NEW PRACTICE TEST I

Attempt	1
Marks Obtained	38 / 65
Your score is	58.46%
Completed on	Monday , 28 January 2019 , 12:34 PM
Time Taken	01 H 39 M 22 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	65	38	26	1

65 Questions	**38** Correct	**26** Incorrect	**1** Unattempted

Show Answers

All

QUESTION 1 INCORRECT

Your company currently has a VPC with EC2 Instances. A new instance being launched which will host an application that works on IPv6. You need to ensure that this instance can initiate traffic outgoing to the Internet. At the same time, you need to ensure that no incoming connection can be imitated from the Internet on to the Instance. Which of the following would you add to the VPC for this requirement?

- A. A NAT Instance
- B. A NAT gateway
- C. An Internet gateway ✖
- D. An egress-only Internet gateway ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
IPv6 addresses are globally unique and are therefore public by default. If you want your instance to be able to access the Internet, but you want to prevent resources on the Internet from initiating communication with your instance, you can use an egress-only Internet gateway.
Options A and B are incorrect since these are used only for Instances in the private subnet to communicate with the Internet
Option C is incorrect since this will not stop incoming connections on IPv6 from the Internet
For more information on the gateway, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/egress-only-internet-gateway.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/egress-only-internet-gateway.html)

Ask our Experts

QUESTION 2 INCORRECT

Your company currently has a VPC with EC2 Instances. A new instance being launched which will host an application that works on IPv6. Which of the following pre-requisite needs to be followed to ensure that the new Instance can communicate over IPv6?

- A. Associate a NAT Instance with the VPC
- B. Attach an egress-only Internet gateway ✖
- C. Ensure your VPC works in Dual stack mode ✔
- D. Associate a NAT gateway to the VPC

Explanation :

Answer – C
The AWS Documentation mentions the following
If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other.
All other options are incorrect since there is no mention in the question for the Instance to have any sort of communication with the Internet.
For more information on enabling IPv6 for your VPC, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html)

Ask our Experts

QUESTION 3 CORRECT

Your development team has currently made changes to an application which is hosted in AWS. Currently the application is in Production and Route 53 is being used as the DNS service. The new version of the application has undergone testing and now needs to be promoted to a separate environment. They need an initial set of traffic to be directed to the new version of the application for testing, before the final cutover can be made. Which of the following would you implement?

- **A.** 2 resource records based on the Simple Routing policy
- **B.** 1 resource record based on the Latency Routing policy
- **C.** 1 resource record based on the Geo-location Routing policy
- **D.** 2 resource records based on the Weighted Routing policy ✔

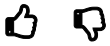
Explanation :

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.
Option A is incorrect since this is used to configure standard DNS records
Option B is incorrect since this is used for resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.
Option C is incorrect since this is used when you want to route traffic based on the location of your users
For more information on Routing policies, please refer to the below URL

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

Ask our Experts



QUESTION 4 CORRECT

A company is planning on hosting a 3-tier application onto AWS. The presentation layer will be hosted on a set of Web servers and the data store will be Oracle based servers using EC2 Instances. You need to ensure that traffic is evenly distributed across all layers. Also you need to ensure that database servers are not accessible to the Internet. Which of the following would you implement? Choose 2 answers from the options given below

- [x] **A.** Create an external load balancer for the web servers ✔
- [ ] **B.** Create an external load balancer for the database servers
- [ ] **C.** Create an Internal load balancer for the web servers
- [x] **D.** Create an Internal load balancer for the database servers ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following

If your application has multiple tiers, for example web servers that must be connected to the Internet and database servers that are only connected to the web servers, you can design an architecture that uses both internal and Internet-facing load balancers. Create an Internet-facing load balancer and register the web servers with it. Create an internal load balancer and register the database servers with it.
Option B is incorrect since it is mentioned that database servers should not be accessible to the Internet, so these need to be internal load balancers
Option C is incorrect since it is mentioned that the main layer accessed by users will be the web layer and hence you need to ensure that this is done via the external load balancer
For more information on Load balancers, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-internal-load-balancers.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-internal-load-balancers.html)

Ask our Experts

QUESTION 5 CORRECT

You've set up an EC2 Instance in one of the default subnets in a default VPC. You need to setup an application on the EC2 Instance. For that you need to ensure that you can log into the Linux Instance. Which of the following changes would you need to implement to be able to log into the Instance

- **A.** Incoming for Security Group for TCP protocol on port 22 ✔
- **B.** Outgoing for Security Group for TCP protocol on port 22
- **C.** Incoming for NACL for TCP protocol on port 22
- **D.** Outgoing for NACL for TCP protocol on port 22

Explanation :

Answer – A
This is given as an example in the AWS Documentation

Inbound			
Source	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
::/0	TCP	80	Allow inbound HTTP access from all IPv6 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
::/0	TCP	443	Allow inbound HTTPS access from all IPv6 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the Internet gateway)
Your network's public IPv4 address range	TCP	3389	Allow inbound RDP access to Windows instances from IPv4 IP addresses in your network (over the Internet gateway)

Option B is incorrect because allowing Outbound traffic is required when your instance needs to connect to a remote host. As in SSH you are initiating the traffic from outside with the EC2 Instance, this must be an Inbound rule.

Options C and D are incorrect since the default NACL's will allow the traffic
For more information on Security Groups, please refer to the below URL

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

Ask our Experts

QUESTION 6 CORRECT

Your company needs to setup a hybrid connection between their on-premise infrastructure and their AWS VPC. They need to ensure to transfer large data sets from their on-premise environment onto AWS. Which of the following would you implement for this requirement?

○ **A.** AWS VPN

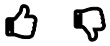
- **B.** AWS Direct Connect ✔
- **C.** AWS VPC peering
- **D.** AWS Placement Groups

Explanation :

Answer – B
Option A is incorrect since this would not guarantee a high bandwidth connection for transferring large data sets
Option C is incorrect since this is used to connect multiple VPC's together
Option D is incorrect since this is used for low latency between EC2 Instances
The AWS Documentation mentions the following
AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
For more information on AWS Direct Connect, please refer to the below URL

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

Ask our Experts



QUESTION 7 CORRECT

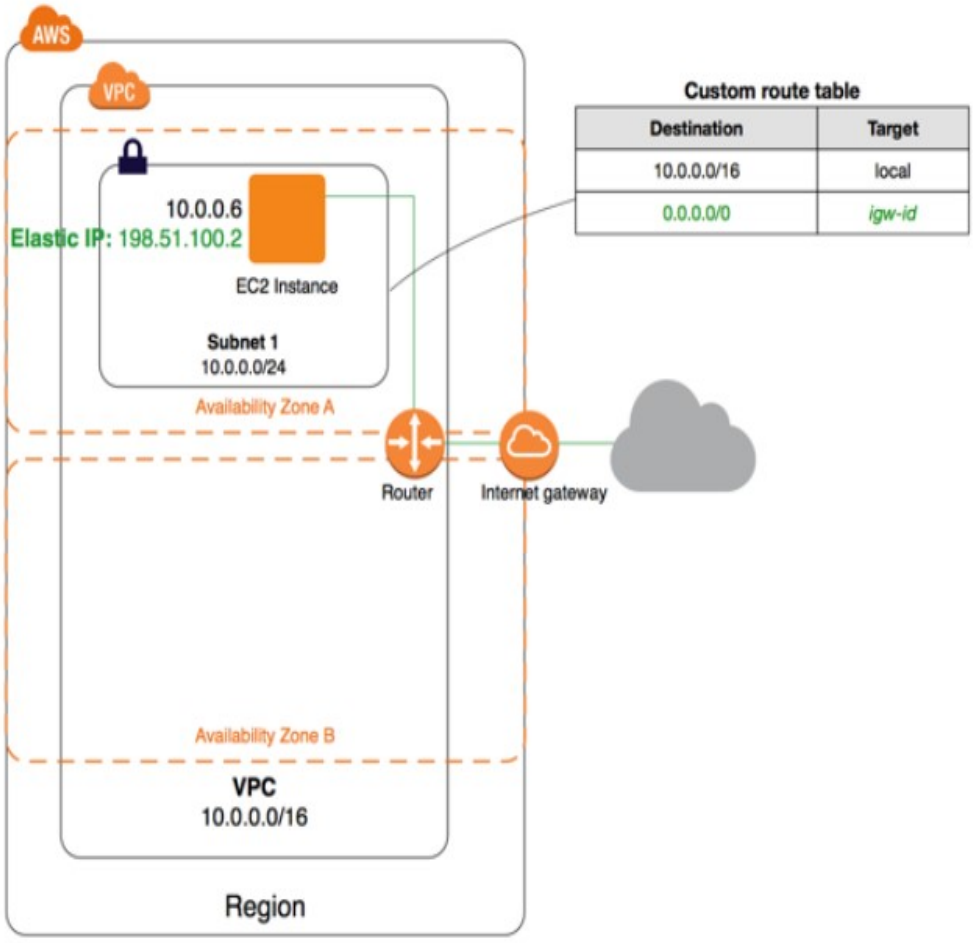
You've setup a new VPC with a subnet. You've created an Internet gateway and attached it to the VPC. You ensured that the VPC is set to allow DNS Resolution and hostnames. You launch an EC2 Instance and ensured that is has a public IP and set the security groups and NACL's for access. But you still can't connect to the Instance. Which one of the following additional step needs to be carried out?

- **A.** Add the Internet gateway to the subnet as well
- **B.** Attach a Private IP to the Instance
- **C.** Ensure the Route table is modified ✔

D. Attach a NAT gateway to the VPC

Explanation :

Answer – C
The following diagrams shows a VPC with a public subnet. The question does not mention the change made to the route table which must also be done for Internet access



Option A is incorrect since the Internet gateway is attached to the VPC only

Option B is incorrect since the Private IP is used for Internal communication only
Option D is incorrect since the NAT gateway is used for Instances in a private subnet to communicate with the Internet.
For more information on public subnets in a VPC, please refer to the below URL

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

Ask our Experts

QUESTION 8 INCORRECT

You're planning on allowing an Administrator to setup an EC2 Instance. This EC2 Instance will host an application that would need access to a DynamoDB table. Which of the following policy permissions are required to ensure that from a security perspective this implementation can be carried out? Choose 2 answers from the options given below.

- [ ] **A.** A trust policy that allows the EC2 Instance to assume a role ✔
- [x] **B.** A trust policy that allows the user to assume a role ✖
- [ ] **C.** An IAM permission policy that allows the user to assume a role
- [x] **D.** An IAM permission policy that allows the user to pass a role ✔

Explanation :

Answer – A and D
This is mentioned in the AWS Documentation

- A *trust policy* for the role that allows the service to assume the role. For example, you could attach the following trust policy to the role with the `UpdateAssumeRolePolicy` action. This trust policy allows Amazon EC2 to use the role and the permissions attached to the role.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "TrustPolicyStatementThatAllowsEC2ServiceToAssumeTheAttachedRole",
        "Effect": "Allow",
        "Principal": { "Service": "ec2.amazonaws.com" },
       "Action": "sts:AssumeRole"
    }
}
```

- An IAM *permissions policy* attached to the IAM user that allows the user to pass only those roles that are approved. `iam:PassRole` usually is accompanied by `iam:GetRole` so that the user can get the details of the role to be passed. In this example, the user can pass only roles that exist in the specified account with names that begin with `EC2-roles-for-XYZ-`:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:GetRole",
            "iam:PassRole"
        ],
        "Resource": "arn:aws:iam::<account-id>:role/EC2-roles-for-XYZ-*"
    }]
}
```

Options B and C are incorrect since the options should be the other way around

For more information on IAM roles and pass roles, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_passrole.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_passrole.html)

Ask our Experts

QUESTION 9 INCORRECT

You are the IT Operations Engineer for a company. The company is planning on starting to use AWS and use services such as EC2, RDS, ELB. For which of the following do you as the IT Operations Engineer have to ensure that scripts are available to manage the high availability of the service?

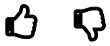
- A. AWS EC2 ✔
- B. AWS RDS
- C. AWS ELB ✖
- D. AWS DynamoDB

Explanation :

Answer – A
As an IT Operations Engineer you need to manage the high availability of EC2 via scripts. So you need to create backups via creating AMI's
Option B is incorrect since this service has features like Multi-AZ , Automated Backups to achieve high availability
Option C is incorrect since this service is already built with high availability in place
Option D is incorrect since this service is fully managed by AWS
For more information on best practices for EC2, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html)

Ask our Experts



QUESTION 10 CORRECT

Your company has an account in AWS which is being actively used. There is an audit being conducted by an external auditor. They have requested for a list of users, their status, to see if MFA is being used etc. How would you achieve in getting this list for them?

- A. Call up AWS support to get the list of credentials
- B. Contact an AWS partner to get the list of credentials
- C. Go to IAM and download the Credentials report ✔
- D. Go to EC2 and download the Credentials report

Explanation :

Answer - C
This is mentioned in the AWS Documentation
You can generate and download a *credential report* that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs (https://aws.amazon.com/tools) and Command Line Tools (https://aws.amazon.com/tools/#Command_Line_Tools), or the IAM API.
All other options are invalid since the report is already available for download from the IAM section.
For more information on getting report credentials, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html)

Ask our Experts

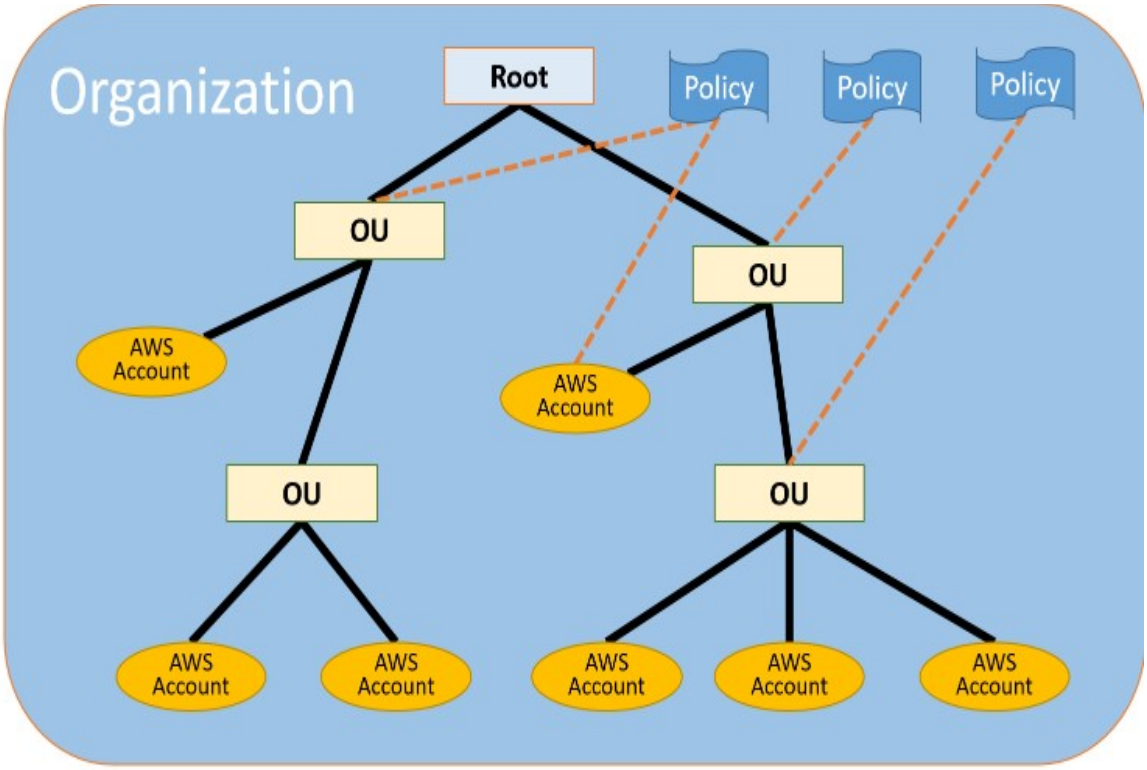
QUESTION 11 INCORRECT

Your company is planning on setting up multiple accounts in AWS. The IT Security department has a requirement to ensure that certain services and actions are not allowed across all accounts. How would you achieve this in the most EFFECTIVE way possible?

- A. Create a common IAM policy that can be applied across all accounts ✖
- B. Create an IAM policy per account and apply them accordingly
- C. Deny the services to be used across accounts by contact AWS
- D. Use AWS Organizations and Service Control Policies ✔

Explanation :

Answer – D
The AWS Documentation mentions the following



An AWS organization is an entity that you create to consolidate your AWS accounts (https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#account).

A service control policy is a policy that specifies the services and actions that users and roles can use in the accounts that the SCP affects.
Option A is incorrect since you can't have a common IAM policy
Option B is incorrect since this is an ineffective way of managing centralized control
Option C is incorrect since AWS should not be responsible for denying usage of services in an account
For more information on AWS organizations, please refer to the below URL

- https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html (https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html)

Ask our Experts

QUESTION 12 INCORRECT

Your company has just started using AWS. You as the IT Administrator have root access to the account. You now need to grant a set of user's access to log into the console. They would have a certain set of defined permissions. Which of the following would you implement?

- A. Grant the users root access via your account
- B. Create IAM users and generate passwords ✔
- C. Create IAM users and generate access keys ✖
- D. Create IAM Roles and ask the user to use the roles to log in

Explanation :

Answer – B
The following is mentioned in the AWS Documentation
You can access AWS in different ways depending on the user credentials:

· Console password (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords.html): A password that the user can type to sign in to interactive sessions such as the AWS Management Console.

· Access keys (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html): A combination of an access key ID and a secret access key. You can assign two to a user at a time. These can be used to make programmatic calls to AWS. For example, you might use access keys when using the API for code or at a command prompt when using the AWS CLI or the AWS PowerShell tools.

Option A is incorrect since this is an insecure way to manage access for users
Option C is incorrect since they need passwords to log into the console
Option D is incorrect since IAM Roles are not used for login purposes.
For more information on IAM users, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

Ask our Experts

QUESTION 13 CORRECT

An S3 bucket exists in an AWS Account. Users have been asked to access files in this bucket. But when they try to access the files they get a '403 Forbidden' error message. As an IT administrator what do you need to check to ensure that the users can access the files?

- A. Ensure that the bucket has the right encryption method
- B. Ensure that the bucket policy allows access ✔
- C. Ensure that versioning is enabled on the bucket
- D. Ensure that MFA is enabled on the bucket

Explanation :

Answer – B
If you look at the S3 Error Codes, the error basically corresponds to an access problem. So the permission on the bucket policy should be checked.

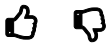
Error Code	Description	HTTP Status Code	SOAP Fault Code Prefix
AccessDenied	Access Denied	403 Forbidden	Client
AccountProblem	There is a problem with your AWS account that prevents the operation from completing successfully. Please contact AWS Support for further assistance, see Contact Us.	403 Forbidden	Client
AllAccessDisabled	All access to this Amazon S3 resource has been disabled. Please contact AWS Support for further assistance, see Contact Us.	403 Forbidden	Client

Option A is incorrect since this is only used for encryption of objects in the bucket

Options C and D are incorrect since these are only used to help to avoid accidental deletion of objects in the bucket
For more information on S3 error responses, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/API/ErrorResponses.html (https://docs.aws.amazon.com/AmazonS3/latest/API/ErrorResponses.html)

Ask our Experts



QUESTION 14 CORRECT

The following policy has been set on a bucket

```
{
 "Version": "2012-10-17",
 "Id": "demopolicy",
 "Statement": [
  {
   "Sid": "IPAllow",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "s3:*",
   "Resource": "arn:aws:s3:::demobucket/*",
   "Condition": {
     "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
     "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
   }
  }
 ]
```

}

What does this policy do?

- A. Ensure that clients outside the range of 54.240.143.0/24 have access to all objects in the demobucket.
- B. Ensure that clients in the range of 54.240.143.0/24 are denied access to all objects in the demobucket
- C. Ensure that the client with the IP of 54.240.143.188 is allowed access to the objects in the demobucket
- D. Ensure that the client with the IP of 54.240.143.188 is denied access to the objects in the demobucket ✔

Explanation :

Answer – D
Such an example is also given in the AWS Documentation

The following example grants permissions to any user to perform any Amazon S3 operations on objects in the specified bucket. However, the request must originate from the range of IP addresses specified in the condition.

The condition in this statement identifies the 54.240.143.* range of allowed Internet Protocol version 4 (IPv4) IP addresses, with one exception: 54.240.143.188.

The `Condition` block uses the `IpAddress` and `NotIpAddress` conditions and the `aws:SourceIp` condition key, which is an AWS-wide condition key. For more information about these condition keys, see Specifying Conditions in a Policy. The `aws:sourceIp` IPv4 values use the standard CIDR notation. For more information, see IP Address Condition Operators in the *IAM User Guide*.

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
         "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

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

- https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html)

Ask our Experts

QUESTION 15 CORRECT

Your company has a set of S3 buckets defined in AWS. The reporting users need to analyse the data in S3 using standard SQL. Which of the following service can help meet their demand?

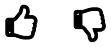
- A. AWS Redshift
- B. AWS Athena ✔
- C. AWS DynamoDB
- D. AWS RDS

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon Athena is an interactive query service that makes it easy to analyse data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.
Option A is incorrect since this is used as a data warehousing solution
Option C is incorrect since this is a fully managed NoSQL database
Option D is incorrect since this is used to manage SQL databases
For more information on AWS Athena, please refer to the below URL

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

Ask our Experts



QUESTION 16 CORRECT

You are an Operations Engineer for a company. The company has just started using AWS RDS-MySQL for their underlying data store. There is a requirement to ensure that the database is available even in the event of a failure. The transition to the backup database should take the least amount of time. Which of the following features would you use to fulfil this requirement?

- A. Use Read Replica's
- B. Use Global tables
- C. Use Multi-AZ ✔
- D. Use Automated Backups

Explanation :

Answer – C
The AWS Documentation mentions the following
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 incorrect since this is used to distribute the read load for databases
Option B is incorrect since this is an option for DynamoDB
Option D is incorrect since this would take a longer time to recover the database
For more information on AWS RDS Multi-AZ, please refer to the below URL

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

Ask our Experts

QUESTION 17 CORRECT

Your operations team is currently managing a set of resources in AWS. There is a need to take in all the log data in real time and scan them for potential threats. Which of the following can be used to process the data in real time?

- A. AWS SQS
- B. AWS SNS

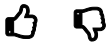
- C. AWS Kinesis ✔
- D. AWS Redshift

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. The data collected is available in milliseconds to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing, and more.
Option A is incorrect since this is a messaging service
Option B is incorrect since this is a notification service
Option D is incorrect since this is a petabyte storage service
For more information on AWS Kinesis Data streams, please refer to the below URL

- https://aws.amazon.com/kinesis/data-streams/ (https://aws.amazon.com/kinesis/data-streams/)

Ask our Experts



QUESTION 18 CORRECT

A company is planning on transferring a large amount of data onto S3. Since they want to start using the data storage on AWS , they are planning on transferring an initial amount of around 100TB of data onto S3. Which of the following would be the ideal way to transfer this amount of data?

- A. Setup a AWS Managed VPN Connection
- B. Setup an AWS Direct Connect connection
- C. Setup VPC Peering
- D. Use the Snowball device ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
AWS Snowball is a service that accelerates transferring large amounts of data into and out of AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at faster-than internet speeds. This transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping containers, complete with E Ink shipping labels. With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premises data centers and Amazon Simple Storage Service (Amazon S3).
Option A is incorrect since there is a lot of data to be transferred and using the Internet VPN connection would not be ideal
Option B is incorrect since there is no mention in the question of on-going data transfer. So setting AWS Direct connect just for a one time transfer might not be so reasonable
Option C is incorrect since this is used for connecting VPC's together
For more information on AWS Snowball, please refer to the below URL

- https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html (https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html)

Ask our Experts

QUESTION 19 CORRECT

Your company has a set of AWS resources which consists mainly of EC2 Instances. The Security departments need to run vulnerability analysis on these machines to ensure that the Instances comply with the latest security standards. Which of the following would you implement for this requirement?

- **A.** AWS Inspector ✔
- **B.** AWS WAF
- **C.** AWS Snowball
- **D.** AWS Cloudfront

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues. Using Amazon Inspector, you can define a collection of AWS resources that you want to include in an assessment target. You can then create an *assessment template* and launch a security *assessment run* of this target.
Option B is incorrect since this is a firewall service
Option C is incorrect since this is used to transfer data from on-premise to AWS
Option D is incorrect since this is used as a content distribution service
For more information on AWS Inspector, please refer to the below URL

- https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html (https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html)

Ask our Experts

QUESTION 20 INCORRECT

You've created your own VPC with Public and Private subnets. You have EC2 Instances setup in the Public and Private subnets. An application has been deployed on an Instance in the private subnet. This Instance needs to interact with the S3 service. But the Instance is not able to interact with the S3 service. You have ensured that an IAM Role with the right permission has been assigned to the EC2 Instance. Which of the following could be the underlying issue?

- **A.** The Route tables don't have an entry to the S3 service
- **B.** The Security Groups for the EC2 Instances are not allowing incoming traffic from S3 ✖
- **C.** A VPC endpoint needs to be attached to the VPC ✔
- **D.** The NACL's for the subnet are not allowing incoming traffic from S3

Explanation :

Answer – C
The AWS Documentation mentions the following

New VPC Endpoint for S3

Today we are simplifying access to S3 resources from within a VPC by introducing the concept of a VPC Endpoint. These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.

EC2 instances running in private subnets of a VPC can now have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.

All other options are wrong because neither the Route tables, Security groups or NACL define the traffic to S3. You need to have a VPC Endpoint or place the Instance in a public subnet.

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

- https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/ (https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/)

Ask our Experts

QUESTION 21 CORRECT

You are the IT Operations Engineer for your company. Your company has a large set of critical resources defined in AWS. You need to be alerted at any time AWS experiences any issues that might have an impact on your resources. Which of the following is the most IDEAL approach for this?

- A. Contact AWS support to relay any issues to you
- B. Contact an AWS Partner to relay any issues to you
- C. Keep a track on all AWS resources and their underlying hardware via CLI scripts
- D. Use the AWS Personal Health Dashboard ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources. The dashboard displays relevant and timely information to help you manage events in progress and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues
All other options are invalid since these are not the ideal implementation steps to look into the health for the underlying AWS resources.
For more information on the AWS Personal Health Dashboard, please refer to the below URL

- https://aws.amazon.com/premiumsupport/phd/ (https://aws.amazon.com/premiumsupport/phd/)

Ask our Experts

QUESTION 22 INCORRECT

You are now the IT administrator for your company. The company has a set of servers sitting in AWS and a set of them sitting in their On-premise locations. They want to monitor the system level metrics for both sets of servers and have a unified dashboard for monitoring. Which of the following can help in this regard? Choose 2 answers from the options given below.

- [ ] **A.** Install the cloudwatch agent on both sets of servers ✔
- [x] **B.** Migrate the on-premise servers to AWS to ensure they can be monitored ✖
- [x] **C.** Setup the metrics dashboard in Cloudwatch ✔
- [ ] **D.** Setup the metrics dashboard in Cloudtrail

Explanation :

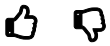
Answer – A and C
The AWS Documentation mentions the following
The unified CloudWatch agent enables you to do the following:

- Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics, in addition to the metrics listed in Amazon EC2 Metrics and Dimensions (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ec2-metricscollected.html). The additional metrics are listed in Metrics Collected by the CloudWatch Agent (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html).
- Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS.
- Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.

Option B is incorrect since you don't need to migrate the servers , since they can be monitored by the Cloudwatch agent.
Option D is incorrect since this is not the monitoring service but the API monitoring service
For more information on the cloudwatch agent, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html)

Ask our Experts



QUESTION 23 CORRECT

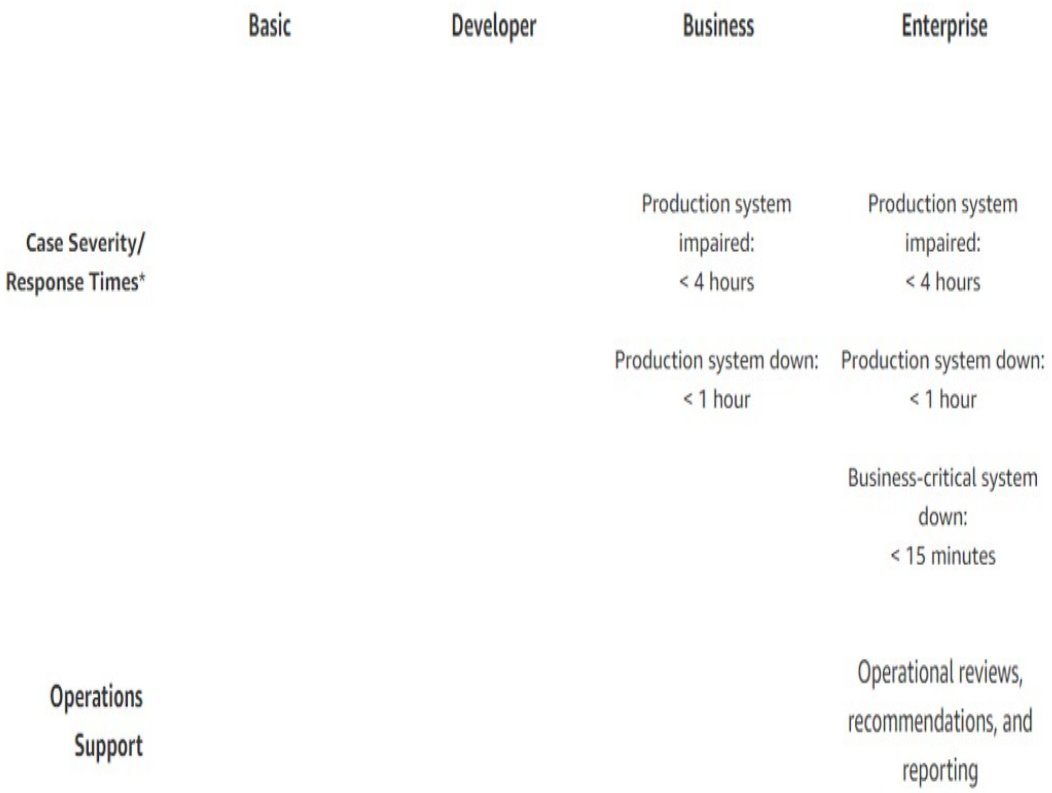
Your company is planning on setting up an AWS account. They would be hosting highly critical revenue generating applications on the AWS platform. They want to purchase the right support plan with AWS. This support plan needs to have operational reviews for the operations department and need to have a response time of 30 mins or less for critical issues. Which of the following support plan would you recommended?

- A. Developer

- B. Basic
- C. Business
- D. Enterprise ✔

Explanation :

Answer – D
If you look at the various support plans, only the Enterprise Plan has this option



All other options become invalid since only the Enterprise Plan has these features

For more information on the various support plans, please refer to the below URL

- https://aws.amazon.com/premiumsupport/compare-plans/ (https://aws.amazon.com/premiumsupport/compare-plans/)

Ask our Experts

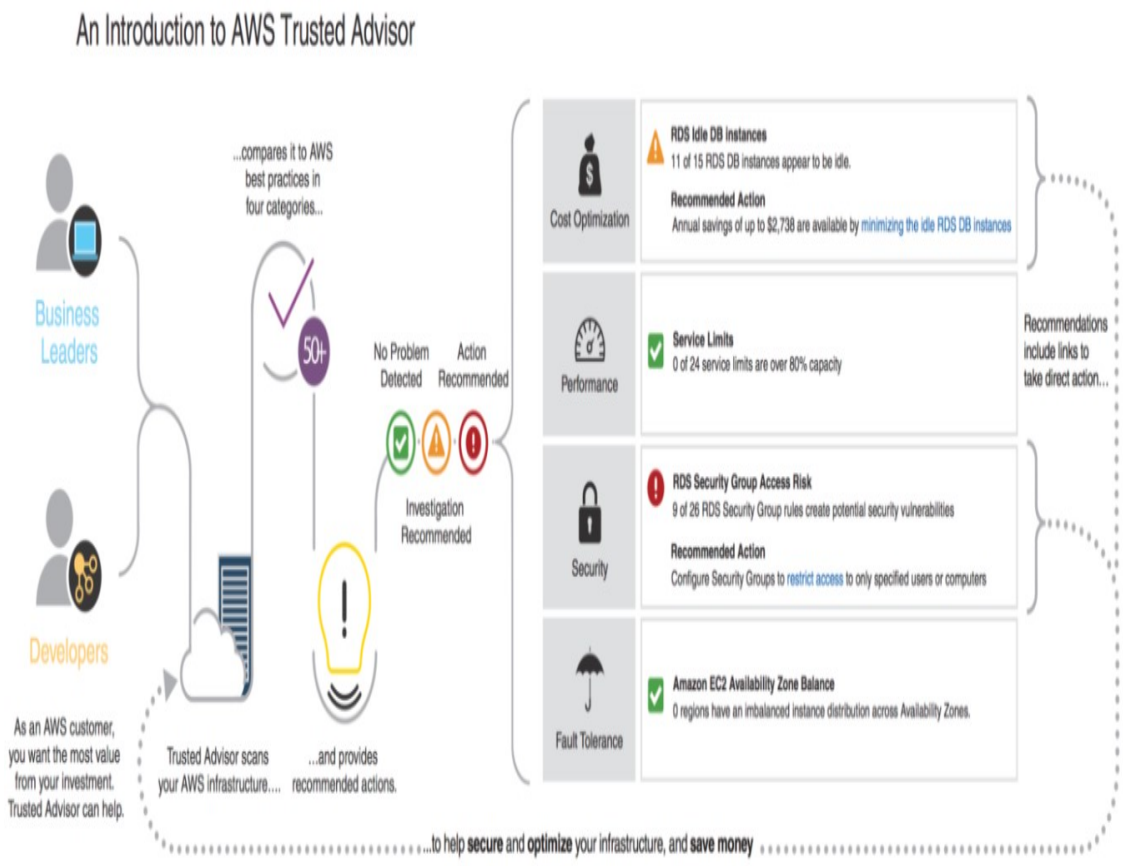
QUESTION 24 CORRECT

Your company is planning on setting up an AWS account. They would be hosting a large number of resources in AWS. As the operations management, you need to be aware of ways to improve on the performance, cost and security of the resources wherever applicable. Which of the following service would you use for this requirement?

- **A.** AWS Trusted Advisor ✔
- **B.** AWS Inspector
- **C.** AWS WAF
- **D.** AWS Cloudfront

Explanation :

Answer – A
The AWS Documentation mentions the following



Option B is incorrect since this is used to check for vulnerabilities in resources such as EC2 Instances

Option C is incorrect since this is used as the Web application firewall
Option D is incorrect since this is used as the Content Distribution Service
For more information on the AWS Trusted Advisor, please refer to the below URL

- https://aws.amazon.com/premiumsupport/trustedadvisor/ (https://aws.amazon.com/premiumsupport/trustedadvisor/)

Ask our Experts

QUESTION 25 CORRECT

Your company has setup EC2 Instances in AWS. These EC2 Instances are normally setup on staging environments and then promoted as production-based instances. You need ensure that SSH is always disabled on these Instances. You normally have around 500 Instances to manage. Which of the following would be the best way to ensure this security check is in place?

- **A.** Use the AWS Inspector to check the Security Groups
- **B.** Use AWS Config Rules to check the Security Groups ✔
- **C.** Create a CLI script to check all the Security groups
- **D.** Use the EC2 Config utility to check all the Security groups

Explanation :

Answer – B
The AWS Documentation mentions the following
Rules can look for any desirable or undesirable condition. For example, you could:

- Ensure that EC2 instances launched in a particular VPC are properly tagged.
- Make sure that every instance is associated with at least one security group.
- Check to make sure that port 22 is not open in any production security group.

Options A and D are incorrect since this cannot be used to check for Security Groups
Option C is incorrect since this is an inefficient way to check for Security Groups compliance
For more information on dynamic compliance checking, please refer to the below URL

- https://aws.amazon.com/blogs/aws/aws-config-rules-dynamic-compliance-checking-for-cloud-resources/ (https://aws.amazon.com/blogs/aws/aws-config-rules-dynamic-compliance-checking-for-cloud-resources/)

Ask our Experts

QUESTION 26 INCORRECT

A developer has configured an S3 bucket in AWS. This bucket is being used as part of development of an application. There is a need for the developer to be notified for any API activity being called on this bucket. How can you configure this?

- A. Create a Cloudwatch log group for the API activity ✖
- B. Configure a cloud trail ✔
- C. Configure cloudwatch agents for S3
- D. Configure cloudwatch metrics for S3

Explanation :

Answer – B
The AWS Documentation mentions the following

Create Multiple Trails

You can use CloudTrail log files to troubleshoot operational or security issues in your AWS account. You can create trails for different users, who can create and manage their own trails. You can configure trails to deliver log files to separate S3 buckets or shared S3 buckets.

Note

Creating multiple trails will incur additional costs. For more information, see AWS CloudTrail Pricing.

For example, you might have the following users:

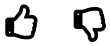
- A security administrator creates a trail in the EU (Ireland) Region and configures KMS log file encryption. The trail delivers the log files to an S3 bucket in the EU (Ireland) Region.
- An IT auditor creates a trail in the EU (Ireland) Region and configures log file integrity validation to ensure the log files have not changed since CloudTrail delivered them. The trail is configured to deliver log files to an S3 bucket in the EU (Frankfurt) Region
- A developer creates a trail in the EU (Frankfurt) Region and configures CloudWatch alarms to receive notifications for specific API activity. The trail shares the same S3 bucket as the trail configured for log file integrity.
- Another developer creates a trail in the EU (Frankfurt) Region and configures SNS. The log files are delivered to a separate S3 bucket in the EU (Frankfurt) Region.

All other options are invalid since they cannot be used to monitor API activity.

For more information on creating multiple trails, please refer to the below URL

- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-multiple-trails.html (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-multiple-trails.html)

Ask our Experts



QUESTION 27 CORRECT

You are working as a Systems Administrator for a company. You need to setup backups for the EBS volumes used in your company's AWS Account. Which of the following would you use for the backups of EBS volumes? Please select 2 correct options.

- [x] **A.** Enable Automated backups for EBS volumes ✔
- [x] **B.** Create EBS Snapshots ✔
- [ ] **C.** Enable volume copy for the EBS volumes
- [ ] **D.** Enable the replication flag on the EBS volumes

Explanation :

Answer – A and B
Option A is correct.
https://aws.amazon.com/blogs/aws/new-lifecycle-management-for-amazon-ebs-snapshots/ (https://aws.amazon.com/blogs/aws/new-lifecycle-management-for-amazon-ebs-snapshots/)
The AWS Documentation mentions the following
You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.
All other options are not valid options in AWS for EBS Volumes.
For more information on EBS Snapshots, please refer to the below URL

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

Ask our Experts

QUESTION 28 INCORRECT

Your company currently is having issues in trying to expand their on-premise storage capabilities. They are looking at AWS for extending their storage for their applications. The new storage should be available as iSCSI targets which can be referenced by the on-premise servers. Which of the following would you use for this purpose?

- A. Storage gateway Cached Volumes ✔
- B. EBS Volumes
- C. DynamoDB tables
- D. S3 storage ✖

Explanation :

Answer – A
The AWS Documentation mentions the following
By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.
Option B is incorrect since this is used for volume storage for EC2 Instances
Option C is incorrect since this is used for NoSQL storage
Option D is incorrect since this is used for object storage
For more information on storage gateway concepts, please refer to the below URL

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

Ask our Experts

QUESTION 29 INCORRECT

You've started a set of EC2 Instances. But the Instances terminate after going into the pending state. Which of the following could be reasons for this? Choose 2 answers from the options given below

- [x] **A.** The EBS volume limit has been reached ✔
- [x] **B.** You've reached the limit for EC2 Instances in your region ✖
- [ ] **C.** AWS does not have sufficient capacity
- [ ] **D.** The EBS snapshot from which the instance is being launched is corrupt ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following
The following are a few reasons why an instance might immediately terminate:

- You've reached your EBS volume limit.
- An EBS snapshot is corrupt.
- The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
- The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.*xx* file).

Option B is incorrect since here you would not be able to even launch the instance
Option C is incorrect since here you can retry creating the instance again
For more information on troubleshooting the launch of EC2 Instances, please refer to the below URL

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

Ask our Experts

QUESTION 30 INCORRECT

Your team is planning on hosting a set of EC2 Instances which is going to host databases. The databases would receive a heavy load. Which of the following EBS volume type would you provision for the underlying EC2 Instances.

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

Explanation :

Answer - B
As per the AWS Documentation, the Provisioned IOPS is good for use for AWS Database workloads

	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

As per the documentation, all other options are invalid.
For more information on EBS volume types, please refer to the below URL

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

Ask our Experts

QUESTION 31 CORRECT

Your development team is looking at developing an application that would be hosted on a set of EC2 Instances. You need to setup storage that can mounted and shared across the multiple EC2 Instances. Which of the following would you use for this purpose?

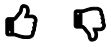
- A. AWS S3
- B. AWS EBS
- C. AWS EFS ✔
- D. AWS RDS

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and 4.1 (NFSv4) protocol.
Option A is invalid because this is object level storage
Option B is invalid because this is block level storage that can only be assigned to individual EC2 Instances
Option D is invalid because this is used to host relational databases
For more information on how the Elastic File System works, please refer to the below URL

- https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html (https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html)

Ask our Experts



QUESTION 32 CORRECT

You are designing a Cloudformation template to create a set of EC2 Instance and install an application package. You need to ensure that the stack is only successful if the software package gets installed successfully. Which of the following would assign in achieving this requirement?

- **A.** Use the cfn-signal helper script ✔
- **B.** Use the Change sets feature
- **C.** Use Cloudwatch logs to signal the completion
- **D.** Use Cloudtrail to signal the completion

Explanation :

Answer – A
The AWS Documentation mentions the following
The cfn-signal helper script signals AWS CloudFormation to indicate whether Amazon EC2 instances have been successfully created or updated. If you install and configure software applications on instances, you can signal AWS CloudFormation when those software applications are ready.
Options C and D are incorrect because these cannot be used to signal the completion of the software packages
Option B is incorrect because this is only used if you need to make changes to the running resources in a stack, you update the stack.
For more information on how cfn signal, please refer to the below URL

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

Ask our Experts

QUESTION 33 INCORRECT

Your developers have created some Lambda functions. They have updated the Lambda functions to access some DynamoDB tables. Which of the following would you need to change specifically to ensure that the Lambda function can access the DynamoDB tables?

- A. Change the Security Groups for the Lambda function ✖
- B. Change the memory assigned for the Lambda function
- C. Change the log group assigned for the Lambda function
- D. Ensure the IAM role attached to the function has DynamoDB access ✔

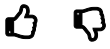
Explanation :

Answer – D
The AWS Documentation mentions the following
Regardless of what invokes a Lambda function, AWS Lambda always executes a Lambda function on your behalf. If your Lambda function needs to access any AWS resources, you need to grant the relevant permissions to access those resources. You also need to grant AWS Lambda permissions to poll your DynamoDB stream. You grant all of these permissions to an IAM role (execution role) that AWS Lambda can assume to poll the stream and execute the Lambda function on your behalf

Option A is incorrect since you need to work with Security Groups for the Lambda function
Option B is incorrect since there is no mention of the programming language being used which would warrant you to change the memory assigned for the Lambda function
Option C is incorrect since the log group is automatically defined.
For more information on using Lambda with DynamoDB, please refer to the below URL

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

Ask our Experts



QUESTION 34 CORRECT

Your team is planning on hosting a set of EC2 Instances which is going to host Memcached which will be used as the Cache for several applications. As the IT admin, you need to provision the EC2 Instances. Which of the following Instance type would you provision for the underlying EC2 Instance?

- A. Compute Optimized
- B. Memory Optimized ✔
- C. Storage Optimized
- D. General Purpose

Explanation :

Answer - B
This is given in the AWS Documentation

Memory Optimized Instances

Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.

R4, R5, and R5d Instances

These instances are well suited for the following applications:

- High-performance, relational (MySQL) and NoSQL (MongoDB, Cassandra) databases.
- Distributed web scale cache stores that provide in-memory caching of key-value type data (Memcached and Redis).
- In-memory databases using optimized data storage formats and analytics for business intelligence (for example, SAP HANA).
- Applications performing real-time processing of big unstructured data (financial services, Hadoop/Spark clusters).
- High-performance computing (HPC) and Electronic Design Automation (EDA) applications.

Because of what the documentation clearly mentions, all other options are invalid
For more information on Memory optimized Instances, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html)

Ask our Experts

QUESTION 35 CORRECT

Your company has a set of EC2 Instances that would be hosting production-based applications. These applications would be running 24*7 throughout the year. You might require to upgrade the instance type during the year as workloads are likely to change and you should adapt as needs evolve. Which of the following is the most cost-effective pricing option for the instances?

- A. On-Demand Instances
- B. Spot Instances
- C. Standard Reserved Instances
- D. Convertible Reserved Instances ✔

Explanation :

Answer – D

The AWS Documentation mentions the following

Types of Reserved Instances (Offering Classes)

When you purchase a Reserved Instance, you can choose between a Standard or Convertible offering class. The Reserved Instance applies to a single instance family, platform, scope, and tenancy over a term. If your computing needs change, you may be able to modify or exchange your Reserved Instance, depending on the offering class. Offering classes may also have additional restrictions or limitations.

The following are the differences between Standard and Convertible offering classes.

Standard Reserved Instance	Convertible Reserved Instance
Some attributes, such as instance size, can be modified during the term; however, the instance type cannot be modified. You cannot exchange a Standard Reserved Instance, only modify it. For more information, see Modifying Reserved Instances.	Can be exchanged during the term for another Convertible Reserved Instance with new attributes including instance family, instance type, platform, scope, or tenancy. For more information, see Exchanging Convertible Reserved Instances. You can also modify some attributes of a Convertible Reserved Instance. For more information, see Modifying Reserved Instances.
Can be sold in the Reserved Instance Marketplace.	Cannot be sold in the Reserved Instance Marketplace.

Option A is incorrect since these are good for temporary workloads

Option B is incorrect since this is good for batch processing workloads

Option C is incorrect since this would not allow to change the instance type during the course of the year.

For more information on Reserved Instance types, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-types.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-types.html)

Ask our Experts

QUESTION 36 INCORRECT

Your company currently has 3 VPC's(VPCA , VPCB and VPCC). There is a requirement to ensure that all instances in all VPC's can communicate with each other. You need to ensure that you apply the minimum configuration required to achieve this. Which of the following would you implement? Choose 2 answer from the options given below

- [ ] **A.** VPC A peered with VPC B and VPC A peered with VPC C and VPC B peered with VPC C ✔
- [x] **B.** VPC A peered with VPC B and VPC B peered with VPC C ✖
- [x] **C.** Ensure that all route tables in each VPC is updated with the respective peering configuration ✔
- [ ] **D.** Ensure that the route tables only in VPC A and VPC B are updated with the respective peering configuration

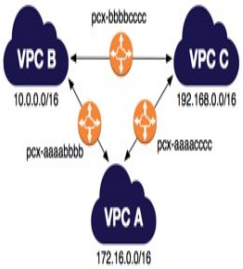
Explanation :

Answer – A and C
This entire example is given in the AWS Documentation

Three VPCs Peered Together

You have peered three VPCs together in a full mesh configuration. The VPCs are in the same AWS account and do not have overlapping CIDR blocks:

- VPC A is peered to VPC B through VPC peering connection pcx-aaaabbbb
- VPC A is peered to VPC C through VPC peering connection pcx-aaaacccc
- VPC B is peered to VPC C through VPC peering connection pcx-bbbbcccc



You may want to use this full mesh configuration when you have separate VPCs that need to share resources with each other without restriction; for example, as a file sharing system.

The route tables for each VPC point to the relevant VPC peering connection to access the entire CIDR block of the peer VPCs.

Route Tables	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-bbbbcccc
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc
	10.0.0.0/16	pcx-bbbbcccc

Options B and D are incorrect since these would be incomplete peering configurations

For more information on VPC peering configuration, please refer to the below URL

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

Ask our Experts

QUESTION 37 CORRECT

Your team has just configured a VPC which will be set up with EC2 Instances. The Instances will be part of a custom domain. You need to ensure that the custom domain is accessible only from the instances within the VPC not from the public internet. How would you achieve this?

- A. Mention the custom domain name when creating the VPC
- B. Mention the custom domain in the DNS Resolution section
- C. Setup a private hosted zone in Route 53 ✔
- D. Setup a public hosted zone in Route 53

Explanation :

Answer – C
The AWS Documentation mentions the following
A *private hosted zone* is a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs that you create with the Amazon VPC service.
Options A and B are incorrect since these settings are not available
Option D is incorrect since you need to setup a private hosted zone
For more information on private hosted zones, please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html)

Ask our Experts

QUESTION 38 CORRECT

Your team currently has a set of EC2 Instances defined in a VPC. They have been created in a private subnet. The Instances now need to download updates from the Internet. You have to ensure that no connections can be initiated from the Internet to the Instances. Also you need to ensure least amount of bandwidth restrictions for the download of the updates. Which of the following is required to be setup?

- A. An Internet gateway attached to the VPC
- B. A NAT Instance setup in the private subnet
- C. A NAT Instance setup in the public subnet
- D. A NAT Gateway setup in the public subnet ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances
Option A is incorrect since here connections can also be established from the Internet.
Options B and C are incorrect since the NAT gateway should be used instead of the NAT instance to ensure there are no bandwidth restrictions
For more information on the NAT gateway, please refer to the below URL

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

Ask our Experts

QUESTION 39 INCORRECT

Your company has a set of EC2 Instances that are defined in a VPC. These are sitting in a public subnet. The IT security team has detected malicious traffic coming from a set of IP addresses. Which of the following can be used to ensure that traffic is blocked from the incoming IP addresses?

- A. Block the incoming traffic using the Security Groups for the EC2 Instances ✖
- B. Block the outgoing traffic using the Security Groups for the EC2 Instances
- C. Block the incoming traffic using the NACL's for the subnets ✔
- D. Block the outgoing traffic using the NACL's for the subnets

Explanation :

Answer – C
The AWS Documentation mentions the following
A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC
Options A and B are incorrect since here you need to use Security Groups to block traffic
Option D is incorrect since you need to primarily block the incoming traffic
For more information on NACL's, please refer to the below URL

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

Ask our Experts

QUESTION 40 CORRECT

Your company has setup a set of EC2 Instances in a VPC. The IT security department needs to view the IP address of the incoming traffic for conducting security-based analysis. Which of the following can be used to assist in this requirement?

- A. Use CloudTrail logs
- B. Use AWS Trusted Advisor
- C. Use AWS Inspector
- D. Use AWS VPC Flow Logs ✔

Explanation :

Answer – D
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.
Flow logs can help you with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance, which in turn helps you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.
Option A is incorrect since this is used for API logging
Option B is incorrect since this service can be used to give recommendations but not block IP Traffic
Option C is incorrect since this can be used to detect vulnerabilities in Instances
For more information on VPC Flow Logs, please refer to the below URL

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

Ask our Experts

QUESTION 41 INCORRECT

Your company needs to connect their on-premise network to their AWS VPC's. You are in charge of setting up the AWS VPN connection to setup this hybrid architecture. Which of the following are part of the implementation steps to have this in place? Choose 3 answers from the options given below.

- A. Ensure that a customer gateway is in place. ✔

- [x] **B.** Attach an Internet gateway to the VPC ✖
- [x] **C.** Attach a virtual private gateway to the VPC ✔
- [x] **D.** Create the VPN connection ✔

Explanation :

Answer – A, C and D
The AWS Documentation mentions the steps involved

Setting Up an AWS VPN Connection

Use the following procedures to manually set up the VPN connection. Alternatively, you can let the VPC creation wizard take care of many of these steps for you. For more information about using the VPC creation wizard to set up the virtual private gateway, see Scenario 3: VPC with Public and Private Subnets and AWS Managed VPN Access or Scenario 4: VPC with a Private Subnet Only and AWS Managed VPN Access.

To set up a VPN connection, you need to complete the following steps:

- Step 1: Create a Customer Gateway
- Step 2: Create a Virtual Private Gateway
- Step 3: Enable Route Propagation in Your Route Table
- Step 4: Update Your Security Group
- Step 5: Create a VPN Connection and Configure the Customer Gateway

Option B is incorrect since you need to attach the virtual private gateway and not the Internet gateway

For more information on setting up VPN connections, please refer to the below URL

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

Ask our Experts

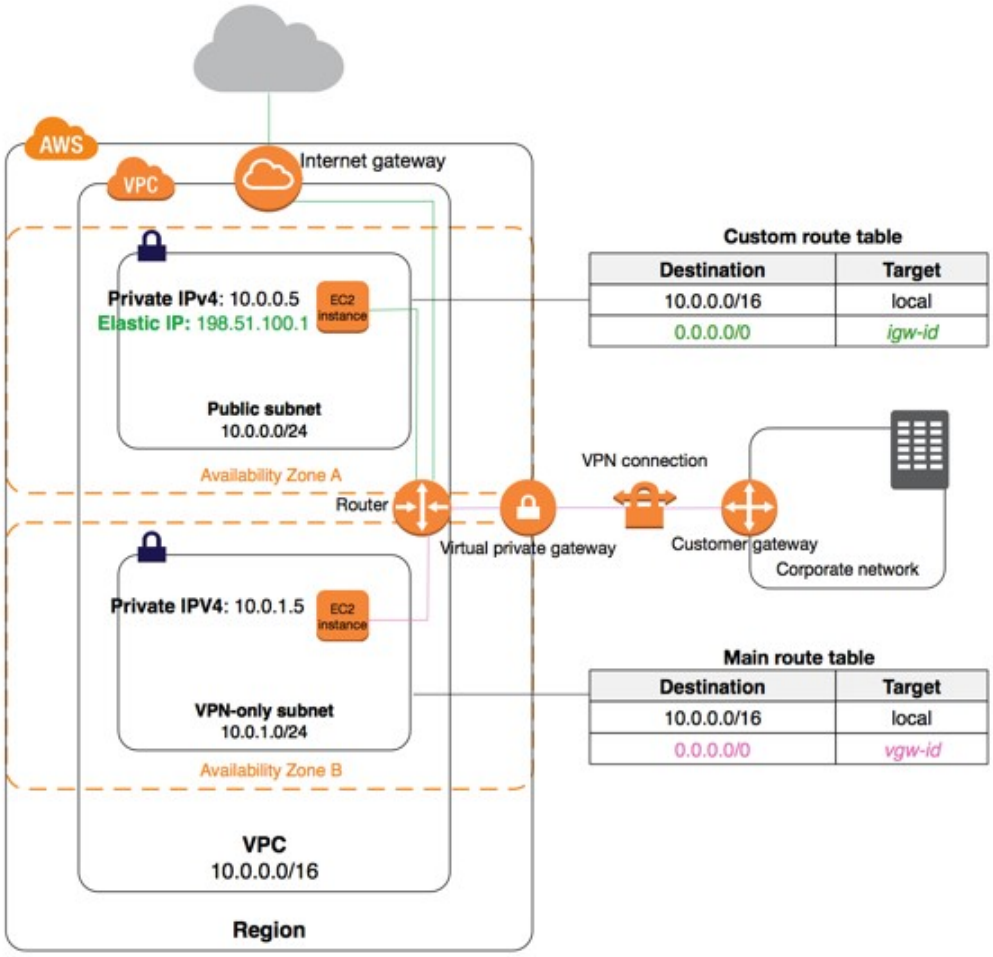
QUESTION 42 CORRECT

You've setup a VPC with a CIDR block of 10.0.0.0/16. You've setup a Public and private subnet with CIDR blocks of 10.0.1.0/24 and 10.0.2.0/24 respectively. You attached an Internet gateway to the VPC. Which of the following changes have to be made to the custom route table for the public subnet to allow for internet connectivity?

- **A.** Add a Route entry of Destination of 10.0.0.0/16 and the Target as the Internet gateway
- **B.** Add a Route entry of Destination of 10.0.1.0/16 and the Target as the Internet gateway
- **C.** Add a Route entry of Destination of 10.0.2.0/16 and the Target as the Internet gateway
- **D.** Add a Route entry of Destination of 0.0.0.0/0 and the Target as the Internet gateway ✔

Explanation :

Answer – D
The AWS Documentation mentions what should be the entry in the route table for the Internet gateway which should have the destination of 0.0.0.0/0



All other options are invalid since the right one is provided in the AWS Documentation.

For more information on VPC Route tables, please refer to the below URL

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

Ask our Experts

QUESTION 43 CORRECT

You're the System administrator for a company that has just started using AWS. You are in the process of creating several IAM users which will be used for privileged access. Which of the following should be done to ensure that the right security measures are being taken up when providing access? Choose 2 answers from the options given below

- [ ] **A.** Provide the root access keys to the Privileged users so that they can carry out their admin related activities
- [x] **B.** Enable MFA for the Privileged users ✔
- [x] **C.** Rotate the credentials regularly for the Privileged users ✔
- [ ] **D.** Grant permissions to the users on an individual basis

Explanation :

Answer – B and C
The AWS Documentation gives the list below of IAM best practises

IAM Best Practices

To help secure your AWS resources, follow these recommendations for the AWS Identity and Access Management (IAM) service.

Topics

- Lock Away Your AWS Account Root User Access Keys
- Create Individual IAM Users
- Use Groups to Assign Permissions to IAM Users
- Use AWS Defined Policies to Assign Permissions Whenever Possible
- Grant Least Privilege
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Your Users
- Enable MFA for Privileged Users
- Use Roles for Applications That Run on Amazon EC2 Instances
- Use Roles to Delegate Permissions
- Do Not Share Access Keys
- Rotate Credentials Regularly
- Remove Unnecessary Credentials
- Use Policy Conditions for Extra Security
- Monitor Activity in Your AWS Account
- Video Presentation About IAM Best Practices

Option A is incorrect since root access should not be provided to the users

Option D is incorrect since you should use groups to delegate access
For more information on IAM best practices, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)

Ask our Experts

QUESTION 44 INCORRECT

An application has currently been deployed on AWS. The application sits on a set of EC2 Instances and sits behind an Elastic Load balancer. The IT Security department has requested for a list of client IP addresses that access the Load Balancer. How can you accomplish this? Choose 2 answers from the options given below

- [x] **A.** Enable cloudwatch logs for the individual EC2 Instances ✖
- [x] **B.** Enable access logging for the ELB ✔
- [ ] **C.** Give access to the S3 bucket for accessing the logs ✔
- [ ] **D.** Give access to Cloudwatch logs for accessing the logs

Explanation :

Answer – B and C
The AWS Documentation mentions the following
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.
Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.
Option A is incorrect since you need to enable access at the ELB
Option D is incorrect since the logs are stored in S3
For more information on ELB Access logging, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html)

Ask our Experts

QUESTION 45 CORRECT

An admin has created an IAM policy with the below policy document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::demobucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": ["arn:aws:s3:::demobucket/*"]
    }
  ]
}
```

Which of the following permissions does the policy grant? Choose 2 answers from the options given below

- [x] **A.** Add an object to the demobucket ✔
- [ ] **B.** Add an object to any bucket
- [x] **C.** Read an object from the demobucket ✔

☐ **D.** Delete any object from the demobucket

Explanation :

Answer – A and C
This example is given in the AWS Documentation

Amazon S3: Allows Read and Write Access to a Specific S3 Bucket

This example shows how you might create a policy that allows `Read` and `Write` access to a specific S3 bucket. This policy provides the permissions necessary to complete this action using the AWS API or AWS CLI only. To use this policy, replace the red text in the example policy with your own information.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["s3:ListBucket"],
         "Resource": ["arn:aws:s3:::<BUCKET-NAME>"]
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": ["arn:aws:s3:::<BUCKET-NAME>/*"]
      }
   ]
}
```

Options B and D are invalid since the policy is only applicable to the demobucket and only gives the read and write permission
For more information on examples on access policies, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_examples.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_examples.html)

Ask our Experts

QUESTION 46 CORRECT

An application team has developed an application that will interact with a DynamoDB table. This application is going to be hosted on an EC2 Instance. As the administrator, you need to ensure that the right implementation steps are carried out when ensuring the application can access the DynamoDB table. Which of the following is the right step to be followed?

- **A.** Create an IAM user, generate the access keys and embed them in the EC2 Instance
- **B.** Create an IAM group, generate the access keys and embed them in the EC2 Instance
- **C.** Create an IAM Role with the necessary permissions and attach it to the EC2 Instance ✔
- **D.** Create a script with the access keys which will be loaded when the EC2 Instance is launched.

Explanation :

Answer – C
This is given in the AWS Documentation

IAM Roles for Amazon EC2

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 behalf, 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. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows:

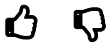
1. Create an IAM role.
2. Define which accounts or AWS services can assume the role.
3. Define which API actions and resources the application can use after assuming the role.
4. Specify the role when you launch your instance, or attach the role to a running or stopped instance.
5. Have the application retrieve a set of temporary credentials and use them.

All other options are invalid since the right security measures to use is Access Keys

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

Ask our Experts



QUESTION 47 CORRECT

Your company is setting up a web site that will be hosted in S3. This is a static web site. They want to ensure that users across the world get a seamless user experience when accessing the web site. As the AWS administrator which of the following would you create to ensure this requirement is fulfilled?

- A. Create a Cloud front distribution and place the S3 bucket as the source ✔
- B. Enable cross region replication for the web site in the S3 bucket
- C. Use ElastiCache to cache the Reponses
- D. Place an Elastic Load balancer in front of the static web site

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon CloudFront is a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to your viewers with low latency and high transfer speeds. CloudFront is integrated with AWS – including physical locations that are directly connected to the AWS global infrastructure, as well as software that works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code close to your viewers.
Option B is incorrect since this is an efficient manner if the objects needs to be accessed from around the world
Option C is incorrect this is not the right option. The objects need to be delivered via CDN
Option D is incorrect since this will not help reduce the latency of access to objects from various locations
For more information on AWS Cloudfront, please refer to the below URL

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

Ask our Experts

QUESTION 48 UNATTEMPTED

Your company has a set of S3 buckets which are used to store office documents. The IT Security department has now mandated that all objects be encrypted at rest. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below.

- A. Use AWS server-side encryption for the S3 bucket with AWS Managed Keys ✔

- [ ] **B.** Use AWS server-side encryption for the S3 bucket with AWS KMS Keys ✔
- [ ] **C.** Enable SSL while accessing objects in the bucket
- [ ] **D.** Use Server-side certificates to encrypt the objects at rest.

Explanation :

Answer – A and B
The different options for server-side encryption are given below

Protecting Data Using Server-Side Encryption

Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a presigned URL, that URL works the same way for both encrypted and unencrypted objects.

Note

You can't apply different types of server-side encryption to the same object simultaneously.

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

- **Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)** - Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. For more information, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).
- **Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)** - Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3. SSE-KMS also provides you with an audit trail of when your key was used and by whom. Additionally, you have the option to create and manage encryption keys yourself, or use a default key that is unique to you, the service you're using, and the region you're working in. For more information, see Protecting Data Using Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).
- **Use Server-Side Encryption with Customer-Provided Keys (SSE-C)** - You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects. For more information, see Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).

Option C is invalid since this is for encryption of objects in transit

Option D is invalid since this is not a valid option in S3 for encryption of objects
For more information on AWS server-side encryption, please refer to the below URL

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

Ask our Experts

QUESTION 49 INCORRECT

Your company currently uses resources in AWS. They now have a need for a data store which can be used to store historical data. There would be inhouse built Business Intelligence solutions which would need to query this data. Which of the following would you use for this purpose?

- A. AWS DynamoDB
- B. AWS Redshift ✔
- C. AWS EBS ✖
- D. AWS EMR

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon Redshift is a fully managed, 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. This enables you to use your data to acquire new insights for your business and customers.
The first step to create a data warehouse is to launch a set of nodes, called an Amazon Redshift cluster. After you provision your cluster, you can upload your data set and then perform data analysis queries. Regardless of the size of the data set, Amazon Redshift offers fast query performance using the same SQL-based tools and business intelligence applications that you use today.
Option A is invalid since this is a NoSQL database solution
Option C is invalid since this is storage for EC2 Instances
Option D is invalid since this is an Elastic Map Reduce solution
For more information on AWS Redshift, please refer to the below URL

- https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html (https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html)

Ask our Experts

QUESTION 50 INCORRECT

Your company currently has a reporting application that access an instance of AWS RDS MySQL. The database performance is becoming a bottleneck because of the high number of read operations on the database. Which of the following would you consider implementing to resolve this issue?

- A. Use Read Replica's ✔
- B. Use Global tables ✖
- C. Use Multi-AZ
- D. Use Automated Backups

Explanation :

Answer – A
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. Read replicas can also be promoted when needed to become standalone DB instances
Option B is incorrect since this is an option for DynamoDB
Option C is incorrect since this is an option for High availability of the RDS solution
Option D is incorrect since this is used for recovery of databases
For more information on AWS Read Replica's, please refer to the below URL

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

Ask our Experts

QUESTION 51 CORRECT

Your team currently has an AWS RDS MySQL database in place. The team is facing issues in terms of the performance for the underlying database. As the system admin you need to see if there are any ways you can improve on the performance of the database. Which of the following can be used for this purpose?

- A. AWS Trusted Advisor
- B. AWS Inspector
- C. AWS Performance Insights ✔
- D. AWS Config

Explanation :

Answer – C
The AWS Documentation mentions the following
Performance Insights expands on existing Amazon RDS monitoring features to illustrate your database's performance and help you analyze any issues that affect it. With the Performance Insights dashboard, you can visualize the database load and filter the load by waits, SQL statements, hosts, or users. Performance Insights is on by default in the console create wizard for the Amazon Aurora MySQL, Amazon Aurora PostgreSQL, and Amazon RDS PostgreSQL DB engines. If you have more than one database on the DB instance, performance data for all of the databases is aggregated for the DB instance.
Option A is incorrect since this cannot give you a deep dive analysis on the database issues
Option B is incorrect since this is used for vulnerability analysis on EC2 Instances
Option D is incorrect since this is a configuration management utility
For more information on AWS performance insights, please refer to the below URL

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

Ask our Experts

QUESTION 52 INCORRECT

Your team is developing an application that will be hosted on AWS. The application needs to send messages across components of the applications. The order of the messages needs to be preserved. Which of the following would you provision for this requirement?

- A. A Standard SQS queue
- B. A FIFO queue ✔
- C. A SNS topic ✖
- D. A Kinesis stream

Explanation :

Answer – B
The AWS Documentation mentions the following
FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated, for example:

- Ensure that user-entered commands are executed in the right order.
- Display the correct product price by sending price modifications in the right order.
- Prevent a student from enrolling in a course before registering for an account.

Option A is incorrect since this does not preserve the order of messages
Option C is incorrect since this is a notification service
Option D is incorrect since this is used for data analytics
For more information on AWS FIFO queues, please refer to the below URL

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

Ask our Experts

QUESTION 53 INCORRECT

Your company has a set of EC2 Instances. The monitoring department needs to get dashboard metrics for the CPU utilization of the Instances at one-minute intervals. You need to comply with this requirement in the easiest and cost-efficient way possible. Which of the following steps would you implement? Choose 2 answers from the options given below.

- [x] **A.** Enable basic monitoring for the EC2 Instances so that costs are kept in check ✖
- [x] **B.** Enable detailed monitoring for the EC2 Instances ✔
- [ ] **C.** Create a dashboard in Cloudwatch ✔
- [ ] **D.** Create a dashboard in Cloudtrail

Explanation :

Answer – B and C
The AWS Documentation mentions the following
Amazon EC2 sends metrics to Amazon CloudWatch. You can use the AWS Management Console, the AWS CLI, or an API to list the metrics that Amazon EC2 sends to CloudWatch. By default, each data point covers the previous 5 minutes of activity for the instance. If you've enabled detailed monitoring, each data point covers the previous 1 minute of activity.
Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, even those resources that are spread across different Regions. You can use CloudWatch dashboards to create customized views of the metrics and alarms for your AWS resources.
Option A is incorrect since this will not meet the requirement of 1-minute interval logging of metrics
Option D is incorrect since this is only used for API based logging
For more information on Cloudwatch metrics, please refer to the below URL

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

For more information on Cloudwatch dashboards, please refer to the below URL

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

Ask our Experts

QUESTION 54 CORRECT

Your company has a set of EC2 Instances defined in AWS. These resources belong to different departments. The company wants to get a monthly costing report for the EC2 Instances department wise. Which of the following is the best way to achieve this requirement?

- A. Create different VPC's for the EC2 Instances based on the departments
- B. Create different subnets for the EC2 Instances based on the departments
- C. Assign tags to the EC2 Instances and generate reports based on the tags ✔
- D. Use different AMI types for the underlying EC2 Instances

Explanation :

Answer – C
The AWS Documentation mentions the following
You can use tags to organize your AWS bill to reflect your own cost structure. To do this, sign up to get your AWS account bill with tag key values included. To see the cost of your combined resources, you can organize your billing information based on resources that have the same tag key values. For example, you can tag several resources with a specific application name, and then organize your billing information to see the total cost of that application across several services
Options A ,B and D are incorrect since these are not the ideal steps to follow for billing segregation of resources.
For more information on using resource tags, please refer to the below URL

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

Ask our Experts

QUESTION 55 INCORRECT

Your company is planning on setting up a database on an EC2 Instance. It is important for the database to be fault tolerant since it is hosting critical data. You are planning on implementing a RAID configuration. Which of the following would you implement for this requirement?

- A. RAID 0 ✖
- B. RAID 1 ✔
- C. RAID 5
- D. RAID 6

Explanation :

Answer - B
The way to implement this is clearly given in the AWS Documentation

RAID Configuration Options

The following table compares the common RAID 0 and RAID 1 options.

Configuration	Use	Advantages	Disadvantages
RAID 0	When I/O performance is more important than fault tolerance; for example, as in a heavily used database (where data replication is already set up separately).	I/O is distributed across the volumes in a stripe. If you add a volume, you get the straight addition of throughput.	Performance of the stripe is limited to the worst performing volume in the set. Loss of a single volume results in a complete data loss for the array.
RAID 1	When fault tolerance is more important than I/O performance; for example, as in a critical application.	Safer from the standpoint of data durability.	Does not provide a write performance improvement; requires more Amazon EC2 to Amazon EBS bandwidth than non-RAID configurations because the data is written to multiple volumes simultaneously.

Also, they have clearly mentioned on why you should not implement RAID 5 and RAID 6

RAID 5 and RAID 6 are not recommended for Amazon EBS because the parity write operations of these RAID modes consume some of the IOPS available to your volumes. Depending on the configuration of your RAID array, these RAID modes provide 20-30% fewer usable IOPS than a RAID

0 configuration. Increased cost is a factor with these RAID modes as well; when using identical volume sizes and speeds, a 2-volume RAID 0 array can outperform a 4-volume RAID 6 array that costs twice as much.
For more information on RAID configuration, please refer to the below URL

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

Ask our Experts

QUESTION 56 CORRECT

Your team is planning on hosting an application on an EC2 Instance. Based on the requirement, the application would need around 15000 – 20000 IOPS per volume. Which of the following volume type would you create for the EC2 Instance?

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

Explanation :

Answer - B
If you look at the AWS documentation, you can see that only the Provisioned IOPS volume can meet this demand.

	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: o MongoDB o Cassandra o Microsoft SQL Server o MySQL o PostgreSQL o 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
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	10,000	32,000***	500	250

Because of what the documentation mentions , all other options are invalid

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

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

Ask our Experts

QUESTION 57 **INCORRECT**

Your company has a set of EC2 Instances. The IT Security department has mandated that all EC2 Instances are patched with the latest security patches. Which of the following can be used for ensuring this requirement is fulfilled?

- A. AWS System Manager ✔
- B. AWS Config
- C. AWS Inspector
- D. AWS Trusted Advisor ✖

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Amazon Linux, and Amazon Linux 2. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option B is incorrect since this is a configuration service
Option C is incorrect since this is used for checking system vulnerabilities
Option D is incorrect since this can only give recommendations
For more information on AWS Systems Manager for patching, please refer to the below URL

- https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html)

Ask our Experts

QUESTION 58 INCORRECT

You are a systems admin for a company. There is a requirement to host a batch processing application. This batch processing application can be interrupted at any point in time and then resumed. You have been told to provision the underlying EC2 Instances ensuring that cost is kept at a minimum. Which of the following would you consider?

- **A.** Spot Instances ✔
- **B.** On-Demand Instances ✖
- **C.** Dedicated Hosts
- **D.** Reserved Instances

Explanation :

Answer - A
The AWS Documentation mentions the following
Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. For example, Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks
Because of what the documentation mentions, all other options are invalid when it comes to a cost-effective option
For more information on Spot Instances, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html)

Ask our Experts

QUESTION 59 CORRECT

You have been assigned the task of creating Cloudformation templates for your company. You have to ensure that the values can be passed to the template at runtime to make the template creation more dynamic in nature. Which part of the template would you use for this purpose?

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

Explanation :

Answer – D
The AWS Documentation mentions the following
Values to pass to your template at runtime (when you create or update a stack). You can refer to parameters from the Resources and Outputs sections of the template.
Option A is incorrect since this is used to describe the values that are returned whenever you view your stack's properties.
Option B is incorrect since this is used to define a mapping of keys and associated values that you can use to specify conditional parameter values, similar to a lookup table
Option C is incorrect since this is used to control whether certain resources are created or whether certain resource properties are assigned a value during stack creation or update
For more information on the structure of a template, please refer to the below URL

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

Ask our Experts

QUESTION 60 CORRECT

You have been tasked with hosting an application on an EC2 Instance. The IP of this Instance will be mapped to a custom domain in Route 53. Which of the following is a key implementation step that should ideally be carried out for the Instance?

- A. Ensure that the Instance is created with an Instance store AMI
- B. Ensure that the Instance is created with a public IP

- C. Ensure that the Instance is created with an Elastic IP ✔
- D. Ensure the Instance is launched with Enhanced Networking

Explanation :

Answer – C
To ensure that the IP address for the Instance does not change in case if the Instance is stopped and started, ensure that the Instance is launched with an Elastic IP
The AWS Documentation mentions the following
An *Elastic IP address* is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
Options A and D are incorrect since there is no mention in the question as to why these options should be used
Option B is incorrect since if the Instance is stopped and started for any reason , the public IP address would change and the domain name mapping in Route 53 would then become invalid
For more information on the Elastic IP address, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html)

Ask our Experts

QUESTION 61 INCORRECT

You've setup a custom VPC with Subnets. You've launched an EC2 Instance in the subnet. After the Instance is launched, you notice that the Instance has not received a public DNS Name. Which of the following should you check to ensure that the EC2 Instance receives a public DNS name? Choose 2 answers from the options given below

- [x] A. Check the enableDnsHostnames setting ✔
- [x] B. Ensure the Instance is launched with the right AMI ✖
- [ ] C. Ensure the Instance is launched with the right EBS volume type

☐ **D.** Check the enableDnsSupport setting ✔

Explanation :

Answer – A and D
This is given in the AWS Documentation

DNS Support in Your VPC

Your VPC has attributes that determine whether your instance receives public DNS hostnames, and whether DNS resolution through the Amazon DNS server is supported.

Attribute	Description
enableDnsHostnames	Indicates whether the instances launched in the VPC get public DNS hostnames. If this attribute is true, instances in the VPC get public DNS hostnames, but only if the enableDnsSupport attribute is also set to true.
enableDnsSupport	Indicates whether the DNS resolution is supported for the VPC. If this attribute is false, the Amazon-provided DNS server in the VPC that resolves public DNS hostnames to IP addresses is not enabled. If this attribute is true, queries to the Amazon provided DNS server at the 169.254.169.253 IP address, or the reserved IP address at the base of the VPC IPv4 network range plus two will succeed. For more information, see Amazon DNS Server.

If both attributes are set to true, the following occurs:

- Your instance receives a public DNS hostname.
- The Amazon-provided DNS server can resolve Amazon-provided private DNS hostnames.

If either or both of the attributes is set to false, the following occurs:

- Your instance does not receive a public DNS hostname that can be viewed in the Amazon EC2 console or described by a command line tool or AWS SDK.
- The Amazon-provided DNS server cannot resolve Amazon-provided private DNS hostnames.
- Your instance receives a custom private DNS hostname if you've specified a custom domain name in your DHCP options set. If you are not using the Amazon-provided DNS server, your custom domain name servers must resolve the hostname as appropriate.

Options B and C are invalid since these do not have an effect on the allocation of a public DNS name for the Instance
For more information on VPC DNS, please refer to the below URL

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

Ask our Experts

QUESTION 62 INCORRECT

You're the systems administrator a company. They are planning on setting up an AWS Direct Connect connection between an AWS VPC and their on-premise data centre. As the Administrator, which of the following pre-requisites that you must have in place? Choose 2 answers from the options given below.

- [ ] **A.** The network must use a single mode fiber with a 1000BASE-LX ✔
- [x] **B.** The network must use a dual mode fiber with a 1000BASE-LX ✖
- [ ] **C.** The network device on your side must support BGP ✔
- [x] **D.** The network device on your side must support static routing ✖

Explanation :

Answer – A and C
This is given in the AWS Documentation

Network Requirements

To use AWS Direct Connect in an AWS Direct Connect location, your network must meet one of the following conditions:

- Your network is colocated with an existing AWS Direct Connect location. For more information about available AWS Direct Connect locations, see AWS Direct Connect Product Details.
- You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN). For information, see APN Partners Supporting AWS Direct Connect.
- You are working with an independent service provider to connect to AWS Direct Connect.

In addition, your network must meet the following conditions:

- Your network must use single mode fiber with a 1000BASE-LX (1310nm) transceiver for 1 gigabit Ethernet, or a 10GBASE-LR (1310nm) transceiver for 10 gigabit Ethernet.
- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually.
- 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on your network. Asynchronous BFD is automatically enabled for AWS Direct Connect virtual interfaces, but will not take effect until you configure it on your router.

Options B and D are incorrect because the requirements are clearly given in the documentation.

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

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

Ask our Experts

QUESTION 63 CORRECT

Your company is planning on hosting an application on a set of EC2 Instances. These Instances need to be scaled on demand. Which of the following configuration would you put in place for this requirement?

- A. Ensure that the Instances are placed behind a CDN
- B. Ensure that the Instances are launch as part of an Autoscaling Group ✔

C. Ensure that the Instances are placed behind a Classic Load Balancer

D. Ensure that the Instances are placed behind an Application Load Balancer

Explanation :

Answer – B
This is given in the AWS Documentation
AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes.
Option A is incorrect since this should be used for Content Distribution
Options C and D are incorrect since this should be used for traffic distribution
For more information on AutoScaling, please refer to the below URL

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

Ask our Experts

QUESTION 64 CORRECT

You work as a system administrator for a company. You have just provisioned a fleet of EC2 instances and realized that none of them have a public IP address. What settings would need to be changed for the next fleet of instances to be created with public IP addresses?

A. Modify the auto-assign public IP setting on the subnet. ✔

B. Modify the auto-assign public IP setting on the instance type.

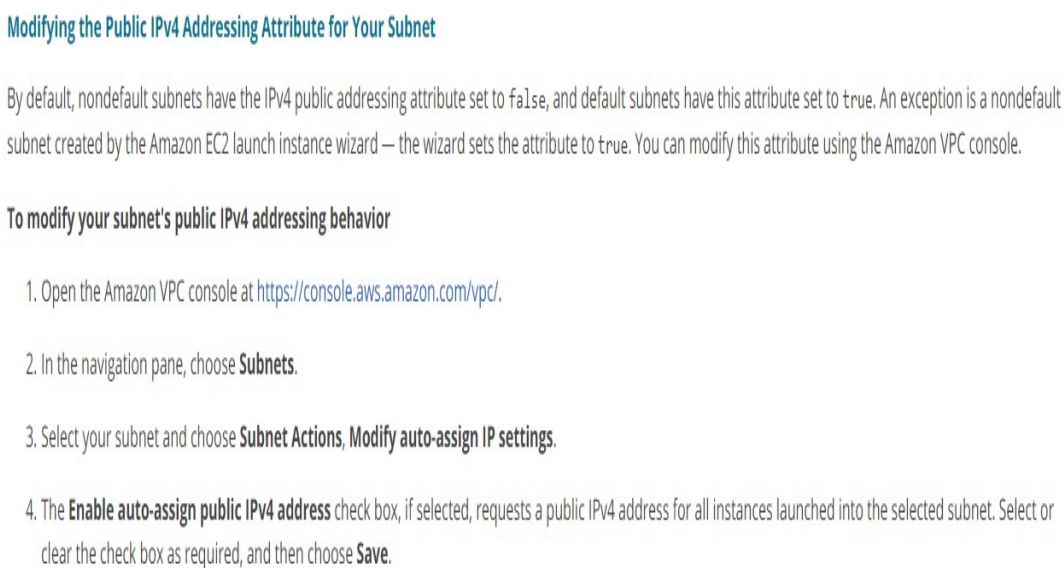
C. Modify the auto-assign public IP setting on the route table.

D. Modify the auto-assign public IP setting on the VPC.

Explanation :

Answer – A

This is given in the AWS Documentation
This setting is done at the subnet level and if marked as true, all instances launched in that subnet will get a public IP address by default.



Modifying the Public IPv4 Addressing Attribute for Your Subnet

By default, nondefault subnets have the IPv4 public addressing attribute set to `false`, and default subnets have this attribute set to `true`. An exception is a nondefault subnet created by the Amazon EC2 launch instance wizard — the wizard sets the attribute to `true`. You can modify this attribute using the Amazon VPC console.

To modify your subnet's public IPv4 addressing behavior

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Subnets**.
3. Select your subnet and choose **Subnet Actions**, **Modify auto-assign IP settings**.
4. The **Enable auto-assign public IPv4 address** check box, if selected, requests a public IPv4 address for all instances launched into the selected subnet. Select or clear the check box as required, and then choose **Save**.

Because of what is mentioned in the AWS Documentation, all other options are incorrect

For more information on IP addressing in a subnet, please refer to the below URL

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

Ask our Experts

QUESTION 65 CORRECT

Your team is currently working on an application that makes use of a DynamoDB table. The application has been promoted to a production region. Now there is a need for users in another region to access the data in the DynamoDB table. Which of the following can be used to ensure that the data can be accessed in the other region with the least latency.

- A. Enable global tables ✔
- B. Enable Read Replica's

- C. Enable Multi-AZ
- D. Enable Autoscaling

Explanation :

Answer – A
This is given in the AWS Documentation
Amazon DynamoDB global tables provide a fully managed solution for deploying a multi-region, multi-master database, without having to build and maintain your own replication solution. When you create a global table, you specify the AWS regions where you want the table to be available. DynamoDB performs all of the necessary tasks to create identical tables in these regions and propagate ongoing data changes to all of them.
Options B and C are incorrect, since these are pertinent to the AWS RDS service
Option D is incorrect since this helps in increasing throughput based on demand.
For more information on DynamoDB global tables, please refer to the below URL

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

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14835)

- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

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

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

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

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