1. A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website   
DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).  
Which configuration should the solutions architect use to meet the company’s needs while minimizing changes and infrastructure overhead?

* A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
* B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
* C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
* D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

2. A company’s application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.  
What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

* A. Configure an Amazon CloudFront distribution in front of the ALB.
* B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
* C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
* D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

3. A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.  
Which action will meet these requirements?

* A. Modify the ALB security group to deny incoming traffic from blocked countries.
* B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
* C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
* D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

4. A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.  
Which set of actions should a solutions architect take to support these needs?

* A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.
* B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.
* C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.
* D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

5. A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data multiple AWS Regions.  
How should a solutions architect design the S3 solution?

* A. Create an additional S3 bucket in another Region and configure cross-Region replication.
* B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
* C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
* D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

6. A company’s website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow.  
Which set of actions will improve website performance for users worldwide?

* A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
* B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
* C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross- Region VPC peering.
* D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

7. A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.  
Which pricing model should the company choose?

* A. Reserved Instances
* B. Spot Block Instances
* C. On-Demand Instances
* D. Scheduled Reserved Instances

8. A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.  
What should a solutions architect do to meet these requirements? (Choose two.)?

* A. Increase the number of EC2 instances.
* B. Decrease the number of EC2 instances.
* C. Configure a Network Load Balancer in front of the EC2 instances.
* D. Configure an Application Load Balancer in front of the EC2 instances.
* E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

9. A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.  
Which configuration should the solutions architect choose to meet these requirements?

* A. Configure Amazon CloudFront with AWS WAF.
* B. Configure Application Load Balancers with AWS WAF.
* C. Configure Amazon Route 53 with a geolocation policy.
* D. Configure Amazon Route 53 with a geoproximity routing policy.

10. A solutions architect has created a new AWS account and must secure AWS account root user access.  
Which combination of actions will accomplish this? (Choose two.)

* A. Ensure the root user uses a strong password.
* B. Enable multi-factor authentication to the root user.
* C. Store root user access keys in an encrypted Amazon S3 bucket.
* D. Add the root user to a group containing administrative permissions.
* E. Apply the required permissions to the root user with an inline policy document.

11. A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.  
Which S3 storage class should be implemented to meet these requirements?

* A. S3 Glacier
* B. S3 Intelligent-Tiering
* C. S3 Standard-Infrequent Access (S3 Standard-IA)
* D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

12. A companyג€™s website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer  
(ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the  
CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.  
What should a solutions architect do to protect the application?

* A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
* B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
* C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
* D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

13. A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.  
What should a solutions architect do to remediate the vulnerability?

* A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
* B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
* C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
* D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

14. A company hosts a static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.  
Which action will accomplish this?

* A. Enable Amazon S3 versioning.
* B. Enable Amazon S3 Intelligent-Tiering.
* C. Enable an Amazon S3 lifecycle policy.
* D. Enable Amazon S3 cross-Region replication.

15. A security team to limit access to specific services or actions in all of the teamג€™s AWS accounts. All accounts belong to a large organization in AWS Organizations.  
The solution must be scalable and there must be a single point where permissions can be maintained.  
What should a solutions architect do to accomplish this?

* A. Create an ACL to provide access to the services or actions.
* B. Create a security group to allow accounts and attach it to user groups.
* C. Create cross-account roles in each account to deny access to the services or actions.
* D. Create a service control policy in the root organizational unit to deny access to the services or actions.

16. A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.  
What should a solutions architect use to accomplish this?

* A. Server-Side Encryption with keys stored in an S3 bucket
* B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
* C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
* D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

17. A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.  
How should security groups be configured in this situation? (Choose two.)

* A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
* B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
* C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
* D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
* E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

18. A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.  
Which action will MOST securely grant the EC2 instance access to the S3 bucket?

* A. Attach a resource-based policy to the S3 bucket.
* B. Create an IAM user for the application with specific permissions to the S3 bucket.
* C. Associate an IAM role with least privilege permissions to the EC2 instance profile.
* D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

19. An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:  
  
What is the effect of this policy?

* A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
* B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
* C. Users can terminate an EC2 instance in the us-east-1 Region when the userג€™s source IP is 10.100.100.254.
* D. Users cannot terminate an EC2 instance in the us-east-1 Region when the userג€™s source IP is 10.100.100.254.

20. A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute- intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.  
Which type of Amazon EC2 instances should be used to reduce the cost of the system?

* A. Spot Instances
* B. On-Demand Instances
* C. Standard Reserved Instances
* D. Scheduled Reserved Instances

21. A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.  
What should the solutions architect recommend?

* A. Leverage Amazon CloudFront with the ALB endpoint as the origin.
* B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.
* C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.
* D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

22. A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instances in the private subnets that use a NAT gateway to connect to the internet. In case of an AZ failure, the company wants to ensure that the instances are not all experiencing internet connectivity issues and that there is a backup plan ready.  
Which solution should a solutions architect recommend that is MOST highly available?

* A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.
* B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.
* C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.
* D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

23. A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range.  
What should a solutions architect recommend to the team?

* A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.
* B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
* C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
* D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

24. An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.  
Which solution is the MOST cost-effective?

* A. DEV with Spot Instances and PROD with On-Demand Instances
* B. DEV with On-Demand Instances and PROD with Spot Instances
* C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
* D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

25. A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.  
What should the solutions architect do to meet these requirements?

* A. Increase the minimum capacity for the Auto Scaling group.
* B. Increase the maximum capacity for the Auto Scaling group.
* C. Configure scheduled scaling to scale up to the desired compute level.
* D. Change the scaling policy to add more EC2 instances during each scaling operation.

26. A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.  
Which configuration will meet this requirement?

* A. Configure the security group for the EC2 instances.
* B. Configure the security group on the Application Load Balancer.
* C. Configure AWS WAF on the Application Load Balancer in a VPC.
* D. Configure the network ACL for the subnet that contains the EC2 instances.

26. A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.  
  
A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

* A. Deleting IAM users
* B. Deleting directories
* C. Deleting Amazon EC2 instances
* D. Deleting logs from Amazon CloudWatch Logs

27. A company has an Amazon EC2 instance running on a private subnet that needs to access a public website to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connections to it.  
How can a solutions architect achieve this objective?

* A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.
* B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.
* C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.
* D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

28. A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before sending it to Amazon  
S3.  
What should a solutions architect recommend to satisfy these requirements?

* A. Server-side encryption with customer-provided encryption keys
* B. Client-side encryption with Amazon S3 managed encryption keys
* C. Server-side encryption with keys stored in AWS key Management Service (AWS KMS)
* D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

29. A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.  
Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

* A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
* B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
* C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
* D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

30. A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central  
AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized.  
How should a solutions architect meet these requirements?

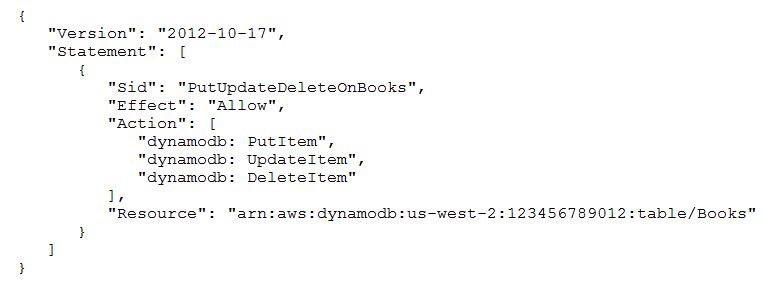
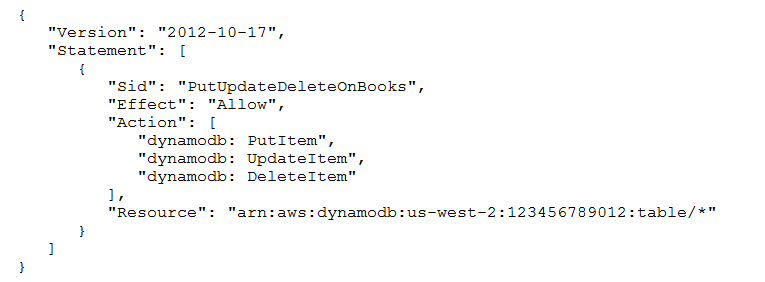
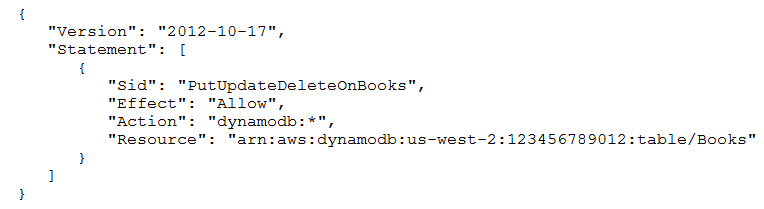
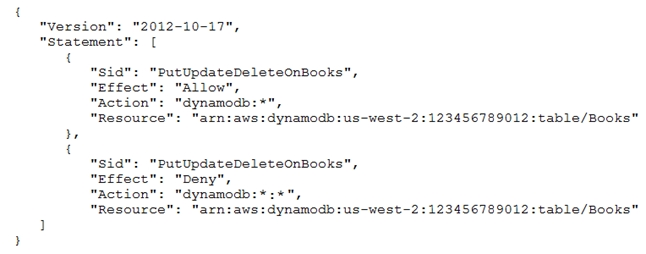
* A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
* B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.
* C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
* D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

31. A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.  
Which solution will accomplish this?

* A. Spot Fleet
* B. Spot Instances
* C. Reserved Instances
* D. On-Demand Instances

32. A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an  
Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another  
Region.  
What should a solutions architect do to automate the failover process?

* A. Enable an ALB health check
* B. Enable an Amazon Route 53 health check.
* C. Crate an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
* D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

33. A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is designing an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books table. The IAM policy must prevent function from performing any other actions on the Books table or any other.  
Which IAM policy would fulfill these needs and provide the LEAST privileged access?  
A.  
  
B.  
  
C.  
  
D.  


34. A company wants to migrate a workload to AWS. The chief information security officer requires that all data be encrypted at rest when stored in the cloud. The company wants complete control of encryption key lifecycle management.  
The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail. The chosen services should integrate with other storage services that will be used on AWS.  
Which services satisfies these security requirements?

* A. AWS CloudHSM with the CloudHSM client
* B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
* C. AWS Key Management Service (AWS KMS) with an external key material origin
* D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

35. A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region. The databases are deployed in a private subnet while the web servers are deployed in a public subnet. An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances. The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead.  
Which solution meets these requirements?

* A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
* B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
* C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.
* D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

36. A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.  
What would allow for automatic recovery of the EC2 instance as quickly as possible?

* A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
* B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
* C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, trigger instance recovery.
* D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

37. A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region.  
Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

* A. Deploy a NAT instance in a private subnet of each Availability Zone.
* B. Deploy a NAT gateway in a public subnet of each Availability Zone.
* C. Deploy a transit gateway in a private subnet of each Availability Zone.
* D. Deploy an internet gateway in a public subnet of each Availability Zone.

38. A company is running a two-tier ecommerce website using services. The current architect uses a publish-facing Elastic Load Balancer that sends traffic to Amazon  
EC2 instances in a private subnet. The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MYSQL database. The application is running in the United States. The company recently started selling to users in Europe and Australia. A solutions architect needs to design solution so their international users have an improved browsing experience.  
Which solution is MOST cost-effective?

* A. Host the entire website on Amazon S3.
* B. Use Amazon CloudFront and Amazon S3 to host static images.
* C. Increase the number of public load balancers and EC2 instances.
* D. Deploy the two-tier website in AWS Regions in Europe and Australia.

39. A company’s website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company’s website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.  
Which combination should a solutions architect recommend to meet these requirements?

* A. Amazon CloudFront and Amazon S3
* B. AWS Lambda and Amazon DynamoDB
* C. Application Load Balancer with Amazon EC2 Auto Scaling
* D. Amazon Route 53 with internal Application Load Balancers

40. A company has established a new AWS account. The account is newly provisioned and no changed have been made to the default settings. The company is concerned about the security of the AWS account root user.  
What should be done to secure the root user?

* A. Create IAM users for daily administrative tasks. Disable the root user.
* B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
* C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
* D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

41. A solutions architect has configured the following IAM policy.  
  
Which action will be allowed by the policy?

* A. An AWS Lambda function can be deleted from any network.
* B. An AWS Lambda function can be created from any network.
* C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
* D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network.

42. A solutions architect is performing a security review of a recently migrated workload. The workload is a web application that consists of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The solutions architect must improve the security posture and minimize the impact of a DDoS attack on resources.  
Which solution is MOST effective?

* A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the WAF ACL on the CloudFront distribution.
* B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.
* C. Enable VPC Flow Logs and store then in Amazon S3. Create a custom AWS Lambda functions that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
* D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch. Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs, looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

43. A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port  
443.  
Which combination of steps will accomplish this task? (Choose two.)

* A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
* B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
* C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
* D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
* E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

44. A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.  
What should a solutions architect recommend to meet the clientsג€™ needs?

* A. A Network Load Balancer with an associated Elastic IP address.
* B. An Application Load Balancer with an associated Elastic IP address
* C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
* D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

45. A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.  
What should the solutions architect do to reduce the overall data transfer costs?

* A. Place all the EC2 instances in an Auto Scaling group.
* B. Place all the EC2 instances in the same AWS Region.
* C. Place all the EC2 instances in the same Availability Zone.
* D. Place all the EC2 instances in private subnets in multiple Availability Zones.

46. A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.  
What should a solutions architect recommend?

* A. Deploy Amazon Inspector and associate it with the ALB.
* B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
* C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
* D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

47. A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.  
What should a solutions architect recommend?

* A. Set up a new Direct Connect connection in another AWS Region.
* B. Set up a new AWS managed VPN connection in another AWS Region.
* C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.
* D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

48. A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.  
What should the solutions architect do to enable internet access for the private subnets?

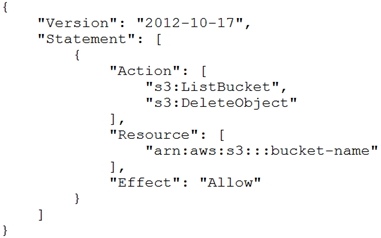
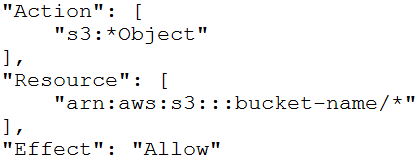
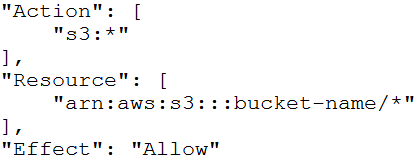
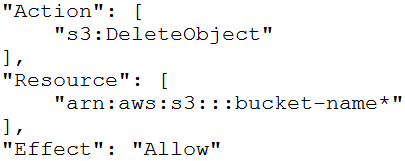
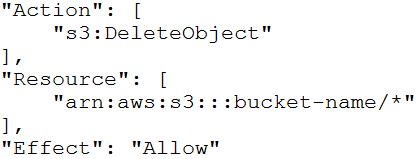
* A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
* B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
* C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
* D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

49. A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.  
What is the MOST cost-effective method to establish this type of connection?

* A. Implement a client VPN.
* B. Implement AWS Direct Connect.
* C. Implement a bastion host on Amazon EC2.
* D. Implement an AWS Site-to-Site VPN connection.

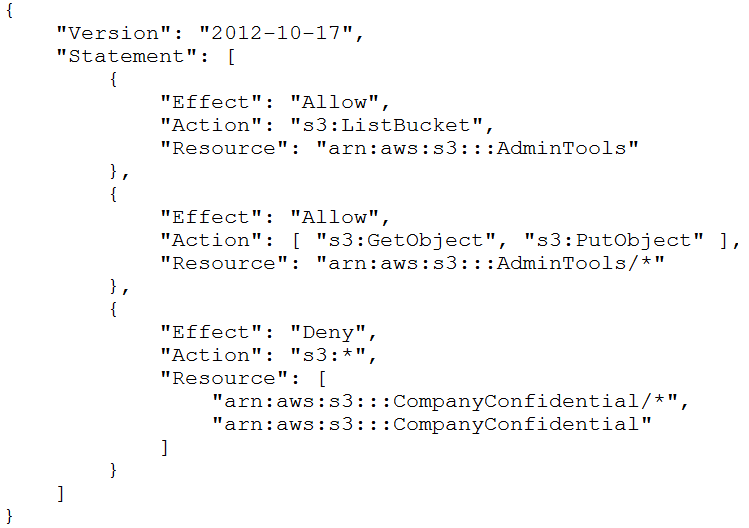
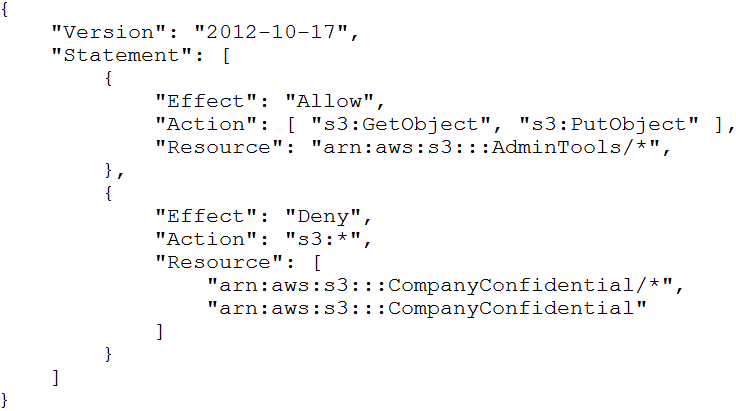
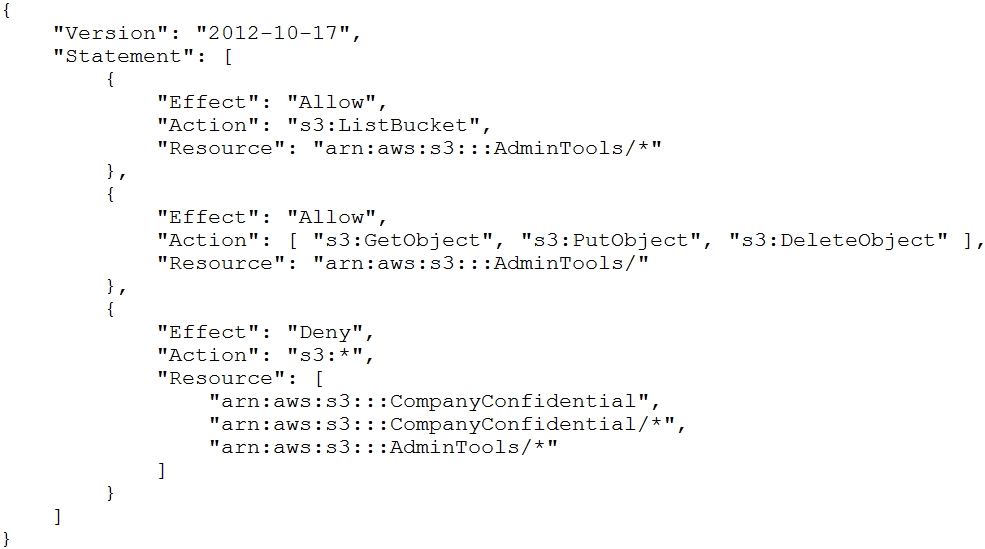
50. A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the  
VPC was designed with two public subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances.  
What should a solutions architect do to ensure these requirements are met?

* A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
* B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.
* C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
* D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

51. A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.  
  
Which statement should a solutions architect add to the policy to correct bucket access?  
A.  
  
B.  
  
C.  
  
D.  


52. A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.  
Which action meets these requirements?

* A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
* B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
* C. Create a service control policy (SCP) the prohibits changes to CloudTrail, and attach it the developer accounts.
* D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master a

53. A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named CompanyConfidential. The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.  
Which IAM policy will meet these requirements?  
A.  
  
B.  
  
{  
C.  
  
D.  


54. A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devices a strategy that maximizes security without increasing operational overhead.  
What should the solutions architect do to meet these requirements?

* A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
* B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
* C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
* D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

55. A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from  
0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.  
Which additional configuration strategy should the solutions architect use to meet these requirements?

* A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
* B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
* C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
* D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.