**Questions Dumps- AWS-SA-Prof-Exam-22nd Dec, 2018**

[**https://www.briefmenow.org/amazon/which-of-the-following-are-true-regarding-encrypted-ama/**](https://www.briefmenow.org/amazon/which-of-the-following-are-true-regarding-encrypted-ama/)

1. You need to pass a custom script to new Amazon Linux instances created in your Auto Scaling group. Which feature allows you to accomplish this?
2. **User data**
3. EC2Config service
4. IAM roles
5. AWS Config
6. Which of the following are true regarding encrypted Amazon Elastic Block Store (EBS) volumes? Choose 2 answer
7. **Supported on all Amazon EBS volume types**
8. **Snapshots are automatically encrypted**
9. Available to all instance types
10. Existing volumes can be encrypted
11. shared volumes can be encrypted

Explanation: This feature is supported on all Amazon EBS volume types (General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic). You can access encrypted Amazon EBS volumes the same way you access existing volumes; encryption and decryption are handled transparently and they require no additional action from you, your Amazon EC2 instance, or your application. Snapshots of encrypted Amazon EBS volumes are automatically encrypted, and volumes that are created from encrypted Amazon EBS snapshots are also automatically encrypted.

<http://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

1. A company has configured and peered two VPCs: VPC-1 and VPC-2. VPC-1 contains only private subnets, and VPC-2 contains only public subnets. The company uses a single AWS Direct Connect connection and private virtual interface to connect their on-premises network with VPC-1. Which two methods increases the fault tolerance of the connection to VPC-1? Choose 2 answers
2. Establish a hardware VPN over the internet between VPC-2 and the on-premises network.
3. **Establish a hardware VPN over the internet between VPC-1 and the on-premises network.**
4. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
5. Establish a new AWS Direct Connect connection and private virtual interface in a different AWS region than VPC-1.
6. **Establish a new AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1**
7. A company needs to monitor the read and write IOPs metrics for their AWS MySQL RDS instance and send real-time alerts to their operations team. Which AWS services can accomplish this? Choose 2 answers
8. Amazon Simple Email Service
9. **Amazon CloudWatch**
10. Amazon Simple Queue Service
11. Amazon Route 53
12. **Amazon Simple Notification Service**
13. A customer wants to track access to their Amazon Simple Storage Service (S3) buckets and also use this information for their internal security and access audits. Which of the following will meet the Customer requirement?
14. Enable AWS CloudTrail to audit all Amazon S3 bucket access.
15. **Enable server access logging for all required Amazon S3 buckets.**
16. Enable the Requester Pays option to track access via AWS Billing
17. Enable Amazon S3 event notifications for Put and Post.

Note: Server access logging provides detailed records for the requests that are made to an S3 bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill.

**AWS-SAP (v.1)**

1. How is AWS readily distinguished from other vendors in the traditional IT computing landscape?
2. Experienced. Scalable and elastic. Secure. Cost-effective. Reliable
3. Secure. Flexible. Cost-effective. Scalable and elastic. Global
4. Secure. Flexible. Cost-effective. Scalable and elastic. Experienced
5. Flexible. Cost-effective. Dynamic. Secure. Experienced.
6. The following are AWS Storage services? Choose 2 Answers
7. AWS Relational Database Service (AWS RDS)
8. AWS ElastiCache
9. AWS Glacier
10. AWS Import/Export
11. What does elasticity mean to AWS?
12. The ability to scale computing resources up easily, with minimal friction and down with latency.
13. The ability to scale computing resources up and down easily, with minimal friction.
14. The ability to provision cloud computing resources in expectation of future demand.
15. The ability to recover from business continuity events with minimal friction.
16. Auto Scaling requests are signed with a \_\_\_\_\_\_\_\_\_ signature calculated from the request and the user’s private key.
17. SSL
18. AES-256
19. HMAC-SHA1
20. X.509
21. The AWS IT infrastructure that AWS provides, complies with the following IT security standards, including:
22. SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2 and SOC 3
23. FISMA, DIACAP, and FedRAMP
24. PCI DSS Level 1, ISO 27001, ITAR and FIPS 140-2
25. HIPAA, Cloud Security Alliance (CSA) and Motion Picture Association of America (MPAA)
26. All of the above
27. You control access to S3 buckets and objects with :
28. Identity and Access Management (IAM) Policies.
29. Access Control Lists (ACLs).
30. Bucket Policies.
31. All of the above
32. Your firm has uploaded a large amount of aerial image data to S3 In the past, in your on premises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ – An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which is correct?
33. Use SQS for passing job messages use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
34. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SOS Once data is processed, change the storage class of the S3 objects to Glacier.
35. Change the storage class of the S3 objects to Reduced Redundancy Storage. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier.
36. Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.
37. A company is storing data on Amazon Simple Storage Service (S3). The company’s security policy mandates that data is encrypted at rest. Which of the following methods can achieve this? Choose 3 answers
38. Use Amazon S3 server-side encryption with AWS Key Management Service managed keys.
39. Use Amazon S3 server-side encryption with customer-provided keys.
40. Use Amazon S3 server-side encryption with EC2 key pair.
41. Use Amazon S3 bucket policies to restrict access to the data at rest.
42. Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.
43. Use SSL to encrypt the data while in transit to Amazon S3.
44. A customer is deploying an SSL enabled web application to AWS and would like to implement a separation of roles between the EC2 service administrators that are entitled to login to instances as well as making API calls and the security officers who will maintain and have exclusive access to the application’s X.509 certificate that contains the private key.
45. Upload the certificate on an S3 bucket owned by the security officers and accessible only by EC2 Role of the web servers.
46. Configure the web servers to retrieve the certificate upon boot from an CloudHSM is managed by the security officers.
47. Configure system permissions on the web servers to restrict access to the certificate only to the authority security officers
48. Configure IAM policies authorizing access to the certificate store only to the security officers and terminate SSL on an ELB.
49. When you put objects in Amazon S3, what is the indication that an object was successfully stored?
50. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
51. Amazon S3 is engineered for 99.999999999% durability. Therefore, there is no need to confirm that data was inserted.
52. A success code is inserted into the S3 object metadata.
53. Each S3 account has a special bucket named \_s3\_logs. Success codes are written to this bucket with a timestamp and checksum.
54. In AWS, which security aspects are the customer’s responsibility? Choose 4 answers
55. Security Group and ACL (Access Control List) settings
56. Decommissioning storage devices
57. Patch management on the EC2 instance’s operating system
58. Life-cycle management of IAM credentials
59. Controlling physical access to compute resources
60. Encryption of EBS (Elastic Block Storage) volumes
61. Which of the following are characteristics of Amazon VPC subnets? Choose 2 answers
62. Each subnet spans at least two Availability Zones to provide a high-availability environment.
63. Each subnet maps to a single Availability Zone.
64. CIDR block mask of /25 is the smallest range supported.
65. By default, all subnets can route between each other, whether they are private or public.
66. Instances in a private subnet can communicate with the Internet only if they have an Elastic IP.
67. After launching an instance that you intend to serve as a NAT (Network Address Translation) device in a public subnet you modify your route tables to have the NAT device be the target of internet bound traffic of your private subnet. When you try and make an outbound connection to the internet from an instance in the private subnet, you are not successful. Which of the following steps could resolve the issue?
68. Disabling the Source/ Destination Check attribute on the NAT instance
69. Attaching an Elastic IP address to the instance in the private subnet
70. Attaching a second Elastic Network Interface (ENI) to the NAT instance, and placing it in the

private subnet

1. Attaching a second Elastic Network Interface (ENI) to the instance in the private subnet, and placing it in the public subnet
2. How can an EBS volume that is currently attached to an EC2 instance be migrated from one

Availability Zone to another?

1. Detach the volume and attach it to another EC2 instance in the other AZ.
2. Simply create a new volume in the other AZ and specify the original volume as the source.
3. Create a snapshot of the volume, and create a new volume from the snapshot in the other AZ.
4. Detach the volume, then use the ec2-migrate-voiume command to move it to another AZ.
5. Which is a valid Amazon Resource name (ARN) for IAM?
6. aws:iam::123456789012:instance-profile/Webserver
7. arn:aws:iam::123456789012:instance-profile/Webserver
8. 123456789012:aws:iam::instance-profile/Webserver
9. arn:aws:iam::123456789012::instance-profile/Webserver
10. You are responsible for a web application that consists of an Elastic Load Balancing (ELB) load balancer in front of an Auto Scaling group of Amazon Elastic Compute Cloud (EC2) instances. For a recent deployment of a new version of the application, a new Amazon Machine Image (AMI) was created, and the Auto Scaling group was updated with a new launch configuration that refers to this new AMI. During the deployment, you received complaints from users that the website was responding with errors. All instances passed the ELB health checks. What should you do in order to avoid errors for future deployments? (Choose 2 answer)
11. Add an Elastic Load Balancing health check to the Auto Scaling group. Set a short period for the

health checks to operate as soon as possible in order to prevent premature registration of the

instance to the load balancer.

1. Enable EC2 instance CloudWatch alerts to change the launch configuration’s AMI to the previous one. Gradually terminate instances that are using the new AMI.
2. Set the Elastic Load Balancing health check configuration to target a part of the application that fully tests application health and returns an error if the tests fail.
3. Create a new launch configuration that refers to the new AMI, and associate it with the group. Double the size of the group, wait for the new instances to become healthy, and reduce back to the original size. If new instances do not become healthy, associate the previous launch configuration.
4. Increase the Elastic Load Balancing Unhealthy Threshold to a higher value to prevent an unhealthy instance from going into service behind the load balancer.
5. You are designing a personal document-archiving solution for your global enterprise with thousands of employee. Each employee has potentially gigabytes of data to be backed up in this archiving solution. The solution will be exposed to the employees as an application, where they can just drag and drop their files to the archiving system. Employees can retrieve their archives through a web interface. The corporate network has high bandwidth AWS Direct Connect connectivity to AWS. You have a regulatory requirement that all data needs to be encrypted before being uploaded to the cloud. How do you implement this in a highly available and cost-efficient way?
6. Manage encryption keys on-premises in an encrypted relational database. Set up an on-premises server with sufficient storage to temporarily store files, and then upload them to Amazon S3, providing a client-side master key.

B. Mange encryption keys in a Hardware Security Module (HSM) appliance on-premises server with sufficient storage to temporarily store, encrypt, and upload files directly into Amazon Glacier.

C. Manage encryption keys in Amazon Key Management Service (KMS), upload to Amazon Simple Storage Service (S3) with client-side encryption using a KMS customer master key ID, and configure Amazon S3 lifecycle policies to store each object using the Amazon Glacier storage tier.

D. Manage encryption keys in an AWS CloudHSM appliance. Encrypt files prior to uploading on the employee desktop, and then upload directly into Amazon Glacier.

1. Your company hosts a social media website for storing and sharing documents. The web application allows user to upload large files while resuming and pausing the upload as needed. Currently, files are uploaded to your PHP front end backed by Elastic load Balancing and an autoscaling fleet of Amazon Elastic Compute Cloud (EC2) instances that scale upon average of bytes received (NetworkIng). After a file has been uploaded, it is copied to Amazon Simple Storage Service (S3). Amazon EC2 instances use an AWS Identity and Access Management (IAM) role that allows Amazon S3 uploads. Over the last six months, your user base and scale have increased significantly, forcing you to increase the Auto Scaling group’s Max parameter a few times. Your CFO is concerned about rising costs and has asked you to adjust the architecture where needed to better optimize costs. Which architecture change could you introduce to reduce costs and still keep your web application secure and scalable?
2. Replace the Auto Scaling launch configuration to include c3.8xlarge instances; those instances can potentially yield a network throuthput of 10gbps.
3. Re-architect your ingest pattern, have the app authenticate against your identity provider, and use your identity provider as a broker fetching temporary AWS credentials from AWS Secure Token Service (GetFederationToken). Securely pass the credentials and S3 endpoint/prefix to your app. Implement client-side logic to directly upload the file to Amazon S3 using the given credentials and S3 prefix.
4. Re-architect your ingest pattern, and move your web application instances into a VPC public subnet. Attach a public IP address for each EC2 instance (using the Auto Scaling launch configuration settings). Use mazon Route 53 Round Robin records set and HTTP health check to DNS load balance the app requests; this approach will significantly reduce the cost by bypassing Elastic Load Balancing.
5. Re-architect your ingest pattern, have the app authenticate against your identity provider, and use your identity provider as a broker fetching temporary AWS credentials from AWS Secure Token Service (GetFederationToken). Securely pass the credentials and S3 endpoint/prefix to your app. Implement client-side logic that used the S3 multipart upload API to directly upload the file to Amazon S3 using the given credentials and S3 prefix.
6. You are looking to migrate your Development (Dev) and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each accounts bill to a Master AWS account using Consolidated Billing. To make sure you Keep within budget you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which option will allow you to achieve this goal.
7. Create IAM users in the Master account with full Admin permissions. Create cross-account roles

in the Dev and Test accounts that grant the Master account access to the resources in the

account by inheriting permissions from the Master account.

1. Create IAM users and a cross-account role in the Master account that grants full Admin

permissions to the Dev and Test accounts.

1. Create IAM users in the Master account Create cross-account roles in the Dev and Test accounts

that have full Admin permissions and grant the Master account access.

1. Link the accounts using Consolidated Billing. This will give IAM users in the Master account access to resources in the Dev and Test accounts
2. Your company has recently extended its datacenter into a VPC on AVVS to add burst computing capacity as needed Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary You don’t want to create new IAM users for each NOC member and make those users sign in again to the AWS Management Console Which option below will meet the needs for your NOC members?
3. Use OAuth 2 0 to retrieve temporary AWS security credentials to enable your NOC members to

sign in to the AWS Management Console.

1. Use web Identity Federation to retrieve AWS temporary security credentials to enable your NOC

members to sign in to the AWS Management Console.

1. Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the NOC members

federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.

1. Use your on-premises SAML 2.0-compliam identity provider (IDP) to retrieve temporary security

credentials to enable NOC members to sign in to the AWS Management Console.

1. An organization, which has the AWS account ID as 999988887777, has created 50 IAM users. All the users are added to the same group examkiller. If the organization has enabled that each IAM user can login with the AWS console, which AWS login URL will the IAM users use??
2. <https://999988887777.aws.amazon.com/examkiller/>
3. <https://signin.aws.amazon.com/examkiller/>
4. <https://examkiller.signin.aws.amazon.com/999988887777/console/>
5. <https://999988887777.signin.aws.amazon.com/console/>
6. An organization has setup RDS with VPC. The organization wants RDS to be accessible from the

internet. Which of the below mentioned configurations is not required in this scenario?

1. The organization must enable the parameter in the console which makes the RDS instance publicly accessible.
2. The organization must allow access from the internet in the RDS VPC security group,
3. The organization must setup RDS with the subnet group which has an external IP.
4. The organization must enable the VPC attributes DNS hostnames and DNS resolution.
5. In Amazon ElastiCache, which of the following statements is correct?
6. When you launch an ElastiCache cluster into an Amazon VPC private subnet, every cache node

is assigned a public IP address within that subnet.

1. You cannot use ElastiCache in a VPC that is configured for dedicated instance tenancy.
2. If your AWS account supports only the EC2-VPC platform, ElastiCache will never launch your

cluster in a VPC.

1. ElastiCache is not fully integrated with Amazon Virtual Private Cloud (VPC).
2. Identify a true statement about the statement ID (Sid) in IAM.
3. You cannot expose the Sid in the IAM API.
4. You cannot use a Sid value as a sub-ID for a policy document’s ID for services provided by SQS

and SNS.

1. You can expose the Sid in the IAM API.
2. You cannot assign a Sid value to each statement in a statement array.
3. Is there any way to own a direct connection to Amazon Web Services?
4. No, AWS only allows access from the public Internet.
5. No, you can create an encrypted tunnel to VPC, but you cannot own the connection.
6. Yes, you can via Amazon Dedicated Connection.
7. Yes, you can via AWS Direct Connect.
8. An organization is hosting a scalable web application using AWS. The organization has configured internet facing ELB and Auto Scaling to make the application scalable. Which of the below mentioned statements is required to be followed when the application is planning to host a web application on VPC?
9. The ELB can be in a public or a private subnet but should have the ENI which is attached to an elastic IP.
10. The ELB must not be in any subnet; instead it should face the internet directly.
11. The ELB must be in a public subnet of the VPC to face the internet traffic.
12. The ELB can be in a public or a private subnet but must have routing tables attached to divert the internet traffic to it.
13. Which of the following statements is correct about the number of security groups and rules applicable for an EC2-Classic instance and an EC2-VPC network interface?
14. In EC2-Classic, you can associate an instance with up to 5 security groups and add up to 50 rules to a security group. In EC2-VPC, you can associate a network interface with up to 500 security groups and add up to 100 rules to a security group.
15. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 50 rules to a security group. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 100 rules to a security group.
16. In EC2-Classic, you can associate an instance with up to 5 security groups and add up to 100 rules to a security group. In EC2-VPC, you can associate a network interface with up to 500 security groups and add up to 50 rules to a security group.
17. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 100 rules to a security group. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 50 rules to a security group.
18. Which of the following statements is correct about AWS Direct Connect?
19. Connections to AWS Direct Connect require double clad fiber for 1 gigabit Ethernet with Auto Negotiation enabled for the port.
20. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with.
21. AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 50 gigabit Ethernet cable.
22. To use AWS Direct Connect, your network must be colocated with a new AWS Direct Connect location.
23. Which of the following cannot be used to manage Amazon ElastiCache and perform

administrative tasks?

1. AWS software development kits (SDKs)
2. Amazon S3
3. ElastiCache command line interface (CLI)
4. AWS CloudWatch
5. A user has created a VPC with public and private subnets using the VPC wizard. The VPC has

CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24 . The NAT instance ID is i-a12345.

Which of the below mentioned entries are required in the main route table attached with the

private subnet to allow instances to connect with the internet?

1. Destination: 20.0.0.0/0 and Target: 80
2. Destination: 20.0.0.0/0 and Target: i-a12345
3. Destination: 20.0.0.0/24 and Target: i-a12345
4. Destination: 0.0.0.0/0 and Target: i-a12345
5. In Amazon ElastiCache, the default cache port is:
6. for Memcached 11210 and for Redis 6380.
7. for Memcached 11211 and for Redis 6380.
8. for Memcached 11210 and for Redis 6379.
9. for Memcached 11211 and for Redis 6379.
10. An organization is setting up their website on AWS. The organization is working on various security measures to be performed on the AWS EC2 instances. Which of the below mentioned security mechanisms will not help the organization to avoid future data leaks and identify security weaknesses?
11. Run penetration testing on AWS with prior approval from Amazon.
12. Perform SQL injection for application testing.
13. Perform a Code Check for any memory leaks.
14. Perform a hardening test on the AWS instance.
15. A user is hosting a public website on AWS. The user wants to have the database and the app server on the AWS VPC. The user wants to setup a database that can connect to the Internet for any patch upgrade but cannot receive any request from the internet. How can the user set this up?
16. Setup DB in a private subnet with the security group allowing only outbound traffic.
17. Setup DB in a public subnet with the security group allowing only inbound data.
18. Setup DB in a local data center and use a private gateway to connect the application with DB.
19. Setup DB in a private subnet which is connected to the internet via NAT for outbound.
20. Which of the following components of AWS Data Pipeline polls for tasks and then performs those tasks?
21. Pipeline Definition
22. Task Runner
23. Amazon Elastic MapReduce (EMR)
24. AWS Direct Connect
25. To get started using AWS Direct Connect, in which of the following steps do you configure Border

Gateway Protocol (BGP)?

1. Complete the Cross Connect
2. Configure Redundant Connections with AWS Direct Connect
3. Create a Virtual Interface
4. Download Router Configuration
5. Can Provisioned IOPS be used on RDS instances launched in a VPC?
6. Yes, they can be used only with Oracle based instances.
7. Yes, they can be used for all RDS instances.
8. No
9. Yes, they can be used only with MySQL based instances.
10. Mike is appointed as Cloud Consultant in ExamKiller.com. ExamKiller has the following VPCs setup in the US East Region:

A VPC with CIDR block 10.10.0.0/16, a subnet in that VPC with CIDR block 10.10.1.0/24 A VPC with CIDR block 10.40.0.0/16, a subnet in that VPC with CIDR block 10.40.1.0/24 ExamKiller.com is trying to establish network connection between two subnets, a subnet with CIDR block 10.10.1.0/24 and another subnet with CIDR block 10.40.1.0/24. Which one of the following solutions should Mike recommend to ExamKiller.com?

1. Create 2 Virtual Private Gateways and configure one with each VPC.
2. Create 2 Internet Gateways, and attach one to each VPC.
3. Create a VPC Peering connection between both VPCs.
4. Create one EC2 instance in each subnet, assign Elastic IPs to both instances, and configure a set up Site-to-Site VPN connection between both EC2 instances.
5. You want to use Amazon Redshift and you are planning to deploy dw1.8xlarge nodes. What is the minimum amount of nodes that you need to deploy with this kind of configuration?
6. 1
7. 4
8. 3
9. 2
10. Which of the following AWS services can be used to define alarms to trigger on a certain activity, such as activity success, failure, or delay in AWS Data Pipeline?
11. Amazon SES
12. Amazon CodeDeploy
13. Amazon SNS
14. Amazon SQS
15. Do you need to use Amazon Cognito to use the Amazon Mobile Analytics service?
16. No. However, it is recommend by AWS to use Amazon Cognito for security best practices.
17. Yes. You need to use it only if you have IAM root access.
18. No. You cannot use it at all, and you need to use AWS IAM accounts.
19. Yes. It is recommended by AWS to use Amazon Cognito to use Amazon Mobile Analytics service.
20. A user has set the IAM policy where it denies all requests if a request is not from IP 10.10.10.1/ 32. The other policy says allow all requests between 5 PM to 7 PM. What will happen when a user is requesting access from IP 55.109.10.12/32 at 6 PM?
21. It will deny access
22. It is not possible to set a policy based on the time or IP
23. IAM will throw an error for policy conflict
24. It will allow access
25. You’re trying to delete an SSL certificate from the IAM certificate store, and you’re getting the

message “Certificate: <certificate-id> is being used by CloudFront.” Which of the following

statements is probably the reason why you are getting this error?

1. Before you can delete an SSL certificate you need to set up https on your server.
2. Before you can delete an SSL certificate, you need to set up the appropriate access level in IAM
3. Before you can delete an SSL certificate, you need to either rotate SSL certificates or revert from using a custom SSL certificate to using the default CloudFront certificate.
4. You can’t delete SSL certificates . You need to request it from AWS.
5. An organization is setting up a web application with the JEE stack. The application uses the JBoss app server and MySQL DB. The application has a logging module which logs all the activities whenever a business function of the JEE application is called. The logging activity takes some time due to the large size of the log file. If the application wants to setup a scalable infrastructure which of the below mentioned options will help achieve this setup?
6. Host the log files on EBS with PIOPS which will have higher I/O.
7. Host logging and the app server on separate servers such that they are both in the same zone.
8. Host logging and the app server on the same instance so that the network latency will be shorter.
9. Create a separate module for logging and using SQS compartmentalize the module such that all

calls to logging are asynchronous.

Note : <https://aws.amazon.com/blogs/architecture/aws-and-compartmentalization/>

1. What is the network performance offered by the c4.8xlarge instance in Amazon EC2?
2. Very High but variable
3. 20 Gigabit
4. 5 Gigabit
5. 10 Gigabit
6. A government client needs you to set up secure cryptographic key storage for some of their extremely confidential data. You decide that the AWS CloudHSM is the best service for this. However, there seem to be a few pre-requisites before this can happen, one of those being a security group that has certain ports open. Which of the following is correct in regards to those security groups?
7. A security group that has no ports open to your network.
8. A security group that has only port 3389 (for RDP) open to your network.
9. A security group that has only port 22 (for SSH) open to your network.
10. A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.
11. What is a possible reason you would need to edit claims issued in a SAML token?
12. The NameIdentifier claim cannot be the same as the username stored in AD.
13. Authentication fails consistently.
14. The NameIdentifier claim cannot be the same as the claim URI.
15. The NameIdentifier claim must be the same as the username stored in AD.

Note:https://azure.microsoft.com/en-us/documentation/articles/active-directory-saml-claimscustomization/

1. A user is creating a PIOPS volume. What is the maximum ratio the user should configure

between PIOPS and the volume size?

1. 5
2. 10
3. 20
4. 30

Note: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

1. A user is planning to host a Highly Available system on the AWS VPC. Which of the below mentioned statements is helpful in this scenario?
2. Create VPC subnets in two separate availability zones and launch instances in different subnets.
3. Create VPC with only one public subnet and launch instances in different AZs using that subnet.
4. Create two VPCs in two separate zones and setup failover with ELB such that if one VPC fails it will divert traffic to another VPC.
5. Create VPC with only one private subnet and launch instances in different AZs using that subnet

Note : https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_Subnets.html#VPCSubnet

1. A user is trying to create a PIOPS EBS volume with 4000 IOPS and 100 GB size. AWS does not allow the user to create this volume. What is the possible root cause for this?
2. PIOPS is supported for EBS higher than 500 GB size
3. The maximum IOPS supported by EBS is 3000
4. The ratio between IOPS and the EBS volume is higher than 30
5. The ratio between IOPS and the EBS volume is lower than 50
6. An organization is planning to host a web application in the AWS VPC. The organization does not want to host a database in the public cloud due to statutory requirements. How can the organization setup in this scenario?
7. The organization should plan the app server on the public subnet and database in the organization’s data center and connect them with the VPN gateway.
8. The organization should plan the app server on the public subnet and use RDS with the private subnet for a secure data operation.
9. The organization should use the public subnet for the app server and use RDS with a storage gateway to access as well as sync the data securely from the local data center.
10. The organization should plan the app server on the public subnet and database in a private subnet so it will not be in the public cloud.
11. Who is responsible for modifying the routing tables and networking ACLs in a VPC to ensure that a DB instance is reachable from other instances in the VPC?
12. AWS administrators
13. The owner of the AWS account
14. Amazon
15. The DB engine vendor

Note : <https://aws.amazon.com/rds/faqs/>

1. What is the average queue length recommended by AWS to achieve a lower latency for the 200

PIOPS EBS volume?

1. 5
2. 1
3. 2
4. 4
5. What is the role of the PollForTask action when it is called by a task runner in AWS Data Pipeline?
6. It is used to retrieve the pipeline definition.
7. It is used to report the progress of the task runner to AWS Data Pipeline.
8. It is used to receive a task to perform from AWS Data Pipeline.
9. It is used to inform AWS Data Pipeline of the outcome when the task runner completes a task.

Note : https://docs.aws.amazon.com/datapipeline/latest/APIReference/API\_PollForTask.html

1. True or False: In Amazon ElastiCache, you can use Cache Security Groups to configure the cache clusters that are part of a VPC.
2. FALSE
3. TRUE
4. True, this is applicable only to cache clusters that are running in an Amazon VPC environment.
5. True, but only when you configure the cache clusters using the Cache Security Groups from the

console navigation pane.

1. In the context of AWS Cloud Hardware Security Module(HSM), does your application need to reside in the same VPC as the CloudHSM instance?
2. No, but the server or instance on which your application and the HSM client is running must have network (IP) reachability to the HSM.
3. Yes, always
4. No, but they must reside in the same Availability Zone.
5. No, but it should reside in same Availability Zone as the DB instance.

Note : <https://aws.amazon.com/cloudhsm/faqs/>

1. Once the user has set ElastiCache for an application and it is up and running, which services, does Amazon not provide for the user:
2. The ability for client programs to automatically identify all of the nodes in a cache cluster, and to initiate and maintain connections to all of these nodes
3. Automating common administrative tasks such as failure detection and recovery, and software patching
4. Providing default Time To Live (TTL) in the AWS Elasticache Redis Implementation for different type of data.
5. Providing detailed monitoring metrics associated with your Cache Nodes, enabling you to diagnose and react to issues very quickly

Note : https://aws.amazon.com/elasticache/faqs/

1. You are setting up some EBS volumes for a customer who has requested a setup which includes a RAID (redundant array of inexpensive disks). AWS has some recommendations for RAID setups. Which RAID setup is not recommended for Amazon EBS?
2. RAID 1 only
3. RAID 5 only
4. RAID 5 and RAID 6
5. RAID 0 only
6. A user is configuring MySQL RDS with PIOPS. What should be the minimum PIOPS that the user should provision?
7. 1000
8. 200
9. 2000
10. 500
11. In AWS IAM, which of the following predefined policy condition keys checks how long ago (in seconds) the MFA-validated security credentials making the request were issued using multifactor authentication (MFA)?
12. aws:MultiFactorAuthAge
13. aws:MultiFactorAuthLast
14. aws:MFAAge
15. aws:MultiFactorAuthPrevious
16. Which of following IAM policy elements lets you specify an exception to a list of actions?
17. NotException
18. ExceptionAction
19. Exception
20. NotAction

Note: <https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_notaction.html>

1. How does AWS Data Pipeline execute activities on on-premise resources or AWS resources that you manage?
2. By supplying a Task Runner package that can be installed on your on-premise hosts
3. None of these
4. By supplying a Task Runner file that the resources can access for execution
5. By supplying a Task Runner json script that can be installed on your on-premise hosts

Note : <https://aws.amazon.com/datapipeline/faqs/>

1. AWS has launched T2 instances which come with CPU usage credit. An organization has a requirement which keeps an instance running for 24 hours. However, the organization has high usage only during 11 AM to 12 PM. The organization is planning to use a T2 small instance for this purpose. If the organization already has multiple instances running since Jan 2012, which of the below mentioned options should the organization implement while launching a T2 instance?
2. The organization must migrate to the EC2-VPC platform first before launching a T2 instance.
3. While launching a T2 instance the organization must create a new AWS account as this account does not have the EC2-VPC platform.
4. Create a VPC and launch a T2 instance as part of one of the subnets of that VPC.
5. While launching a T2 instance the organization must select EC2-VPC as the platform.

Note : <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/vpc-migrate.html>

1. When using Numeric Conditions within IAM, short versions of the available comparators can be used instead of the more verbose versions. Which of the following is the short version of the Numeric Condition “NumericLessThanEquals”?
2. numlteq
3. numlteql
4. numltequals
5. numeql
6. In Amazon Cognito what is a silent push notification?
7. It is a push message that is received by your application on a user’s device that will not be seen by the user.
8. It is a push message that is received by your application on a user’s device that will return the user’s geolocation.
9. It is a push message that is received by your application on a user’s device that will not be heard by the user.
10. It is a push message that is received by your application on a user’s device that will return the user’s authentication credentials.

Note: <http://aws.amazon.com/cognito/faqs/>

1. In the context of Amazon ElastiCache CLI, which of the following commands can you use to view all ElastiCache instance events for the past 24 hours?
2. elasticache-events –duration 24
3. elasticache-events –duration 1440
4. elasticache-describe-events –duration 24
5. elasticache describe-events –source-type cache-cluster –duration 1440

Note : https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/ECEvents.Viewing.html

1. In the context of IAM roles for Amazon EC2, which of the following NOT true about delegating permission to make API requests?
2. You cannot create an IAM role.
3. You can have the application retrieve a set of temporary credentials and use them.
4. You can specify the role when you launch your instances.
5. You can define which accounts or AWS services can assume the role.

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

1. Out of the striping options available for the EBS volumes, which one has the following disadvantage: ‘Doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you’re mirroring all writes to a pair of volumes, limiting how much you can stripe.’ ?
2. Raid 1
3. Raid 0
4. RAID 1+0 (RAID 10)
5. Raid 2

Note : <http://jayendrapatil.com/aws-automated-backups/>

1. Identify a true statement about using an IAM role to grant permissions to applications running on Amazon EC2 instances.
2. When AWS credentials are rotated, developers have to update only the root Amazon EC2 instance that uses their credentials.
3. When AWS credentials are rotated, developers have to update only the Amazon EC2 instance on which the password policy was applied and which uses their credentials.
4. When AWS credentials are rotated, you don’t have to manage credentials and you don’t have to worry about long-term security risks.
5. When AWS credentials are rotated, you must manage credentials and you should consider precautions for long-term security risks.

Note: http://docs.aws.amazon.com/IAM/latest/UserGuide/role-usecase-ec2app.html

1. In Amazon Redshift, how many slices does a dw2.8xlarge node have?
2. 16
3. 8
4. 32
5. 2

Note:https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-clusters.html#rs-about-clusters-and-nodes

1. True or False: The Amazon ElastiCache clusters are not available for use in VPC at this time.
2. TRUE
3. True, but they are available only in the GovCloud.
4. True, but they are available only on request.
5. FALSE

Note : <https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/VPCs.EC.html>

1. A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?
2. The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
3. The second subnet will be created
4. It will throw a CIDR overlaps error
5. It is not possible to create a subnet with the same CIDR as VPC

Note : http://jayendrapatil.com/aws-virtual-private-cloud-vpc/

1. ExamKiller has created a multi-tenant Learning Management System (LMS). The application is hosted for five different tenants (clients) in the VPCs of the respective AWS accounts of the tenant. ExamKiller wants to setup a centralized server which can connect with the LMS of each tenant upgrade if required. ExamKiller also wants to ensure that one tenant VPC should not be able to connect to the other tenant VPC for security reasons. How can ExamKiller setup this scenario?
2. ExamKiller has to setup one centralized VPC which will peer in to all the other VPCs of the tenants.
3. ExamKiller should setup VPC peering with all the VPCs peering each other but block the IPs from

CIDR of the tenant VPCs to deny them.

1. ExamKiller should setup all the VPCs with the same CIDR but have a centralized VPC. This way only the centralized VPC can talk to the other VPCs using VPC peering.
2. ExamKiller should setup all the VPCs meshed together with VPC peering for all VPCs.
3. Can a Direct Connect link be connected directly to the Internet?
4. Yes, this can be done if you pay for it.
5. Yes, this can be done only for certain regions.
6. Yes
7. No
8. An organization is having a VPC for the HR department, and another VPC for the Admin department. The HR department requires access to all the instances running in the Admin VPC while the Admin department requires access to all the resources in the HR department. How can the organization setup this scenario?
9. Setup VPC peering between the VPCs of Admin and HR.
10. Setup ACL with both VPCs which will allow traffic from the CIDR of the other VPC.
11. Setup the security group with each VPC which allows traffic from the CIDR of another VPC.
12. It is not possible to connect resources of one VPC from another VPC.
13. An organization has developed an application which provides a smarter shopping experience. They need to show a demonstration to various stakeholders who may not be able to access the in premise application so they decide to host a demo version of the application on AWS. Consequently they will need a fixed elastic IP attached automatically to the instance when it is launched. In this scenario which of the below mentioned options will not help assign the elastic IP automatically?
14. Write a script which will fetch the instance metadata on system boot and assign the public IP using that metadata.
15. Provide an elastic IP in the user data and setup a bootstrapping script which will fetch that elastic IP and assign it to the instance.
16. Create a controlling application which launches the instance and assigns the elastic IP based on the parameter provided when that instance is booted.
17. Launch instance with VPC and assign an elastic IP to the primary network interface.

Note: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AESDG-chapter-instancedata.html

1. You create a VPN connection, and your VPN device supports Border Gateway Protocol (BGP). Which of the following should be specified to configure the VPN connection?
2. Classless routing
3. Classfull routing
4. Dynamic routing
5. Static routing

Note: <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>

1. An organization is setting up RDS for their applications. The organization wants to secure RDS access with VPC. Which of the following options is not required while designing the RDS with VPC?
2. The organization must create a subnet group with public and private subnets. Both the subnets can be in the same or separate AZ.
3. The organization should keep minimum of one IP address in each subnet reserved for RDS failover.
4. If the organization is connecting RDS from the internet it must enable the VPC attributes DNS hostnames and DNS resolution.
5. The organization must create a subnet group with VPC using more than one subnet which are a part of separate AZs.

Note: [https ://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\_VPC.WorkingWithRDSInstanceinaVPC](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC) .html

1. What happens when Dedicated instances are launched into a VPC?
2. If you launch an instance into a VPC that has an instance tenancy of dedicated, you must manually create a Dedicated instance.
3. If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is created as a Dedicated instance, only based on the tenancy of the instance.
4. If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is automatically a Dedicated instance, regardless of the tenancy of the instance.
5. None of these are true.
6. An organization is planning to use NoSQL DB for its scalable data needs. The organization wants to host an application securely in AWS VPC. What action can be recommended to the organization?
7. The organization should setup their own NoSQL cluster on the AWS instance and configure route tables and subnets.
8. The organization should only use a DynamoDB because by default it is always a part of the default subnet provided by AWS.
9. The organization should use a DynamoDB while creating a table within the public subnet.
10. The organization should use a DynamoDB while creating a table within a private subnet.
11. IAM users do not have permission to create Temporary Security Credentials for federated users and roles by default. In contrast, IAM users can call \_\_\_\_\_\_ without the need of any special permissions
12. GetSessionName
13. GetFederationToken
14. GetSessionToken
15. GetFederationName

Note : <http://docs.aws.amazon.com/STS/latest/UsingSTS/STSPermission.html>

1. Regarding Identity and Access Management (IAM), Which type of special account belonging to your application allows your code to access Google services programmatically?
2. Service account
3. Simple Key
4. OAuth
5. Code account

Note : https://cloud.google.com/iam/docs/service-accounts

1. Within an IAM policy, can you add an IfExists condition at the end of a Null condition?
2. Yes, you can add an IfExists condition at the end of a Null condition but not in all Regions.
3. Yes, you can add an IfExists condition at the end of a Null condition depending on the condition.
4. No, you cannot add an IfExists condition at the end of a Null condition.
5. Yes, you can add an IfExists condition at the end of a Null condition.

Note: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\_policies\_elements\_condition\_operators.html#Conditions\_IfExists

1. With respect to AWS Lambda permissions model, at the time you create a Lambda function, you specify an IAM role that AWS Lambda can assume to execute your Lambda function on your behalf. This role is also referred to as the \_\_\_\_\_ role.
2. configuration
3. execution
4. delegation
5. Dependency

Note: https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html

1. Identify an application that polls AWS Data Pipeline for tasks and then performs those tasks.
2. A task executor
3. A task deployer
4. A task runner
5. A task optimizer

Note:https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-how-remote-taskrunner-client.html

1. AWS Direct Connect itself has NO specific resources for you to control access to. Therefore, there are no AWS Direct Connect Amazon Resource Names (ARNs) for you to use in an Identity and Access Management (IAM) policy. With that in mind, how is it possible to write a policy to control access to AWS Direct Connect actions?
2. You can leave the resource name field blank.
3. You can choose the name of the AWS Direct Connection as the resource.
4. You can use an asterisk (\*) as the resource.
5. You can create a name for the resource.

Note: <https://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html>

1. Which of the following cannot be done using AWS Data Pipeline?
2. Create complex data processing workloads that are fault tolerant, repeatable, and highly available.
3. Regularly access your data where it’s stored, transform and process it at scale, and efficiently transfer the results to another AWS service.
4. Generate reports over data that has been stored.
5. Move data between different AWS compute and storage services as well as on-premise data sources at specified intervals
6. In Amazon RDS for PostgreSQL, you can provision up to 3TB storage and 30,000 IOPS per database instance. For a workload with 50% writes and 50% reads running on a cr1.8xlarge instance, you can realize over 25,000 IOPS for PostgreSQL. However, by provisioning more than this limit, you may be able to achieve:
7. higher latency and lower throughput.
8. lower latency and higher throughput.
9. higher throughput only.
10. higher latency only.

Note : <https://aws.amazon.com/about-aws/whats-new/2013/03/13/amazon-rds-3tb-30k-iops/>

1. Select the correct statement about Amazon ElastiCache.
2. It makes it easy to set up, manage, and scale a distributed in-memory cache environment in the cloud.
3. It allows you to quickly deploy your cache environment only if you install software.
4. It does not integrate with other Amazon Web Services.
5. It cannot run in the Amazon Virtual Private Cloud (Amazon VPC) environment.
6. Attempts, one of the three types of items associated with the schedule pipeline in the AWS Data Pipeline, provides robust data management. Which of the following statements is NOT true about Attempts?
7. Attempts provide robust data management.
8. AWS Data Pipeline retries a failed operation until the count of retries reaches the maximum number of allowed retry attempts.
9. An AWS Data Pipeline Attempt object compiles the pipeline components to create a set of actionable instances.
10. AWS Data Pipeline Attempt objects track the various attempts, results, and failure reasons if applicable.
11. When using string conditions within IAM, short versions of the available comparators can be used instead of the more verbose ones. streqi is the short version of the \_\_\_\_\_ string condition.
12. StringEqualsIgnoreCase
13. StringNotEqualsIgnoreCase
14. StringLikeStringEquals
15. StringNotEquals
16. Which of the following is true while using an IAM role to grant permissions to applications running on Amazon EC2 instances?
17. All applications on the instance share the same role, but different permissions.
18. All applications on the instance share multiple roles and permissions.
19. Multiple roles are assigned to an EC2 instance at a time.
20. Only one role can be assigned to an EC2 instance at a time.

Note : <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html>

1. In the context of policies and permissions in AWS IAM, the Condition element is \_\_\_\_\_\_
2. crucial while writing the IAM policies
3. an optional element
4. always set to null
5. a mandatory element

Note : <https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html>

1. Which of the following is true of an instance profile when an IAM role is created using the console?
2. The instance profile uses a different name.
3. The console gives the instance profile the same name as the role it corresponds to.
4. The instance profile should be created manually by a user.
5. The console creates the role and instance profile as separate actions.
6. An organization is setting up a multi-site solution where the application runs on premise as well as on AWS to achieve the minimum recovery time objective(RTO). Which of the below mentioned configurations will not meet the requirements of the multi-site solution scenario?
7. Configure data replication based on RTO.
8. Keep an application running on premise as well as in AWS with full capacity.
9. Setup a single DB instance which will be accessed by both sites.
10. Setup a weighted DNS service like Route 53 to route traffic across sites.
11. How can a user list the IAM Role configured as a part of the launch config?
12. as-describe-launch-configs -iam-profile
13. as-describe-launch-configs -show-long
14. as-describe-launch-configs -iam-role
15. as-describe-launch-configs -role
16. A user is thinking to use EBS PIOPS volume. Which of the below mentioned options is a right use case for the PIOPS EBS volume?
17. Analytics
18. System boot volume
19. Mongo DB
20. Log processing
21. How does in-memory caching improve the performance of applications in ElastiCache?
22. It improves application performance by deleting the requests that do not contain frequently accessed data.
23. It improves application performance by implementing good database indexing strategies.
24. It improves application performance by using a part of instance RAM for caching important data.
25. It improves application performance by storing critical pieces of data in memory for low-latency access.

Note : <https://aws.amazon.com/elasticache/faqs/#g4>

1. An organization is making software for the CIA in USA. CIA agreed to host the application on AWS but in a secure environment. The organization is thinking of hosting the application on the AWS GovCloud region. Which of the below mentioned difference is not correct when the organization is hosting on the AWS GovCloud in comparison with the AWS standard region?
2. The billing for the AWS GovCLoud will be in a different account than the Standard AWS account.
3. GovCloud region authentication is isolated from Amazon.com.
4. Physical and logical administrative access only to U.S. persons.
5. It is physically isolated and has logical network isolation from all the other regions.

Note : <https://docs.aws.amazon.com/govcloud-us/latest/ug-west/whatis.html>

1. An organization has created multiple components of a single application for compartmentalization. Currently all the components are hosted on a single EC2 instance. Due to security reasons the organization wants to implement two separate SSLs for the separate modules although it is already using VPC. How can the organization achieve this with a single instance?
2. You have to launch two instances each in a separate subnet and allow VPC peering for a single IP.
3. Create a VPC instance which will have multiple network interfaces with multiple elastic IP addresses.
4. Create a VPC instance which will have both the ACL and the security group attached to it and have separate rules for each IP address.
5. Create a VPC instance which will have multiple subnets attached to it and each will have a separate IP address.

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

1. An EC2 instance that performs source/destination checks by default is launched in a private VPC subnet. All security, NACL, and routing definitions are configured as expected. A custom NAT instance is launched. Which of the following must be done for the custom NAT instance to work?
2. The source/destination checks should be disabled on the NAT instance.
3. The NAT instance should be launched in public subnet.
4. The NAT instance should be configured with a public IP address.
5. The NAT instance should be configured with an elastic IP address.

Note : https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_NAT\_Instance.html#EIP\_Disable\_SrcDestCheck

1. An organization is setting up a highly scalable application using Elastic Beanstalk. They are using Elastic Load Balancing (ELB) as well as a Virtual Private Cloud (VPC) with public and private subnets. They have the following requirements:

– All the EC2 instances should have a private IP

– All the EC2 instances should receive data via the ELB’s.

Which of these will not be needed in this setup?

1. Launch the EC2 instances with only the public subnet.
2. Create routing rules which will route all inbound traffic from ELB to the EC2 instances.
3. Configure ELB and NAT as a part of the public subnet only.
4. Create routing rules which will route all outbound traffic from the EC2 instances through NAT.

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

1. True or False : “In the context of Amazon ElastiCache, from the application’s point of view,

connecting to the cluster configuration endpoint is no different than connecting directly to an

individual cache node.”

1. True, from the application’s point of view, connecting to the cluster configuration endpoint is no different than connecting directly to an individual cache node since, each has a unique node identifier.
2. True, from the application’s point of view, connecting to the cluster configuration endpoint is no different than connecting directly to an individual cache node.
3. False, you can connect to a cache node, but not to a cluster configuration endpoint.
4. False, you can connect to a cluster configuration endpoint, but not to a cache node.
5. In Amazon SNS, to send push notifications to mobile devices using Amazon SNS and ADM, you

need to obtain the following, except:

1. Device token
2. Client ID
3. Registration ID
4. Client secret

Note : https://docs.aws.amazon.com/sns/latest/dg/mobile-push-pseudo.html

1. With Amazon Elastic MapReduce (Amazon EMR) you can analyze and process vast amounts of data. The cluster is managed using an open-source framework called Hadoop. You have set up an application to run Hadoop jobs. The application reads data from DynamoDB and generates a temporary file of 100 TBs. The whole process runs for 30 minutes and the output of the job is stored to S3. Which of the below mentioned options is the most cost effective solution in this case?
2. Use Spot Instances to run Hadoop jobs and configure them with EBS volumes for persistent data storage.
3. Use Spot Instances to run Hadoop jobs and configure them with ephermal storage for output file storage.
4. Use an on demand instance to run Hadoop jobs and configure them with EBS volumes for persistent storage.
5. Use an on demand instance to run Hadoop jobs and configure them with ephemeral storage for output file storage.
6. One of the AWS account owners faced a major challenge in June as his account was hacked and the hacker deleted all the data from his AWS account. This resulted in a major blow to the business. Which of the below mentioned steps would not have helped in preventing this action?
7. Setup an MFA for each user as well as for the root account user.
8. Take a backup of the critical data to offsite / on premise.
9. Create an AMI and a snapshot of the data at regular intervals as well as keep a copy to separate regions.
10. Do not share the AWS access and secret access keys with others as well do not store it inside programs, instead use IAM roles.
11. What RAID method is used on the Cloud Block Storage back-end to implement a very high level of reliability and performance?
12. RAID 1 (Mirror)
13. RAID 5 (Blocks striped, distributed parity)
14. RAID 10 (Blocks mirrored and striped)
15. RAID 2 (Bit level striping)
16. By default, temporary security credentials for an IAM user are valid for a maximum of 12 hours, but you can request a duration as long as \_\_\_\_\_\_ hours.
17. 24
18. 36
19. 10
20. 48
21. An organization has hosted an application on the EC2 instances. There will be multiple users connecting to the instance for setup and configuration of application. The organization is planning to implement certain security best practices. Which of the below mentioned pointers will not help the organization achieve better security arrangement?
22. Allow only IAM users to connect with the EC2 instances with their own secret access key.
23. Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.
24. Apply the latest patch of OS and always keep it updated.
25. Disable the password based login for all the users. All the users should use their own keys to connect with the instance securely.

Note: https://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/

1. Which statement is NOT true about a stack which has been created in a Virtual Private Cloud (VPC) in AWS OpsWorks?
2. Subnets whose instances cannot communicate with the Internet are referred to as public subnets.
3. Subnets whose instances can communicate only with other instances in the VPC and cannot communicate directly with the Internet are referred to as private subnets.
4. All instances in the stack should have access to any package repositories that your operating system depends on, such as the Amazon Linux or Ubuntu Linux repositories.
5. Your app and custom cookbook repositories should be accessible for all instances in the stack.

**Note:** https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks-vpc.html#workingstacksvpc-basi%20cs

1. A bucket owner has allowed another account’s IAM users to upload or access objects in his bucket. The IAM user of Account A is trying to access an object created by the IAM user of account B. What will happen in this scenario?
2. It is not possible to give permission to multiple IAM users
3. AWS S3 will verify proper rights given by the owner of Account A, the bucket owner as well as by the IAM user B to the object
4. The bucket policy may not be created as S3 will give error due to conflict of Access Rights
5. It is not possible that the IAM user of one account accesses objects of the other IAM user

Note : http://jayendrapatil.com/aws-s3-permisions/

1. In a VPC, can you modify a set of DHCP options after you create them?
2. Yes, you can modify a set of DHCP options within 48 hours after creation and there are no VPCs associated with them.
3. Yes, you can modify a set of DHCP options any time after you create them.
4. No, you can’t modify a set of DHCP options after you create them.
5. Yes, you can modify a set of DHCP options within 24 hours after creation.

Note : https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_DHCP\_Options.html#DHCPOptions

1. You have been given the task to define multiple AWS Data Pipeline schedules for different activities in the same pipeline. Which of the following would successfully accomplish this task?
2. Creating multiple pipeline definition files
3. Defining multiple pipeline definitions in your schedule objects file and associating the desired schedule to the correct activity via its schedule field
4. Defining multiple schedule objects in your pipeline definition file and associating the desired schedule to the correct activity via its schedule field
5. Defining multiple schedule objects in the schedule field
6. Which of the following cache engines does Amazon ElastiCache support?
7. Amazon ElastiCache supports Memcached and Redis.
8. Amazon ElastiCache supports Redis and WinCache.
9. Amazon ElastiCache supports Memcached and Hazelcast.
10. Amazon ElastiCache supports Memcached only.
11. If a single condition within an IAM policy includes multiple values for one key, it will be evaluated using a logical \_\_\_\_\_\_.
12. OR
13. NAND
14. NOR
15. AND

Note : http://jayendrapatil.com/tag/policy-evaluation/

1. A user has configured EBS volume with PIOPS. The user is not experiencing the optimal throughput. Which of the following could not be factor affecting I/O performance of that EBS volume?
2. EBS bandwidth of dedicated instance exceeding the PIOPS
3. EC2 bandwidth
4. EBS volume size
5. Instance type is not EBS optimized
6. A user is trying to create a PIOPS EBS volume with 3 GB size and 90 IOPS. Will AWS create the volume?
7. No, since the PIOPS and EBS size ratio is less than 30
8. Yes, since the ratio between EBS and IOPS is less than 30
9. No, the EBS size is less than 4GB
10. Yes, since PIOPS is higher than 100
11. What is the maximum length for a certificate ID in AWS IAM?
12. 1024 characters
13. 512 characters
14. 64 characters
15. 128 characters
16. In Amazon Cognito, your mobile app authenticates with the Identity Provider (IdP) using the provider’s SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new \_\_\_\_\_\_\_\_\_ for the user and a set of temporary, limited-privilege AWS credentials.
17. Cognito Key Pair
18. Cognito API
19. Cognito ID
20. Cognito SDK

Note : <http://aws.amazon.com/cognito/faqs/>

1. An organization is planning to create a secure scalable application with AWS VPC and ELB. The organization has two instances already running and each instance has an ENI attached to it in addition to a primary network interface. The primary network interface and additional ENI both have an elastic IP attached to it. If those instances are registered with ELB and the organization wants ELB to send data to a particular EIP of the instance, how can they achieve this?
2. The organization should ensure that the IP which is required to receive the ELB traffic is attached to a primary network interface.
3. It is not possible to attach an instance with two ENIs with ELB as it will give an IP conflict error.
4. The organization should ensure that the IP which is required to receive the ELB traffic is attached to an additional ENI.
5. It is not possible to send data to a particular IP as ELB will send to any one EIP.
6. Cognito Sync is an AWS service that you can use to synchronize user profile data across mobile devices without requiring your own backend. When the device is online, you can synchronize data. If you also set up push sync, what does it allow you to do?
7. Notify other devices that a user profile is available across multiple devices
8. Synchronize user profile data with less latency
9. Notify other devices immediately that an update is available
10. Synchronize online data faster
11. What is the maximum length for an instance profile name in AWS IAM?
12. 512 characters
13. 128 characters
14. 1024 characters
15. 64 characters
16. An organization is undergoing a security audit. The auditor wants to view the AWS VPC configurations as the organization has hosted all the applications in the AWS VPC. The auditor is from a remote place and wants to have access to AWS to view all the VPC records. How can the organization meet the expectations of the auditor without compromising on the security of their AWS infrastructure?
17. The organization should not accept the request as sharing the credentials means compromising on security.
18. Create an IAM role which will have read only access to all EC2 services including VPC and assign that role to the auditor .
19. Create an IAM user who will have read only access to the AWS VPC and share those credentials with the auditor.
20. The organization should create an IAM user with VPC full access but set a condition that will not allow to modify anything if the request is from any IP other than the organization’s data center.

Note : <https://docs.aws.amazon.com/vpc/latest/userguide/VPC_IAM.html>

1. ExamKiller has three separate departments and each department has their own AWS accounts. The HR department has created a file sharing site where all the on roll employees’ data is uploaded. The Admin department uploads data about the employee presence in the office to their DB hosted in the VPC. The Finance department needs to access data from the HR department to know the on roll employees to calculate the salary based on the number of days that an employee is present in the office. How can ExamKiller setup this scenario?
2. It is not possible to configure VPC peering since each department has a separate AWS account.
3. Setup VPC peering for the VPCs of Admin and Finance.
4. Setup VPC peering for the VPCs of Finance and HR as well as between the VPCs of Finance and Admin.
5. Setup VPC peering for the VPCs of Admin and HR
6. An organization is purchasing licensed software. The software license can be registered only to a

specific MAC Address. The organization is going to host the software in the AWS environment.

How can the organization fulfil the license requirement as the MAC address changes every time

an instance is started/stopped/terminated?

1. It is not possible to have a fixed MAC address with AWS.
2. The organization should use VPC with the private subnet and configure the MAC address with that subnet.
3. The organization should use VPC with an elastic network interface which will have a fixed MAC Address.
4. The organization should use VPC since VPC allows to configure the MAC address for each EC2 instance.
5. A user is trying to create a vault in AWS Glacier. The user wants to enable notifications. In which of the below mentioned options can the user enable the notifications from the AWS console?
6. Glacier does not support the AWS console
7. Archival Upload Complete
8. Vault Upload Job Complete
9. Vault Inventory Retrieval Job Complete
10. An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the webserver on a single VPC instance such that it allows the internet traffic as well as the back-end management traffic. The organization wants to make so that the back end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing webserver will have an IP address which can receive traffic from all the internet IPs. How can the organization achieve this by running web server on a single instance?
11. It is not possible to have two IP addresses for a single instance.
12. The organization should create two network interfaces with the same subnet and security group to assign separate IPs to each network interface.
13. The organization should create two network interfaces with separate subnets so one instance can have two subnets and the respective security groups for controlled access.
14. The organization should launch an instance with two separate subnets using the same network interface which allows to have a separate CIDR as well as security groups.
15. A user is planning to use EBS for his DB requirement. The user already has an EC2 instance running in the VPC private subnet. How can the user attach the EBS volume to a running instance?
16. The user can create EBS in the same zone as the subnet of instance and attach that EBS to instance.
17. It is not possible to attach an EBS to an instance running in VPC until the instance is stopped.
18. The user can specify the same subnet while creating EBS and then attach it to a running instance.
19. The user must create EBS within the same VPC and then attach it to a running instance.
20. The user has provisioned the PIOPS volume with an EBS optimized instance. Generally speaking, in which I/O chunk should the bandwidth experienced by the user be measured by AWS?
21. 128 KB
22. 256 KB
23. 64 KB
24. 32 KB
25. An organization has created 5 IAM users. The organization wants to give them the same login ID but different passwords. How can the organization achieve this?
26. The organization should create each user in a separate region so that they have their own URL to login
27. The organization should create a separate login ID but give the IAM users the same alias so that each one can login with their alias
28. It is not possible to have the same login ID for multiple IAM users of the same account
29. The organization should create various groups and add each user with the same login ID to different groups. The user can login with their own group ID
30. In Amazon VPC, what is the default maximum number of BGP advertised routes allowed per

route table?

1. 15
2. 100
3. 5
4. 10
5. The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?
6. “Effect”: “Allow”, “Action”: [“Describe”], “Resource”: “Billing”
7. “Effect”: “Allow”, “Action”: [“aws-portal: ViewBilling”], “Resource”: “\*”
8. “Effect”: “Allow”, “Action”: [“aws-portal:ViewUsage”], “Resource”: “\*”
9. “Effect”: “Allow”, “Action”: [“AccountUsage], “Resource”: “\*”
10. In IAM, which of the following is true of temporary security credentials?
11. Once you issue temporary security credentials, they cannot be revoked.
12. None of these are correct.
13. Once you issue temporary security credentials, they can be revoked only when the virtual MFA device is used.
14. Once you issue temporary security credentials, they can be revoked.
15. What types of identities do Amazon Cognito identity pools support?
16. They support both authenticated and unauthenticated identities.
17. They support only unauthenticated identities.
18. They support neither authenticated nor unauthenticated identities.
19. They support only authenticated identities.
20. What feature of the load balancing service attempts to force subsequent connections to a service to be redirected to the same node as long as it is online?
21. Node balance
22. Session retention
23. Session multiplexing
24. Session persistence
25. Which of the following components of AWS Data Pipeline specifies the business logic of your data management?
26. Task Runner
27. Pipeline definition
28. AWS Direct Connect
29. Amazon Simple Storage Service (Amazon S3)
30. Does an AWS Direct Connect location provide access to Amazon Web Services in the region it is associated with as well as access to other US regions?
31. No, it provides access only to the region it is associated with.
32. No, it provides access only to the US regions other than the region it is associated with.
33. Yes, it provides access.
34. Yes, it provides access but only when there’s just one Availability Zone in the region.
35. By default, what is the maximum number of Cache Nodes you can run in Amazon ElastiCache?
36. 20
37. 50
38. 100
39. 200
40. An organization is setting up a backup and restore system in AWS of their in premise system.

The organization needs High Availability (HA) and Disaster Recovery(DR) but is okay to have a

longer recovery time to save costs. Which of the below mentioned setup options helps achieve

the objective of cost saving as well as DR in the most effective way?

1. Setup pre- configured servers and create AMIs.. Use EIP and Route 53 to quickly switch over to AWS from in premise.
2. Setup the backup data on S3 and transfer data to S3 regularly using the storage gateway.
3. Setup a small instance with AutoScaling; in case of DR start diverting all the load to AWS from on premise.
4. Replicate on premise DB to EC2 at regular intervals and setup a scenario similar to the pilot light.
5. Does Amazon RDS API provide actions to modify DB instances inside a VPC and associate them

with DB Security Groups?

1. Yes, Amazon does this but only for MySQL RDS.
2. Yes
3. No
4. Yes, Amazon does this but only for Oracle RDS.
5. An organization is having an application which can start and stop an EC2 instance as per schedule. The organization needs the MAC address of the instance to be registered with its software. The instance is launched in EC2-CLASSIC. How can the organization update the MAC registration every time an instance is booted?
6. The organization should write a boot strapping script which will get the MAC address from the instance metadata and use that script to register with the application.
7. The organization should provide a MAC address as a part of the user data. Thus, whenever the instance is booted the script assigns the fixed MAC address to that instance.
8. The instance MAC address never changes. Thus, it is not required to register the MAC address every time.
9. AWS never provides a MAC address to an instance; instead the instance ID is used for identifying the instance for any software registration.
10. An organization is setting up an application on AWS to have both High Availabilty (HA) and Disaster Recovery (DR). The organization wants to have both Recovery point objective (RPO) and Recovery time objective (RTO) of 10 minutes. Which of the below mentioned service configurations does not help the organization achieve the said RPO and RTO?
11. Take a snapshot of the data every 10 minutes and copy it to the other region.
12. Use an elastic IP to assign to a running instance and use Route 53 to map the user’s domain with that IP.
13. Create ELB with multi-region routing to allow automated failover when required.
14. Use an AMI copy to keep the AMI available in other regions.
15. Which of the following is NOT an advantage of using AWS Direct Connect?
16. AWS Direct Connect provides users access to public and private resources by using two different connections while maintaining network separation between the public and private environments.
17. AWS Direct Connect provides a more consistent network experience than Internet-based connections.
18. AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS.
19. AWS Direct Connect reduces your network costs.
20. True or False: Amazon ElastiCache supports the Redis key-value store.
21. True, ElastiCache supports the Redis key-value store, but with limited functionalities.
22. False, ElastiCache does not support the Redis key-value store.
23. True, ElastiCache supports the Redis key-value store.
24. False, ElastiCache supports the Redis key-value store only if you are in a VPC environment.
25. IAM Secure And Scalable is an organization which provides scalable and secure SAAS to its clients. They are planning to host a web server and App server on AWS VPC as separate tiers. The organization wants to implement the scalability by configuring Auto Scaling and load balancer with their app servers (middle tier) too. Which of the below mentioned options suits their requirements?
26. Since ELB is internet facing, it is recommended to setup HAProxy as the Load balancer within the VPC.
27. Create an Internet facing ELB with VPC and configure all the App servers with it.
28. The user should make ELB with EC2-CLASSIC and enable SSH with it for security.
29. Create an Internal Load balancer with VPC and register all the App servers with it.

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

1. You want to define permissions for a role in an IAM policy. Which of the following configuration formats should you use?
2. An XML document written in the IAM Policy Language
3. An XML document written in a language of your choice
4. A JSON document written in the IAM Policy Language
5. A JSON document written in a language of your choice
6. Regarding Amazon SNS, you can send notification messages to mobile devices through any of the following supported push notification services, EXCEPT:
7. Microsoft Windows Mobile Messaging (MWMM)
8. Google Cloud Messaging for Android (GCM)
9. Amazon Device Messaging (ADM)
10. Apple Push Notification Service (APNS)
11. How many cg1.4xlarge on-demand instances can a user run in one region without taking any limit

increase approval from AWS?

1. 20
2. 2
3. 5
4. 10
5. How much memory does the cr1.8xlarge instance type provide?
6. 224 GB
7. 124 GB
8. 184 GB
9. 244 GB
10. True or False: In Amazon ElastiCache replication groups of Redis, for performance tuning reasons, you can change the roles of the cache nodes within the replication group, with the primary and one of the replicas exchanging roles.
11. True, however, you get lower performance.
12. FALSE
13. TRUE
14. False, you must recreate the replication group to improve performance tuning.
15. One of your AWS Data Pipeline activities has failed consequently and has entered a hard failure state after retrying thrice. You want to try it again. Is it possible to increase the number of automatic retries to more than thrice?
16. Yes, you can increase the number of automatic retries to 6.
17. Yes, you can increase the number of automatic retries to indefinite number.
18. No, you cannot increase the number of automatic retries.
19. Yes, you can increase the number of automatic retries to 10.
20. The MySecureData company has five branches across the globe. They want to expand their data centers such that their web server will be in the AWS and each branch would have their own database in the local data center. Based on the user login, the company wants to connect to the data center. How can MySecureData company implement this scenario with the AWS VPC?
21. Create five VPCs with the public subnet for the app server and setup the VPN gateway for each VPN to connect them individually.
22. Use the AWS VPN CloudHub to communicate with multiple VPN connections.
23. Use the AWS CloudGateway to communicate with multiple VPN connections.
24. It is not possible to connect different data centers from a single VPC.
25. The two policies that you attach to an IAM role are the access policy and the trust policy. The trust policy identifies who can assume the role and grants the permission in the AWS Lambda account principal by adding the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ action.
26. aws:AssumeAdmin
27. lambda:InvokeAsync
28. sts:InvokeAsync
29. sts:AssumeRole
30. How can multiple compute resources be used on the same pipeline in AWS Data Pipeline?
31. You can use multiple compute resources on the same pipeline by defining multiple cluster objects in your definition file and associating the cluster to use for each activity via its runsOn field.
32. You can use multiple compute resources on the same pipeline by defining multiple cluster definition files.
33. You can use multiple compute resources on the same pipeline by defining multiple clusters for your activity.
34. You cannot use multiple compute resources on the same pipeline.
35. A user has configured EBS volume with PIOPS. The user is not experiencing the optimal throughput. Which of the following could not be factor affecting I/O performance of that EBS volume?
36. EBS bandwidth of dedicated instance exceeding the PIOPS
37. EBS volume size
38. EC2 bandwidth
39. Instance type is not EBS optimized
40. An organization (account ID 123412341234) has configured the IAM policy to allow the user to modify his credentials. What will the below mentioned statement allow the user to perform?

{

“Version”: “2012-10-17”,

“Statement”: [{

“Effect”: “Allow”,

“Action”: [

“iam:AddUserToGroup”,

“iam:RemoveUserFromGroup”,

“iam:GetGroup”

],

“Resource”: “arn:aws:iam:: 123412341234:group/TestingGroup”

}

]

1. Allow the IAM user to update the membership of the group called TestingGroup
2. The IAM policy will throw an error due to an invalid resource name
3. The IAM policy will allow the user to subscribe to any IAM group
4. Allow the IAM user to delete the TestingGroup
5. An organization is hosting a scalable web application using AWS. The organization has configured ELB and Auto Scaling to make the application scalable. Which of the below mentioned statements is not required to be followed for ELB when the application is planning to host a web application on VPC?
6. The ELB and all the instances should be in the same subnet.
7. Configure the security group rules and network ACLs to allow traffic to be routed between the subnets in the VPC.
8. The internet facing ELB should have a route table associated with the internet gateway.
9. The internet facing ELB should be only in a public subnet.
10. If no explicit deny is found while applying IAM’s Policy Evaluation Logic, the enforcement code

looks for any \_\_\_\_\_\_ instructions that would apply to the request.

1. “cancel”
2. “suspend”
3. “allow”
4. “valid”
5. The Statement element, of an AWS IAM policy, contains an array of individual statements. Each

individual statement is a(n) \_\_\_\_\_\_ block enclosed in braces { }.

1. XML
2. JavaScript
3. JSON
4. AJAX
5. A user is configuring MySQL RDS with PIOPS. What should be the minimum size of DB storage

provided by the user?

1. 1 TB
2. 50 GB
3. 5 GB
4. 100 GB
5. Doug has created a VPC with CIDR 10.201.0.0/16 in his AWS account. In this VPC he has created a public subnet with CIDR block 10.201.31.0/24. While launching a new EC2 from the console, he is not able to assign the private IP address 10.201.31.6 to this instance. Which is the most likely reason for this issue?
6. Private address IP 10.201.31.6 is currently assigned to another interface.
7. Private IP address 10.201.31.6 is reserved by Amazon for IP networking purposes.
8. Private IP address 10.201.31.6 is blocked via ACLs in Amazon infrastructure as a part of platform security.
9. Private IP address 10.201.31.6 is not part of the associated subnet’s IP address range.
10. The Principal element of an IAM policy refers to the specific entity that should be allowed or

denied permission, whereas the \_\_\_\_\_\_\_ translates to everyone except the specified entity.

1. NotPrincipal
2. Vendor
3. Principal
4. Action
5. What bandwidths do AWS Direct Connect currently support?
6. 10Mbps and 100Mbps
7. 10Gbps and 100Gbps
8. 100Mbps and 1Gbps
9. 1Gbps and 10 Gbps
10. When does an AWS Data Pipeline terminate the AWS Data Pipeline-managed compute resources?
11. AWS Data Pipeline terminates AWS Data Pipeline-managed compute resources every 2 hours.
12. When the final activity that uses the resources is running
13. AWS Data Pipeline terminates AWS Data Pipeline-managed compute resources every 12 hours.
14. When the final activity that uses the resources has completed successfully or failed
15. MapMySite is setting up a web application in the AWS VPC. The organization has decided to use an AWS RDS instead of using its own DB instance for HA and DR requirements. The organization also wants to secure RDS access. How should the web application be setup with RDS?
16. Create a VPC with one public and one private subnet. Launch an application instance in the public subnet while RDS is launched in the private subnet.
17. Setup a public and two private subnets in different AZs within a VPC and create a subnet group. Launch RDS with that subnet group.
18. Create a network interface and attach two subnets to it. Attach that network interface with RDS while launching a DB instance.
19. Create two separate VPCs and launch a Web app in one VPC and RDS in a separate VPC and connect them with VPC peering.
20. In Amazon ElastiCache, the failure of a single cache node can have an impact on the availability of your application and the load on your back-end database while ElastiCache provisions a replacement for the failed cache node and it get repopulated. Which of the following is a solution to reduce this potential availability impact?
21. Spread your memory and compute capacity over fewer number of cache nodes, each with smaller capacity.
22. Spread your memory and compute capacity over a larger number of cache nodes, each with smaller capacity.
23. Include fewer number of high capacity nodes.
24. Include a larger number of cache nodes, each with high capacity.
25. An organization is creating a VPC for their application hosting. The organization has created two private subnets in the same AZ and created one subnet in a separate zone. The organization wants to make a HA system with the internal ELB. Which of these statements is true with respect to an internal ELB in this scenario?
26. ELB can support only one subnet in each availability zone.
27. ELB does not allow subnet selection; instead it will automatically select all the available subnets of the VPC.
28. If the user is creating an internal ELB, he should use only private subnets.
29. ELB can support all the subnets irrespective of their zones.
30. Which of the following is the Amazon Resource Name (ARN) condition operator that can be used within an Identity and Access Management (IAM) policy to check the case-insensitive matching of the ARN?
31. ArnCheck
32. ArnMatch
33. ArnCase
34. ArnLike
35. A user authenticating with Amazon Cognito will go through a multi-step process to bootstrap their credentials. Amazon Cognito has two different flows for authentication with public providers. Which of the following are the two flows?
36. Authenticated and non-authenticated
37. Public and private
38. Enhanced and basic
39. Single step and multistep
40. A user has created a MySQL RDS instance with PIOPS. Which of the below mentioned statements will help user understand the advantage of PIOPS?
41. The user can achieve additional dedicated capacity for the EBS I/O with an enhanced RDS option
42. It uses a standard EBS volume with optimized configuration the stacks
43. It uses optimized EBS volumes and optimized configuration stacks
44. It provides a dedicated network bandwidth between EBS and RDS
45. How many g2.2xlarge on-demand instances can a user run in one region without taking any limit increase approval from AWS?
46. 20
47. 2
48. 5
49. 10
50. While implementing the policy keys in AWS Direct Connect, if you use \_\_\_\_\_ and the request comes from an Amazon EC2 instance, the instance’s public IP address is evaluated to determine if access is allowed.
51. aws:SecureTransport
52. aws:EpochIP
53. aws:SourceIp
54. aws:CurrentTime
55. You have subscribed to the AWS Business and Enterprise support plan. Your business has a backlog of problems, and you need about 20 of your IAM users to open technical support cases. How many users can open technical support cases under the AWS Business and Enterprise support plan?
56. 5 users
57. 10 users
58. Unlimited
59. 1 user
60. A user is planning to host a web server as well as an app server on a single EC2 instance which is a part of the public subnet of a VPC. How can the user setup to have two separate public IPs and separate security groups for both the application as well as the web server?
61. Launch VPC with two separate subnets and make the instance a part of both the subnets.
62. Launch a VPC instance with two network interfaces. Assign a separate security group and elastic IP to them.
63. Launch a VPC instance with two network interfaces. Assign a separate security group to each and AWS will assign a separate public IP to them.
64. Launch a VPC with ELB such that it redirects requests to separate VPC instances of the public subnet.
65. In Amazon IAM, what is the maximum length for a role name?
66. 128 characters
67. 512 characters
68. 64 characters
69. 256 characters
70. In which step of using AWS Direct Connect should the user determine the required port speed?
71. Complete the Cross Connect
72. Verify Your Virtual Interface
73. Download Router Configuration
74. Submit AWS Direct Connect Connection Request
75. An organization is planning to host an application on the AWS VPC. The organization wants dedicated instances. However, an AWS consultant advised the organization not to use dedicated instances with VPC as the design has a few limitations. Which of the below mentioned statements is not a limitation of dedicated instances with VPC?
76. All instances launched with this VPC will always be dedicated instances and the user cannot use a default tenancy model for them.
77. It does not support the AWS RDS with a dedicated tenancy VPC.
78. The user cannot use Reserved Instances with a dedicated tenancy model.
79. The EBS volume will not be on the same tenant hardware as the EC2 instance though the user has configured dedicated tenancy.
80. An organization has 4 people in the IT operations team who are responsible to manage the AWS infrastructure. The organization wants to setup that each user will have access to launch and manage an instance in a zone which the other user cannot modify. Which of the below mentioned options is the best solution to set this up?
81. Create four AWS accounts and give each user access to a separate account.
82. Create an IAM user and allow them permission to launch an instance of a different sizes only.
83. Create four IAM users and four VPCs and allow each IAM user to have access to separate VPCs.
84. Create a VPC with four subnets and allow access to each subnet for the individual IAM user.
85. An organization is setting a website on the AWS VPC. The organization has blocked a few IPs to

avoid a D-DOS attack. How can the organization configure that a request from the above mentioned IPs does not access the application instances?

1. Create an IAM policy for VPC which has a condition to disallow traffic from that IP address.
2. Configure a security group at the subnet level which denies traffic from the selected IP.
3. Configure the security group with the EC2 instance which denies access from that IP address.
4. Configure an ACL at the subnet which denies the traffic from that IP address
5. A customer has a website which shows all the deals available across the market. The site experiences a load of 5 large EC2 instances generally. However, a week before Thanksgiving vacation they encounter a load of almost 20 large instances. The load during that period varies over the day based on the office timings. Which of the below mentioned solutions is cost effective as well as help the website achieve better performance?
6. Setup to run 10 instances during the pre-vacation period and only scale up during the office time by launching 10 more instances using the AutoScaling schedule.
7. Keep only 10 instances running and manually launch 10 instances every day during office hours.
8. During the pre-vacation period setup 20 instances to run continuously.
9. During the pre-vacation period setup a scenario where the organization has 15 instances running and 5 instances to scale up and down using Auto Scaling based on the network I/O policy.
10. What is the default maximum number of VPCs allowed per region?
11. 5
12. 10
13. 100
14. 15
15. An organization is planning to host a WordPress blog as well a joomla CMS on a single instance launched with VPC. The organization wants to have separate domains for each application and assign them using Route 53. The organization may have about ten instances each with two applications as mentioned above. While launching the instance, the organization configured two separate network interfaces (primary + ENI) and wanted to have two elastic IPs for that instance. It was suggested to use a public IP from AWS instead of an elastic IP as the number of elastic IPs is restricted. What action will you recommend to the organization?
16. I agree with the suggestion but will prefer that the organization should use separate subnets with each ENI for different public IPs.
17. I do not agree as it is required to have only an elastic IP since an instance has more than one ENI and AWS does not assign a public IP to an instance with multiple ENIs.
18. I do not agree as AWS VPC does not attach a public IP to an ENI; so the user has to use only an elastic IP only.
19. I agree with the suggestion and it is recommended to use a public IP from AWS since the organization is going to use DNS with Route 53.
20. In the context of AWS IAM, identify a true statement about user passwords (login profiles).
21. They must contain Unicode characters.
22. They can contain any Basic Latin (ASCII) characters.
23. They must begin and end with a forward slash (/).
24. They cannot contain Basic Latin (ASCII) characters.
25. An organization is planning to extend their data center by connecting their DC with the AWS VPC using the VPN gateway. The organization is setting up a dynamically routed VPN connection. Which of the below mentioned answers is not required to setup this configuration?
26. The type of customer gateway, such as Cisco ASA, Juniper J-Series, Juniper SSG, Yamaha.
27. Elastic IP ranges that the organization wants to advertise over the VPN connection to the VPC.
28. Internet-routable IP address (static) of the customer gateway’s external interface.
29. Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway.
30. An IAM user is trying to perform an action on an object belonging to some other root account’s bucket. Which of the below mentioned options will AWS S3 not verify?
31. The object owner has provided access to the IAM user
32. Permission provided by the parent of the IAM user on the bucket
33. Permission provided by the bucket owner to the IAM user
34. Permission provided by the parent of the IAM user
35. You want to use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC). What criterion must be met for this to be possible?
36. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access only the public AWS CodeDeploy endpoint.
37. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access only the public Amazon S3 service endpoint.
38. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access the public AWS CodeDeploy and Amazon S3 service endpoints.
39. It is not currently possible to use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC.)

Note: https://aws.amazon.com/codedeploy/faqs/

1. By default, Amazon Cognito maintains the last-written version of the data. You can override this behavior and resolve data conflicts programmatically. In addition, push synchronization allows you to use Amazon Cognito to send a silent \_\_\_\_\_\_\_\_ notification to all devices associated with an identity to notify them that new data is available.
2. get
3. post
4. pull
5. Push
6. You are designing a data leak prevention solution for your VPC environment. You want your VPC instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CDNs by their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the Internet. Which of the following options would you consider?
7. Implement security groups and configure outbound rules to only permit traffic to software depots.
8. Configure a web proxy server in your VPC and enforce URL-based rules for outbound access. Remove default routes.
9. Implement network access control lists to allow specific destinations, with an implicit deny all rule.
10. Move all your instances into private VPC subnets. Remove default routes from all routing tables and add specific routes to the software depots and distributions only.
11. Which AWS instance address has the following characteristics? :”If you stop an instance, its

Elastic IP address is unmapped, and you must remap it when you restart the instance.”

1. Both A and B
2. None of these
3. VPC Addresses
4. EC2 Addresses
5. Select the correct set of options.

These are the initial settings for the default security group:

1. Allow no inbound traffic, Allow all outbound traffic and Allow instances associated with this security group to talk to each other
2. Allow all inbound traffic, Allow no outbound traffic and Allow instances associated with this security group to talk to each other
3. Allow no inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
4. Allow all inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
5. The \_\_\_\_\_ service is targeted at organizations with multiple users or systems that use AWS

products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console.

1. Amazon RDS
2. AWS Integrity Management
3. AWS Identity and Access Management
4. Amazon EMR
5. You are developing a new mobile application and are considering storing user preferences in AWS. This would provide a more uniform cross-device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size. Additionally, 5 million customers are expected to use the application on a regular basis. The solution needs to be cost- effective, highly-available, scalable and secure. How would you design a solution to meet the above requirements?
6. Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data. The mobile application will query the user preferences from the read replicas. Leverage the MySQL user management and access privilege system to manage security and access credentials.
7. Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials.
8. Store the user preference data in S3. Setup a DynamoDB table with an item for each user and an item attribute pointing to the user’s S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly. Utilize STS, Web Identity Federation, and S3 ACLs to authenticate and authorize access.
9. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS, Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access.

Note : https://aws.amazon.com/blogs/aws/fine-grained-access-control-for-amazon-dynamodb/

1. A company is building a voting system for a popular TV show, viewers will watch the performances then visit the show’s website to vote for their favorite performer. It is expected that in a short period of time after the show has finished the site will receive millions of visitors, the visitors will first login to the site using theirAmazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that it can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum. Which of the design patters below should they use?
2. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login With Amazon service to authenticate the user, the web servers will process the users vote and store the result into a DynamoDB table using IAM Roles for EC2 Instances to gain permissions to the DynamoDB table.
3. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login With Amazon service to authenticate the user, the web servers will process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table.
4. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login With Amazon service to authenticate the user then process the users vote and store the result into a multi-AZ Relational Database Service instance.
5. Use CloudFront and the static website hosting feature of S3 with the Javascript SDK to call the Login with Amazon service to authenticate the user, use IAM Roles to gain permissions to a DynamoDB table to store the users vote.
6. A web company is looking to implement an external payment service into their highly available application deployed in a VPC. Their application EC2 instances are behind a public facing ELB. Auto Scaling is used to add additional instances as traffic Increases. Under normal load the application runs 2 Instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet, which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisted IP addresses are allowed at a time and can be added through an API. How should they architect their solution?
7. Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway.
8. Automatically assign public IP addresses to the application instances in the Auto Scaling group and run a script on boot that adds each instances public IP address to the payment validation whitelist API.
9. Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the NAT instances.
10. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.
11. Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design for the application that leverages multiple regions for the most recently accessed content and latency sensitive portions of the web site. The most latency sensitive component of the application Involves reading user preferences to support web site personalization and ad selection. In addition to running your application in multiple regions, which option will support this application’s requirements?
12. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3, CloudFront with dynamic content, and an ELB in each region. Retrieve user preferences from an ElastiCache cluster in each region and leverage SNS notifications to propagate user preference changes to a worker node in each region.
13. Serve user content from S3, CloudFront with dynamic content, and an ELB in each region. Retrieve user preferences from an ElastiCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of user preferences from a centralized DB to each ElastiCache cluster.
14. Serve user content from S3, CloudFront, and use Route53 latency-based routing between ELBs in each region. Retrieve user preferences from a local DynamoDB table in each region and leverage SQS to capture changes to user preferences with SQS workers for propagating updates to each table.
15. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3, CloudFront, and Route53 latency-based routing between ELBs in each region. Retrieve user preferences from a DynamoDB table and leverage SQS to capture changes to user preferences with SQS workers for propagating DynamoDB updates.

Note:http://media.amazonwebservices.com/architecturecenter/AWS\_ac\_ra\_mediasharing\_09.pdf  
http://media.amazonwebservices.com/architecturecenter/AWS\_ac\_ra\_adserving\_06.pdf

1. You are responsible for a legacy web application whose server environment is approaching end of life. You would like to migrate this application to AWS as quickly as possible, since the application environment currently as the following limitations:

– the VM’s single 10GB VMDK is almost full;

– the virtual network Interface still uses the 10Mbps dnver, which

leaves your 100Mbps WAN connection completely underutilized;

– it is currently running on a highly customized, Windows VM within a

VMware environment; ?you do not have the installation media. This is a mission critical application with an RTO (Recovery Time Objective) of 8 hours, RPO (Recovery Point Objective) of 1 hour. How could you best migrate this application to AWS while meeting your business continuity requirements?

1. Use S3 to create a backup of the VM and restore the data into EC2.
2. Use the EC2 VM Import Connector for vCenter to import the VM into EC2.
3. Use the ec2-bundle-instance API to import an image of the VM into EC2.
4. Use Import/Export to import the VM as an EBS snapshot and attach to EC2.
5. You are running a news website in the eu-west-1 region that updates every 15 minutes. The website has a world-wide audience. It uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database. Static content resides on Amazon S3, and is distributed through Amazon CloudFront. Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization.

You use an Amazon RDS extra large DB instance with 10,000 Provisioned IOPS, its CPU utilization is around 80%, while freeable memory is in the 2 GB range. web analytics reports show that the average load time of your web pages is around 1.5 to 2 seconds, but your SEO consultant wants to bring down the average load time to under 0.5 seconds. How would you Improve page load times for your users? Choose 3 answers

1. Configure Amazon CloudFront dynamic content support to enable caching of re-usable content from your site.
2. Set up a second installation in another region, and use the Amazon Route 53 latency-based routing feature to select the right region.
3. Lower the scale up trigger of your Auto Scaling group to 30% so it scales more aggressively.
4. Add an Amazon ElastiCache caching layer to your application for storing sessions and frequent DB queries.
5. Switch the Amazon RDS database to the high memory extra large instance type.
6. To serve Web traffic for a popular product, your chief financial officer and IT director have purchased 10 m1.large heavy utilization Reserved Instances (RIs), evenly spread across two availability zones; Route 53 is used to deliver the traffic to an Elastic Load Balancer (ELB). After several months, the product grows even more popular and you need additional capacity. As a result, your company purchases two c3.2xlarge medium utilization RIs. You register the two c3.2xlarge instances with your ELB and quickly find that the m1.large instances are at 100% of capacity and the c3.2xlarge instances have significant capacity that’s unused. Which option is the most cost effective and uses EC2 capacity most effectively?
7. Configure Auto scaling group and Launch Configuration with ELB to add up to 10 more on demand m1.large instances when triggered by Cloudwatch. Shut off c3.2xlarge instances.
8. Configure ELB with two c3.2xlarge instances and use on-demand Auto scaling group for up to two additional c3.2xlarge instances. Shut off m1.large instances.
9. Route traffic to EC2 m1.large and c3.2xlarge instances directly using Route 53 latency based routing and health checks. Shut off ELB.
10. Use a separate ELB for each instance type and distribute load to ELBs with Route 53 weighted round robin.
11. A company is running a batch analysis every hour on their main transactional DB. running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift During the execution of the batch their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required The on-premises system cannot be modified because is managed by another team. How would you optimize this scenario to solve performance issues and automate the process as much as possible?
12. Replace RDS with Redshift for the batch analysis and SNS to notify the on-premises system to update the dashboard
13. Replace ROS with Redshift for the oaten analysis and SQS to send a message to the on premises system to update the dashboard
14. Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard
15. Create an RDS Read Replica for the batch analysis and SQS to send a message to the on premises system to update the dashboard.
16. You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTP/S connections to specific domains from their EC2-hosted applications. You deploy a single EC2 instance running proxy software and configure it to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration. You have a nightly maintenance window of 10 minutes where all instances fetch new software updates. Each update is about 200MB in size and there are 500 instances in the VPC that routinely fetch updates. After a few days you notice that some machines are falling to successfully download some, but not all, of their updates within the maintenance window. The download URLs used for these updates are correctly listed in the proxy’s whitelist configuration and you are able to access them manually using a web browser on the instances. What might be happening? Choose 2 answers
17. You are running the proxy on an undersized EC2 instance type so network throughput is not sufficient for all instances to download their updates in time
18. You are running the proxy on a sufficiently-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance
19. The route table for the subnets containing the affected EC2 instances is not configured to direct network traffic for the software update locations to the proxy
20. You have not allocated enough storage to the EC2 instance running the proxy so the network buffer is filling up, causing some requests to fail
21. You are running the proxy in a public subnet but have not allocated enough EIPs to support the needed network throughput through the Internet Gateway (IGW)
22. You have a periodic image analysis application that gets some files in input, analyzes them and for each file writes some data in output to a text file. The number of files in input per day is high and concentrated in a few hours of the day. Currently you have a server on EC2 with a large EBS volume that hosts the input data and the results. It takes almost 20 hours per day to complete the process. What services could be used to reduce the elaboration time and improve the availability of the solution?
23. S3 to store I/O files, SQS to distribute elaboration commands to a group of hosts working in parallel, Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue.
24. S3 to store I/O files, SNS to distribute elaboration commands to a group of hosts working in parallel, Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications.
25. EBS with Provisioned IOPS (PIOPS) to store I/O files, SNS to distribute elaboration commands to a group of hosts working in parallel, Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications.
26. EBS with Provisioned IOPS (PIOPS) to store I/O files, SQS to distribute elaboration commands to a group of hosts working in parallel. Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue.
27. A large real-estate brokerage is exploring the option of adding a cost-effective location based alert to their existing mobile application. The application backend infrastructure currently runs on AWS. Users who opt in to this service will receive alerts on their mobile device regarding realestate offers in proximity to their location. For the alerts to be relevant delivery time needs to be in the low minute count. The existing mobile app has 5 million users across the US. Which one of the following architectural suggestions would you make to the customer?
28. The mobile application will send device location using SQS, EC2 instances will retrieve the relevant offers from DynamoDB. AWS Mobile Push will be used to send offers to the mobile application.
29. Use AWS DirectConnect or VPN to establish connectivity with mobile carriers. EC2 instances will receive the mobile applications location through earner connection; RDS will be used to store and retrieve relevant offers.
30. EC2 instances will communicate with mobile carriers to push alerts back to the mobile application.
31. The mobile application will submit its location to a web service endpoint utilizing Elastic Load Balancing and C2 instances; DynamoDB will be used to store and retrieve relevant offers. EC2 instances will communicate with mobile carriers/device providers to push alerts back to mobile application.
32. The mobile application will send device location using AWS Mobile Push, EC2 instances will retrieve the relevant offers from DynamoDB. EC2 instances will communicate with mobile carriers/device providers to push alerts back to the mobile application.
33. You require the ability to analyze a customer’s clickstream data on a website, so they can do behavioral analysis. Your customer needs to know what sequence of pages and ads their customer clicked on. This data will be used in real time to modify the page layouts as customers dick through the site, to increase stickiness and advertising click-through. Which option meets the requirements for capturing and analyzing this data?
34. Log dicks in weblogs by URL, store to Amazon S3, and then analyze with Elastic MapReduce.
35. Publish web clicks by session to an Amazon SQS queue; then periodically drain these events to Amazon RDS and analyze with SQL.
36. Push web clicks by session to Amazon Kinesis, then analyze behavior using Kinesis workers.
37. Write click events directly to Amazon Redshift, and then analyze with SQL.
38. An AWS customer runs a public blogging website. The site users upload two million blog entries a month. The average blog entry size is 200 KB. The access rate to blog entries drops to negligible 6 months after publication and users rarely access a blog entry 1 year after publication. Additionally, blog entries have a high update rate during the first 3 months following publication, this drops to no updates after 6 months. The customer wants to use CloudFront to improve his user’s load times. Which of the following recommendations would you make to the customer?
39. Duplicate entries into two different buckets and create two separate CloudFront distributions where S3 access is restricted only to CloudFront identity.
40. Create a CloudFront distribution with “US/Europe” price class for US/Europe users and a different CloudFront distribution with “All Edge Locations” for the remaining users.
41. Create a CloudFront distribution with Restrict Viewer Access, Forward Query String set to true and minimum TTL of 0.
42. Create a CloudFront distribution with S3 access restricted only to the CloudFront identity and partition the blog entry’s location in S3 according to the month it was uploaded to be used with CloudFront behaviors.
43. Your company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with an Multi-AZ RDS MySQL Extra Large DB Instance backend. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests you discover that there is read contention on RDS MySQL. Which are the best approaches to meet these requirements? Choose 2 answers
44. Add an RDS MySQL read replica in each availability zone.
45. Deploy ElastiCache in-memory cache running in each availability zone.
46. Increase the RDS MySQL instance size and implement provisioned IOPS.
47. Implement sharding to distribute load to multiple RDS MySQL Instances.
48. A read only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically. What AWS services should be used meet these requirements?
49. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch, and RDS with read replicas
50. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch, and multi-AZ RDS
51. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch, and RDS with read replicas
52. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch, and multi-AZ RDS
53. Your company has an on-premises, multi-tier PHP web application, which recently experienced downtime due to a large burst in web traffic due to a company announcement. Over the coming days, you’re expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructures ability to handle unexpected increases in traffic. The application currently consists of 2 tiers: A web tier, which consists of a load balancer and several Linux Apache web servers, as well as a database tier, which hosts a Linux server hosting a MySQL database. Which scenario below will provide full site functionality, while helping to improve the availability of your application in the short timeframe required?
54. Failover environment: Create an S3 bucket and configure it for website hosting. Migrate your DNS to Route53 using zone file import, and leverage Route53 DNS failover to failover to the S3 hosted website.
55. Hybrid environment: Create an AMI, which can be used to launch web servers in EC2. Create an Auto Scaling group, which uses the AMI to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted In AWS.
56. Offload traffic from on-premises environment: Setup a CIoudFront distribution, and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behavior, and select a TTL that objects should exist in cache.
57. Migrate to AWS: Use VM Import/Export to quickly convert an on-premises web server to an AMI. Create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic. Create an RDS read replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.
58. Your team has a tomcat-based java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC. The optimal setup for persistence and security that meets the above requirements would be the following:
59. Create your RDS instance separately and add its IP address to your application’s DB connection strings in your code. Alter its security group to allow access to it from hosts within your VPC’s IP address block.
60. Create your RDS instance separately and pass its DNS name to your’s DB connection string as an environment variable. Alter its security group to allow access to it from hosts in your application subnets.
61. Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets.
62. Create your RDS instance separately and pass its DNS name to your app’s DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.
63. A web-startup runs its very successful social news application on Amazon EC2 with an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application-servers, and DynamoDB as data store. The main web-application best runs on m2.xlarge instances since it is highly memorybound. Each new deployment requires semi-automated creation and testing of a new AMI for the application servers, which takes quite a while and is therefore only done once per week. Recently, a new chat feature has been implemented in node.js and waits to be integrated in the

architecture. First tests show that the new component is CPU bound. Because the company has some experience with using Chef, they decided to streamline the deployment process and use AWS OpsWorks as an application life cycle tool to simplify management of the application and reduce the deployment cycles. What configuration in AWS OpsWorks is necessary to integrate the new chat module in the most cost-efficient and flexible way?

1. Create one AWS OpsWorks stack, create one AWS OpsWorks layer, create one custom recipe
2. Create two AWS OpsWorks stacks, create two AWS OpsWorks layers, create one custom recipe
3. Create one AWS OpsWorks stack, create two AWS OpsWorks layers, create one custom recipe
4. Create two AWS OpsWorks stacks, create two AWS OpsWorks layers, create two custom recipes
5. Your customer is willing to consolidate their log streams (access logs, application logs, security logs, etc.) in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours. What is the best approach to meet your customer’s requirements?
6. Configure Amazon CloudTrail to receive custom logs, use EMR to apply heuristics the logs
7. Send all the log events to Amazon SQS, setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics
8. Setup an Auto Scaling group of EC2 syslogd servers, store the logs on S3, use EMR to apply heuristics on the logs
9. Send all the log events to Amazon Kinesis, develop a client process to apply heuristics on the logs
10. If I write the below command, what does it do? ec2-run ami-e3a5408a -n 20 -g appserver
11. Start twenty instances as members of appserver group.
12. Creates 20 rules in the security group named appserver
13. Terminate twenty instances as members of appserver group.
14. Start 20 security groups
15. When you resize the Amazon RDS DB instance, Amazon RDS will perform the upgrade during the next maintenance window. If you want the upgrade to be performed now, rather than waiting for the maintenance window, specify the \_\_\_\_\_ option.
16. ApplyNow
17. ApplySoon
18. ApplyThis
19. ApplyImmediately
20. What is the name of licensing model in which I can use your existing Oracle Database licenses to run Oracle deployments on Amazon RDS?
21. Bring Your Own License
22. Role Bases License
23. Enterprise License
24. License Included
25. You are implementing AWS Direct Connect. You intend to use AWS public service endpoints, such as Amazon S3, across the AWS Direct Connect link. You want other Internet traffic to use your existing link to an Internet Service Provider. What is the correct way to configure AWS Direct Connect for access to services such as Amazon S3?
26. Create a public interface on your AWS Direct Connect link. Redistribute BGP routes into your existing routing infrastructure; advertise specific routes for your network to AWS.
27. Create a private interface on your AWS Direct Connect link. Redistribute BGP routes into your existing routing infrastructure and advertise a default route to AWS.
28. Create a private interface on your AWS Direct Connect link. Configure a static route via your AWS Direct Connect link that points to Amazon S3. Configure specific routes to your network in your VPC.
29. Configure a public interface on your AWS Direct Connect link. Configure a static route via your AWS Direct Connect link that points to Amazon S3. Advertise a default route to AWS using BGP.
30. Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using this new connection. After configuring Direct Connect settings in the AWS Console, which of the following options will provide the most seamless transition for your users?
31. Configure your Direct Connect router, update your VPC route tables to point to the Direct Connect connection, configure your VPN connection with a higher BGP priority, and verify network traffic is leveraging the Direct Connect connection.
32. Delete your existing VPN connection to avoid routing loops, configure your DirectConnect router with the appropriate settings, and verify network traffic is leveraging DirectConnect.
33. Update your VPC route tables to point to the DirectConnect connection, configure your DirectConnect router with the appropriate settings, verify network traffic is leveraging DirectConnect, and then delete the VPN connection.
34. Configure your DirectConnect router with a higher BGP priority than your VPN router, verify network traffic is leveraging DirectConnect, and then delete your existing VPN connection.
35. You have deployed a three-tier web application in a VPC with a CIDR block of 10.0.0.0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance for a total of seven EC2 instances. The web, application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS. Web traffic gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load. Unfortunately some of these new Instances fall to launch. Which of the following could be the root cause? Choose 2 answers
36. AWS reserves the first and the last private IP address in each subnet’s CIDR block so you do not have enough addresses left to launch all of the new EC2 instances
37. The Internet Gateway (IGW) of your VPC has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
38. The ELB has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
39. AWS reserves one IP address in each subnet’s CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances
40. AWS reserves the first four and the last IP address in each subnet’s CIDR block so you do not have enough addresses left to launch all of the new EC2 instances
41. A customer has established an AWS Direct Connect connection to AWS. The link is up and routes are being advertised from the customer’s end; however the customer is unable to connect from EC2 instances inside its VPC to servers residing in its datacenter. Which of the following options provide a viable solution to remedy this situation? Choose 2 answers
42. Modify the instances VPC subnet route table by adding a route back to the customer’s on premises environment.
43. Enable route propagation to the customer gateway (CGW).
44. Add a route to the route table with an IPsec VPN connection as the target.
45. Enable route propagation to the virtual private gateway (VGW).
46. Modify the route table of all instances using the route’ command.
47. You are designing Internet connectivity for your VPC. The Web servers must be available on the Internet. The application must have a highly available architecture. Which alternatives should you consider? Choose 2 answers
48. Assign EIPs to all Web servers. Configure a Route53 record set with all EIPs, with health checks and DNS failover.
49. Configure a NAT instance in your VPC. Create a default route via the NAT Instance and associate it with all subnets. Configure a DNS A record that points to the NAT Instance public IP address.
50. Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
51. Place all your Web servers behind ELB. Configure a Route53 CNAME to point to the ELB DNS name.
52. Configure ELB with an EIP. Place all your Web servers behind ELB. Configure a Route53 A record that points to the EIP.
53. A newspaper organization has a on-premises application which allows the public to search Its back catalogue and retrieve individual newspaper pages via a website written in Java. They have scanned the old newspapers into JPEGs (approx. 17TB) and used Optical Character Recognition (OCR) to populate a commercial search product. The hosting platform and software are now end of life and the organization wants to migrate its archive to AWS and produce a cost efficient architecture and still be designed for availability and durability. Which is the most appropriate?
54. Model the environment using CloudFormation, use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index
55. Use a single-AZ RDS MySQL instance to store the search index and the JPEG Images, use an EC2 Instance to serve the website and translate user queries into SQL
56. Use a CloudFront download distribution to serve the JPEGs to the end users and install the current commercial search product, along with a Java Container for the website on EC2 instances and use Route53 with DNS round-robin
57. Use S3 with standard redundancy to store and serve the scanned files, use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones
58. Use S3 with reduced redundancy to store and serve the scanned files, install the commercial search application on EC2 instances and configure with auto-scaling and an Elastic Load Balancer
59. Your company produces customer commissioned one-of-a-kind skiing helmets, combining high fashion with custom technical enhancements. Customers can show off their individuality on the ski slopes and have access to head-up-displays, GPS, rear-view cams and any other technical Innovation they wish to embed in the helmet.The current manufacturing process is data rich and complex, including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards. Assessments are a mixture of human and automated assessments. You need to add a new set of assessment to model the failure modes of the custom electronics using GPUs with CUDA, across a cluster of servers with low latency networking. What architecture would allow you to automate the existing process using a hybrid approach, and ensure that the architecture can support the evolution of processes over time.
60. Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an auto-scaling group of G2 instances in a placement group.
61. Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an auto-scaling group of C3 instances with SR-IOV (Single Root I/O Visualization).
62. Use AWS Data Pipeline to manage movement of data & meta-data and assessments. Use auto-scaling group of C3 with SR-IOV (Single Root I/O Visualization).
63. Use AWS Data Pipeline to manage movement of data & meta-data and assessments. Use an auto- scaling group of G2 instances in a placement group.
64. You are migrating a legacy client-server application to AWS. The application responds to a specific DNS domain (e.g. www.example.com) and has a 2-tier architecture, with multiple application servers and a database server. Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket. A Multi-AZ RDS MySQL instance will be used for the database. During the migration you can change the application code, but you have to file a change request. How would you implement the architecture on AWS in order to maximize scalability and high availability?
65. File a change request to implement Alias Resource support in the application. Use Route 53 Alias Resource Record to distribute load on two application servers in different AZs.
66. File a change request to implement Latency Based Routing support in the application. Use Route 53 with Latency Based Routing enabled to distribute load on two application servers in different AZs.
67. File a change request to implement Cross-Zone support in the application. Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
68. File a change request to implement Proxy Protocol support in the application. Use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.
69. You are looking to migrate your Development (Dev) and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each account’s bill to a Master AWS account using Consolidated Billing. To make sure you keep within budget you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which option will allow you to achieve this goal.
70. Create IAM users in the Master account with full Admin permissions. Create cross-account roles in the Dev and Test accounts that grant the Master account access to the resources in the account by inheriting permissions from the Master account.
71. Create IAM users and a cross-account role in the Master account that grants full Admin permissions to the Dev and Test accounts.
72. Link the accounts using Consolidated Billing.This will give IAM Users in the Master account access to resources in the Dev and Test accounts.
73. Create IAM users in the Master account. Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access.
74. An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 instances.

The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique X.509 certificate that contains the specific Instance-id. In addition, all X.509 certificates must be signed by the customer’s key management service in order to be trusted for authentication. Which of the following configurations will support these requirements:

1. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure the Auto Scaling group to launch instances with this role. Have the instances bootstrap get the certificate from Amazon S3 upon first boot.
2. Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the key management service generate a signed certificate and send it directly to the newly launched instance.
3. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group. Have the launched instances generate a certificate signature request with the Instance’s assigned instance-id to the key management service for signature.
4. Configure the launched instances to generate a new certificate upon first boot. Have the key management service poll the AutoScaling group for associated instances and send new instances a certificate signature that contains the specific Instance-id.
5. What is the maximum write throughput I can provision for a single Dynamic DB table?
6. 1,000 write capacity units
7. 100,000 write capacity units
8. Dynamic DB is designed to scale without limits, but if you go beyond 10,000 you have to contact AWS first.
9. 10,000 write capacity units
10. An administrator is using Amazon CloudFormation to deploy a three tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage. When creating the CloudFormation template which of the following would allow the application Instance access to the DynamoDB tables without exposing API credentials?
11. Create an Identity and Access Management Role that has the required permissions to read and write from the .required DynamoDB table and associate the Role to the application instances by referencing an instance profile.
12. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance.
13. Use the Parameter section in the CloudFormation template to have the user input Access and Secret keys from an already created IAM user that has the permissions required to read and write from the required DynamoDB table.
14. Create an Identity and Access Management user in the CloudFormation template that has permissions to read and write from the required DynamoDB table, use the GetAtt function to retrieve the Access and Secret keys and pass them to the application instance through user-data.
15. Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware. The outcome was that all employees would be granted access to use Amazon S3 for storage of their personal documents. Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a

designated user folder in a bucket? Choose 3 answers

1. Using AWS Security Token Service to generate temporary tokens.
2. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket.
3. Tagging each folder in the bucket.
4. Configuring an IAM role.
5. Setting up a federation proxy or identity provider.
6. Your company has recently extended its datacenter into a VPC on AWS to add burst computing capacity as needed. Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary. You don’t want to create new IAM users for each NOC member and make those users sign in again to the AWS Management Console. Which option below will meet the needs for your NOC members?
7. Use your on-premises SAML 2.0-compliant identity provider (IdP) to grant the NOC members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.
8. Use Web Identity Federation to retrieve AWS temporary security credentials to enable your NOC members to sign in to the AWS Management Console.
9. Use your on-premises SAML 2.0-compllant identity provider (IdP) to retrieve temporary security credentials to enable NOC members to sign in to the AWS Management Console.
10. Use OAuth 2.0 to retrieve temporary AWS security credentials to enable your NOC members to sign in to the AWS Management Console.
11. You’ve been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected, multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3. They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access. Which approach provides a cost effective, scalable mitigation to this kind of attack?
12. Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC. They would then establish Internet connectivity into their space, filter the traffic in a hardware Web Application Firewall (WAF), and then pass the traffic through the DirectConnect connection into their application running in their VPC.
13. Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
14. Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would then pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group.
15. Remove all but TLS 1.2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.
16. You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient. Which of the following options would you consider for configuring the Web server infrastructure?Choose 2 answers
17. Configure your Web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution.
18. Configure ELB with TCP listeners on TCP/443, and place the Web servers behind it.
19. Configure your Web servers with EIPs. Place the Web servers in a Route53 Record Set, and configure health checks against all Web servers.
20. Configure ELB with HTTPS listeners, and place the Web servers behind it.
21. A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload for the new fiscal year benefit enrollment period plus some extra overhead. Enrollment proceeds nicely for a few days and then the web tier becomes unresponsive. Upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrollment administrators cannot even SSH into them. Which activity would be useful in defending against this attack?
22. Change the EIP (Elastic IP Address) of the NAT instance in the Web tier subnet and update the Main Route Table with the new EIP
23. Create 15 Security Group rules to block the attacking IP addresses over port 80
24. Create a custom route table associated with the Web tier and block the attacking IP addresses from the IGW (Internet Gateway)
25. Create an inbound NACL (Network Access Control List) associated with the Web tier subnet with deny rules to block the attacking IP addresses
26. You have an application running on an EC2 instance which will allow users to download files from a private S3 bucket using a pre-signed URL. Before generating the URL, the application should verify the existence of the file in S3. How should the application use AWS credentials to access the S3 bucket securely?
27. Use the AWS account access keys; the application retrieves the credentials from the source code of the application.
28. Create an IAM role for EC2 that allows list access to objects In the S3 bucket; launch the Instance with the role, and retrieve the role’s credentials from the EC2 instance metadata.
29. Create an IAM user for the application with permissions that allow list access to the S3 bucket; the application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the Application user.
30. Create an IAM user for the application with permissions that allow list access to the S3 bucket; launch the instance as the IAM user, and retrieve the IAM user’s credentials from the EC2 instance user data.
31. You currently operate a web application in the AWS US-East region. The application runs on an auto- scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM, and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?
32. Create a new CloudTrail trail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
33. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
34. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies, and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
35. Create three new CloudTrail trails with three new S3 buckets to store the logs: one for the AWS Management Console, one for AWS SDKs, and one for command line tools. Use 1AM roles and S3 bucket policies on the S3 buckets that store your logs.
36. You are designing a social media site and are considering how to mitigate distributed denial-ofservice (DDoS) attacks. Which of the below are viable mitigation techniques? Choose 3 answers
37. Use Dedicated Instances to ensure that each Instance has the maximum performance possible.
38. Add alerts to Amazon CloudWatch to look for high Network In and CPU utilization.
39. Create processes and capabilities to quickly add and remove rules to the instance OS firewall.
40. Use an Elastic Load Balancer with auto scaling groups at the web, app, and Amazon Relational Database Service (RDS) tiers.
41. Use an Amazon CloudFront distribution for both static and dynamic content.
42. Add multiple elastic network Interfaces (ENIs) to each EC2 instance to Increase the network bandwidth.
43. You are designing a photo-sharing mobile app. The application will store all pictures in a single Amazon S3 bucket. Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3. You want to configure security to handle potentially millions of users in the most secure manner possible. What should your server-side application do when a new user registers on the photo sharing mobile application?
44. Create an IAM user. Update the bucket policy with appropriate permissions for the IAM user. Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
45. Create an IAM user. Assign appropriate permissions to the IAM user. Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
46. Create a set of long-term credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app and use them to access Amazon S3.
47. Record the user’s information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app, create temporary credentials using the AWS Security Token Service “AssumeRole” function. Store these credentials in the mobile app’s memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
48. Record the user’s information in Amazon DynamoDB. When the user uses their mobile app, create temporary credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app’s memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
49. Your company policies require encryption of sensitive data at rest. you are considering the possible options or protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance. Which of these options would allow you to encrypt your data at rest? Choose 3 answers
50. Implement third party volume encryption tools
51. Implement SSL/TLS for all services running on the server
52. Encrypt data inside your applications before storing it on EBS
53. Encrypt data using native data encryption drivers at the file system level
54. Do nothing as EBS volumes are encrypted by default
55. An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise’s account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege, and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions:
56. Create an IAM role for cross-account access, allow the SaaS provider’s account to assume the role, and assign it a policy that allows only the actions required by the SaaS application.
57. From the AWS Management Console navigate to the Security Credentials page and retrieve the access and secret key for your account.
58. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider to use when launching their application instances.
59. Create an IAM user within the enterprise account, assign a user policy to the IAM user that allows only the actions required by the SaaS application, create a new access and secret key for the user and provide these credentials to the SaaS provider.
60. You are designing an intrusion detection/prevention (IDS/IPS) solution for a customer web application in a single VPC. You are considering the options for Implementing IDS/IPS protection for traffic coming from the Internet. Which of the following options would you consider? Choose 2 answers
61. Implement IDS/IPS agents on each instance running in VPC.
62. Implement Elastic Load Balancing with SSL listeners in front of the web applications.
63. Implement a reverse proxy layer in front of web servers, and configure IDS/IPS agents on each reverse proxy server.
64. Configure an instance in each subnet to switch its network interface card to promiscuous mode and analyze network traffic.
65. You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your servers on-premises will be communicating with your VPC instances.You will be establishing IPsec tunnels over the Internet.You will be using VPN gateways, and terminating the IPsec tunnels on AWS supported customer

gateways.Which of the following objectives would you achieve by implementing an IPsec tunnel as outlined

above? Choose 4 answers

1. Peer identity authentication between VPN gateway and customer gateway.
2. End-to-end identity authentication.
3. Data integrity protection across the Internet.
4. End-to-end protection of data in transit.
5. Data encryption across the Internet.
6. Protection of data in transit over the Internet.
7. You are tasked with moving a legacy application from a virtual machine running inside your datacenter to an Amazon VPC. Unfortunately, this app requires access to a number of onpremises services and no one who configured the app still works for your company. Even worse, there’s no documentation for it. What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured? Choose 3 answers
8. A VM Import of the current virtual machine
9. An Internet Gateway to allow a VPN connection
10. Entries in Amazon Route 53 that allow the Instance to resolve its dependencies’ IP addresses
11. An IP address space that does not conflict with the one on-premises
12. An Elastic IP address on the VPC instance
13. An AWS Direct Connect link between the VPC and the network housing the internal services
14. You are designing a multi-platform web application for AWS. The application will run on EC2 instances and will be accessed from PCs, tablets and smart phones, supported accessing platforms are Windows, MacOS, IOS and Android. Separate sticky session and SSL certificate setups are required for different platform types. Which of the following describes the most cost effective and performance efficient architecture setup?
15. Setup a hybrid architecture to handle session state and SSL certificates on-prem and separate EC2 Instance groups running web applications for different platform types running in a VPC.
16. Set up one ELB for all platforms to distribute load among multiple instance under it. Each EC2 instance implements all functionality for a particular platform.
17. Assign multiple ELBs to an EC2 Instance or group of EC2 instances running the common components of the web application. One ELB for each platform type. Session stickiness and SSL termination are done at the ELBs.
18. Set up two ELBs. The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms. For each ELB, run separate EC2 instance groups to handle the web application for each platform.
19. A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC), and is connected to the corporate data center via an IPsec VPN. The application must authenticate against the on- premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user. Which two approaches can satisfy these objectives? Choose 2 answers
20. The application authenticates against IAM Security Token Service using the LDAP credentials. The application uses those temporary AWS security credentials to access the appropriate S3 bucket.
21. Develop an identity broker that authenticates against LDAP, and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the Identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
22. The application authenticates against LDAP, and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket.
23. The application authenticates against LDAP. The application then calls the AWS Identity and Access Management (IAM) Security Service to log in to IAM using the LDAP credentials. The application can use the IAM temporary credentials to access the appropriate S3 bucket.
24. Develop an identity broker that authenticates against IAM Security Token Service to assume an IAM role in order to get temporary AWS security credentials. The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.
25. You’re running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible, block-based storage. You have 140TB of data and would like to mount it as a single folder on your file server. Users must be able to access portions of this data while the backups are taking place. What backup solution would be most appropriate for this use case?
26. Use Storage Gateway and configure it to use Gateway Cached volumes
27. Use Storage Gateway and configure it to use Gateway Stored volumes
28. Configure your backup software to use S3 as the target for your data backups
29. Configure your backup software to use Glacier as the target for your data backups
30. Your firm has uploaded a large amount of aerial image data to S3. In the past, in your onpremises environment, you used a dedicated group of servers to batch process this data and used RabbitMQ, an open source messaging system, to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which is correct?
31. Use SNS to pass job messages, use CloudWatch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.
32. Use SQS for passing job messages, use CloudWatch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
33. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
34. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS.Once data is processed, change the storage class of the S3 objects to Glacier
35. You are running a successful multitier web application on AWS and your marketing department has asked you to add a reporting tier to the application. The reporting tier will aggregate and publish status reports every 30 minutes from user-generated information that is being stored in your web application’s database. You are currently running a Multi-AZ RDS MySQL instance for the database tier. You also have implemented ElastiCache as a database caching layer between the application tier and database tier. Please select the answer that will allow you to successfully implement the reporting tier with as little impact as possible to your database:
36. Launch a RDS Read Replica connected to your Multi AZ master database and generate reports by querying the Read Replica.
37. Continually send transaction logs from your master database to an S3 bucket and generate the reports off the S3 bucket using S3 byte range requests.
38. Generate the reports by querying the ElastiCache database caching tier.
39. Generate the reports by querying the synchronously replicated standby RDS MySQL instance maintained through Multi-AZ.
40. A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC. How should they architect their solution to achieve these goals?
41. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.
42. Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see all traffic across the VPC.
43. Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.
44. Configure servers running in the VPC using the host-based “route” commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
45. You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic MapReduce Job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO. You recently improved overall performance of the website using CloudFront for dynamic content delivery and your website as the origin. After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude. How do you fix your usage dashboard?
46. Change your log collection process to use CloudWatch ELB metrics as input of the Elastic MapReduce Job.
47. Turn on CloudTrail and use trail log files on S3 as input of the Elastic MapReduce job.
48. Enable CloudFront to deliver access logs to S3 and use them as input of the Elastic MapReduce job.
49. Use Elastic Beanstalk “Restart App Server(s)” option to update log delivery to the Elastic MapReduce job.
50. Use Elastic Beanstalk “Rebuild Environment” option to update log delivery to the ElasticMapReduce job.
51. Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high resolution MP4 format. Your workforce is distributed globally, often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no video transcoding expertise and If required you may need to pay for a consultant. How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery?
52. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2.
53. Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2.
54. Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. S3 to host videos with Lifecycle Management to archive original files to Glacier after a few days. CloudFront to serve HLS transcoded videos from S3.
55. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days. CloudFront to serve HLS transcoded videos from Glacier.
56. Your department creates regular analytics reports from your company’s log files. All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in .csv format for an Amazon Redshift data warehouse. Your CFO requests that you optimize the cost structure for this system. Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data?
57. Use reduced redundancy storage (RRS) for all data In S3. Use a combination of Spot Instances and Reserved Instances for Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
58. Use reduced redundancy storage (RRS) for PDF and .csv data in S3. Add Spot Instances to EMR jobs. Use Spot Instances for Amazon Redshift.
59. Use reduced redundancy storage (RRS) for PDF and .csv data In Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
60. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
61. You are the new IT architect in a company that operates a mobile sleep tracking application. When activated at night, the mobile app is sending collected data points of 1 kilobyte every 5 minutes to your backend. The backend takes care of authenticating the user and writing the data points into an Amazon DynamoDB table.

Every morning, you scan the table to extract and aggregate last night’s data on a per user basis, and store the results in Amazon S3. Users are notified via Amazon SNS mobile push notifications that new data is available, which is parsed and visualized by the mobile app. Currently you have around 100k users who are mostly based out of North America. You have been tasked to optimize the architecture of the backend system to lower cost. What would you recommend? Choose 2 answers

1. Have the mobile app access Amazon DynamoDB directly Instead of JSON files stored on Amazon S3.
2. Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.
3. Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput.
4. Introduce Amazon Elasticache to cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.
5. Create a new Amazon DynamoDB table each day and drop the one for the previous day after its data is on Amazon S3.
6. You require the ability to analyze a large amount of data which is stored on Amazon S3 using Amazon Elastic MapReduce. You are using the cc2.8xlarge instance type, whose CPUs are mostly idle during processing. Which of the below would be the most cost efficient way to reduce the runtime of the job?
7. Create fewer, larger files m Amazon S3.
8. Use smaller instances that have higher aggregate I/O performance.
9. Create more, smaller files on Amazon S3.
10. Add additional cc2.8xlarge instances by introducing a task group.
11. A 3-tier e-commerce web application is currently deployed on-premises, and will be migrated to AWS for greater scalability and elasticity. The web tier currently shares read-only data using a network distributed file system. The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast. The database tier uses shared-storage clustering to provide database failover capability, and uses several read slaves for scaling. Data on all servers and the distributed file system directory is backed up weekly to off-site tapes. Which AWS storage and database architecture meets the requirements of the application?
12. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more read replicas. Backup: web servers, app servers, and database backed up weekly to Glacier using snapshots.
13. Web servers: store read-only data in an EC2 NFS server, mount to each web server at boot time. App servers: share state using a combination of DynamoDB and IP multicast. Database: use RDS with multi- AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
14. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
15. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment. Backup: web and app servers backed up weekly via AMIs, database backed up via DB Snapshots
16. You need a persistent and durable storage to trace call activity of an IVR (Interactive Voice Response) system. Call duration is mostly in the 2-3 minutes timeframe. Each traced call can be either active or terminated. An external application needs to know each minute the list of currently active calls. Usually there are a few calls/second, but once per month there is a periodic peak up to 1000 calls/second for a few hours. The system is open 24/7 and any downtime should be avoided. Historical data is periodically archived to files. Cost saving is a priority for this project.What database implementation would better fit this scenario, keeping costs as low as possible?
17. Use DynamoDB with a “Calls” table and a Global Secondary Index on a “State” attribute that can equal to “active” or “terminated”. In this way the Global Secondary Index can be used for all items in the table.
18. Use RDS Multi-AZ with a “CALLS” table and an indexed “STATE” field that can be equal to “ACTIVE” or ‘TERMINATED”. In this way the SQL query is optimized by the use of the Index.
19. Use RDS Multi-AZ with two tables, one for “ACTIVE\_CALLS” and one for “TERMINATED\_CALLS”. In this way the “ACTIVE\_CALLS” table is always small and effective to access.
20. Use DynamoDB with a “Calls” table and a Global Secondary Index on a “IsActive” attribute that is present for active calls only. In this way the Global Secondary Index is sparse and more effective.
21. Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets. Each collar will push 30kb of biometric data in JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending information back to the pet owners and veterinarians via a web portal. Management has tasked you to architect the collection platform ensuring the following requirements are met:

– Provide the ability for real-time analytics of the inbound biometric data

– Ensure processing of the biometric data is highly durable, elastic and parallel

– The results of the analytic processing should be persisted for data mining

Which architecture outlined below will meet the initial requirements for the collection platform?

1. Utilize Amazon Kinesis to collect the inbound sensor data, analyze the data with Kinesis clients and save the results to a Redshift cluster using EMR.
2. Utilize SQS to collect the inbound sensor data, analyze the data from SQS with Amazon Kinesis and save the results to a Microsoft SQL Server RDS Instance.
3. Utilize S3 to collect the inbound sensor data, analyze the data from S3 with a daily scheduled Data Pipeline and save the results to a Redshift Cluster.
4. Utilize EMR to collect the inbound sensor data, analyze the data from EMR with Amazon Kinesis and save the results to DynamoDB.
5. A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files. They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and keep costs to a minimum. What AWS architecture would you recommend?
6. Ask their customers to use an S3 client instead of an FTP client. Create a single S3 bucket.Create an IAM User for each customer. Put the IAM Users in a Group that has an IAM policy that permits access to sub-directories within the bucket via use of the ‘username’ Policy Variable.
7. Create a single S3 bucket with Requester Pays turned on and ask their customers to use an S3 client instead of an FTP client. Create a bucket for each customer with a Bucket Policy that permits access only to that one customer.
8. Create a single S3 bucket with Reduced Redundancy Storage turned on and ask their customers to use an S3 client instead of an FTP client. Create a bucket for each customer with a Bucket Policy that permits access only to that one customer.
9. Create an auto-scaling group of FTP servers with a scaling policy to automatically scale-in when minimum network traffic on the auto-scaling group is below a given threshold. Load a central list of FTP users from S3 as part of the User Data startup script on each instance.
10. You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months. Each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS. During the pilot, you measured a peak of 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database. The current deployment consists of a load-balanced, auto scaled Ingestion layer using EC2 instances, and a PostgreSQL RDS database with 500GB standard storage The pilot is considered a success and your CEO has managed to get the attention of some potential Investors. The business plan requires a deployment of at least 100k sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year improvements. To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling. Which setup will meet the requirements?
11. Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage
12. Keep the current architecture, but upgrade RDS storage to 3TB and 10k provisioned IOPS
13. Ingest data into a DynamoDB table and move old data to a Redshift cluster
14. Add an SQS queue to the ingestion layer to buffer writes to the RDS Instance
15. Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account. To streamline data capture, Company B would like to directly save player data and scoring information from the mobile app to a DynamoDB table named ScoreData. When a user saves their game, the progress data will be stored to the GameState S3 bucket. What is the best approach for storing data to DynamoDB and S3?
16. Use Login with Amazon allowing users to sign in with an Amazon account providing the mobile app with access to the ScoreData DynamoDB table and the GameState S3 bucket.
17. Use temporary security credentials that assume a role providing access to the ScoreData DynamoDB table and the GameState S3 bucket using web identity federation
18. Use an IAM user with access credentials assigned a role providing access to the ScoreData DynamoDB table and the GameState S3 bucket for distribution with the mobile app
19. Use an EC2 instance that is launched with an EC2 role providing access to the ScoreData DynamoDB table and the GameState S3 bucket that communicates with the mobile app via web Services
20. Your company has HQ in Tokyo and branch offices all over the world and is using a logistics software with a multi-regional deployment on AWS in Japan, Europe and US. The logistic software has a 3-tier architecture and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database. In the HQ region you run an hourly batch process reading data from every region to compute cross- regional reports that are sent by email to all offices. This batch process must be completed as fast as possible to quickly optimize logistics. How do you build the database architecture in order to meet the requirements?
21. For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files hourly to the HQ region.
22. For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS snapshots to the HQ region.
23. Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network latency for the batch process.
24. For each regional deployment, use RDS MySQL with a master in the region and a read replica In the HQ region.
25. For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS snapshots to the HQ region.
26. You have been asked to design the storage layer for an application. The application requires disk performance of at least 100,000 IOPS. In addition, the storage layer must be able to survive the loss of an individual disk, EC2 instance, or Availability Zone without any data loss. The volume you provide must have a capacity of at least 3 TB. Which of the following designs will meet these objectives?
27. Instantiate a c3 8xlarge instance in us-east-1. Provision 4x1TB EBS volumes, attach them to the instance, and configure them as a single RAID 5 volume. Ensure that EBS snapshots are performed every 15 minutes.
28. Instantiate a c3 8xlarge instance in us-east-1. Provision 3xlTB EBS volumes, attach them to the Instance, and configure them as a single RAID 0 volume. Ensure that EBS snapshots are performed every 15 minutes.
29. Instantiate an 12 8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Provision 3x1TB EBS volumes, attach them to the instance, and configure them as a second RAID 0 volume. Configure synchronous, block-level replication from the ephemeral-backed volume to the EBSbacked volume.
30. Instantiate a c3 8xlarge instance in us-east-1. Provision an AWS Storage Gateway and configure it for 3 TB of storage and 100,000 IOPS. Attach the volume to the instance.
31. Instantiate an 12 8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Configure synchronous, block-level replication to an identically configured instance in us-east-1b.
32. Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes.To be certain that you do not drop any writes to a database hosted on AWS, which service should you use?
33. Amazon Simple Queue Service (SQS) for capturing the writes and draining the queue to write to the database.
34. Amazon DynamoDB with provisioned write throughput up to the anticipated peak write throughput.
35. Amazon ElastiCache to store the writes until the writes are committed to the database.
36. Amazon RDS with provisioned IOPS up to the anticipated peak write throughput.
37. A customer has a 10 GB AWS Direct Connect connection to an AWS region where they have a web application hosted on Amazon Elastic Computer Cloud (EC2). The application has dependencies on an on-premises mainframe database that uses a BASE (Baste Available, Soft state, Eventual consistency) rather than an ACID (Atomicity, Consistency, Isolation, Durability) consistency model. The application is exhibiting undesirable behavior because the database is not able to handle the volume of writes. How can you reduce the load on your on-premises database resources in the most cost-effective way?
38. Provision an RDS read-replica database on AWS to handle the writes and synchronize the two databases using Data Pipeline.
39. Modify the application to use DynamoDB to feed an EMR cluster which uses a map function to write to the on-premises database.
40. Modify the application to write to an Amazon SQS queue and develop a worker process to flush the queue to the on-premises database.
41. Use an Amazon Elastic Map Reduce (EMR) S3DistCp as a synchronization mechanism between the on- premises database and a Hadoop cluster on AWS.
42. You have launched an EC2 instance with four (4) 500 GB EBS Provisioned IOPS volumes attached. The EC2 instance is EBS-Optimized and supports 500 Mbps throughput between EC2 and EBS. The four EBS volumes are configured as a single RAID 0 device, and each Provisioned IOPS volume is provisioned with 4,000 IOPS (4,000 16KB reads or writes), for a total of 16,000 random IOPS on the instance. The EC2 instance initially delivers the expected 16,000 IOPS random read and write performance. Sometime later, in order to increase the total random I/O performance of the instance, you add an additional two 500 GB EBS Provisioned IOPS volumes to the RAID. Each volume is provisioned to 4,000 IOPs like the original four, for a total of 24,000 IOPS on the EC2 instance. Monitoring shows that the EC2 instance CPU utilization increased from 50% to 70%, but the total random IOPS measured at the instance level does not increase at all. What is the problem and a valid solution?
43. The EBS-Optimized throughput limits the total IOPS that can be utilized; use an EBS-Optimized instance that provides larger throughput.
44. Small block sizes cause performance degradation, limiting the I/O throughput; configure the instance device driver and filesystem to use 64KB blocks to increase throughput.
45. The standard EBS Instance root volume limits the total IOPS rate; change the instance root volume to also be a 500GB 4,000 Provisioned IOPS volume.
46. Larger storage volumes support higher Provisioned IOPS rates; increase the provisioned volume storage of each of the 6 EBS volumes to 1TB.
47. RAID 0 only scales linearly to about 4 devices; use RAID 0 with 4 EBS Provisioned IOPS volumes, but increase each Provisioned IOPS EBS volume to 6,000 IOPS.
48. Your customer wishes to deploy an enterprise application to AWS, which will consist of several web servers, several application servers, and a small (50GB) Oracle database. Information is stored both in the database and the filesystems of the various servers. The backup system must support database recovery, whole server and whole disk restores, and individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database. Which backup architecture will meet these requirements?
49. Backup RDS using automated daily DB backups. Backup the EC2 Instances using AMIs, and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore.
50. Backup RDS database to S3 using Oracle RMAN. Backup the EC2 instances using AMIs, and supplement with EBS snapshots for individual volume restore.
51. Backup RDS using a Multi-AZ Deployment. Backup the EC2 instances using AMIs, and supplement by copying filesystem data to S3 to provide file level restore.
52. Backup RDS using automated daily DB backups. Backup the EC2 instances using EBS snapshots, and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore.
53. Your system recently experienced down time. During the troubleshooting process, you found that a new administrator mistakenly terminated several production EC2 instances. Which of the following strategies will help prevent a similar situation in the future? The administrator still must be able to:

– launch, start, stop, and terminate development resources,

– launch and start production instances.

1. Leverage EC2 termination protection and multi-factor authentication, which together require users to authenticate before terminating EC2 instances.
2. Leverage resource based tagging, along with an IAM user which can prevent specific users from terminating production EC2 resources.
3. Create an IAM user which is not allowed to terminate instances by leveraging production EC2 termination protection.
4. Create an IAM user and apply an IAM role which prevents users from terminating production EC2 instances.
5. Refer to the architecture diagram above of a batch processing solution using Simple Queue Service (SQS) to set up a message queue between EC2 instances which are used as batch processors. CloudWatch monitors the number of job requests (queued messages) and an Auto Scaling group adds or deletes batch servers automatically based on parameters set in CloudWatch alarms. You can use this architecture to implement which of the following features in a cost effective and efficient manner?
6. Coordinate number of EC2 instances with number of Job requests automatically, thus improving cost effectiveness.
7. Reduce the overall time for executing Jobs through parallel processing by allowing a busy EC2 instance that receives a message to pass it to the next instance in a daisy-chain setup.
8. Implement fault tolerance against EC2 instance failure since messages would remain in SQS and work can continue with recovery of EC2 instances. Implement fault tolerance against SQS failure by backing up messages to S3.
9. Handle high priority Jobs before lower priority Jobs by assigning a priority metadata field to SQS messages.
10. Implement message passing between EC2 instances within a batch by exchanging messages through SQS.
11. An ERP application is deployed across multiple AZs in a single region. In the event of failure, the Recovery Time Objective (RTO) must be less than 3 hours, and the Recovery Point Objective(RPO) must be 15 minutes. The customer realizes that data corruption occurred roughly 1.5 hours ago. What DR strategy could be used to achieve this RTO and RPO in the event of this kind of failure?
12. Take 15 minute DB backups stored in Glacier with transaction logs stored in S3 every 5 minutes.
13. Use synchronous database master-slave replication between two availability zones.
14. Take hourly DB backups to EC2 instance store volumes with transaction logs stored In S3 every 5 minutes.
15. Take hourly DB backups to S3, with transaction logs stored in S3 every 5 minutes.
16. Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence. The database CPU is often above 80% usage and 90% of I/O operations on the database are reads. To improve performance you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results. In the next weeks the overall workload is expected to grow by 30%. Do you need to change anything in the architecture to maintain the high availability of the application with the anticipated additional load? Why?
17. Yes, you should deploy two Memcached ElastiCache Clusters in different AZs because the RDS instance will not be able to handle the load if the cache node fails.
18. No, if the cache node fails you can always get the same data from the DB without having any availability impact.
19. No, if the cache node fails the automated ElastiCache node recovery feature will prevent any availability impact.
20. Yes, you should deploy the Memcached ElastiCache Cluster with two nodes in the same AZ as the RDS DB master instance to handle the load if one cache node fails.
21. Your company runs a customer facing event registration site. This site is built with a 3-tier architecture with web and application tier servers and a MySQL database. The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs), which architecture provides high availability?
22. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each A2 inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 3 EC2 instances In each AZ inside an Auto Scaling Group behind an ELB, and one RDS (Relational Database Service) instance deployed with read replicas in the other AZ.
23. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 3 AZs with 2 EC2 instances In each AZ inside an Auto Scaling Group behind an ELB, and a Multi-AZ RDS (Relational Database Service) deployment.
24. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 3 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB, and a Multi-AZ RDS (Relational Database Service) deployment
25. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB, and one RDS (Relational Database Service) instance deployed with read replicas in the two other AZs.
26. Your startup wants to implement an order fulfillment process for selling a personalized gadget that needs an average of 3-4 days to produce with some orders taking up to 6 months.You expect 10 orders per day on your first day, 1000 orders per day after 6 months and 10,000 orders after 12 months. Orders coming in are checked for consistency, then dispatched to your manufacturing plant for production, quality control, packaging, shipment and payment processing. If the product does not meet the quality standards at any stage of the process, employees may force the process to repeat a step. Customers are notified via email about order status and any critical issues with their orders such as payment failure. Your base architecture includes AWS Elastic Beanstalk for your website with an RDS MySQL instance for customer data and orders. How can you implement the order fulfillment process while making sure that the emails are delivered reliably?
27. Add a business process management application to your Elastic Beanstalk app servers and reuse the RDS database for tracking order status. Use one of the Elastic Beanstalk instances to send emails to customers.
28. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1. Use SES to send emails to customers.
29. Use an SQS queue to manage all process tasks. Use an Auto Scaling group of EC2 instances that poll the tasks and execute them. Use SES to send emails to customers.
30. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1. Use the decider instance to send emails to customers.
31. You would like to create a mirror image of your production environment in another region for disaster recovery purposes. Which of the following AWS resources do not need to be recreated in the second region? Choose 2 answers
32. Route S3 Record Sets
33. Launch Configurations
34. EC2 Key Pairs
35. Security Groups
36. IAM Roles
37. Elastic IP Addresses (EIP)
38. Your company currently has a 2-tier web application running in an on-premises data center.You have experienced several infrastructure failures in the past few months resulting in significant financial losses. Your CIO is strongly considering moving the application to AWS. While working on achieving buy-In from the other company executives, he asks you to develop a disaster recovery plan to help improve business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks. Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?
39. Create an EBS backed private AMI which includes a fresh install of your application. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying the application across Multiple-Availability-Zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection.
40. Deploy your application on EC2 instances within an Auto Scaling group across multiple availability zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection.
41. Create an EBS backed private AMI which includes a fresh install of your application. Setup a script in your data center to backup the local database every 1 hour and to encrypt and copy the resulting file to an S3 bucket using multi-part upload.
42. Install your application on a compute-optimized EC2 instance capable of supporting the application’s average load. Synchronously replicate transactions from your on-premises database to a database instance in AWS across a secure Direct Connect connection.
43. An international company has deployed a multi-tier web application that relies on DynamoDB in a single region. For regulatory reasons they need disaster recovery capability in a separate region with a Recovery Time Objective of 2 hours and a Recovery Point Objective of 24 hours. They should synchronize their data on a regular basis and be able to provision the web application rapidly using CloudFormation. The objective is to minimize changes to the existing web application, control the throughput of DynamoDB used for the synchronization of data, and synchronize only the modified elements. Which design would you choose to meet these requirements?
44. Use AWS Data Pipeline to schedule a DynamoDB cross region copy once a day, create a “LastUpdated” attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter
45. Use AWS Data Pipeline to schedule an export of the DynamoDB table to S3 in the current region once a day, then schedule another task Immediately after it that will import data from S3 to DynamoDB in the other region
46. Use EMR and write a custom script to retrieve data from DynamoDB in the current region using a SCAN operation and push it to DynamoDB in the second region
47. Send also each write into an SQS queue in the second region, use an auto-scaling group behind the SQS queue to replay the write in the second region
48. You have deployed a web application, targeting a global audience across multiple AWS Regions under the domain name You have been asked to propose a multi-region deployment. You decide to use Route53 Latency-Based Routing to serve web requests to users from the region closest to the user. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region. During a DR test you notice that when you disable all web servers in one of the regions Route53 does not automatically direct all users to the other region. What could be happening? Choose 2 answers
49. You did not set “Evaluate Target Health” to ‘Yes” on the latency alias resource record set associated with example.com in the region where you disabled the servers
50. The value of the weight associated with the latency alias resource record set in the region with the disabled servers is higher than the weight for the other region
51. One of the two working web servers in the other region did not pass its HTTP health check
52. Latency resource record sets cannot be used in combination with weighted resource record sets
53. You did not setup an HTTP health check for one or more of the weighted resource record sets associated with the disabled web servers
54. In the Amazon RDS Oracle DB engine, the Database Diagnostic Pack and the Database Tuning Pack are only available with \_\_\_\_\_\_\_\_\_\_\_\_\_\_
55. Oracle Standard Edition
56. Oracle Express Edition
57. Oracle Enterprise Edition
58. None of these
59. Amazon EC2 provides a repository of public data sets that can be seamlessly integrated into AWS cloud-based applications. What is the monthly charge for using the public data sets?
60. A 1 time charge of 10$ for all the datasets.
61. 1$ per dataset per month
62. 10$ per month for all the datasets
63. There is no charge for using the public data sets
64. Within the IAM service a GROUP is regarded as a:
65. A collection of AWS accounts
66. It’s the group of EC2 machines that gain the permissions specified in the GROUP.
67. There’s no GROUP in IAM, but only USERS and RESOURCES.
68. A collection of users
69. You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet, as well as from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link. How would you design routing to meet the above requirements?
70. Configure a single routing table with a default route via the Internet gateway. Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.
71. Configure a single routing table with a default route via the Internet gateway. Propagate specific routes for the on-premises networks via BGP on the AWS Direct ConnectGet Latest & Actual Amazon Exam’s Question and Answers from Passleader. customer router. Associate the routing table with all VPC subnets.
72. Configure two routing tables: one that has a default route via the Internet gateway, and another that has a default route via the VPN gateway. Associate both routing tables with each VPC subnet.
73. Configure a single routing table with two default routes: one to the Internet via an Internet gateway, the other to the on-premises network via the VPN gateway. Use this routing table across all subnets in your VPC.
74. You’ve been brought in as solutions architect to assist an enterprise customer with their migration of an e-commerce platform to Amazon Virtual Private Cloud (VPC).The previous architect has already deployed a 3-tier VPC. The configuration is as follows:

VPC: vpc-2f8bc447

IGW: igw-2d8bc445

NACL: ad-208bc448

Subnets and Route Tables:

Web servers: subnet-258bc44d

Application servers: subnet-248bc44c

Database servers: subnet-9189c6f9

Route Tables:

rtb-218bc449

rtb-238bc44b

Associations:

subnet-258bc44d : rtb-218bc449

subnet-248bc44c : rtb-238bc44b

subnet-9189c6f9 : rtb-238bc44b

You are now ready to begin deploying EC2 instances into the VPC. Web servers must have direct access to the Internet. Application and database servers cannot have direct access to the Internet. Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?

1. Create a bastion and NAT instance in subnet-258bc44d, and add a route from rtb-238bc44b to the NAT instance.
2. Add a route from rtb-238bc44b to igw-2d8bc445 and add a bastion and NAT instance within subnet-248bc44c.
3. Create a bastion and NAT instance in subnet-248bc44c, and add a route from rtb-238bc44b to subnet-258bc44d.
4. Create a bastion and NAT instance in subnet-258bc44d, add a route from rtb-238bc44b to Igw-2d8bc445, and a new NACL that allows access between subnet-258bc44d and subnet- 248bc44c.