Question 1: Your engineers have asked you for guidance on deploying and removing web applications hosted in their development VPC. They have been using Elastic Beanstock successfully but now not able to create new versions of their applications. What suggestion would you give the engineers to solve their problem?

[1] Apply an application version lifecycle policy to your applications per region
[2] From the management console delete all versions no longer required
[3] **Apply an application version lifecycle policy to your applications**
[4] Elastic Beanstalk deletes all versions automatically

Comments: Version control can be automated

AWS DOCUMENTATION: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/applications-lifecycle.html

Question 2: Once your application has been launched using Elastic Beanstalk, what type of DNS record is used to direct the associated Load Balancer to your hosted environment?

[1] A record
[2] AAAA record
[3] **CNAME Record**
[4] MX Record
[5] Alias Record

Comments: Route 53 uses a CNAME record to perform scalable operations

AWS DOCUMENTATION:
http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.concepts.architecture.html

Question 3: Your developers want to use Elastic Beanstalk to deploy web tier applications at AWS without worrying about the underlying infrastructure. When launching their Elastic beanstalk environment, what environmental tier should they select

[1] **Web server tier**
[2] Worker tier
[3] Application tier
[4] Background job tier

Comments: Choice of environmental tier selected determines either the foreground or background environment

AWS DOCUMENTATION:
http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.concepts.architecture.html

Question 4: Developers want to save the Elastic Beanstalk settings that are applied to deploy resources in their environment. What two methods are currently supported for saving configuration option settings?

[1] PS1
[2] **YAML**
[3] **JSON**
[4] XML

Comments: Configuration files are templates created from the running environment

AWS DOCUMENTATION: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environment-configuration-methods-before.html

Question 5: What AWS components utilize network access control lists to control inbound and outbound traffic.

[1] Customer gateway
[2] EC2 instance
[3] **Full VPC**
[4] **Peering Connections**
[5] **Endpoints**

Comments: NACLs control stateless access at the subnet level for all ingress and egress traffic

AWS DOCUMENTATION:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#ACLs

Question 7: Failover from an application server hosted on a dedicated subnet to another application server on another dedicated subnet is mandated. In order to test the failover scenario and additional network interface must also be added to each instance. What two of the following options are correct in respect to this scenario?

[1] The instance must be turned off before adding the interface as a warm attach
[2] The instance can remain running as the instance can be added as a hot attach
[3] Both subnets must reside in the same availability zone
[4] Both subnets must reside in the same region
[5] Both subnets must be peered

Comments: NICs can be attached both cold, hot, and warm Instances; Subnets must reside in the same availability zone

AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#best-practices-for-configuring-network-interfaces

Question 8: Which of these statements are true when associating a subnet with a specific network NCL?

[1] **All subnets associated with a network ACL will have the associated rules applied**
[2] **Subnets can be associated with more than one network ACL**
[3] Subnets can be associated with only one network ACL
[4] **Subnets not associated with any custom ACL will be associated with the default network ACL**
[5] Network ACLs can't be disassociated from a subnet after being assigned

Comments: Subnets have specific rules when associated with network ACLs

AWS DOCUMENTATION:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#NetworkACL

Question 9: New compliance regulations require network technicians to begin logging IP traffic going to and from specific network interfaces on the private network using flow logs to capture the network traffic. The current network design is a mixture of newer VPCs, and older EC2-Classic networks. What IP traffic information will the flow logs not capture?

[1] **Metadata requests for 169.254.169.254**
[2] IPV4 and IPv6 traffic from elastic network adapters
[3] Amazon WorkSpaces traffic within a VPC
[4] **DNS communications**

Comments: Flow logs are not supported for EC2 Classic, and have limitations for all networks.

AWS DOCUMENTATION: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#flow-logs-limitations

Question 9: EC2 instances are deployed in a public subnet of a custom VPC. What tasks must be completed in order for the instance to be accessible from the Internet. Choose all that could apply.

[1] **Attach an elastic IP to the instance**
[2] Insure that the associated NACLs restrict traffic flow to the public subnet
[3] **Attach an Internet gateway to the public subnet**
[4] **Create security groups for port 80 and 443 access**

Comments: Public and private subnets with the exception of the default VPC do not automatically have Internet access enabled

AWS DOCUMENTATION:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

Question 10: An instance is connected to an elastic network interface hosted on a private subnet. The elastic network interface of the instance is then changed to a different Instance hosted on a different subnet. What changes occur in regards to the instance and the NACLs assigned at the subnet.

[1] The instance follows the rules of the original subnet
[2] The NACLs of the original subnet apply to the instance
[3] The instance follows both rules of both subnets
[4] **The instance follows the rules of the newer subnet**
[5] **The NACLs of the new subnet apply to the instance**

Comments: The EIN subnet location is controlled by the associated NACLs
AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html
Multiple choice: 4 s

Question 11: What two types of environments can be created when using Elastic Beanstalk?
[1] Load-balancing environment
[2] **Load-balancing and auto scaling environment**
[3] **Single instance environment**
[4] Multi-region multiple instance environment

Comments: Elastic Beanstalk functions within a region

AWS DOCUMENTATION: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html

Question 12: Due to compliance rules and regulations your company has decided to use dedicated instances for the network design. In order to protect their network infrastructure how should the tenancy of the VPC be designed?

[1] Secured instances
[2] **Dedicated instances**
[3] Dedicated host
[4] Selecting VPC tenancy is not required

Comments: You can create a VPC with an instance tenancy of dedicated to ensure that all instances launched into the VPC are Dedicated instances

AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html#dedicated-usage-overview

Question 13: Developers want to attach an additional network interface for additional private network connections within their VPC on select EC2 instances. What type of network component should they add to complete this task?

[1] Elastic IP address
[2] **Elastic Network interface**
[3] Multi-homed instance
[4] Network ACL

Comments: elastic network interfaces add an additional network interface to selected EC2 instances

AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

Question 14: Your company needs hybrid connectivity to the Amazon cloud. What hardware or software component is required on the customer site in order to connect successfully?

[1] Virtual private gateway
[2] Virtual private cloud
[3] **Customer gateway**
[4] VPN connection
[5] Direct connect

Comments: Each customer must have a compatible hardware or software customer gateway on site

AWS DOCUMENTATION:
http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html#CustomerGateway

Question 15: When developers are connecting using a SSH connection to a newly deployed EC2 instance, they receive connectivity errors about issues connecting to the instance. What could be the source of this problem? Check all that apply.

[1] **Reconfirm that the private key being used matches the key pair that was assigned at launch**
[2] Confirm the associated IAM user policy has permissions to launch EC2 instances
[3] **Reconfirm your logon information**
[4] Confirm that the EC2 instance is associated with the desired IAM role
[5] Recheck the public IP address

Comments: The public-private key selected during deployment of an instance must match the public-private key used when authenticating
AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

Question 16: Your company hosts an application on AWS that users utilize to retrieve highly sensitive data records. Users connect using SSL. You need to ensure a high level of performance and also maintain security with regards to the storage of the SSL private key using the least amount of administration. Choose from the following options.

[1] Store the SSL key on the web servers
[2] Use Cloud HSM to provide SSL authentication and authorization
[3] **Upload the private key to the load balancer configuring the load balancer to perform SSL offload**
[4] Configure your load balancer to retrieve the SSL key from a private S3 bucket

Comments: Cloud HSM solution requires additional administration and cost
AWS DOCUMENTATION: http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html

Question 17: A web application hosted at AWS handles requests for technical journal publications. The frontend web application is hosted in a VPC with multiple availability zones, auto scaling groups and cross zone load-balancing. The relational database service hosts the database services that serve the technical journals from S3 buckets. At certain times, specific technical journals become quite popular causing viewing issues. What additional design components could be utilized to help alleviate the pressure on the deployed infrastructure? Choose two answers.

[1] **Deploy cloudfront to help serve content delivery**
[2] **Deploy elasticache with lazy loading to cache the most frequently accessed data**
[3] Utilize the SQS service to speed up response to requests
[4] **Deploy elasticache with write through to update the most frequently written data**

Comments: Lazy loading keeps cache up to date based on requests
AWS DOCUMENTATION:
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/Strategies.html

Question 18: Your security team needs to define resource-based permissions for instances. Select all that apply when designing resource-based permissions for instances.

[1] Resource-based policies are managed policies
[2] **Resource-based policies are inline only**
[3] **Resource-based policies are attached to a resource**
[4] Resource-based policies are attached to a resource and IAM user
[5] **Resource-based policies define both access levels and actions allowed**

Comments: Resource-based permissions are directly attached to an AWS resource
AWS DOCUMENTATION:
http://docs.aws.amazon.com/IAM/latest/UserGuide/access_permissions.html

Question 19: After reviewing the reports from the Trusted Advisor your company has decided to enable multifactor authentication for IAM users and the root account. Which of the following MFA options can be utilized for both account types?

[1] **Security token for a virtual MFA software device**
[2] SMS text message based
[3] **Security token for a hardware-based MFA device**
[4] AWS CodeCommit
[5] AWS Security Token Service

Comments: SMS text messages are only usable for IAM users
AWS DOCUMENTATION:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

Question 20: Your company has begun deploying corporate resources on AWS. They want to ensure AWS compliance levels match against their corporate requirements. Choose the answers that reflect best practices for carrying out a security audit.

[1] **Review applicable third-party AWS compliance reports and attestations**
[2] Carry out a detailed audit of on premise computer operations
[3] **Request approval to perform relevant network scans and penetration tests of your systems instances**
[4] Meet with relevant third-party auditors to discuss AWS compliance standards

Comments: SOC-2 audit is available to current AWS customers
AWS DOCUMENTATION: https://aws.amazon.com/compliance/soc-faqs/

Question 21: Your web-based application has been launched publicly. Your design has implemented auto scaling and classic load balancing and your design is responding to the changes in demand as expected. Over the next few months during the holiday season expected demand will be quite robust. You estimate the number of instances required to meet your customers demand to be 100 EC2 instances. How should you plan properly for growth?

[1] **Change your auto scaling configuration setting a desired maximum capacity of 100 instances**
[2] Use the trusted advisor to analyze your workload requirements
[3] **Contact Amazon to pre-warm your elastic load balancer to match the expected demands**
[4] Add a second load balancer for additional redundancy

Comments: Prewarming requires direct communication with AWS providing detailed requirements
AWS DOCUMENTATION: https://aws.amazon.com/articles/1636185810492479#pre-warming

Question 22: Your engineers are concerned about application availability during in-place updates to a live Elastic Beanstalk stack. You advise that they consider a blue/green deployment. List the necessary steps to carry out a blue green deployment.

[1] **Clone your current environment**
[2] Launch a backed-up environment
[3] **Deploy the new version of the application**
[4] **From the new environments dashboard, swap environmental URL's and click Swap**
[5] From the new environments dashboard, choose Restart Environment

Comments: Blue / Green deployments resolve application unavailability during updates
AWS DOCUMENTATION: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

Question 23: A member of your network operations center team needs to find out which services the IAM management group has utilized over the last month. What AWS feature is best suited to quickly access this information?

[1] Use AWS Inspector
[2] **Use the Access Advisor in the IAM Console**
[3] Enable flow logs to track traffic flow
[4] Run the Trusted Advisor

Comments: Access advisor allows you to inspect a user, group, role, or policy
AWS DOCUMENTATION: http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials
28: Your developers need to create security rules to control the inbound traffic access to their instances on a public subnet. They wish to provide access to port 80 and port 443 but deny access to specific IP addresses. How should they proceed when creating their security rules?

[1] Create security groups to control port access, and deny access from specific IP addresses
[2] Create NACLs to control port access and security groups to deny access from specific IP addresses
[3] Create security groups to control port access, and NACLs to deny access from specific IP addresses
[4] Create IAM role based policy for all security rules

Comments: Security groups cannot deny access, their design is permissive only
AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

Question 24: In order to provide adequate computer resources during busy sales cycles for your company portal, you have your instances assigned to an auto scaling group associated with an elastic load balancer and associated health checks. From time to time the instances within the auto scaling group are being marked unhealthy as expected but the unhealthy instances are not terminated. What do you have to change to ensure that instances marked unhealthy will be terminated?

[1] **Configure the auto scaling group to use both instance status checks and load balancer health checks**
[2] Enable connection draining
[3] Add an additional availability zone for failover
[4] Enable cross-zone replication
[5] Increase the pool of initial instances in the auto scaling group

Comments: Both instance status checks and health checks must be enabled before unhealthy instances will be terminated
AWS DOCUMENTATION: https://aws.amazon.com/articles/1636185810492479

Question 25: Your organization is migrating applications to AWS. Your new security policy mandates that all user accounts will be created and managed through IAM. Currently your corporation is using Active Directory as their on site LDAP service. Once applications go live at AWS, all users must utilize applications using temporary access credentials, and, all IAM users must have passwords rotated on a set schedule. Which of the following options will allow you to enforce this security policy?

[1] Create required IAM user accounts
[2] Deploy federation services that support the Security Token Service
[3] All IAM users must have multifactor authentication enabled
[4] Create and enforce a single use password policy option for al IAM users
[5] Disable the root account for your AWS account

Comments: STS provides temporary access credentials for federation

AWS DOCUMENTATION:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html

Question 26: An application load balancer needs to be configured with support for SSL offload using the default security policy. When negotiating the SSL connections between the client and the load balancer, you want the application load balancer to determine which cipher is used for the SSL connection. Which of the below options perform this process?

[1] Enable SSL offload
[2] Select the default security policy
[3] Select client configuration preference
[4] Choose server order preference
[5] Upload a custom security policy

Comments: The ELB is designed for ssl offload and multiple security policy settings
AWS DOCUMENTATION: http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html#config-backend-auth

Question 27: You've deployed an application in a custom AMI image into the Amazon cloud. It is deployed in a separate VPC. You would like to take advantage of being able to failover to another instance without having to reconfigure the application. Which of these solutions could be utilized?

[1] Use an additional elastic network interface for failover to another instance
[2] Use load-balancing to balance traffic to additional instances
[3] Utilize cloud watch health checks for failover
[4] Add a secondary private IP address to the primary network interface that could then be used to failover to move to a specified instance

Comments: The eni can be attached to an instance only hosted in a VPC

AWS DOCUMENTATION: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

Question 28: Your company will be connecting to Amazon utilizing a hybrid design. It will be necessary to create an IPsec VPN connection using the Internet as the pathway. The solution must provide for two separate VPN endpoints for additional redundancy to be located at AWS. In addition, both BGP and IPsec connections must be terminated on the same user gateway device. Select the options below that support this design criteria.

[1] Hardware VPN solution with IPsec
[2] Dynamic routing support
[3] Software VPN solution
[4] Cloud Hub VPN Access

Comments: Hardware VPN provides dual redundant paths and BGP support

AWS DOCUMENTATION:
http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf

Question 29: A legacy web application has been deployed in a single availability zone. It is used sporadically by your company but needs to be available. Due to your heavy workload of administration and support you wish to automate a process that if the application fails, it is rebuilt automatically.

[1] Configure the server in an auto scaling group with the minimum and maximum size of one
[2] Monitor the server availability using cloud watch metrics and be emailed when the server fails its health checks
[3] Add an additional availability zone and a load balancer
[4] Perform snapshots of EBS volumes on a set schedule

Comments: Auto scale provides redundancy for a single server

AWS DOCUMENTATION: http://docs.aws.amazon.com/autoscaling/latest/userguide/create-launch-config.html

Question 30: You are migrating your Oracle database to AWS using the AWS database migration service. Due to the large amount of data being replicated you need the replication process to be continuous. What must be changed on your replication instance to use ongoing replication?

1. Increase the number of tables that are cached in RAM
2. Enable Multi-AZ option on the replication instance
3. Increase the amount of data written to your database change log
4. Disable backups on the target instance
5. Disable multi-AZ on the target instance

Comments: Enabling the Multi-AZ option is required to provide high-availability and failover support for the replication instance

AWS DOCUMENTATION:
http://docs.aws.amazon.com/dms/latest/userguide/CHAP_BestPractices.html#CHAP_BestPractices.OnGoingReplication