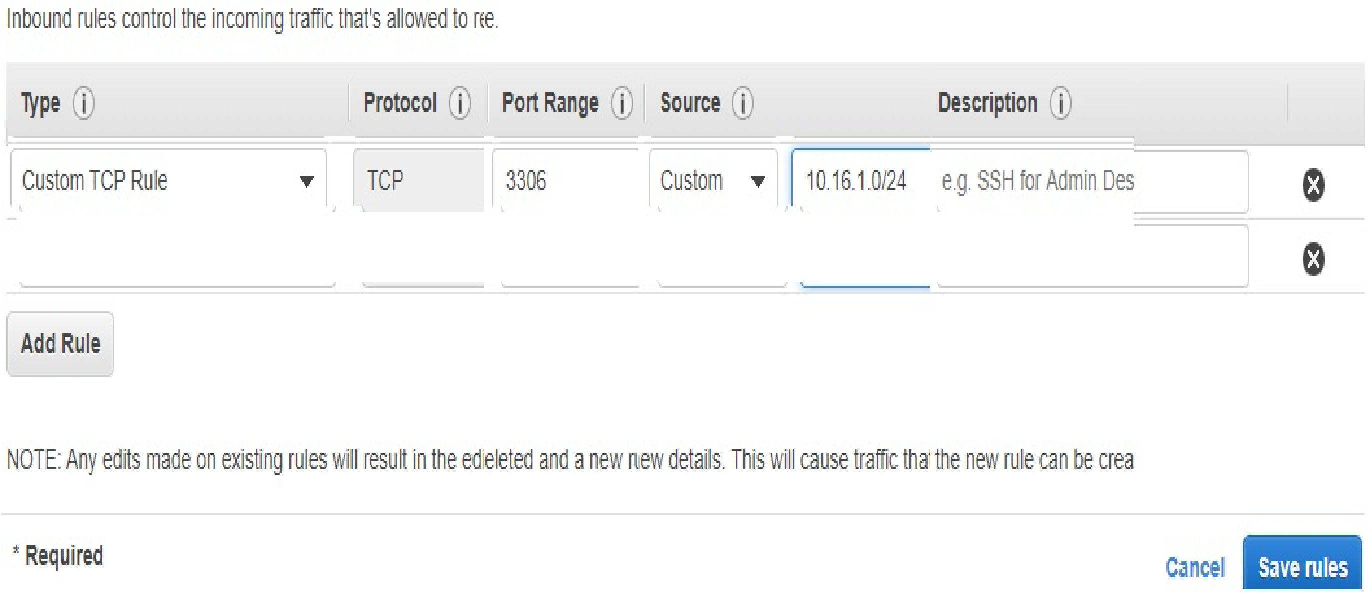
* Required

Similarly, create 2 more VPC for DB and 2 VPC for Application Type

thereafter in creating 1 Rule in SG for outbound to while listing for DB Layer and attach to the Application tier

Similarly, Crate one More SG and Create Inbound to whitelist Application Tier and attach to DB Tier

So we need to create the following rule in SG



Inbound rules control the incoming traffic that's allowed to re.

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	3306	Custom	10.16.1.0/24	e.g. SSH for Admin Des

NOTE: Any edits made on existing rules will result in the edeleted and a new new details. This will cause traffic thai the new rule can be crea

* Required

So Option C is the best answer

Options A, B, and D are incorrect because source should be 10.16.1.0/24

Or alternatively, two inbound rules from Port 3306 but different sources i.e. 10.16.1.0/25 and 10.16.1.128/25

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 33 Unattempted

Domain :Design Cost-Optimized Architectures

You launched 9 spot instances for a specific workload in your AWS Account. Your bid price was $0.07 per hour and the spot price at the time of launch was $0.06 per hour. After 1.5 hours, the spot price rose to $0.08 an hour. What is the cost incurred?

A. **$0.54**

B. **$0.24**

C. **$0.00**

D. **$0.44**

Explanation:

Answer : A

Spot instance are those instances for which a user has to place a bid on the AWS portal. If the bid price is greater than the amazon price (i.e. spot price) then the spot instances are automatically granted. The user would be charged based on the 'spot' price instead of the 'bid' price.

If the bid price is lower than the amazon price (i.e. spot price) then the spot instances are cancelled

Now, if a user has got a spot instance running and if suddenly the spot price goes up, then amazon automatically cancels the instance and the user is not charged for the extra minutes (rounded to one hour). This is called as amazon's termination of the spot instance

In a second case, if a user has got a spot instance running (when the bid price is greater than the spot price and the user is granted the 'spot instance' on the 'spot' price) and the user by himself voluntarily terminates the spot instance then the user is charged till the minute he has used the spot instance. This is called as the user's voluntary termination of the spot instance

With the above introduction we can proceed with the below calculation

In the first hour,

Bid price = $0.07

Spot price = $0.06

Therefore the user is granted the spot instance. Now the price for '9' instances for the first hour would be = $0.06 * 9 = $0.54

In the second hour (i.e. for 0.5 hour)

Bid price = $0.07

Spot price = $0.08

Now the spot price is greater than the bid price which will end up in the spot instance being terminated by amazon and the user is not charged any amount for the instances, for the 0.5 hours that the instances ran.

Therefore the total payable amount by the user for '9' instances are = $0.54.

Therefore Option 'A' is the correct answer.

Option 'B' is incorrect because the total cost is $0.24 which is lesser than $0.54

Option 'C' is incorrect because the total cost is $0.00 which is lesser than $0.54

Option 'D' is incorrect because the total cost is $0.44 which is lesser than $0.54

For details on spot instances please refer to the following link:

https://aws.amazon.com/ec2/spot/pricing/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 34 Unattempted

Domain :Design High-Performing Architectures

You have just launched an EC2 instance, and get the following error message when you try to connect to it from a workstation running Windows 7.
Error: Server refused our key or No supported authentication methods available
What could be the reason for this error? (**Select TWO**)

A. **Verify that the key (.pem) has been converted to the format recognized by Putty (.ppk)**

B. **The security group attached to the EC2 instance has not been configured for 'inbound' on '3389' port**

C. **The security group attached to the EC2 instance has not been configured for 'inbound' on '389' port**

D. **AWS console credentials are incorrect**

E. **The user has not used the correct username for the AMI**

Explanation:

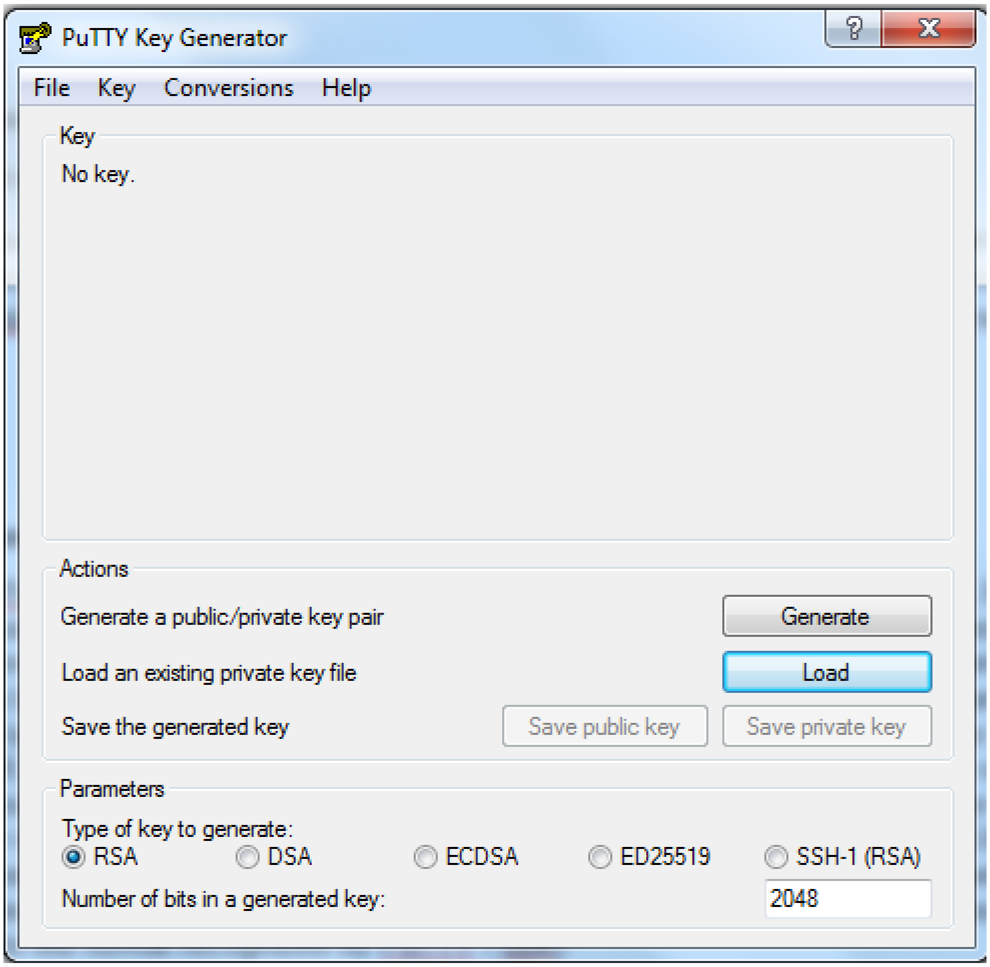
Answer: A and E

There are two parts of the error message.

The first part is that ‘Server refused our key’

Putty: This is a CLI (Command Line Interface) tool in Windows. To log in to this Putty tool we need to have the keys in the Putty readable format which would have the extension of ‘.ppk’.

There is a tool called ‘**PuttyGen**’ by which we can convert our ‘.pem’ key to the ‘.ppk’ format and if we feed this key to the Putty tool we can log in to our respective instance.



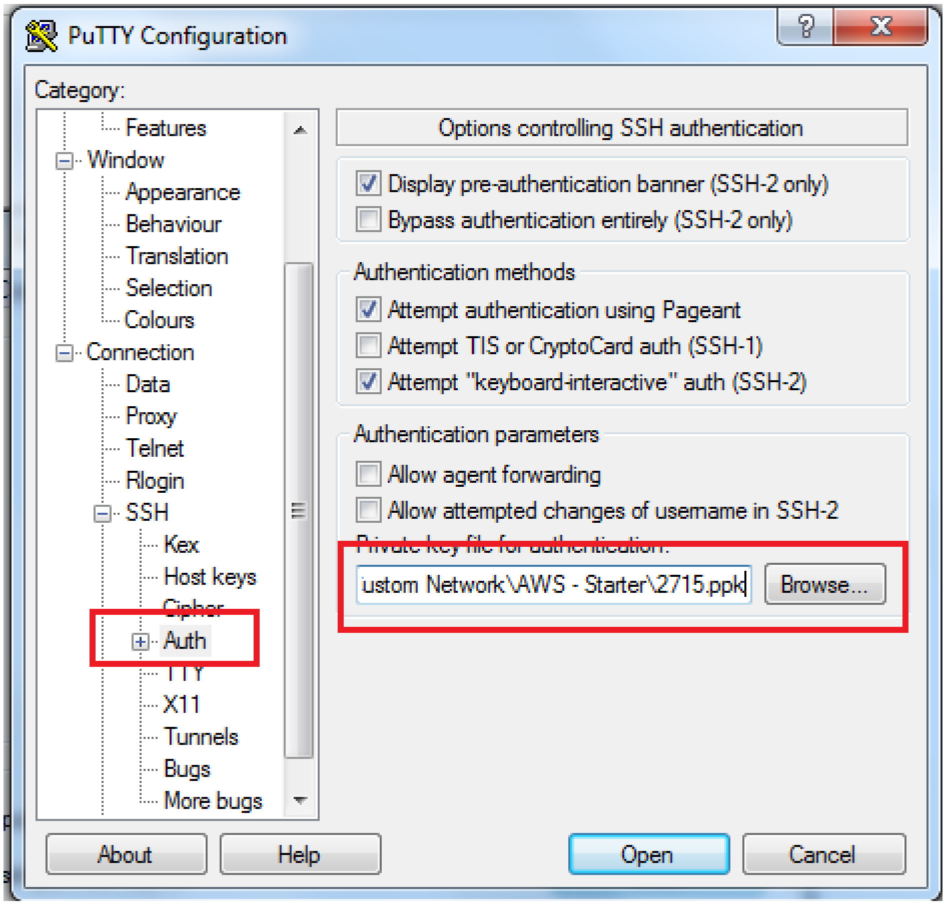
No key.

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Load the '.pem' key in the 'PuttyGen' tool and use the 'Save private key' in the 'PuttyGen' to save the private key in '.ppk' format.

Then load this key in the 'Auth' section of 'Putty' tool as shown below



PuTTY Configuration

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)

□ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

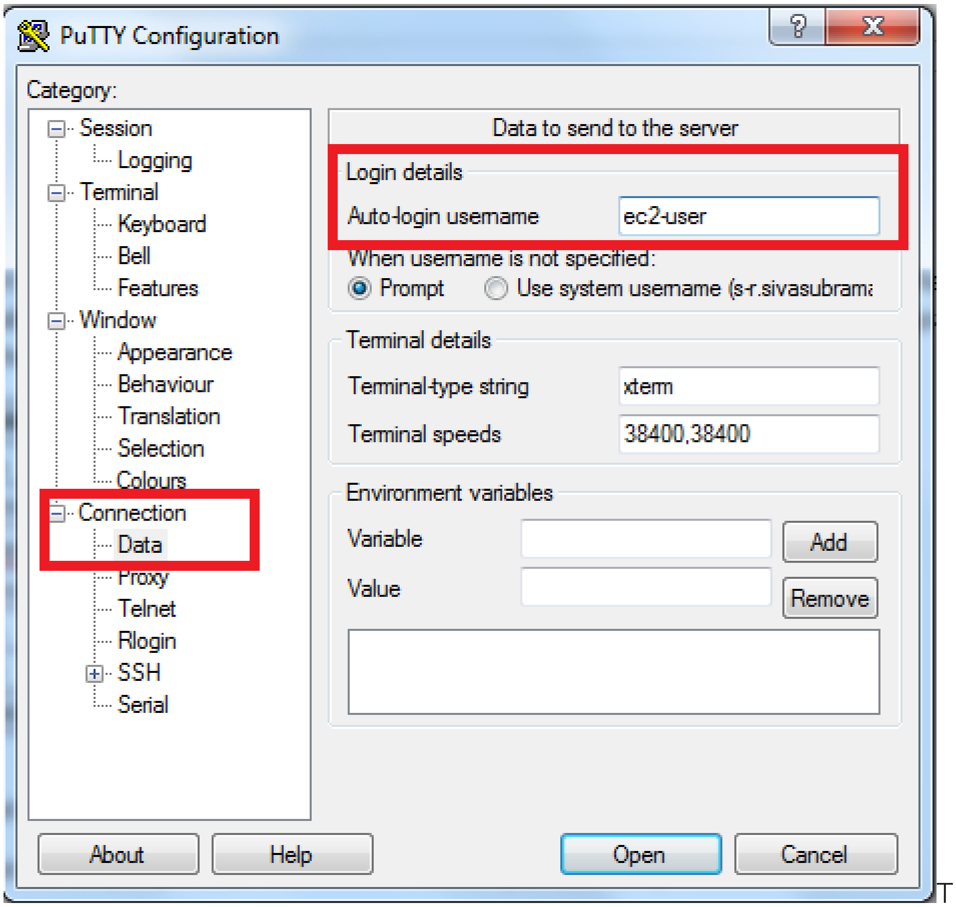
□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

ustom Network\AWS - Starter\2715.ppk

The username should be provided in the 'Data' section as shown below



Data to send to the server

Login details

Auto-login username: ec2-user

When username is not specified:
● Prompt ○ Use system username (s-r.sivasubrama

Terminal details

Terminal-type string: xterm

Terminal speeds: 38400,38400

Environment variables

Variable:

Value:

The second part of the error message is ‘No supported authentication methods available’.

Please refer to the below table for the AMI (Amazon Machine Images, which means the copy or the snapshot of an instance) and their corresponding usernames

S.No.	AMI	Username
1	Linux	ec2-user
2	Centos	centos

3	Debian	admin / root
4	Fedora	ec2-user / fedora
5	RHEL	ec2-user / root
6	SUSE	ec2-user / root
7	UBUNTU	ubuntu

Therefore Option ‘**A**’ and ‘**E**’ are correct.

Option ‘B’ is incorrect, as port ‘3389’ denotes RDP (Remote Desktop access)

Option C is incorrect as port '389' denotes 'LDAP'

Option ‘D’ is incorrect, as the login to AWS console is not at all related to the error message.

For more information, check out the following URLs:

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

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

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 **Time** 0 : 30 Try Now

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 35 Unattempted

Domain :Design High-Performing Architectures

A company has a requirement to monitor API activity for audit purposes for their AWS account. This audit would be conducted in the future as well and should be applicable to all regions. How would you design your solution to meet the present and future needs?

A. **Ensure CloudTrail logs is enabled for each region and then enable for each future region.**

B. **Ensure one CloudTrail log is enabled for all regions**

C. **Enable AWS Config to record the events in all regions.**

D. **Enable AWS Inspector to record the events in all regions.**

Explanation:

Answer – B

The AWS Documentation mentions the following

When you create a trail that applies to all regions, CloudTrail records events in each region and delivers the CloudTrail event log files to an S3 bucket that you specify. If a region is added after you create a trail that applies to all regions that the new region is automatically included, and events in that region are logged.

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Option A is incorrect since this is an overhead to enable it each time for every new region

Options C is incorrect since **AWS Config** is a service that enables you to assess, audit, and evaluate the configurations of your **AWS** resources. **Config** continuously monitors and records your **AWS** resource configurations

Option D is incorrect since Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices

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

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 36 Unattempted

Domain :Design Secure Applications and Architectures

Your team is planning on developing and deploying an application onto AWS with the following architecture

- A set of EC2 Instances in a VPC hosting the web tier
- A database hosted using the AWS RDS MySQL instance

Which of the following should ideally be set so that only HTTPS users to be able to access the web application and for the web application to access the database? (Choose 2)

A. **An Inbound Security group rule for the web EC2 Instances allowing traffic from the source of 0.0.0.0/0 and port 443**

B. **An Inbound Security group rule for the database layer allowing traffic from the source of 0.0.0.0/0 and port 443**

C. **An Inbound Security group rule for the web EC2 Instances allowing traffic from the source of the database on port 3306**

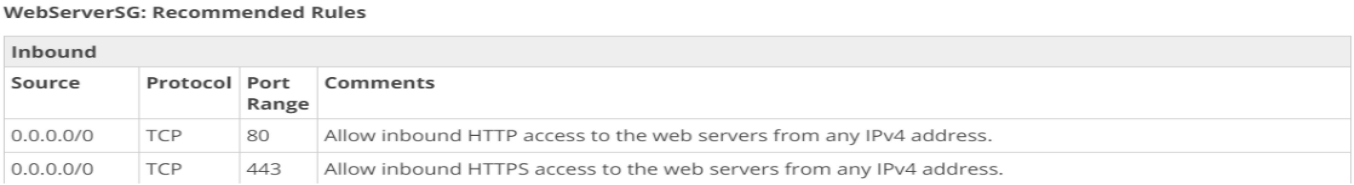
D. **An Inbound Security group rule for the database layer allowing traffic from the source of the web layer on port 3306**

Explanation:

Answer – A and D

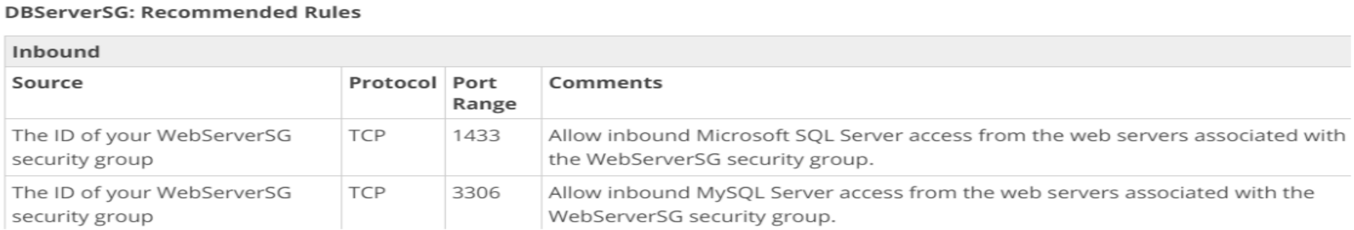
Option A is correct because port 443 will allow only HTTPS traffic from all sources.

Option D is correct because Database server Security Group must allow traffic from the source Web server on port 3306



WebServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access to the web servers from any IPv4 address.
0.0.0.0/0	TCP	443	Allow inbound HTTPS access to the web servers from any IPv4 address.



DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.

Option B is invalid since the database should not be exposed to the Internet

Option C is invalid since the database security group should allow incoming traffic on port 3306

For more information on this scenario, please refer to the below URL and go to Security section

https://docs.aws.amazon.com/vpc/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 37 Unattempted

Domain :Design High-Performing Architectures

In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances. Which IPv4 CIDR block would you use to achieve the same?

A. **151.0.0.0/27**

B. **151.0.0.0/28**

C. **151.0.0.0/29**

D. **151.0.0.0/30**

Explanation:

Correct Answer: A

AWS reserves 5 ip addresses.

The formula to calculate the number of assignable IP addresses to CIDR networks is similar to classful networking. Subtract the number of network bits from 32. Raise 2 to that power and subtract 2 for the network and broadcast addresses. For example, a /24 network has 2^(32-24) - 2 addresses available for host assignment.

A. Prefix Length is '27'

Therefore 32-27 = 5 and 2 ^ 5 (i.e 2 * 2 * 2 * 2 * 2) – 5 = 27

B. Prefix Length is '28'

Therefore 32-28 = 4 and 2 ^ 4 (i.e 2 * 2 * 2 * 2) - 5= 11

C. Prefix Length is '29'

Therefore 32-29 = 3 and 2 ^ 3 (i.e 2 * 2 * 2) - 2 = 3

D. Prefix Length is '30'

Therefore 32-30 = 2 and 2 ^ 2 (i.e 2 * 2) - 5 = -1

For option 'A' we get '27' IP addresses (or indirectly the number of instances to be provisioned) as shown above

Since the user has to provision '20' EC2 instances, we need to go with option '**A**' which is the only correct IPv4 CIDR block.

Option 'B' is incorrect because we get only '11' IP address (or indirectly the number of instances to be provisioned)

Option 'C' is incorrect because we get only '3' IP address

Option 'D' is incorrect because we get only '-1' IP address

For more information, please refer to the below URL:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html#vpc-sizing-ipv4

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 38 Unattempted

Domain :Design High-Performing Architectures

A Company is currently hosting an application which connects to a MySQL AWS RDS Instance. Of late there have been many performance issues being encountered. After careful analysis, it has been determined that the issue is occurring as a result of similar queries being fired against the database. Which of the following can be added to the architecture to alleviate the performance issue?

A. **Enable Multi-AZ for the database**

B. **Use the Elastic Cache Service**

C. **Use Read replica**

D. **Use Cloudfront in front of the database**

Explanation:

Answer – B

ElastiCache can be used to reduce the latency of requests as it is a caching service

Let's understand the difference in Read replica and ElastiCache

In terms of load, they have the same goal, but they differ in other areas:

Up-to-dateness of data:

A read replica will continuously sync from the master. So your results will probably lag 0 - 3s (depending on the load) behind the master.

A cache takes the query result at a specific point in time and stores it for a certain amount of time.

Performance:

A cache can only return results for queries it has already seen. So if you run the same queries over and over again, it's a good match.

If you have many different, frequently changing, or dynamic queries, a read replica will be a better match.

ElastiCache should be much faster since it's returning values directly from RAM. However, this also limits the number of results you can store.

Option A is incorrect since this is used for high availability of the database

Option C is incorrect since using ElastiCache is a better choice.

Option D is incorrect since Cloudfront should be used with Web distributions

For more information on ElastiCache, please refer to the below URL

https://aws.amazon.com/elasticache

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 39

Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Administrator for a media company. They are using AWS resources in various regions for broadcasting live sports matches. Multiple EC2 On-Demand, Spot & Reserved Instances are launched as per user traffic on a daily basis resulting in huge monthly charges. Top management is looking for customized analysis for these charges based upon various factors like month-wise, instance-wise to deep dive into the incurred cost and they should be able to visualize the costs analysis. To meet this requirement, the accounts team is looking for a simpler way to analyze these charges and query this report. Suggest a cost-effective solution that can be set up with the least efforts?

A. **Upload the AWS Cost and Usage Reports to S3. Integrate these reports with Amazon Athena to analyze billing data**

B. **Upload AWS Cost & Usage Reports to Amazon QuickSight & analyze billing data**

C. **Download CSV report from Amazon S3 & analyze cost & usage using a third-party tool.**

D. **Upload AWS Cost & Usage Reports to Amazon Redshift & analyze billing data**

Explanation:

Correct Answer – B

Amazon QuickSight is a business analytics service you can use to build visualizations, perform ad hoc analysis, and get business insights from your data. It can automatically discover AWS data sources and also works with your data sources.

Option A is incorrect AWS Athena doesn't provide visualizations.

Option C is incorrect as using a third-party tool to analyze cost & usage reports can be costly.

Option D is incorrect as Amazon Redshift is a petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. It is not used for such cost analysis. It is used for complex queries and data warehousing.

For more information on Amazon QuickSight, refer to the following URL,

https://docs.aws.amazon.com/quicksight/latest/user/welcome.html#analyses

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 40 Unattempted

Domain :Design High-Performing Architectures

A Company is currently hosting an application which connects to a MySQL AWS RDS Instance The application behaves fine when there are 20 lookups against the database. When the lookups start to increase, the performance of the application starts to degrade. Which of the following can be added to the architecture to alleviate the performance issue?

A. **Create a Read Replica for the database**

B. **Enable Multi-AZ for the database**

C. **Place the database behind a Cloudfront distribution**

D. **Create a snapshot of the database**

Explanation:

Answer – A

Option B is incorrect since this is used for high availability of the database

Option C is incorrect since Cloudfront is used for web distributions

Option D is incorrect since this is used for backups of databases

The AWS Documentation mentions the following

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.

For more information on AWS Read Replica's, please refer to the below URL https://aws.amazon.com/rds/details/read-replicas/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 41 Unattempted

Domain :Design Secure Applications and Architectures

Your company needs to develop an application that needs to have a login module in place. Their key requirement is to ensure that users can also use their current identities which they have with various providers such as facebook to log into the application. Which of the following can help you accomplish this?

A. Using the AWS Cognito service

B. Using the AWS Config service

C. Using the AWS SQS service

D. Using the AWS WAF service

Explanation:

Answer – A

The AWS Documentation mentions the following

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.

The two main components of Amazon Cognito are user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools enable you to grant your users access to other AWS services. You can use identity pools and user pools separately or together.

Option B is incorrect since this is a configuration service

Option C is incorrect since this is a messaging service

Option D is incorrect since this is a web application firewall service

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

https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 42 Unattempted

Domain :Design Cost-Optimized Architectures

A mid-sized Fintech company is using AWS Organization to manage multiple AWS accounts created for each department. Each of the accounts has purchased a Reserved Instance & are running web applications on a mix of On-Demand & Reserved Instance pool. A default IAM policy is configured for all accounts. Due to high recurring cost, Management has appointed you as an AWS consultant to suggest recommendations to reduce cost. Post analysis, you suggested purchasing more Reserved Instance as compared to using On-Demand EC2 instance. How would you justify your recommendations to the management?

A. **Use organization master account to create RI coverage budgets for all the accounts in an organization and receive SNS alert once the threshold is below 50%.**

B. **Use Organization member account owners to create RI coverage budgets for their individual accounts in an organization & receive SNS alert once the threshold is below 50%.**

C. **Use Organization member account owners to create RI utilization budgets for their individual accounts in an organization and receive SNS alert once the threshold is below 50%.**

D. **Use Organization master account to create RI utilization budgets for all the accounts in an organization and receive SNS alert once the threshold is below 50%.**

Explanation:

Correct Answer – B

The Reserved Instance Utilization and Coverage reports are not the same

EC2 RI Utilization % offers relevant data to identify and act on opportunities to increase your Reserved Instance usage efficiency. It's calculated by dividing the Reserved Instance used hours by total Reserved Instance purchased hours.

EC2 RI Coverage % shows how much of your overall instance usage is covered by Reserved Instances. This lets you make informed decisions about when to purchase or modify a Reserved Instance to ensure maximum coverage. It's calculated by dividing the Reserved Instance used hours by total EC2 On-Demand and Reserved Instance hours.

RI Coverage Budget reports the number of instances that are part of the Reserved Instance. This helps you to get an alert when the number of instances covered by reservation falls below 50% of the total number of instances launched. This report can identify the instance which is consistently running using On-Demand instance & can be converted to Reserved Instance for cost savings. AWS Organization member accounts' owners can create a budget for individual accounts. AWS Organization master account pays for usage incurred by all accounts in the organization.

Option A is incorrect since the company is using a default IAM policy, each member account owner needs to create a budget policy for individual accounts & not by master account.

Option C is incorrect as RI utilization Budget reports the utilization of your RI instance and you need RI Coverage report to check when the number of instances covered by reservation falls below 50% of the total number of instances launched.

Option D is incorrect since the company is using a default IAM policy, each member account owner needs to create a budget policy for individual accounts & not by master account. Also, you need RI Coverage report to check when the number of instances covered by reservation falls below 50% of the total number of instances launched

For more information, refer to the following URLs:

https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/aws-cost-explorer.html

https://aws.amazon.com/aws-cost-management/reserved-instance-reporting/

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/grantaccess.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 43 Unattempted

Domain :Design Secure Applications and Architectures

Your current architecture consist of a set of web servers that are spun up as part of an Autoscaling group. These web servers then communicate with a set of database servers. You need to ensure that the security groups of the database servers are set properly to accept traffic from the web servers. Which of the following is the best way to accomplish this?

A. **Ensure that the Private IP addresses of the web servers are put as sources for the incoming rules in the database server security group**

B. **Ensure that the Public IP addresses of the web servers are put as sources for the incoming rules in the database server security group**

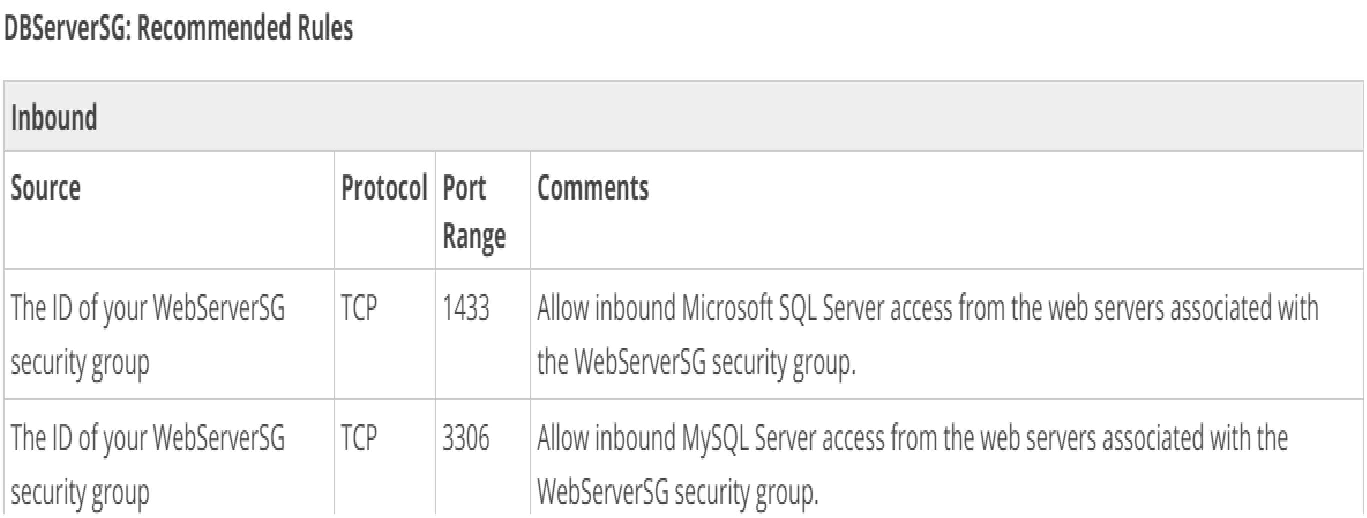
C. **Ensure that the web server security group is placed as the source for the incoming rules in the database server security group**

D. **Ensure that the Instance ID of the web servers are put as sources for the incoming rules in the database server security group**

Explanation:

Answer – C

The below example from the AWS Documentation also shows the Source of the database security group involving the ID of the web server security groups.



DBServerSG: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comments
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.

Options A and B are invalid or not the best practise. Since they are part of the Autoscaling Group , the IP addresses of the instances can change.

Option D is incorrect since normally you don't specify the Instance ID in security Groups

For more information on the Security Groups for the VPC, please refer to the below URL

https://docs.aws.amazon.com/vpc/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 44 Unattempted

Domain :Design Resilient Architectures

Your company needs to host an application on an EC2 Instance. There is a requirement based on the compliance rules for the application that you need to have control over the number of cores allocated to the application. Which of the following should be used in such a case?

A. **AWS Lambda**

B. **EC2 - Dedicated Hosts**

C. **EC2 – Reserved Instances**

D. **Elastic Beanstalk**

Explanation:

Answer – B

The AWS Documentation mentions the following

When you launch instances on a Dedicated Host, the instances run on a physical server that is dedicated to your use. While Dedicated instances also run on dedicated hardware, Dedicated Hosts provide further visibility and control by allowing you to place your instances on a specific, physical server. This enables you to deploy instances using configurations that help address corporate compliance and regulatory requirements.

You have visibility of the number of sockets and physical cores that support your instances on a Dedicated Host. You can use this information to manage to license for your own server-bound software that is licensed per-socket or per-core.

Option A is incorrect because AWS Lambda was launched to eliminate infrastructure management of computing. It enables developers to concentrate on writing the function code without having to worry about provisioning infrastructure. You don't need to do any forecasting of the resources (CPU, Memory, Storage, etc.). It can scale resources up and down automatically.

Dedicated instances are placed on an EC2 Host machine dedicated to your account, but you use them exactly like shared tenancy instance types (On-Demand, Spot, and Reserved). Dedicated Hosts are the same thing, but with additional visibility into the hardware that your instances run on. Check here for more details.

From the above explanation, Option C, D stands invalid.

For more details on Dedicated hosts, please refer below URL

https://aws.amazon.com/elasticbeanstalk/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 45 Unattempted

Domain :Design Secure Applications and Architectures

Your company is planning to store sensitive documents in a bucket in the Simple Storage service. They need to ensure that all objects are encrypted at rest in the bucket. Which of the following can help accomplish this? Choose 2 answers from the options given below

A. **Ensure that the default encryption is enabled for the S3 bucket**

B. **Ensure that the bucket policy is set to encrypt all objects that are added to the bucket**

C. **Ensure that the bucket ACL is set to encrypt all objects that are added to the bucket**

D. **Ensure to change the configuration of the bucket to use a KMS key to encrypt the objects**

Explanation:

Answer – A and D

Options B and C are incorrect since these options cannot be used to actually encrypt the objects as by using an S3 bucket policy, you can enforce the encryption requirement when users upload objects

Refer below URL for more details,

https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/

The term 'rest' means when data is resting (not in transition - while data is traveling to s3).

Server-side encryption - facilitates encryption at rest.

Client-side encryption - facilitates encryption both in transition and at rest.

You have three options depending on how you choose to manage the encryption keys:

SSE-S3 requires that Amazon S3 manage the data and master encryption keys.
SSE-C requires that you manage the encryption key

SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS

For more information, please refer the following URL.
https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket. You can set default encryption on a bucket so that all new objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or customer master keys (CMKs) stored in AWS Key Management Service (AWS KMS).

For more information on Server - Side encryption, please refer to the below URL

https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

To know about default encryption (Option A) please refer to the below URL.

https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.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 46 Unattempted

Domain :Design Cost-Optimized Architectures

A global software company is using Amazon EC2 Reserved and On-Demand Instance for all project-related work. They are having different accounts created for each vertical like Finance, Project, HR which are managed individually by account owners in each vertical. Management is looking for options to decrease these recurring charges. How could the management save monthly billing charges without impacting the performance? **[Choose TWO]**

A. **Each account should launch a Spot Instance instead of using On-Demand Instance.**

B. **Each account should share Reserved Instance which they have purchased with other accounts.**

C. **create AWS organization and leverage consolidated billing feature to get the discounts on Amazon EC2.**

D. **Use Budgets to limit the charges incurred for using Amazon EC2.**

Explanation:

Correct Answer – B and C

Consolidated Billing combines usage from all the accounts & billing is generated based on the total usage. Services like Amazon EC2, Amazon S3, etc. have volume pricing tiers where the overall charges decrease with more usage volume.

Option A is incorrect. Although this will save the cost but will impact the performance.

Spot Instance and On-demand Instance are very similar in nature. The main difference between these is commitment. In Spot Instance there is no commitment. As soon as the Bid price exceeds Spot price, a user gets the Instance. In an On-demand Instance, a user has to pay the On-demand rate specified by Amazon. Once they have bought the Instance they have to use it by paying that rate.
In Spot Instance, once the Spot price exceeds the Bid price, Amazon will shut the instance. The benefit to users is that they will not be charged for the partial hour in which Instance was taken back from them.

Spot instances are not *always* cheaper than on-demand, they can and do sometimes fluctuate wildly, even to very high per hour amounts, higher than the on-demand price at times

Option B is correct as Reserved Instance discounts can be applied to accounts in an organization but Reserved Instance sharing has to be turned on or off for the account

For details, please refer below URL

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/

Option D is incorrect as the Budget will limit charges but will not provide discounts in services being used by various accounts.

For more information on using consolidated billing, refer to the following URL:

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

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/useconsolidatedbilling-discounts.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 47 Unattempted

Domain :Design High-Performing Architectures

A company is planning to host an active-active site. One site will be deployed in AWS and the other one on their On-premise data center. They need to ensure that traffic is distributed proportionately between both sites. Which of the following routing policy would you use for this purpose?

A. **Simple Routing**

B. **Failover Routing**

C. **Latency Routing**

D. **Weighted Routing**

Explanation:

Answer – D

The AWS Documentation mentions the following

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.

To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group

Option A is incorrect since this should be used when you want to configure standard DNS records

Option B is incorrect since this should be used when you want to route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy

Option C is incorrect since this should be used when you want to improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.

For more information on a Routing policy, please refer to the below URL

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 48 Unattempted

Domain :Design High-Performing Architectures

Your company is planning to store sensitive documents in a S3 bucket. They want to keep the documents as private but serve content only to selected users based on a particular time frame. Which of the following can help you accomplish this?

A. **Enable CORS for the S3 bucket**

B. **Use KMS and enable encryption for the files**

C. **Create pre-signed URL's**

D. **Enable versioning for the S3 bucket**

Explanation:

Answer – C

The AWS Documentation mentions the following

A pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permissions to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and expiration date and time. The pre-signed URLs are valid only for the specified duration.

Option A is incorrect since this is used for Cross-origin access

Option B is incorrect since this is used for encryption purposes.

Option D is incorrect since this is used for versioning

For more information on pre-signed URL's, please refer to the below 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 49 Unattempted

Domain :Design Resilient Architectures

A company currently is hosting a Redshift cluster. As part of the disaster recovery drill , you need to ensure that the cluster would be made available even if the primary region goes down. How can you accomplish this?

A. **Use the Elastic Beanstalk service to copy the cluster to another region**

B. **Use Cloudformation templates to copy the cluster to another region**

C. **Configure cross-region snapshots for the underlying Redshift cluster.**

D. **Use the snapshots stored in S3 to create a new Redshift cluster in another region**

Explanation:

Answer - C

You can configure Amazon Redshift to automatically copy snapshots (automated or manual) for a cluster to another region. When a snapshot is created in the cluster's primary region, it will be copied to a secondary region; these are known respectively as the source region and destination region. By storing a copy of your snapshots in another region, you have the ability to restore your cluster from recent data if anything affects the primary

Snapshots are point-in-time backups of a cluster. There are two types of snapshots: automated and manual. Amazon Redshift stores these snapshots internally in Amazon S3 by using an encrypted Secure Sockets Layer (SSL) connection.

Amazon Redshift automatically takes incremental snapshots that track changes to the cluster since the previous automated snapshot. Automated snapshots retain all of the data required to restore a cluster from a snapshot. You can create a snapshot schedule to control when automated snapshots are taken, or you can take a manual snapshot at any time.

When you restore from a snapshot, Amazon Redshift creates a new cluster and makes the new cluster available before all of the data is loaded, so you can begin querying the new cluster immediately. The cluster streams data on demand from the snapshot in response to active queries then loads the remaining data in the background.

https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/

Option A is invalid since AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and not used to copy snapshots for disaster recovery.

Option B is invalid since the CloudFormation template can help in creating clusters but it won't help in disaster recovery.

To check how to create Cluster using CloudFormation, refer below URL

https://aws.amazon.com/blogs/big-data/automate-amazon-redshift-cluster-creation-using-aws-cloudformation/

Option D is invalid since it will be a manual process

For more information on working with snapshots, please refer to the below URL

https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 50 Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Architect for a global Pharma company. They have multiple accounts created in an organization & are using Consolidated billing. Account A has 6 reserved instances while Account B do not have any Reserved Instance. Based on the current utilization, Account A uses 4 Reserved Instance at any time. Account B uses On-Demand Instance for its Web-based application. What will be True with regards to discounts offered by the use of Consolidated billing?

A. **To receive hourly benefits of Reserved Instance from other accounts, Accounts B should have prior approval from Account A to launch the Reserved Instance purchased by Account A.**

B. **To receive hourly benefits of Reserved Instance from other accounts, Accounts B should launch an Instance in any AZ in the same region**

C. **To receive hourly benefits of Reserved Instance from other accounts, Account B should launch an Instance of the same VPC, where account A has purchased a Reserved Instance.**

D. **To receive hourly benefits of Reserved Instance from other accounts, Account B should launch Instance in any AZ in a different region**

Explanation:

Correct Answer – B

Consolidate Billing combines the usage of all Accounts within an organization & shares Reserved Instance between multiple accounts. This discount is valid only if the account which has purchased Reserved Instance is not using its all Instances & other accounts have launched Instance in the same AZ as that of the account which has purchased this Instance.

When you purchase a Reserved Instance, you determine the scope of the Reserved Instance. The scope is either regional or zonal.

As you might be aware AWS Randomizes in AZs but you can choose the scope as Zonal RIs in case you want to be in specific AZ or if you want to get discount in any AZ, you should go for Regional Reserved Instances

For more details on Zonal and Regional RIs, please refer below URL

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-scope.html#reserved-instances-regional-zonal-differences

Below given example is for Zonal RIs,

For an Amazon EC2 Reserved Instances example, suppose that Bob and Susan each have an account in an organization. Susan has five Reserved Instances of the same type, and Bob has none. During one particular hour, Susan uses three instances and Bob uses six, for a total of nine instances on the organization's consolidated bill. AWS bills five instances as Reserved Instances, and the remaining four instances as regular instances.

Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances. For example, if Susan specifies (`us-west-2a)` when she purchases her Reserved Instances, Bob must specify (`us-west-2a)` when he launches his instances to get the cost-benefit on the organization's consolidated bill.

Option A is incorrect. When Consolidated Billing is enabled, Reserved Instance is by default shared between all accounts. No prior approvals are required to be granted for this sharing. You can turn it off also.

Option C is incorrect as for Reserved Instance to be used by other accounts in the same organization, Instance should be launched in the any AZ and it can be part of different VPC.

Option D is incorrect as to avail Reserved Instance discounts, each Account should use launch instance in the same region.

For more information on Consolidating Billing, refer to the following URL

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidatedbilling-other.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 51 Unattempted

Domain :Design Secure Applications and Architectures

Your company currently has a set of web servers in a public subnet and database servers in the private subnet. You need to ensure administrators from your on-premises environment can access the database servers. Which of the following is a secure way to access the database servers?

A. **Create a bastion host in the private subnet as the database servers. Ask the IT administrators to log into the database servers via the bastion host**

B. **Create a bastion host in the public subnet. Ask the IT administrators to log into the database servers via the bastion host**

C. **Create a NAT instance in the private subnet as the database servers. Ask the IT administrators to log into the database servers via the NAT Instance**

D. **Create a NAT instance in the public subnet as the database servers. Ask the IT administrators to log into the database servers via the NAT Instance**

Explanation:

Answer – B

The AWS Documentation mentions the following

A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration. For example, you can use a bastion host to mitigate the risk of allowing SSH connections from an external network to the Linux instances launched in a private subnet of your Amazon Virtual Private Cloud (VPC).

Option A is incorrect since the bastion host needs to be in the public subnet

Options C and D are incorrect since the NAT instance should not be used as a jump server to the database servers

For more information on using a bastion host, please refer to the below URL

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 52 Unattempted

Domain :Design Secure Applications and Architectures

A company needs to access a service provided by a consultant company. The service from the consultant company and the application of the primary company exist in their respective VPCs. The VPC's are located in different regions. What are the steps that are needed to take to establish communication between these VPCs such that data should not traverse via the Internet? Choose 2 answers from the options below

A. **Create a VPC peering between the VPC's in the primary company and consultant company's account**

B. **Create a Network Load Balancer in the consultant VPC in front of the service. Create a VPC Endpoint. Make the application in the other VPC access this endpoint**

C. **Modify the route tables for each VPC point to the VPC peering connection to access all the IPv4 CIDR blocks of the peer VPC (either way)**

D. **Create an IPSec Virtual Private connection between both accounts. Access the resources accordingly**

Explanation:

Answer – A and C

Option B is incorrect since for VPC Endpoint interfaces, they have to be in the same region

Option D is incorrect since here the traffic will traverse via the Internet

The AWS Documentation mentions the following

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

For more information on AWS Direct Connect and VPC peering, please refer to the below URL

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

the 2 answers provided for the question are correct. Let me explain to you why?

1. Both Primary & Consultant company are existing within there own VPCs in different AWS Regions.
In order to have the connection among them, we create VPC Peering across the region.
Hence, **Option A** is correct answer.

https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/

https://aws.amazon.com/blogs/aws/new-almost-inter-region-vpc-peering/

2. Please refer to the below link, section "Two VPCs with Multiple CIDRs Peered Together" for further details

https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-full-access.html#many-vpcs-full-access

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 53 Unattempted

Domain :Design High-Performing Architectures

Your team has deployed an application which consists of a web and database tier hosted on separate EC2 Instances. Both EC2 Instances are using General Purpose SSD for their underlying volume type. Of late, there are performance issues related to the read and writes of the database EC2 Instance. Which of the following could be used to alleviate the issue?

A. **Change the Instance type to a higher Instance Type**

B. **Change the EBS volume to Provisioned IOPS SSD**

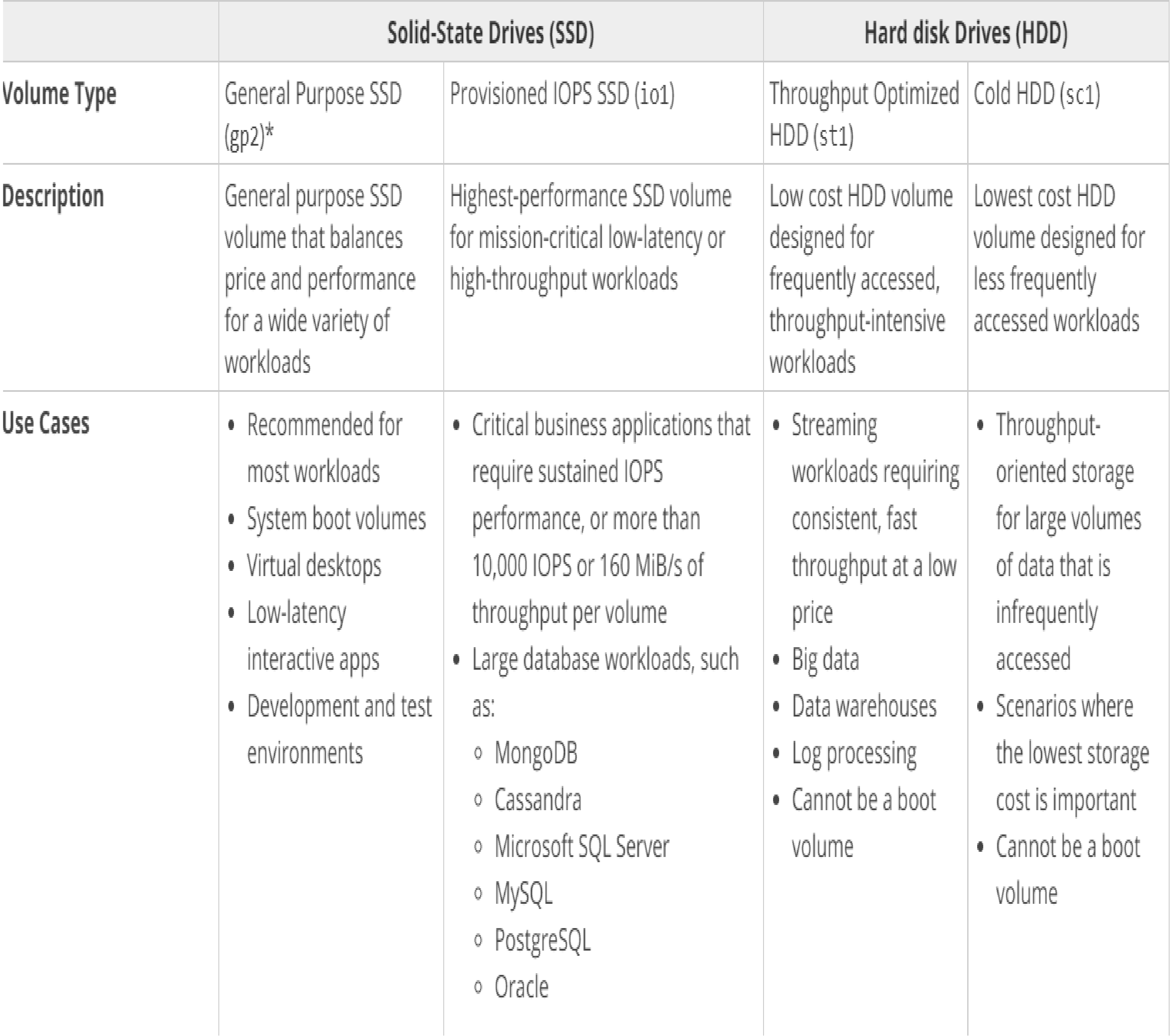
C. **Enable Enhanced Networking on the Instance**

D. **Enable Multi-AZ for the database**

Explanation:

Answer – B

The Provisioned IOPS SSD EBS volume type is perfect for these types of workloads. The below excerpt from the documentation shows the key differences between the different volume types



	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: ○ MongoDB ○ Cassandra ○ Microsoft SQL Server ○ MySQL ○ PostgreSQL ○ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume

Option A is incorrect since the primary issue is that the volume type is not correct

Option C is incorrect since networking is not an issue here

Option D is incorrect since this option is applicable for the AWS RDS service

For more information on EBS volume types, please refer to the below URL

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 54 Unattempted

Domain :Design Cost-Optimized Architectures

Your company currently stores documents in an S3 bucket. They want to transfer the files to a low-cost storage unit after a duration of 2 months to save on cost. Which of the following can be used to perform this activity automatically?

A. **Use the events of the S3 bucket to transfer the files to Amazon Glacier**

B. **Use the events of the S3 bucket to transfer the files to EBS volumes – Cold HDD**

C. **Use the lifecycle policies of the S3 bucket to transfer the files to Amazon Glacier**

D. **Use the lifecycle policies of the S3 bucket to transfer the files to EBS volumes – Cold HDD**

Explanation:

Answer – C

The AWS Documentation mentions the following

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

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

Options B and D are incorrect because ideally you don't transfer to EBS volumes – Cold HDD

Option A is incorrect because you need to use lifecycle policies

For more information on lifecycle policies, please refer to the below URL

https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.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 55 Unattempted

Domain :Design Resilient Architectures

You are working as an AWS architect for a global financial company that offers real-time stock trading quotes to customers. You are using Kinesis Data Streams to process stock market feeds from stock exchanges & provide a real-time dashboard to the customers. During stock market hours, there are a large number of users accessing these dashboards while after market hours, there are very few users accessing these dashboards. The management team is looking for an optimum number of Kinesis Shards within Kinesis Data Streams. Which of the following would be an automated solution to achieve this? (Choose 2)

A. **Use Application Auto Scaling**

B. **Use Amazon Kinesis Scaling Utility to modify the number of Shards in Kinesis Data Streams.**

C. **Use Amazon Kinesis Scaling Utility along with AWS Elastic Beanstalk to automatically modify the number of Shards in Kinesis Data Streams.**

D. **Use UpdateShardCount to scale Shard count as per requirement.**

Explanation:

Correct Answer – A and C

AWS Application Auto scaling can be used to automatically scale Kinesis Streams. For this, CloudWatch can be used to monitor Kinesis Data Stream shard metrics. Based on the changes in these metrics, CloudWatch can initiate a notification to Application Auto Scaling. This will trigger an API Gateway to call Lambda Functions to increase/decrease the number of Kinesis Data Stream Shards based upon metric values.

Alternatively, you can use the Amazon Kinesis Scaling Utilities. To do so, you can use each utility manually, or automated with an AWS Elastic Beanstalk environment.

Option B is incorrect because Amazon Kinesis Scaling Utility alone is a manual process as per documentation

Option D is incorrect as using UpdateShardCount will be a manual process

For more information on Scaling Kinesis Data Streams using Application Auto Scaling and Amazon Kinesis Scaling Utilities, refer to the following URLs:

https://aws.amazon.com/blogs/big-data/scaling-amazon-kinesis-data-streams-with-aws-application-auto-scaling/

https://aws.amazon.com/blogs/big-data/under-the-hood-scaling-your-kinesis-data-streams/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Question 56 Unattempted

Domain :Design Secure Applications and Architectures

You have currently contacted an AWS partner to carry out an audit for your AWS account. You need to ensure that the partner can carry out an audit on your resources. Which one of the following steps would you ideally carry out?

A. **Create an IAM user for the partner account for login purposes**

B. **Create a cross account IAM Role**

C. **Create an IAM group for the partner account for login purposes**

D. **Create an IAM profile for the partner account for login purposes**

Explanation:

Answer - B

The AWS Documentation mentions the following

Cross-account IAM roles allow customers to securely grant access to AWS resources in their account to a third party, like an APN Partner, while retaining the ability to control and audit who is accessing their AWS account. Cross-account roles reduce the amount of sensitive information APN Partners need to store for their customers so that they can focus on their product instead of managing keys.

Cross Account access is safer because,

A basic analogy of the difference is handing someone an access badge (which could be used by anyone) vs handing someone an access badge that requires that person's fingerprints to successfully use.

Using an IAM user to control 3rd party access involves handing over a Access Key/Secret Key - this is the simple "access badge"

Using AssumeRole to control 3rd party access uses the same information plus a security token. To assume a role, your AWS account must be trusted by the role. The trust relationship is defined in the role's trust policy when the role is created. This is the "access badge with fingerprint validation".

(Also, for added security, the Access key/secret key for AssumeRole can be temporary credentials that expire after a specific time period.)

Anyone can use the IAM keys - they're just a key-pair. Anyone can take them and use them later on, and you would not be able to be identify from the trusted party they were given to. To use the AssumeRole, you must be first authenticated as the trusted entity, and in the case of temporary credentials, use them while they haven't expired. These extra security features are what make it more secure.

Typically, you use `AssumeRole` for cross-account access

Option A and C are invalid since it is not secured as IAM users and IAM group (a set of users) will be given permissions just like giving keys to them without extra security token.

Option D is invalid since IAM Profile doesn't exists in AWS

For more information on cross account roles, please refer to the below URL

https://aws.amazon.com/blogs/apn/securely-accessing-customer-aws-accounts-with-cross-account-iam-roles/

https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌵

Question 57 Unattempted

Domain :Design High-Performing Architectures

You are working for a start-up company using Amazon DynamoDB for mobile applications. During performing POC for a new application using AWS SDK, most of the cases are successfully executed, but for certain cases, Amazon DynamoDB is returning an error message. Development Team is asking for your help to verify this error message & suggest a solution for the same so that application logic can be modified. For which of the following HTTP 400 status code returned by Amazon DynamoDB, will you suggest the development team to resubmit the request from the application for successful execution? (Select Two.)

A. **ResourceNotFoundException**

B. **Internal Server Error**

C. **ThrottlingException**

D. **Service Unavailable**

E. **ConditionalCheckFailedException**

F. **LimitExceededException**

Explanation:

Correct Answer – C, F

ThrottlingException & LimitExceededException are part of HTTP status code 4xx. ThrottlingException is an error message generated when you are executing operations like CreateTable, UpdateTable, DeleteTable, very rapidly. LimitExceededException is an error message generated when you are doing concurrent control plane operations. Both error messages can be resolved after trying the same request again.

Option A is incorrect as this exception is part of HTTP status code 4xx & for this error, you will need to fix errors before retrying. This error is generated when a table being requested does not exist or in a CREATING state. Before retrying, you need to check if the table exists.

Options B & D are incorrect as these exceptions are part of HTTP status code 5xx which indicates issues at AWS end. AWS should take corresponding actions from their end.

Option E is incorrect as this exception is part of HTTP status code 4xx & for this error, you will need to fix errors before retrying. This error is generated when a condition being process is failed before moving to the next query.

For more information, refer to the following URL,

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.Errors.html#Pr

Please refer to page 222 and 223 of the below link

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/dynamodb-dg.pdf

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 58 Unattempted

Domain :Design Cost-Optimized Architectures

Your company is planning on making use of the Elastic Container service for managing their container-based applications. They are going to process both critical and non-critical workloads with these applications. Which of the following COST effective setup would they consider?

A. **Use ECS orchestration and Spot Instances for processing critical data and On-Demand for the non-critical data**

B. **Use ECS orchestration and On-Demand Instances for processing critical data and Spot Instances for the non-critical data**

C. **Use ECS orchestration and Spot Instances for both the processing of critical data and non-critical data**

D. **Use ECS orchestration and On-Demand Instances for both the processing of critical data and non-critical data**

Explanation:

Answer – B

Spot Instance and On-demand Instance are very similar in nature. The main difference between these is a commitment. In Spot Instance there is no commitment. As soon as the Bid price exceeds Spot price, a user gets the Instance. In an On-demand Instance, a user has to pay the On-demand rate specified by Amazon. Once they have bought the Instance they have to use it by paying that rate.
In Spot Instance, once the Spot price exceeds the Bid price, Amazon will shut the instance. The benefit to the user is that they will not be charged for the partial hour in which Instance was taken back from them.

Spot instances are not always cheaper than on-demand, they can and do sometimes fluctuate wildly, even to very high per hour amounts, higher than the on-demand price at times

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2 and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

Options A and C are incorrect since Spot Instances can be taken back or interrupted and should not be used for critical workloads

Option D is not a cost-effective solution. You can use Spot Instances for non-critical workloads

For more information on Spot Instances, please refer to the below URL https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 59 Unattempted

Domain :Design Secure Applications and Architectures

Your company is planning on setting up an application that will consists of a web layer. This web layer will consist of EC2 Instances sitting behind an Application Load Balancer. The company wants to protect the application against application level attacks. Which of the following can be used for this purpose?

A. **AWS Cloudfront**

B. **AWS WAF**

C. **AWS Config**

D. **AWS VPC NACL**

Explanation:

Answer – B

The AWS Documentation mentions the following

You use AWS WAF to control how Amazon CloudFront or an Application Load Balancer responds to web requests. You start by creating conditions, rules, and web access control lists (web ACLs). You define your conditions, combine your conditions into rules, and combine the rules into a web ACL.

Option A is invalid because this is used for content delivery

Option C is invalid because this is a configuration service

Option D is invalid because this is used to just block traffic based on simple rules

For more information on how the AWS WAF works, please refer to the below URL https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 60 Unattempted

Domain :Design Resilient Architectures

Your company is planning on setting up an application that will consist of a presentation layer and a data store in DynamoDB. The data in DynamoDB will only be used frequently within the week in which the data is inserted. After a week, the data would tend to become stale. But the stale data would need to be available on durable storage for future analysis on historical data. Also, management overhead should not be there. Which of the following would be the ideal implementation steps for this sort of architecture?

A. **Setup DynamoDB tables. Scan the tables for older data and transfer them to another DynamoDB table.**

B. **Setup DynamoDB TTL(Time-to-live) and transfer the old data to S3 using AWS Lambda**

C. **Use the AWS Data Pipeline service to transfer the older data to EBS volumes**

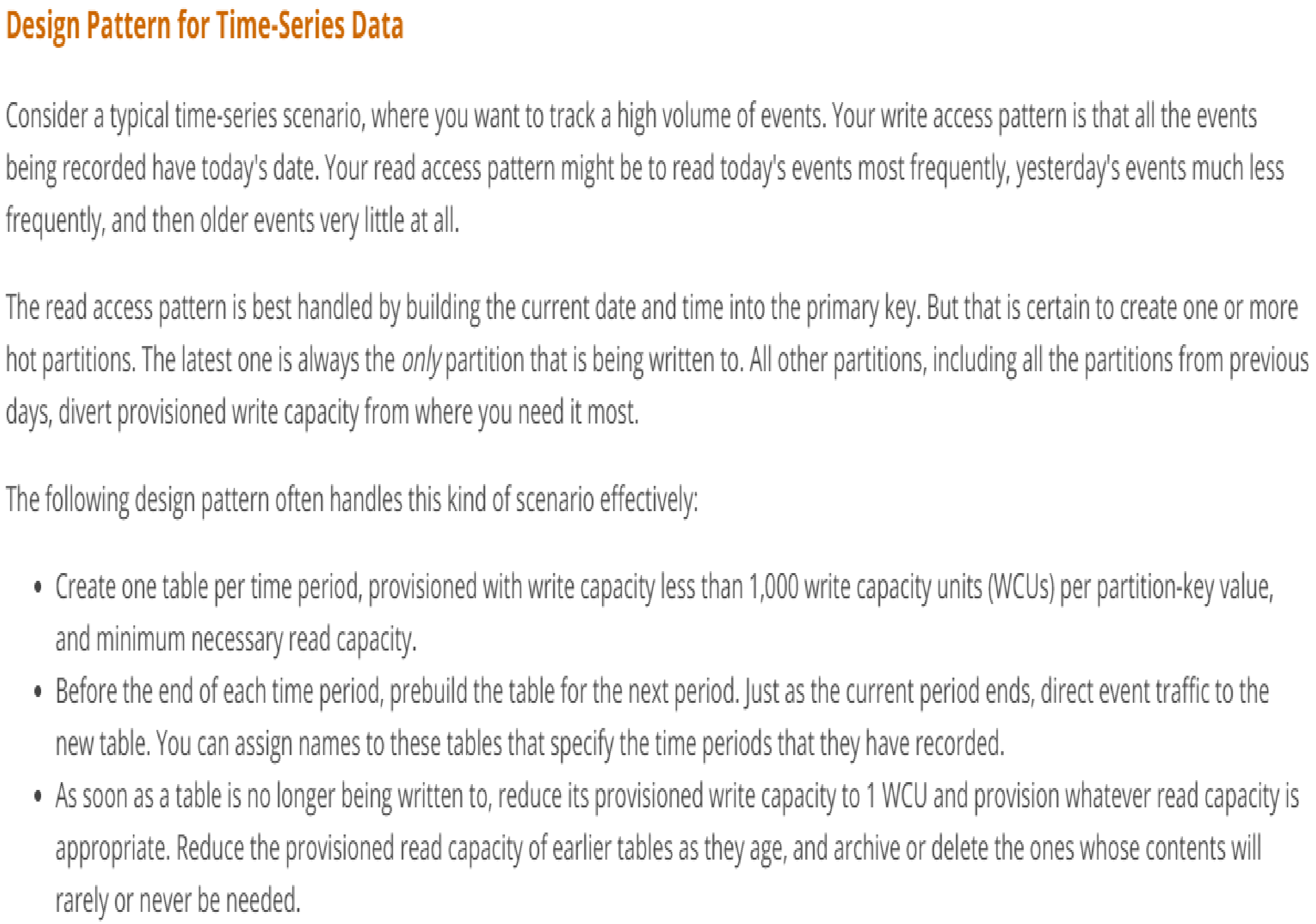
D. **Use the AWS Data Pipeline service to transfer the older data to Amazon S3**

Explanation:

Answer – D

The AWS Documentation mentions the following

AWS Data Pipeline is a web service that you can use to automate the movement and transformation of data. With AWS Data Pipeline, you can define data-driven workflows, so that tasks can be dependent on the successful completion of previous tasks. You define the parameters of your data transformations and AWS Data Pipeline enforces the logic that you've set up.



Design Pattern for Time-Series Data

Consider a typical time-series scenario, where you want to track a high volume of events. Your write access pattern is that all the events being recorded have today's date. Your read access pattern might be to read today's events most frequently, yesterday's events much less frequently, and then older events very little at all.

The read access pattern is best handled by building the current date and time into the primary key. But that is certain to create one or more hot partitions. The latest one is always the *only* partition that is being written to. All other partitions, including all the partitions from previous days, divert provisioned write capacity from where you need it most.

The following design pattern often handles this kind of scenario effectively:

- Create one table per time period, provisioned with write capacity less than 1,000 write capacity units (WCUs) per partition-key value, and minimum necessary read capacity.
- Before the end of each time period, prebuild the table for the next period. Just as the current period ends, direct event traffic to the new table. You can assign names to these tables that specify the time periods that they have recorded.
- As soon as a table is no longer being written to, reduce its provisioned write capacity to 1 WCU and provision whatever read capacity is appropriate. Reduce the provisioned read capacity of earlier tables as they age, and archive or delete the ones whose contents will rarely or never be needed.

Option A is invalid because this would be an inefficient way to handle the data. You will be using too much throughput in the scan process.

Option B is invalid since it involves a lot of management overhead, So better choice is to use Data Pipeline. However, it is possible to do so. Refer below URL for implementation details,

https://aws.amazon.com/blogs/database/automatically-archive-items-to-s3-using-dynamodb-time-to-live-with-aws-lambda-and-amazon-kinesis-firehose/

Option C is invalid because EBS volumes are not durable storage

For more information on AWS Data Pipeline, please refer to the below URL

https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html

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 61 Unattempted

Domain :Design High-Performing Architectures

A company is going to setup an application that will be based on Docker-based containers. The containers will be setup in the Elastic Container Service. You need to also setup load balancing for the underlying services which are based on dynamic port values. Which of the following would be the fully managed service to use for this purpose?

A. **Classic Load Balancer**

B. **Route 53**

C. **Network Load Balancer**

D. **Application Load Balancer**

Explanation:

Answer - D

Application Load Balancers offer several features that make them attractive for use with Amazon ECS services:

Application Load Balancers allow containers to use dynamic host port mapping (so that multiple tasks from the same service are allowed per container instance).

Application Load Balancers support path-based routing and priority rules (so that multiple services can use the same listener port on a single Application Load Balancer).

Application Load Balancer provides enhanced container support by load balancing across multiple ports on a single Amazon EC2 instance. Deep integration with the Amazon EC2 Container Service

(ECS), provides a fully-managed container offering. ECS allows you to specify a dynamic port in the ECS task definition, giving the container an unused port when it is scheduled on the EC2 instance. The ECS scheduler automatically adds the task to the load balancer using this port.

An Application Load Balancer is more suited for Microservices based architecture or container-based architecture.

Options A, C, and D are incorrect because Network Load Balancers support dynamic host port mapping but it doesn't provide fully managed support for Containers and Classic load balancer doesn't support dynamic host port mapping and Route53 is DNS based routing across multiple regions and not balance containers.

For more information on Load balancing, please refer to the below URL

https://aws.amazon.com/elasticloadbalancing/features/#details

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ∨

Question 62 Unattempted

Domain :Design Resilient Architectures

You have an architecture which consists of a set of web servers in the public subnets. And database servers in the private subnet along with a NAT instance. The NAT instance is now becoming a bottleneck and you are looking to replace it with a NAT gateway. Which of the following would ensure a high availability setup for the NAT device?

A. **Disable source/destination check on the NAT Instances**

B. **Deploy the NAT gateway in 2 availability zones**

C. **Deploy a NAT gateway along with the NAT instance**

D. **Deploy the NAT Gateway in 2 regions**

Explanation:

Answer – B

First, here we have a difference between NAT Instance and NAT Gateway

A NAT instance is an Amazon EC2 instance configured to forward traffic to the Internet. It can be launched from an existing AMI.

Instances in a private subnet that want to access the Internet can have their Internet-bound traffic forwarded to the NAT Instance via a Route Table configuration. The NAT Instance will then make the request to the Internet (since it is in a Public Subnet) and the response will be forwarded back to the private instance.

Traffic sent to a NAT Instance will typically be sent to an IP address that is not associated with the NAT Instance itself (it will be destined for a server on the Internet). Therefore, it is important to turn off the **Source/Destination Check** option on the NAT Instance otherwise the traffic will be blocked.

AWS introduced a **NAT Gateway Service** that can take the place of a NAT Instance. The benefits of using a NAT Gateway service are:

It is a fully-managed service -- just create it and it works automatically, including fail-over

It can burst up to 10 Gbps (a NAT Instance is limited to the bandwidth associated with the EC2 instance type)

However,

Security Groups **cannot** be associated with a NAT Gateway

You'll need one in each AZ since they only operate in a single AZ

For more differences, please refer below URL

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

Ensure that your NAT gateways are deployed in at least two Availability Zones (AZs) in order to enable EC2 instances available within private subnets to connect to the Internet or to other AWS services but prevent the Internet from initiating a connection with those instances. AWS Availability Zones are distinct locations that are engineered to be isolated from failures that occurred in other zones. Each NAT gateway must be deployed within a specific Availability Zone to receive the redundancy implemented in that zone.

Option A is invalid since this is a requirement for the NAT instance to function and will not satisfy the requirement for the question

Option C is invalid since you should just use one type of device

Option D is invalid since you should achieve redundancy via Availability Zones

For more information on the NAT gateway, please refer to the below URL

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 63 Unattempted

Domain :Design Resilient Architectures

Your company is planning on setting up an application with the following architecture

A set of EC2 Instances hosting a web application.

The application will sit behind an Elastic Load balancer

The users will access the application from the internet via the Elastic Load balancer

The application will connect to a backend database server

A NAT Gateway is also implemented

Which of the following is the right architecture for the network, keeping high availability and security in mind?

A. **2 public subnets for the Elastic Load balancer and NAT Gateway, 2 public subnets for the Web server EC2 Instances, 2 private subnets for the database server**

B. **2 public subnets for the Elastic Load balancer and NAT Gateway, 2 private subnets for the Web server EC2 Instances, 2 private subnets for the database server**

C. **2 public subnets for the Elastic Load balancer and NAT Gateway, 2 public subnets for the Web server EC2 Instances, 2 public subnets for the database server**

D. **2 public subnets for the Elastic Load balancer and NAT Gateway, 2 private subnets for the Web server EC2 Instances, 2 public subnets for the database server**

Explanation:

Answer – B

You need to have public subnets for the Elastic Load balancer to ensure that traffic can flow via the Internet

The Web servers can be in the Private subnet since the communication between the instances and the ELB happens via the private IP and also it provide better security for the Web Servers.

The database servers should be in the private subnet since it does not need to communicate with the Internet

Option A is invalid since the ELB is in the Public subnet, there is no need to place the Web Server in the Public subnet because ELB and Web Server communicate via Private IP.

Option C is invalid since the database servers don't need to be in the public subnet

Option D is invalid since the database servers don't need to be in the public subnet

For more information on Elastic Load balancing, please refer to the below URL

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

Note: There is no requirement for ec2 instances to be in public subnet as route53 will route the request to elb whose endpoint is exposed as lb(Load Balancer) is in public subnet and the communication between elb and ec2 instances happen via private ip. So its better for security purpose.

URL: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-internet-facing-load-balancers.html

reate an Internet-Facing Load Balancer

When you create a load balancer in a VPC, you can make it an internal load balancer or an Internet-facing load balancer. You create an Internet-facing load balancer in a public subnet. Load balancers in EC2-Classic are always Internet-facing load balancers.

When you create your load balancer, you configure listeners, configure health checks, and register back-end instances. You configure a listener by specifying a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instances) connections. You can configure multiple listeners for your load balancer.

Try now labs related to this question

Introduction to AWS Elastic Load Balancing

This lab walks you through AWS Elastic Load Balancing. Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. In this lab, we will demonstrate elastic load balancing with 2 EC2 Instances.

Credit Needed 10 **Time** 0 : 30 Try Now

Ask our Experts

Rate this Question? ☺ ☹

View Queries

open

Question 64 Unattempted

Domain :Design Resilient Architectures

You are working as an AWS consultant for a Bio-technology company that is working on the Human genome data processing. They are using HDFS to process this large amount of data. They are planning to migrate these systems to AWS Instance where 50 x EC2 C5 instance will be used to compute data. This is a critical project where any failure will result in huge financial loss. The company is seeking your recommendation for the best solution to avoid correlated failures. Which ways can be used to limit the impact of any Hardware failure in this scenario? (Select two)

A. **Use AWS CLI to deploy EC2 instance in the Partitioned Placement group.**

B. **Use AWS CLI to deploy EC2 instance in the Cluster Placement group.**

C. **Use AWS CLI to deploy EC2 instance in the Spread Placement group.**

D. **Use AWS Console to deploy EC2 instance in Partitioned Placement group.**

Explanation:

Correct Answer – A and D

Launching EC2 in the Placement group is possible using both CLI and Console.

Please refer below URL for details,

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/placement-groups.html#launch-instance-placement-group

Firstly, a Rack server is a computer dedicated to use as a server and designed to be installed in a framework called a rack. Each rack has its own network and power source.

In the **Partition Placement group**, each logical partition within the placement group has its own set of racks. If a rack fails (hardware failure), it may affect multiple instances on that rack within that logical partition. So, if you have replication in other partitions, then your data will be safe. This will be good for Big data applications like HDFS, HBase, Cassandra, Kafka, or any other fault-tolerant systems. This placement group strikes a balance between High Performance and High Availability

Option B is incorrect because, in the **Cluster Placement group**, all instances are placed within a rack. If the rack fails (hardware failure), all instances fail at the same time. Ideal for High-Performance applications.

Option C is incorrect because, in the **Spread Placement group**, each instance is placed in its own distinct rack. Each rack has at most one instance. A rack failure (hardware failure) will not affect more than one instance. Ideal for High Availability or mission-critical applications.

For more information on Placement Groups, refer to the following URL:

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

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 **Time** 0 : 30 Try Now

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 65 Unattempted

Domain :Design Cost-Optimized Architectures

An application needs to be set up on AWS. It consists of several components. Two primary components are required to run for 3 hours every day. The other components are required every day for more than 6-8 hours. Which of the following would you use to ensure COSTS are minimized for the underlying EC2 Instances?
Please select :

A. **Reserved instances for the primary components and On-Demand Instances for the remaining components.**

B. **Spot instances for the primary components and On-Demand Instances for the remaining components.**

C. **On-Demand instances for the primary components and Spot Instances for the remaining components.**

D. **On-Demand instances for the primary components and Reserved Instances for the remaining components.**

Explanation:

Answer – D

The AWS Documentation mentions the following

Reserved Instances provide you with a significant discount compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. These On-Demand Instances must match certain attributes in order to benefit from the billing discount.

On-Demand Instances – Pay, by the second, for the instances that you launch.

> Option A is incorrect since the primary component just runs for 3 hours and also keeping minimal costs in mind, On-demand instances would be the correct choice here (since using reserved instances incur upfront costs)

Options B and C are incorrect since we don't know the type of workload to decide whether Spot Instances are required

For more information on On-Demand and Reserved Instances, please refer to the below URL

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open ⌄

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Support

Contact Us

Help Topics

Company

Become Our Instructor

Support

Discussions

Blog

Business

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