AWS-Certified Solutions Architect-Professional
(考试题目数量：75 题； 考试时长 190min)

1. A Solutions Architect is responsible for redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high-memory Amazon EC2 instance It accepts HTTP requests from upstream clients, adds them to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them, and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average, most of which is spent waiting on external service calls, but the application is written to process multiple items in parallel.
Traffic to this service is unpredictable. During periods of high load, items may sit in the internal queue for over an hour while the application processes the backlog. In addition, the current system has issues with availability and data loss if the single application node fails.
Clients that access this service cannot be modified They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request
Which approach would improve the availability and durability of the system while decreasing the processing latency and minimizing costs?
A. Create an Amazon API Gateway REST API that uses Lambda proxy integration to pass requests to an AWS Lambda function Migrate the core processing code to a Lambda function and write a wrapper class that provides a handler method that converts the proxy events to the internal application data model and invokes the processing module
B. Create an Amazon APl Gateway REST API that uses a service proxy to put items in an Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS instead of an in-memory queue. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SQS queue
C. Modify the application to use Amazon DynamoDB instead of Amazon RDS. Configure Auto Scaling for the DynamoDB table. Deploy the application within an Auto Scaling group with a scaling policy based on CPU utilization. Back the in-memory queue with a memory-mapped file to an instance store volume and periodically write that file to Amazon S3
D. Update the application to use a Redis task queue instead of the in-memory queue, Build a Docker container image for the application. Create an Amazon ECS task definition that includes the application container and a separate container to host Redis Deploy the new task definition as an ECS service using AWS Fargate, and enable Auto Scaling
答案：C

2. A company runs its containerized batch jobs on Amazon ECS. The jobs are scheduled by submitting a container image, a task definition, and the relevant data to an Amazon S3 bucket. Container images may be unique per job. Running the jobs as quickly as possible is of utmost importance, so submitting job artifacts to the S3 bucket triggers the job to run immediately. Sometimes there may be no jobs running at all. However, jobs of any size can be submitted with no prior warning to the IT Operations team. Job definitions include CPU and memory resource requirements.
What solution will allow the batch jobs to complete as quickly as possible after being scheduled?
A. Schedule the jobs on an Amazon ECS cluster using the Amazon EC2 launch type Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs
B. Schedule the jobs directly on EC2 instances Use Reserved Instances for the baseline minimum load, and use On-Demand Instances in an Auto Scaling group to scale up the platform based on demand
C. Schedule the jobs on an Amazon ECS cluster using the Fargate launch type Use Service Auto Scaling to

increase or decrease the number of running tasks to suit the number of running jobs

D. Schedule the jobs on an Amazon ECS cluster using the Fargate launch type Use Spot Instances in an Auto Scaling group to scale the platform based on demand. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs

答案：C

3. A company is moving a business-critical application onto AWS. It is a traditional three-tier web application using an Oracle database Data must be encrypted in transit and at rest. The database hosts 12 TB of data Network connectivity to the source Oracle database over the internet is allowed, and the company wants to reduce operational costs by using AWS Managed Services where possible. All resources within the web and application tiers have been migrated. The database has a few tables and a simple schema using primary keys only; however, it contains many Binary Large OBject（BLOB）fields. It was not possible to use the database's native replication tools because of licensing restrictions.

Which database migration solution will result in the LEAST amount of impact to the application's availability?

A. Provision an Amazon RDS for Oracle instance, Host the RDS database within a virtual private cloud（VPS）subnet with internet access, and set up the RDS database as an encrypted Read Replica of the source database Use SSL to encrypt the connection between the two databases. Monitor the replication performance by watching the RDS ReplicaLag metric During the application maintenance window, shut down the on-premises database and switch over the application connection to the RDS instance when there is no more replication lag. Promote the Read Replica into a standalone database instance.

B. Provision an Amazon EC2 instance and install the same Oracle database software. Create a backup of the source database using the supported tools. During the application maintenance window, restore the backup into the Oracle database running in the EC2 instance Set up an Amazon RDS for Oracle instance, and create an import job between the databases hosted in AWS. shut down the source database and switch over the database connections to the RDS instance when the job is complete

C. Use AWS DMS to load and replicate the dataset between the on-premises Oracle database and the replication instance hosted on AWS Provision an Amazon RDS for Oracle instance with Transparent Data Encryption （TDE）enabled and configure it as a target for the replication instance. Create a customer-managed AWS KMS master key to set it as the encryption key for the replication instance. Use AWS DMS tasks to load the data into the target RDS instance. During the application maintenance window and after the load tasks reach the ongoing replication phase, switch the database connections to the new database

D. Create a compressed full database backup of the on-premises Oracle database during an application maintenance window. While the backup is being performed, provision 10 Gbps AWS Direct Connect connection to increase the transfer speed of the database backup files to Amazon S3 and shorten the maintenance window period. Use SSL/TLS to copy the files over the Direct Connect connection. When the backup files are successfully copied, start the maintenance window, and use any of the Amazon RDS supported tools to import the data into a newly provisioned Amazon RDS for Oracle instance with encryption enabled. Wait until the data is fully loaded and switch over the database connections to the new database. Delete the Direct Connect connection to cut unnecessary charges

答案：C

4. A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month -end load with the LEAST

impact on performance?
A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes
B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month
C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or lOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
D. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards
答案：B

5. A company has an application behind a load balancer with enough Amazon EC2 instances to satisfy peak demand. Scripts and third-party deployment solutions are used to configure EC2 instances when demand increases or an instance fails. The team must periodically evaluate the utilization of the instance types to ensure that the correct sizes are deployed.
How can this workload be optimized to meet these requirements?
A. Use CloudFormer to create AWS CloudFormation stacks from the current resources. Deploy that stack by using CloudFormation in the same region. Use Amazon CloudWatch alarms to send notifications about underutilized resources to provide cost-savings suggestions
B. Create an Auto Scaling group to scale the instances, and use AWS CodeDeploy to perform the configuration Change from a load balancer to an Application Load Balancer. Purchase a third-party product that provides suggestions for cost savings on AWS resources
C. Deploy the application by using AWS Elastic Beanstalk with default options. Register for an AWS Support Developer plan. Review the instance usage for the application by using Amazon CloudWatch, and identify less expensive instances that can handle the load Hold monthly meetings to review new instance types and determine whether Reserved Instances should be purchased
D. Deploy the application as a Docker image by using Amazon ECS. Set up Amazon EC2 Auto Scaling and Amazon ECS scaling. Register for AWS Business Support and use Trusted Advisor checks to provide suggestions on cost savings
一家公司在负载平衡器后面有一个应用程序，它有足够的 Amazon EC2 实例来满足峰值需求。 脚本和第三方部署解决方案用于在需求增加或实例失败时配置 EC2 实例。 团队必须定期评估实例类型的利用率，以确保部署了正确的大小。如何优化此工作负载以满足这些需求？
A. 使用 CloudFormer 从当前资源创建 AWS CloudFormation 堆栈。 通过在同一区域使用 AWS CloudFormation 来部署堆栈。 使用 Amazon CloudWatch 警报发送关于未充分利用资源的通知，以提供节省成本的建议。
B. 创建一个 Auto Scaling 组来扩展实例，并使用 AWS CodeDeploy 进行配置。将负载平衡器的配置更改为 Application Load Balancer。 购买第三方产品。为 AWS 资源成本节约提供建议。
C. 使用带有默认选项的 AWS Elastic Beanstalk 部署应用程序。注册 AWS Support Developer 计划，通过使用 Amazon CloudWatch 检查应用程序的实例使用情况，找到可以处理负载同时成本较低的实例。每月召开会议，审查新的实例类型，并确定是否应该购买预留实例。
D. 使用 Amazon ECS 将应用程序部署为 Docker 映像。设置 Amazon EC2 Auto Sca1ing 和 Amazon ECS 扩展。注册 AWS Business Support，并使用 Trusted Advisor 检查来提供节省成本相关的建议
答案：D

6. A company has an application written using an in-house software framework. The framework installation takes 30 minutes and is performed with a user data script. Company Developers deploy changes to the

application frequently. The framework installation is becoming a bottleneck in this process
Which of the following would speed up this process?
A. Create a pipeline to build a custom AMI with the framework installed and use this AMI as a baseline for application deployments.
B. Employ a user data script to install the framework but compress the installation files to make them smaller
C. Create a pipeline to parallelize the installation tasks and call this pipeline from a user data script
D. Configure an AWS OpsWorks cookbook that installs the framework instead of employing user data. Use this cookbook as a base for all deployments
答案：A

7. A company had a tight deadline to migrate its on-premises environment to AWS. It moved over Microsoft SQL Servers and Microsoft Windows Servers using the virtual machine import/export service and rebuilt other applications native to the cloud. The team created both Amazon EC2 databases and used Amazon RDS. Each team in the company was responsible for migrating their applications, and they have created individual accounts for isolation of resources. The company did not have much time to consider costs, but now it would like suggestions on reducing its AWS spend.
Which steps should a Solutions Architect take to reduce costs?
A. Enable AWS Business Support and review AWS Trusted Advisor's cost checks. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand. Save AWS Simple Monthly Calculator reports in Amazon S3 for trend analysis. Create a master account under Organizations and have teams join for consolidated billing
B. Enable Cost Explorer and AWS Business Support. Reserve Amazon EC2 and Amazon RDS DB instances Use Amazon CloudWatch and AWS Trusted Advisor for monitoring and to receive cost-saving suggestions. Create a master account under Organizations and have teams join for consolidated billing
C. Create an AWS Lambda function that changes the instance size based on Amazon CloudWatch alarms. Reserve instances based on AWS Simple Monthly Calculator suggestions. Have an AWS Well-Architected framework review and apply recommendations. Create a master account under Organizations and have teams join for consolidated billing
D. Create a budget and monitor for costs exceeding the budget. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand. Create an AWS Lambda function that changes instance sizes based on Amazon CloudWatch alarms. Have each team upload their bill Amazon S3 bucket for analysis of team spending. Use Spot Instances on nightly batch processing jobs.
答案：B

8. A company has an Amazon VPC that is divided into a public subnet and a private subnet. A web application runs in Amazon VPC, and each subnet has its own NACL. The public subnet has a CIDR of 10.0.0.0/24. An Application Load Balancer is deployed to the public subnet. The private subnet has a CIDR of 10.0.1.0/24. Amazon EC2 instances that run a web server on port 80 are launched into the private subnet
Only network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets
What collection of rules should be written to ensure that the private subnet's NACL meets the requirement? （Select TWO ）
A. An inbound rule for port 80 from source 0.0.0.0/0
B. An inbound rule for port 80 from source 10.0.0.0/24
C. An outbound rule for port 80 to destination 0.0.0.0/0
D. An outbound rule for port 80 to destination 10.0.0.0/24

E. An outbound rule for ports 1024 through 65535 to destination 10.0.0.0/24

答案：BE

解析：因为 E 是 nat 网关的端口，你的 web 服务器在私有子网上，回复查询必须走 nat gw，nat gw 的临时端口是 1024-65535

9. A company is running a large application on premises. Its technology stack consists of Microsoft NET for the web server platform and Apache Cassandra for the database. The company wants to migrate this application to AWS to improve service reliability. The IT team also wants to reduce the time it spends on capacity management and maintenance of this infrastructure. The Development team is willing and available to make code changes to support the migration

Which design is the LEAST complex to manage after the migration?

A. Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running NET. Migrate the existing Cassandra database to Amazon Aurora with multiple read replicas, and run both in a Multi-AZ mode

B. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the NET platform in a Multi-AZ Auto Scaling configuration. Migrate the Cassandra database to Amazon EC2 instances that are running in a Multi-AZ configuration

C. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the NET platform in a Multi-AZ Auto Scaling configuration. Migrate the existing Cassandra database to Amazon DynamoDB

D. Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running NET Migrate the existing Cassandra database to Amazon DynamoDB.

答案：C

10. A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4 Company policy requires systems that communicate with external vendors use a security group that limits access to only approved external vendors, The virtual private cloud （VPC）uses the default network ACL

The Systems Operator successfully assigns IPv6 addresses to each of the backend systems. The Systems Operator also updates the outbound security group to include the IPv6 CIDR of the external vendor （destination ） The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor.

What changes are required to enable communication with the external vendor?

A. Create an IPv6 NAT instance. Add a route for destination 0.0.0.0/0 pointing to the NAT instance

B. Enable IPv6 on the NAT gateway. Add a route for destination ::/0 pointing to the NAT gateway

C. Enable IPv6 on the internet gateway. Add a route for destination 0.0.0.0/0 pointing to the IGW

D. Create an egress-only internet gateway. Add a route for destination ::/0 pointing to the gateway

答案：D

11. A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that, if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted

How can the company prevent users from accidentally deleting data in this way?

A. Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources

B. Configure a stack policy that disallows the deletion of RDS and EBS resources

C. Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an " aws:cloudformation:

stack-name" tag.

D. Use AWS Config rules to prevent deleting RDS and EBS resources
答案：A

12. A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon.
The Finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.
The Security team requires a centralized mechanism to control IAM usage in all the company's accounts
What combination of the following options meet the company's needs with the LEAST effort？（Select Two）
A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.
B. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations
C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks
D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts
E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and the IAM's Access Advisor feature to enforce the least privilege model
一家大公司正在将其整个 IT 产品组合迁移到 AWS。公司中的每个业务部门都有一个独立的 AWS 账户支持开发和测试环境。不久将需要创建可支持生量的新账户
财务部需要一套集中的支付方法，但必须掌握每个集团的支出以分配成本
安全团队需要一套集中的机制来控制公司所有账户 IAM 的使用
以下哪种组合能够最不费力地满足公司的需求？（请选择两项。）
A. 使用一组参数化的 AWS CloudFormation 模板，这些模板定义了分配到每个账户的常见 IAM 权限。要求所有新账户和现有账户启动适当的堆栈，以实施最低权限模型
B. 从选定的付款人账户中使用 AWS Organizations 来创建新组织并定义组织单位的层次结构。邀请现有账户加入组织并使用 AWS Organizations 创建新账户。
C. 要求每个业务部门需使用自己的 AWS 账户。对每个 AWS 账户进行适当标记并启用 Cost Exp1orex 管理退款。
D. 启用 AWS Organizations 的所有功能，并建立适当的服务控制政策，针对子账户过滤 IAM 权限
E.将公司的所有 AWS 账户整合到一个 AWS 账户中。使用标记进行计费并使用 IAM 的 Access Advisor 功能实施最小权限模型
答案：BD

13. A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda, and Amazon DynamoDB They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept Amazon CloudWatch metrics did not indicate any issues with DynamoDB but showed that some Lambda functions were hitting their timeout
Which of the following actions should the Solutions Architect consider to improve performance？（Select TWO）
A. Configure the AWS Lambda function to reuse containers to avoid unnecessary startup time
B. Increase the amount of memory and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal memory and timeout configuration for the Lambda function
C. Increase the amount of CPU, and adjust the timeout on the Lambda function Complete performance

testing to identify the deal CPU and timeout configuration for the Lambda function
D. Create an Amazon ElastiCache cluster running Memcached, and configure the Lambda function for VPC integration with access to the Amazon ElastiChche cluster
E. Enable API cache on the appropriate stage in Amazon API Gateway, and override the TTL for individual methods that require a lower TTL than the entire stage
答案：BE

14. A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.
Which would enable the collection of this data MOST cost effectively?
A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center
B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs
C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment
D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN
答案：A

15. A company runs a three-tier application in AWS Users report that the application performance can vary greatly depending on the time of day and functionality being accessed
The application includes the following components
•Eight t2. large front-end web servers that serve static content and proxy dynamic content from the application tier
•Four t2 large application servers
• One db.m4. large Amazon RDS MySQL Multi-AZ DB instance
Operations has determined that the web and application tiers are network constrained
Which of the following should cost effective improve application performance？（Select TWO ）
A. Replace web and app tiers with t2.xlarge instances
B. Use AWS Auto Scaling and m4 large instances for the web and application tiers
C. Convert the MySQL RDS instance to a self-managed MySQL cluster on Amazon EC2
D. Create an Amazon Cloud Front distribution to cache content
E. Increase the size of the Amazon RDS instance to db.m4.xlarge
答案：BD

16. A company has a large on-premises Apache Hadoop cluster with a 20 PB HDFS database. The cluster is growing every quarter by roughly 200 instances and 1 PB. The company' s goals are to enable resiliency for its Hadoop data, limit the impact of losing cluster nodes, and significantly reduce costs. The current cluster runs 24/7 and supports a variety of analysis workloads, including interactive queries and batch processing
Which solution would meet these requirements with the LEAST expense and down time？
A. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster, Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create

job-specific, optimized clusters for batch workloads that are similarly optimized

B. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster of a similar size and configuration to the current cluster. Store the data on EMRFS. Minimize costs by using Reserved Instances. As the workload grows each quarter, purchase additional Reserved Instances and add to the cluster

C. Use AWS Snowball to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster Store the data on EMRFS Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized

D. Use AWS Direct Connect to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized

答案：A

17. A company is using AWS to run an internet-facing production application written in Node.js. The Development team is responsible for pushing new versions of their software directly to production. The application software is updated multiple times a day. The team needs guidance from a Solutions Architect to help them deploy the software to the production fleet quickly and with the least amount of disruption to the service

Which option meets these requirements?

A. Prepackage the software into an AMI and then use Auto Scaling to deploy the production fleet. For software changes update the AMI and allow Auto Scaling to automatically push the new AMI to production

B. Use AWS CodeDeploy to push the prepackaged AMI to production. For software changes, reconfigure Code Deploy with new AMI identification to push the new AMI to the production fleet

C. Use AWS Elastic Beanstalk to host the production application For software changes, upload the new application version to Elastic Beanstalk to push this to the production fleet using a blue/green deployment method

D. Deploy the base AMI through Auto Scaling and bootstrap the software using user data. For software changes, SSH to each of the instances and replace the software with the new version

答案：C

18. The Security team needs to provide a team of interns with an AWS environment so they can build a serverless video transcoding application. The project will use Amazon S3， AWS Lambda, Amazon API Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder

The interns should be able to create and configure the necessary resources, but they may not have access to create or modify AWS IAM roles. The Solutions Architect creates a policy and attaches it to the interns' group.

How should the Security team configure the environment to ensure that the interns are self-sufficient?

A. Create a policy that allows creation of project-related resources only. Create roles with required service permissions, which are assumable by the services.

B. Create a policy that allows creation of all project-related resources, including roles that allow access only to specified resources.

C. Create roles with the required service permissions, which are assumable by the services Have the interns create and use a bastion host to create the project resources in the project subnet only

D. Create a policy that allows creation of project-related resources only. Require the interns to raise a

request for roles to be created with the Security team. The interns will provide the requirements for the permissions to be set in the role
答案：A

19. A company has a High Performance Computing（HPC）cluster in its on-premises data center, which runs thousands of jobs in parallel for one week every month, processing petabytes of images. The images are stored on a network file server, which is replicated to a disaster recovery site. The on-premises data center has reached capacity and has started to spread the jobs out over the course of the month in order to better utilize the cluster, causing a delay in the job completion
The company has asked its Solutions Architect to design a cost-effective solution on AWS to scale beyond the current capacity of 5,000 cores and 10 petabytes of data. The solution must require the least amount of management overhead and maintain the current level of durability
Which solution will meet the company's requirements?
A. Create a container in the Amazon Elastic Container Registry with the executable file for the job. Use Amazon ECS with Spot Fleet in Auto Scaling groups, Store the raw data in Amazon EBS SC1 volumes and write the output to Amazon S3
B. Create an Amazon EMR cluster with a combination of On Demand and Reserved Instance Task Nodes that will use Spark to pull data from Amazon S3. Use Amazon DynamoDB to maintain a list of jobs that need to be processed by the Amazon EMR cluster
C. Store the raw data in Amazon S3， and use AWS Batch with Managed Compute Environments to create Spot Fleets Submit jobs to AWS Batch Job Queues to pull down objects from Amazon S3 onto Amazon EBS volumes for temporary storage to be processed, and then write the results back to Amazon S3
D. Submit the list of jobs to be processed to an amazon SQS to queue the jobs that need to be processed. Create a diversified cluster of Amazon EC2 worker instances using Spot Fleet that will automatically scale based on the queue depth. Use Amazon EFS to store all the data sharing it across all instances in the cluster
答案：C

20. A company collects a steady stream of 10 million data records from 100， 000 sources each day. These records are written to an Amazon RDS MySQL DB. A query must produce the daily average of a data source over the past 30 days. There are twice as many reads as writes. Queries to the collected data are for one source ID at a time
How can the Solutions Architect improve the reliability and cost effectiveness of this solution?
A. Use Amazon Aurora with MySQL in a Multi-AZ mode. Use four additional read replicas
B. Use Amazon DynamoDB with the source ID as the partition key and the timestamp as the sort key. Use a Time to Live (TTL) to delete data after 30 days
C. Use Amazon DynamoDB with the source ID as the partition key. Use a different table each day
D. Ingest data into Amazon Kinesis using a retention period of 30 days. Use AWS Lambda to write data records to Amazon ElastiCache for read access
答案：B

21. A Solutions Architect must establish a patching plan for a large mixed fleet of windows and Linux servers. The patching plan must be implemented securely, be audit-ready, and comply with the company's business requirements
Which option will meet these requirements with MINIMAL effort?
A. Install and use an OS-native patching service to manage the update frequency and release approval for all instances. Use AWS Config to verify the OS state on each instance and report on any patch compliance issues
B. Use AWS Systems Manager on all instances to manage patching. Test patches outside of production and

then deploy during a maintenance window with the appropriate appropriate approval.
C. Use AWS OpsWorks for Chef Automate to run a set of scripts that will iterate through all instances of a given type Issue the appropriate OS command to get and install updates on each instance, including any required restarts during the maintenance window
D. Migrate all applications to AWS OpsWorks and use OpsWorks automatic patching support to keep the OS up-to-date following the initial installation. Use AWS Config to provide audit and compliance reporting
一位解决方案架构师必须为大量 Windows 和 Linux 服务器制定修补计划。修补计划必须能够安全实施，做好审计准备，并满足企业业务要求。
以下哪个选项可以最轻松地满足这些要求？
A. 安装并使用系统原生修补服务来管理更新频率，并发布所有实例的批准。使用 AWS Config 验证每个实例的操作系统状态，并报告所有修补程序是否合规
B. 在所有实例上使用 AWS Systems Manager 来管理修补。在生产区之外测试修补程序，然后在维护窗口期间通过适当的批准进行部署。
C.使用 AWS OpsWorks for Chef Automate 运行一组脚本，这些脚本将迭代给定类型的所有实例。发出适当的操作系统命令以获取并在每个实例上安装更新，包括维护窗口期间所需的任何重启行为。
D. 将所有应用程序迁移到 AWS OpsWorks，使用 OpsWorks 完成自动修补，从而使操作系统在初始安装后保持最新状态。使用 AWS Config 提供审计和合规性报告。
答案：B

22. A media company has a 30-TB repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management（MAM）system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.
The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system.
How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?
A. Set up an AWS Storage Gateway, file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution
B. Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution
C. Configure a video ingestion stream by using Amazon Kinesis video Streams. Use the catalog of faces to build a collection in Amazon Rekognition Stream the videos from the MAM solution into Kinesis Video Streams. Configure Amazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3
D. Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required metadata, and push the metadata into the MAM solution, while also copying the

video files to an Amazon S3 bucket
答案：A

23. A company has a standard three-tier architecture using two Availability Zones. During the company' s off season, users report that the website is not working. The Solutions Architect finds that no changes have been made to the environment recently the website is reachable, and it is possible to log in. However, when the Solutions Architect selects the "find a store near you " function, the maps provided on the site by a third- party RESTful API call do not work about 50% of the time after refreshing the page. The outbound API calls are made through Amazon EC2 NAT instances
What is the MOST likely reason for this failure and how can it be mitigated in the future?
A. The network ACL for one subnet is blocking outbound web traffic. Open the network ACL and prevent administration from making future changes though IAM
B. The fault is in the third-party environment. Contact the third party that provides the maps and request a fix that will provide better uptime
C. One NAT instance has become overloaded. Replace both EC2 NAT instances with a larger-sized instance and make sure to account for growth when making the new instance size
D. One of the NAT instances failed. Recommend replacing the EC2 NAT instances with a NAT gateway
答案：D

24. A Solutions Architect must design a highly available, stateless, REST service. The service will require multiple persistent storage layers for service object meta information and the delivery of content. Each request needs to be authenticated and securely processed. There is a requirement to keep costs as low as possible.
How can these requirements be met?
A. Use AWS Fargate to host a container that runs a self-contained REST service. Set up an Amazon ECS service that is fronted by an Application Load Balancer（ALB）. Use a custom authenticator to control access to the API. Store request meta information in Amazon DynamoDB with Auto Scaling and static content in a secured S3 bucket. Make secure signed requests for Amazon S3 objects and proxy the data through the REST service interface
B. Use AWS Fargate to host a container that runs a self-contained REST service. Set up an ECS service that is fronted by a cross-zone ALB. Use an Amazon Cognito user pool to control access to the APl. Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket Generate resigned URLs when returning references to content stored in Amazon S3
C. Set up Amazon API Gateway and create the required API resources and methods Use an Amazon Cognito user pool to control access to the APl. Configure the methods to use AWS Lambda proxy integrations, and process each resource with a unique AWS Lambda function. Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket Generate resigned URLs when returning references to content stored in Amazon S3
D. Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon API Gateway custom authorizer to control access to the APl. Configure the methods to use AWS Lambda custom integrations, and process each resource with a unique Lambda function. Store request meta information in an Amazon ElastiCache Multi-AZ cluster and static content in a secured S3 bucket Generate presigned URLs when returning references to content stored in Amazon S3
答案：C

25. A large global financial services company has multiple business units. The company wants to allow Developers to try new services, but there are multiple compliance requirements for different workloads. The Security team is concerned about the access strategy for on-premises and AWS implementations. They

would like to enforce governance for AWS services used by business teams for regulatory workloads, including Payment Card Industry（PCI）requirements.
Which solution will address the Security team's concerns and allow the Developers to try new services?
A. Implement a strong identity and access management model that includes users, groups, and roles in various AWS accounts. Ensure that centralized AWS CloudTrail logging is enabled to detect anomalies. Build automation with AWS Lambda to tear down unapproved AWS resources for governance
B. Build a multi-account strategy based on business units, environments, and specific regulatory requirements. Implement SAML-based federation across all AWS accounts with an on-premises identity store. Use AWS Organizations and build an organizational units（OUs）structure based on regulations and service governance. Implement service control policies across OUs
C. Implement a multi-account strategy based on business units, environments, and specific regulatory requirements. Ensure that only PCI-compliant services are approved for use in the accounts. Build IAM policies to give access to only PCI-compliant services for governance
D. Build one AWS account for the company for strong security controls. Ensure that all the service limits are raised to meet company scalability requirements, Implement SAML federation with an on-premises identity store, and ensure that only approved services are used in the account
答案：B

26. The CISO of a large enterprise with multiple IT departments, each with its own AWS account, wants one central place where AWS permissions for users can be managed and users authentication credentials can be synchronized with the company's existing on-premises solution
Which solution will meet the CISO's requirements?
A. Define AWS IAM roles based on the functional responsibilities of the users in a central account. Create a SAML-based identity management provider. Map users in the on-premises groups to IAM roles. Establish trust relationships between the other accounts and the central account
B. Deploy a common set of AWS IAM users, groups, roles, and policies in all of the AWS accounts using AWS Organizations Implement federation between the on-premises identity provider and the AWS accounts
C. Use AWS Organizations in a centralized account to define service control policies （SCPs）。 Create a SAML-based identity management provider in each account and map users in the on-premises groups to AWS IAM roles
D. Perform a thorough analysis of the user base and create AWS IAM users accounts that have the necessary permissions. Set up a process to provision and deprovision accounts based on data in the on-premises solution
一家大型企业的首席信息安全官配有多个 IT 部门，每个 IT 部门拥有自己的 AWS 账户。他希望在一个中心位置管理用户的 AWS 权限，并且可以将用户身份验证凭据与公司的现有本地解决方案同步。
哪一种解决方案将满足首席信息安全官的需求?
A. 在中心账户中基于用户的职能责任定义 AWS IAM 角色。创建基于 SAML 的身份管理提供者。将本地组中的用户映射至 IAM 角色。建立其他账户和中心账户的信任关系。
B. 使用 AWS Organizations 在全部 AWS 账户中部署 AYS IAM 用户、组、角色和策略的暂通集合。实施本地身份验证标识提供者和 AWS 账户之间的联合。
C. 在中心账户中使用 AWS Organizations 定义服务控制策略（SCPs）。在每个账户中创建基于 SAML 的身份管理提供者，并且将本地组中的用户映射至 AWS IAM 角色。
D.对用户群体进行全面的分析，并创建拥有所需权限的 AWS IAM 角色账户。基于本地解决方案中的数据设置提供和注销账户的流程。
答案：A

27. A company runs a dynamic mission-critical web application that has an SLA of 99.99%. Global application users access the application 24/7. The application is currently hosted on premises and routinely

fails to meet its SLA, especially when millions of users access the application concurrently. Remote users complain of latency How should this application be redesigned to be scalable and allow for automatic failover at the lowest cost?

A. Use Amazon Route 53 failover routing with geolocation-based routing. Host the website on automatically scaled Amazon EC2 instances behind an Application Load Balancer with an additional Application Load Balancer and EC2 instances for the application layer in each region. Use a Multi-AZ deployment with MySQL as the data layer

B. Use Amazon Route 53 round robin routing to distribute the load evenly to several regions with health checks. Host the website on automatically scaled Amazon ECS with AWS Fargate technology containers behind a Network Load Balancer, with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora replicas for the data layer

C. Use Amazon Route 53 latency-based routing to route to the nearest region with health checks. Host the website in Amazon S3 in each region and use Amazon API Gateway with AWS Lambda for the application layer, Use Amazon DynamoDB global tables as the data layer with Amazon DynamoDB Accelerator（DAX）for caching

D. Use Amazon Route 53 geolocation-based routing Host the website on automatically scaled AWS Fargate containers behind a Network Load Balancer with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora Multi-Master for Aurora MySQL as the data layer

答案：C

28. A Solutions Architect has been asked to look at a company's Amazon Redshift cluster, which has quickly become an integral part of its technology and supports key business process. The Solutions Architect is to increase the reliability and availability of the cluster and provide options to ensure that if an issue arises, the cluster can either operate or be restored within four hours

Which of the following solution options BEST addresses the business need in the most cost-effective manner?

A. Ensure that the Amazon Redshift cluster has been set up to make use of Auto Scaling groups with the nodes in the cluster spread across multiple Availability Zones

B. Ensure that the Amazon Redshift cluster creation has been templated using AWS CloudFormation so it can easily be launched in another Availability Zone and data populated from the automated Redshift back-ups stored in Amazon S3

C. Use Amazon Kinesis Data Firehose to collect the data ahead of ingestion into Amazon Redshift and create clusters using AWS CloudFormation in another region and stream the data to both clusters

D. Create two identical Amazon Redshift clusters in different regions （one as the primary one as the secondary）。 Use Amazon S3 cross-region replication from the primary to secondary region, which triggers an AWS Lambda function to populate the cluster in the secondary region

答案：B

29. A company is running a . NET three-tier web application on AWS. The team currently uses XL storage optimized instances to store and serve the website' s image and video files on local instance storage. The company has encountered issues with data loss from replication and instance failures. The Solutions Architect has been asked to redesign this application to improve its reliability while keeping costs low .

Launch memory optimized

A. Set up a new Amazon EFS share, move all image and video files to this share, and then attach this new drive as a mount point to all existing servers. Create an Elastic Load Balancer with Auto Scaling general purpose instances. Enable Amazon CloudFront to the Elastic Load Balancer Enable Cost Explorer and use AWS Trusted Advisor checks to continue monitoring the environment for future savings

B. Implement Auto Scaling with general purpose instance types and an Elastic Load Balancer Enable an Amazon CloudFront distribution to Amazon S3 and move images and video files to Amazon S3. Reserve general purpose instances to meet base performance requirements. Use Cost Explorer and AWS Trusted Advisor checks to continue monitoring the environment for future savings

C. Move the entire website to Amazon S3 using the S3 website hosting feature. Remove all the web servers and have Amazon S3 communicate directly with the application servers in Amazon VPC

D. Use AWS Elastic Beanstalk to deploy the NET application. Move all images and video files to Amazon EFS. Create an Amazon CloudFront distribution that points to the EFS share, Reserve the m4.4xl instances needed to meet base performance requirements

答案：B

30. A company is currently running a production workload on AWS that is very I/O intensive. Its workload consists of a single tier with 10 c4.8xlarge instances, each with 2 TB gp2 volumes. The number of processing jobs has recently increased, and latency has increased as well. The team realizes that they are constrained on the lOPS. For the application to perform efficiently, they need to increase the lOPS by 3,000 for each of the instances

Which of the following designs will meet the performance goal MOST cost effectively?

A. Change the type of Amazon EBS volume from gp2 to io1 and set provisioned IOPS to 9，000

B. Increase the size of the gp2 volumes in each instance to 3 TB

C. Create a new Amazon EFS file system and move all the data to this new file system. Mount this file system to all 10 instances

D. Create a new Amazon S3 bucket and move all the data to this new bucket. Allow each instance to access this S3 bucket and use it for storage

答案：B

31. A large company has many business units. Each business unit has multiple AWS accounts for different purposes. The ClO of the company sees that each business unit has data that would be useful to share with other parts of the company. In total, there are about 10 PB of data that needs to be shared with users in 1,000 AWS accounts. The data is proprietary, so some of it should only be available to users with specific job types. Some of the data is used for throughput of intensive workloads, such as simulations. The number of accounts changes frequently because of new initiatives, acquisitions, and divestitures

A Solutions Architect has been asked to design a system that will allow for sharing data for use in AWS with all of the employees in the company.

Which approach will allow for secure data sharing in scalable way?

A. Store the data in a single Amazon S3 bucket Create an lAM role for every combination of job type and business unit that allows for appropriate read/write access based on object prefixes in the S3 bucket. The roles should have trust policies that allow the business unit's AWS accounts to assume their roles. Use IAM in each business unit's AWS account to prevent them from assuming roles for a different job type. Users get credentials to access the data by using AssumeRole from their business unit’s AWS account. Users can then use those credentials with an S3 client

B. Store the data in a single Amazon S3 bucket. Write a bucket policy that uses conditions to grant read and write access where appropriate, based on each user's business unit and job type. Determine the business unit with the AWS account accessing the bucket and the job type with a prefix in the lAM user's name. Users can access data by using IAM credentials from their business unit’s AWS account with an S3 client

C. Store the data in a series of Amazon S3 buckets. Create an application running in Amazon EC2 that is integrated with the company’s identity provider（ldP）that authenticates users and allows them to download or upload data through the application. The application uses the business unit and job type information in the ldP to control what users can upload and download through the application. The users

can access the data through the application's API

D. Store the data in a series of Amazon S3 buckets. Create an AWS STS token vending machine that is integrated with the company's identity provider（IdP）。 When a user logs in, have the token vending machine attach an IAM policy that assumes the role that limits the user's access and/or upload only the data the user is authorized to access. Users can get credentials by authenticating to the token vending machine's website or API and then use those credentials with an S3 client.

答案：D

32. A company runs a legacy system on a single m4. 2xlarge Amazon EC2 instance with Amazon EBS storage. The EC2 instance runs both the web server and a self-managed Oracle database. A snapshot is made of the EBS volume every 12 hours, and an AMI was created from the fully configured EC2 instance

A recent event that terminated the EC2 instance led to several hours of downtime. The application was successfully launched from the AMI, but the age of the EBS snapshot and the repair of the database resulted in the loss of 8 hours of data. The system was also down for 4 hours while the Systems Operators manually performed these processes

What architectural changes will minimize downtime and reduce the chance of lost data?

A. Create an Amazon CloudWatch alarm to automatically recover the instance. Create a script that will check and repair the database upon reboot. Subscribe the Operations team to the Amazon SNS message generated by the CloudWatch alarm

B. Run the application on m4.xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of two. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance

C. Run the application on m4. 2xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of one. Migrate the database to an Amazon RDS Oracle multi-AZ DB instance

D. Increase the web server instance count to two m4.xlarge instances and use Amazon Route 53 round-robin load balancing to spread the load. Enable Route 53 health checks on the web servers. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance

答案：B

33.A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:

1. The data must be highly durable and available
2. The data must always be encrypted at rest and in transit
3. The encryption key must be managed by the company and rotated periodically

Which of the following solutions should the Solutions Architect recommend?

A. Deploy the storage gateway to AWS in file gateway mode Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes

B. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption

C. Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest

D. Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data

一家公司正在将应用程序迁移至 AWS. 它希望在迁移期间尽可能地使用完全托管的服务。公司需要在满足以下需求的应用程序中存储大量的重要文件:

1.数据必须高度耐久和可用。

2.数据在静止和传输过程中必须一直加密
3.加密密匙必须由公司管理，并且进行周期性轮换。
解决方案架构师应该推荐以下哪一种解决方案?
A. 在文件网关模式下，将存储网关部署至 AWS。使用利用 AWS KMS 密匙的 Amazon EBS 卷加密，来加密存储网关卷。
B. 使用带存储桶策略的 Amazon S3 强制 HTTPS 连接至存储桶，并且强制服务器端加密和 AWS KMS 来加密对象。
C. 使用带 SSL 的 Amazon DynamoDB 连接至 DynamoDB. 使用 AWS KMS 密匙对 DynamoDB 对象进行静态加密。
D. 部署带 Amazon EBS 卷的实例以存储此数据。使用利用 AWS KMS 密匙的 EBS 卷加密来加密数据。
答案：B

34. A Solutions Architect must migrate an existing on-premises web application with 70 TB of static files supporting a public open-data initiative. The Architect wants to upgrade to the latest version of the host operating system as part of the migration effort.
Which is the FASTEST and MOST cost-effective way to perform the migration
A. Run a physical-to-virtual conversion on the application server. Transfer the server image over the internet, and transfer the static data to Amazon S3
B. Run a physical-to-virtual conversion on the application server. Transfer the server image over AWS Direct Connect, and transfer the static data to Amazon S3
C. Re- platform the server to Amazon EC2， and use AWS Snowball to transfer the static data to Amazon S3
D. Re-platform the server by using the AWS Server Migration Service to move the code and data to a new Amazon EC2
答案：C

35. A company plans to move regulated and security-sensitive businesses to AWS. The Security team is developing a framework to validate the adoption of AWS best practices and industry-recognized compliance standards. The AWS Management Console is the preferred method for teams to provision resources
Which strategies should a Solutions Architect use to meet the business requirements and continuously assess, audit, and monitor the configurations of AWS resources？（Select Two）
A. Use AWS Config rules to periodically audit changes to AWS resources and monitor the compliance of the configuration Develop AWS Config custom rules using AWS Lambda to establish a test-driven development approach, and further automate the evaluation of configuration changes against the required controls
B. Use Amazon CloudWatch Logs agent to collect all the AWS SDK logs. Search the log data using a pre-defined set of filter patterns that matches mutating API calls. Send notifications using Amazon CloudWatch alarms when unintended changes are performed. Archive log data by using a batch export to Amazon S3 and then Amazon Glacier for long-term retention and auditability
C. Use AWS Cloud Trail events to assess management activities of all AWS accounts. Ensure that CloudTrail is enabled in all accounts and available AWS services. Enable trails, encrypt Cloud Trail event log files with an AWS KMS key, and monitor recorded activities with CloudWatch Logs
D. Use the Amazon CloudWatch Events near-real-time capabilities to monitor system events patterns, and trigger AWS Lambda functions to automatically revert non-authorized changes in AWS resources. Also, target Amazon SNS topics to enable notifications and improve the response time of incident response
E. Use Cloud Trail integration with Amazon SNS to automatically notify unauthorized APl activities. Ensure that Cloud Trail is enabled in all accounts and available AWS services. Evaluate the usage of Lambda functions to automatically revert non-authorized changes in AWS resources.
答案：AC

36.A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer（ALB）and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume.
The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos
Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?
A. Reconfigure Amazon EFS to enable maximum I/O
B. Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown
C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3
D. Set up an Amazon Cloud Front distribution for all site contents, and point the distribution at the ALB
答案：C

37. A group of Amazon EC2 instances have been configured as a high performance computing（HPC）cluster. The instances are running in a placement group, and are able to communicate with each other at network speeds of up to 20 Gbps
The cluster needs to communicate with a control EC2 instance outside of the placement group. The control instance has the same instance type and AMI as the other instances, and is configured with a public IP address How can the Solutions Architect improve the network speeds between the control instance and the instances in the placement group?
A. Terminate the control instance and relaunch it in the placement group
B. Ensure that the instances are communicating using their private IP addresses
C. Ensure that the control instance is using an Elastic Network Adapter
D. Move the control instance inside the placement group
答案：D

38. A company has decided to move some workloads onto AWS to create a grid environment to run market analytics. The grid will consist of many similar instances, spun-up by a job-scheduling function. Each time a large analytics workload is completed, a new VPC is deployed along with job scheduler and grid nodes. Multiple grids could be running in parallel.
Key requirements are:
- Grid instances must communicate with Amazon S3 to retrieve data to be processed
- Grid instances must communicate with Amazon DynamoDB to track intermediate data
- The job scheduler need only to communicate with the Amazon EC2 API to start new grid nodes

A key requirement is that the environment has no access to the internet, either directly or via the on-premises proxy. However, the application needs to be able to seamlessly communicate with Amazon S3, Amazon DynamoDB, and Amazon EC2 API, without the need for reconfiguration for each new deployment
Which of the following should the Solutions Architect do to achieve this target architecture?（Select THREE）
A. Enable VPC endpoints for Amazon S3 and DynamoDB
B. Disable Private DNS Name Support
C. Configure the application on the grid instances to use the private DNS name of the Amazon S3 endpoint
D. Populate the on-premises DNS server with the private IP addresses of the EC2 endpoint
E. Enable an interface VPC endpoint for EC2
F. Configure Amazon S3 endpoint policy to permit access only from the grid nodes
答案：ADE

39. A company runs an e-commerce platform with front-end and e-commerce tiers. Both tiers run on LAMP stacks with the front-end instances running behind a load balancing appliance that has a virtual offering on AWS. Currently the Operations team uses SSH to log in to the instances to maintain patches and address other concerns. The platform has recently been the target of multiple attacks including:

•A DDoS attack

•An SQL injection attack

•Several successful dictionary attacks on SSH accounts on the web servers

The company wants to improve the security of the e-commerce platform by migrating to AWS. The company's Solutions Architects have decided to use the following approach

•Code review the existing application and fix any SQL injection issues

•Migrate the web application to AWS and leverage the latest AWS Linux AMI to address initial security patching

•Install AWS Systems Manager to manage patching and allow the system administrators to run commands on all instances, as needed

What additional steps will address all of the identified attack types while providing high availability and minimizing risk ?

A. Enable SSH access to the amazon EC2 instances using a security group that limits access to specific IPs. migrate on-premises MySQL to Amazon RDS Multi-AZ Install the third-party load balancer from the AWS Marketplace and migrate the existing rules to the load balancer's AWS instances. Enable AWS Shield Standard for DDoS protection

B. Disable SSH access to the Amazon EC2 instances Migrate on-premises MySQL to Amazon RDS Multi-AZ Leverage an Elastic Load Balancer to spread the load and enable AWS Shield Advanced for protection, Add an Amazon CloudFront distribution in front of the website. Enable AWS WAF on the distribution to manage the rules

C. Enable SSH access to the Amazon EC2 instances through a bastion host secured by limiting access to specific IP addresses Migrate on-premises MySQL to a self-managed EC2 instance Leverage an AWS Elastic Load Balancer to spread the load, and enable AWS Shield Standard for DDoS protection. Add an Amazon Cloud Front distribution in front of the website

D. Disable SSH access to the EC2 instances Migrate on-premises MySQL to Amazon RDS Single-AZ, Leverage an AWS Elastic Load Balancer to spread the load. Add an Amazon Cloud Front distribution in front of the website. Enable AWS WAF on the distribution to manage the rules

答案： B

40. A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege

A Solutions Architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster

What steps are required after the deployment to meet the requirements？ （Select TWO）

A. Create tasks using the bridge network mode

B. Create tasks using the awsvpc network mode

C. Apply security groups to Amazon EC2 instances, and use lAM roles for EC2 instances to access other resources

D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources

E. Apply security groups to the tasks, and use lAM roles for tasks to access other resources

答案：BE

41. A company wants to manage the costs associated with a group of 20 applications that are infrequently used, but are still business-critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology
Most of the applications are part of month-end processing routines with of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1GB,though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group a billing report written in Java that accesses multiple data sources and often runs for several hours
Which is the MOST cost-effective solution?
A. Deploy a separate AWS Lambda function for each application Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs
B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch
C. Deploy AWS Elastic Beanstalk for each application with auto Scaling to ensure that all requests have sufficient resources Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms
D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group
答案：C

42. A company currently uses a single 1 Gbps AWS Direct Connect connection to establish connectivity between an AWS Region and its data center. The company has five Amazon VPCs, all of which are connected to the data center using the same Direct Connect connection. The Network team is worried about the single point of failure and is interested in improving the redundancy of the connections to AWS while keeping costs to a minimum Which solution would improve the redundancy of the connection to AWS while meeting the cost requirements?
A. Provision another 1 Gbps Direct Connect connection and create new VIFs to each of the VPCs. Configure the VIFs in a load balancing fashion using BGP
B. Set up VPN tunnels from the data center to each VPC. Terminate each VPN tunnel at the virtual private gateway （VGW）of the respective VPC and set up BGP for route management
C. Set up a new point-to-point Multiprotocol Label Switching（MPLS） connection to the AWS Region that's being used Configure BGP to use this new circuit as passive, so that no traffic flows through this unless the AWS Direct Connect fails
D. Create a public VIF on the Direct Connect connection and set up a VPN tunnel which will terminate on the virtual private gateway (VGW）of the respective VPC using the public VIF. Use BGP to handle the failover to the VPN connection
答案：B

43. A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications

Which solution meets the requirements by using the LEAST amount of management overhead?
A. Connect the Active Directory to AWS by using single sign-on and an Active Directory Federation Services （AD FS）with SAML 2.0， and then configure the Identity Provider（IdP）system to use form-based authentication. Build the AD FS portal page with corporate branding, and integrate third-party applications that support SAML 2.0 as required
B. Create a two-way Forest trust relationship between the on-premises Active Directory and the AWS Directory Service. Set up AWS Single Sign-On with AWS Organizations. Use single sign-on integrations for connections with third-party applications
C. Configure single sign-on by connecting the on-premises Active Directory using the AWS Directory Service AD Connector Enable federation to the AWS services and accounts by using the lAM applications and services linking function. Leverage third-party single sign-on as needed
D. Connect the company's Active Directory to AWS by using AD FS and SAML 2.0 Configure the AD FS claim rule to leverage Regex and a common Active Directory naming convention for the security group to allow federation of all AWS accounts Leverage third-party single sign-on as needed, and add it to the AD FS server
答案： B

44. A Solutions Architect is working with a company that operates a standard three- tier web application in AWS. The web and application tiers run on Amazon EC2 and the database tier runs on Amazon RDS. The company is redesigning the web and application tiers to use Amazon API Gateway and AWS Lambda, and the company intends to deploy the new application within 6 months. The IT Manager has asked the solutions Architect to reduce costs in the interim
Which solution will be MOST cost effective while maintaining reliability?
A. Use Spot Instances for the web tier, On-Demand Instances for the application tier, and Reserved Instances for the database tier
B. Use On-Demand Instances for the web and application tiers, and reserved Instances for the database tier
C. Use Spot Instances for the web and application tiers and Reserved Instances for the database tie
D. Use Reserved Instances for the web, application, and database tiers
答案： B

45. A company deployed a three-tier web application in two regions us-east-1 and eu-west-1 The application must be active in both regions at the same time The database tier of the application uses a single Amazon RDS Aurora database globally, with a master in us-east-1 and a read replica in eu-west-1 Both regions are connected by a VPN
The company wants to ensure that the application remains available even in the event of a region-level failure of all of the application’s components. It is acceptable for the application to be in read-only mode for up to 1 hour. The company plans to configure two Amazon Route 53 record sets, one for each of the regions
How should the company complete the configuration to meet its requirements while providing the lowest latency for the application end-users? （Select TWO ）
A. Use failover routing and configure the us-east- 1 record set as primary and the eu-west-1 record set as secondary Configure an HTTP health check for the web application in us-east-1， and associate it to the us-east- 1 record set
B. Use weighted routing and configure each record set with a weight of 50. Configure an HTTP health check for each region and attach it to the record set for that region
C. Use latency-based routing for both record sets. Configure a health check for each region and attach it to the record set for that region
D. Configure an Amazon CloudWatch alarm for the health checks in us-east-1， and have it invoke at AWS Lambda function that promotes the read replica in eu-west-1

E. Configure Amazon RDS event notifications to react to the failure of the database in us-east- 1 by invoking an AWS Lambda function that promotes the read replica in eu-west-1

答案：CE

46. A Solutions Architect is designing a network solution for a company that has applications running in a data center in Northern Virginia The applications in the company's data center require predictable performance to applications running in a virtual private cloud （VPC）located in us-east-1， and a secondary VPC in us-west-2 within the same account. The company data center is collocated in an AWS Direct Connect facility that serves the us-east-1 region. The company has already ordered an AWS Direct Connect connection and a cross-connect has been established

Which solution will meet the requirements at the LOWEST cost？

A. Provision a Direct Connect gateway and attach the virtual private gateway（VGW）for the VPC in us-east-1 and the VGW for the VPC in us-west-2 Create a private VIF on the Direct Connect connection and associate it to the Direct Connect

B. Create private VIFs on the Direct Connect connection for each of the company's VPCs in the us-east-1 and us-west-2 regions Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFs

C. Deploy a transit VPC solution using Amazon EC2-based router instances in the us-east-1 region. Establish IPsec VPN tunnels between the transit routers and virtual private gateways （VGWs）located in the us-east-1 and us-west-2 regions which are attached to the company's VPCs in those regions. Create a public VIF on the Direct Connect connection and establish IPsec VPN tunnels over the public VIF between the transit routers and the company's data center router

D, Order a second Direct Connect connection to a Direct Connect facility with connectivity to the us-west -2 region Work with a partner to establish a network extension link over dark fiber from the Direct Connect facility to the company’s data center Establish private VIFs on the Direct Connect connections for each of the company's VPCs in the respective regions Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFS

答案：A

47. A large company experienced a drastic increase in its monthly AWS spend. This is after Developers accidentally launched Amazon EC2 instances in unexpected regions. The company has established practices around least privileges for Developers and controls access to on-premises resources using Active Directory groups. The company now want to control costs by restricting the level of access that Developers have to the AWS Management Console without impacting their productivity. The company would also like to allow Developers to launch Amazon EC2 in only one region, without limiting access to other services in any region How can this company achieve these new security requirements while minimizing the administrative burden on the Operations team？

A. Set up SAML-based authentication tied to an IAM role that has an AdministrativeAccess managed policy attached to it Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required

B. Create an IAM user for each Developer and add them to the developer IAM group that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that allows the Developers access to Amazon EC2 only in the required region

C. Set up SAML-based authentication tied to an lAM role that has a PowerUserAccess managed policy and a customer managed policy that deny all the Developers access to any AWS services except AWS Service Catalog. Within AWS Service Catalog create a product containing only the EC2 resources in the approved region

D. Set up SAML-based authentication tied to an IAM role that has the PowerUserAccess managed policy

attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required

答案：D

48. As a part of building large applications in the AWS Cloud, the Solutions Architect is required to implement perimeter security protection Applications running on AWS have the following endpoints :

- Application Load Balancer
- Amazon API Gateway regional endpoint
- Elastic IP address-based EC2 instances
- Amazon S3 hosted websites
- Classic Load Balancer

The Solutions Architect must design a solution to protect all of the listed web front ends and provide the following security capabilities :

- DDoS protection
- SQL injection protection
- IP address whitelist/blacklist
- HTTP flood protection
- Bad bot scraper protection

How should the Solutions Architect design the solution?

A. Deploy AWS WAF and AWS Shield Advanced on all web endpoints. Add AWS WAF rules to enforce the company's requirements

B. Deploy Amazon CloudFront in front of all the endpoints. The Cloud Front distribution provides perimeter protection. Add AWS Lambda-based automation to provide additional security

C. Deploy Amazon CloudFront in front of all the endpoints. Deploy AWS WAF and AWS Shield Advanced. Add AWS WAF rules to enforce the company’s requirements. Use AWS Lambda to automate and enhance the security posture

D. Secure the endpoints by using network ACLs and security groups and adding rules to enforce the company's requirements Use AWS Lambda to automatically update the rules

答案：C

49. A company has created an account for individual Development teams, resulting in a total of 200 accounts. All accounts have a single virtual private cloud （VPC）in a single region with multiple microservices running in Docker containers that need to communicate with microservices in other accounts. The Security team requirements state that these microservices must not traverse the public internet and only certain internal services should be allowed to call other individual services. If there is any denied network traffic for a service, the Security team must be notified of any denied requests, including the source IP

How can connectivity be established between services while meeting the security requirements?

A. Create a VPC peering connection between the VPCs. Use security groups on the instances to allow traffic from the security group IDs that are permitted to call the microservice. Apply network ACLs to and allow traffic from the local VPC and peered VPCs only. Within the task definition in Amazon ECS for each of the microservices, specify a log configuration by using the awslogs driver Within Amazon CloudWatch Logs, create a metric filter and alarm off of the number of HTTP 403 responses. Create an alarm when the number of messages exceeds a threshold set by the Security team

B. Ensure that no CIDR ranges are overlapping and attach a virtual private gateway （VGW） to each VPC. Provision an IPsec tunnel between each VGW and enable route propagation on the route table. Configure security groups on each service to allow the CIDR ranges of the VPCs in the other accounts. Enable VPC Flow Logs, and use an Amazon CloudWatch Logs subscription filter for rejected traffic. Create an IAM role

and allow the Security team to call the AssumeRole action for each account

C. Deploy a transit VPC by using third-party marketplace VPN appliances running on Amazon EC2, dynamically routed VPN connections between the VPN appliance, and the virtual private gateways （VGWs) attached to each VPC within the region. Adjust network ACLs to allow traffic from the local VPC only. Apply security groups to the microservices to allow traffic from the VPN appliances only. Install the awslogs agent on each VPN appliance, and configure logs to forward to Amazon CloudWatch Logs in the security account for the Security team to access

D. Create a Network Load Balancer（NLB） for each microservice. Attach the NLB to a PrivateLink endpoint service and whitelist the accounts that will be consuming this service. Create an interface endpoint in the consumer VPC and associate a security group that allows only the security group IDs of the services authorized to call the producer service On the producer services, create security groups for each microservice and allow only the CIDR range of the allowed services Create VPC Flow Logs on each VPC to capture rejected traffic that will be delivered to an Amazon CloudWatch Logs group, Create a CloudWatch Logs subscription that streams the log data to a security account

答案：c

50. A Company had a security event whereby an Amazon S3 bucket with sensitive information was made public Company policy is to never have public S3 objects, and the Compliance team must be informed immediately when any public objects are identified

How can the presence of a public S3 object be detected, set to trigger alarm notifications, and automatically remediated in the future？ （Select TWO）

A. Turn on object-level logging for Amazon S3. Turn on Amazon S3 event notifications to notify by using an Amazon SNS topic then a PutObject APl call is made with a public-read permission

B. Configure an Amazon CloudWatch Events rule that invokes an AWS Lambda function to secure the S3 bucket

C. Use the S3 bucket permissions for AWS Trusted Advisor and configure a CloudWatch event to notify by using Amazon SNS

D. Turn on object-level logging for Amazon S3. Configure a CloudWatch event to notify by using an SNS topic when a putObject APl call with public-read permission is detected in the AWS Cloud Trail logs

E. Schedule a recursive Lambda function to regularly change all object permissions inside the S3 bucket

答案：DE

51. An organization has two Amazon EC2 instances :

- The first is running an ordering application and an inventory application
- The second is running a queuing system.

During certain times of the year, several thousand orders are placed per second.Some orders were lost when the queuing system was down. Also, the organization’s inventory application has the incorrect quantity of products because some orders were processed twice

What should be done to ensure that the applications can handle the increasing number of orders？

A. Put the ordering and inventory applications into their own AWS Lambda functions. Have the ordering application write the messages into an Amazon SQS FIFO queue

B. Put the ordering and inventory applications into their own Amazon ECS containers, and create an Auto Scaling group for each application. Then, deploy the message queuing server in multiple Availability Zones

C. Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each application Use Amazon SQS standard queues for the incoming orders, and implement idempotency in the inventory application

D. Put the ordering and inventory applications into their own Amazon EC2 instances. Write the incoming orders to an Amazon Kinesis data stream. Configure AWS Lambda to poll the stream and update the

inventory application
答案：C

52. A company is moving a business-critical, multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A Solutions Architect must re-architect the application to ensure that it can meet or exceed the SLA
The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application
Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?
A. Migrate the database to a PostgreSQL database in Amazon EC2. Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer Allocate an Amazon WorkSpaces WorkSpace for each end user to improve the user experience
B. Migrate the database to an Amazon RDS Aurora PostgreSQL configuration, Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer. Use Amazon App Stream 2.0 to improve the user experience
C. Migrate the database to an Amazon RDS PostgreSQL Multi- AZ configuration. Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balancer. Use Amazon ElastiCache to improve the user experience
D. Migrate the database to an Amazon Redshift cluster with at least two nodes. Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer, Use Amazon CloudFront to improve the user experience.
答案：B

53. A company has an application that generates a weather forecast that is updated every 15 minutes with an output resolution of 1 billion unique positions, each approximately 20 bytes in size（20 Gigabytes per forecast）。 Every hour, the forecast data is globally accessed approximately 5 million times （1， 400 requests per second）， and up to 10 times more during weather events. The forecast data is overwritten every update. Users of the current weather forecast application expect responses to queries to be returned in less than two seconds for each request
Which design meets the required request rate and response time?
A. Store forecast locations in an Amazon ES cluster. Use an Amazon Cloud Front distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Enable APl caching on the API Gateway stage with a cache-control timeout set for 15 minutes
B. Store forecast locations in an Amazon EFS volume. Create an Amazon CloudFront distribution that targets an Elastic Load Balancing group of an Auto Scaling fleet of Amazon EC2 instances that have mounted the Amazon EFS volume Set the cache-control timeout for 15 minutes in the CloudFront distribution
C. Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an APl Gateway endpoint with AWS Lambda functions responding to queries as the origin. Create an Amazon Lambda@Edge function that caches the data locally at edge locations for 15 minutes
D. Store forecast locations in Amazon S3 as individual objects. Create an Amazon CloudFront distribution targeting an Elastic Load Balancing group of an Auto Scaling fleet of EC2 instances, querying the origin of the S3 object. Set the cache-control timeout for 15 minutes in the CloudFront distribution
一家公司有一个应用程序，它可以生成每 15 分钟更新一次的天气预报，输出分辨率为 10 亿个独特位置，每个位置的大小约为 20 字节(每个预报 20 Gb).每小时，预测数据在全球范围内被访问约 500 万次(每秒 1400 次)，在天气事件期间，访问次数最多可增加 10 倍。每次更新都会覆盖原预测数据。当

前天气预报应用程序的用户期望，对于每个请求，在不到两秒钟的时间内就能对查询问题给出回应。以下哪个设计可满足所需的请求速率和响应时间?

A. 将预测位置存储到 Amazon ES 群集中。使用针对 Amazon API Gateway 端点的 Amazon C1oudFront 分发，以响应查询的 AWS Lambda 函数作为数据源。在 API Gateway 阶段启用 API 缓存，缓存控制超时设置为 15 分钟。

B. 将预测位置存储在 Amazon EFS 卷中。创建一个 Amazon C1oudFront 分发，目标是一个装载了 Amazon EFS 卷的 Amazon EC2 实例的 Auto Scaling 机队的 E1astic Load Ba1ancing 组。在 C1oudFront 分发中将缓存控制超时设置为 15 分钟。

C. 将预测位置存储在 Amazon ES 群集中。使用针对 API Gateway 端 点的 Amazon C1oudFront 分发，以响应查询的 AWS Lambda 函数作为数据源。创建 Amazon Lambda@Edge 函数，该函数在本地边缘位置缓存数据 15 分钟。

D. 将预测位置作为单独的对象存储在 Amazon S3 中。创建一个 Amazon C1oudFront 分发，目标是 EC2 实例的 Auto Scaling 机队的 Elastic Load Balancing 组，该 EC2 实例会查询 S3 对象的数据源。在 C1oudFront 分发中将缓存控制超时设置为 15 分钟。

答案：A

54. A large multinational company runs a timesheet application on AWS that is used by staff across the world. The application runs Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing（ELB）load balancer, and stores data in an Amazon RDS MySQL Multi-AZ database instance

The CFO is concerned about the impact on the business if the application is not available. The application must not be down for more than two hours, but the solution must be as cost-effective as possible

How should the Solutions Architect meet the CFO's requirements while minimizing data loss?

A. In another region, configure a read replica and create a copy of the infrastructure. When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance. Update the DNS record to point to the other region's ELB

B. Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance. Create an AWS CloudFormation template of the application infrastructure that uses the latest snapshot When an issue occurs, use the AWS CloudFormation template to create the environment in another region. Update the DNS record to point to the other region's ELB

C. Configure a 1-day window of 60 minute snapshots of the Amazon RDS Multi-AZ database instance which is copied to another region. Create an AWS CloudFormation template of the application infrastructure that uses the latest copied snapshot. When an issue occurs, use the AWS CloudFormation template to create the environment in another region Update the DNS record to point to the other region's ELB

D. Configure a read replica in another region. Create an AWS CloudFormation template of the application infrastructure When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance and use the AWS CloudFormation template to create the environment in another region using the promoted Amazon RDS instance. Update the DNS record to point to the other region's ELB

答案：D

55. The Solutions Architect manages a serverless application that consists of multiple API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables Customers say that a few application components slow while loading dynamic images, and some are timing out with the "504 Gateway Timeout" error While troubleshooting the scenario, the Solutions Architect confirms that DynamoDB monitoring metrics are at acceptable levels

Which of the following steps would be optimal for debugging these application issues? （Select Two）

A. Parse HTTP logs in Amazon API Gateway for HTTP errors to determine the root cause of the errors

B. Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals

C. Parse VPC Flow Logs to determine if there is packet loss between the Lambda function and S3
D. Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors
E. Parse S3 access logs to determine if objects being accessed are from specific IP addresses to narrow the scope to geographic latency issues
答案：BD

56. A company's application is increasingly popular and experiencing latency because of high volume reads on the database server
The service has the following properties :
- •A highly available REST API hosted in one region using an Application Load Balancer（ALB）with auto scaling
- •A MySQL database hosted on an Amazon EC2 instance in a single Availability Zone

The company wants to reduce latency, increase in-region database read performance, and have multi-region disaster recovery capabilities that can perform a live recovery automatically without any data or performance loss（HA/DR）
Which deployment strategy will meet these requirements?
A. Use AWS CloudFormation Stack Sets to deploy the API layer in two regions Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region and a read replica in a different region than the source database cluster. Use Amazon Route 53 health checks to trigger a DNS failover to the standby region if the health checks to the primary load balancer fail. In the event of Route 53 failover, promote the cross-region database replica to be the master and build out new read replicas in the standby region
B. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries Use AWS OpsWorks to deploy the APl layer, cache layer, and existing database layer in two regions. In the event of failure, use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail Back up the MySQL database frequently and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database
C. Use AWS Cloud Formation Stack Sets to deploy the API layer in two regions. Add the database to an Auto Scaling group Add a read replica to the database in the second region. Use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Promote the cross-region database replica to be the master and build out new read replicas in the standby region
D. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries, Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions .Use Amazon Route 53 health checks on the ALB to trigger a DNS failover to the standby region if the health checks in the primary region fail Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database
答案：A

57. AnyCompany has acquired numerous companies over the past few years. The ClO for Any Company would like to keep the resources for each acquired company separate. The CIO also would like to enforce a chargeback model where each company pays for the AWS services it uses
The Solutions Architect is tasked with designing an AWS architecture that allows Any Company to achieve the following
- •Implementing a detailed chargeback mechanism to ensure that each company pays for the resources it uses •Any Company can pay for AWS services for all its companies through a single invoice
- •Developers in each acquired company have access to resources in their company only

•Developers in an acquired company should not be able to affect resources in any other company
•A single identity store is used to authenticate Developers across all companies
Which of the following approaches would meet these requirements? (Select Two)
A. Create a multi-account strategy with an account per company. Use consolidated billing to ensure that Any Company needs to pay a single bill only
B. Create a single account strategy with a virtual private cloud (VPC) for each company Reduce impact across companies by not creating any VPC peering links. As everything is in a single account, there will be a single invoice. Use tagging to create a detailed bill for each company
C. Create lAM users for each Developer in the account to which they require access. Create policies that allow the users access to all resources in that account. Attach the policies to the lAM user
D. Create a federated identity store against the company's Active Directory. Create lAM roles with appropriate permissions and set the trust relationships with AWS and the identity store. Use AWS STS to grant users access based on the groups they belong to in the identity store
E. Create a multi-account strategy with an account per company. For billing purposes, use a tagging solution that uses a tag to identify the company that creates each resource
答案: AD

58. A company that is new to AWS reports it has exhausted its service limits across several accounts that are on the Basic Support plan. The company would like to prevent this from happening in the future
What is the MOST efficient way of monitoring and managing all service limits in the company's accounts?
A. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor; provide notifications using Amazon SNS if the limits are close to exceeding the threshold
B. Reach out to AWS Support to proactively increase the limits across all accounts. That way, the customer avoids creating and managing infrastructure just to raise the service limits
C. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, programmatically increase the limits that are close to exceeding the threshold
D. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, and use Amazon SNS for notifications if a limit is close to exceeding the threshold. Ensure that the accounts are using the AWS Business Support plan at a minimum
答案: D

59. An on-premises application will be migrated to the cloud. The application consists of a single Elasticsearch virtual machine with data source feeds from local systems that will not be migrated, and a Java web application on Apache Tomcat running on three virtual machines. The Elasticsearch server currently uses 1 TB of storage out of 16 TB available storage, and the web application is updated every 4 months. Multiple users access the web application from the internet. There is a 10Gbit AWS Direct Connect connection established, and the application can be migrated over a scheduled 48-hour change window
Which strategy will have the LEAST impact on the Operations staff after the migration?
A. Create an Elasticsearch server on Amazon EC2 right-sized with 2 TB of Amazon EBS and a public AWS Elastic Beanstalk environment for the web application. Pause the data sources, export the Elasticsearch index from on premises, and import into the EC2 Elasticsearch server move data source feeds to the new Elasticsearch server and move users to the web application
B. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application Use AWS DMS to replicate Elasticsearch data When replication has finished, move data source feeds to the new Amazon ES cluster endpoint and move users to the new web application
C. Use the AWS SMS to replicate the virtual machines into AWS. When the migration is complete, pause the data source feeds and start the migrated Elasticsearch and web application instances. Place the web

application instances behind a public Elastic Load Balancer. Move the data source feeds to the new Elasticsearch server and move users to the new web Application Load Balancer

D. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application Pause the data source feeds, export the Elasticsearch index from on premises, and import into the Amazon ES cluster Move the data source feeds to the new Amazon ES cluster endpoint and move users to the new web application

答案：D

60.A Development team has created a series of AWS Cloud Formation templates to help deploy services. They created a template for a network/virtual private cloud （VPC） stack, a database stack, a bastion host stack, and a web application-specific stack. Each service requires the deployment of at least:

·A network/VPC stack

·A bastion host stack

·A web application stack

Each template has multiple input parameterschat make it difficult to deploy the services individually from the AWS CloudFormation console. The input parameters from one stack are typically outputs from other stacks. For example, the VPC ID, subnet IDs, and security groups from the network stack may need to be used in the application stack or database stack.

Which actions will help reduce both the operational burden and the number of parameters passed into a service deployment？(Select TWO)

A. Create a new AWS Cloud Formation template for each service. Alter the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Call the newly created service stack from the AWS CloudFormation console to deploy the specific service with a subset of the parameters previously required

B. Create a new portfolio in AWS Service Catalog for each service. Create a product for each existing AWS CloudFormation template required to build the service. Add the products to the portfolio that represents that service in Aws Service Catalog. To deploy the service, select the specific service portfolio and launch the portfolio with the necessary parameters to deploy all templates

C. Set up an AWS Code Pipeline workflow for each service. For each existing template, choose AWS CloudFormation as a ployment action. Add the oud Formation template to the deployment action. Ensure that the deployment actions are processed to make sure that dependencies are obeyed. Use configuration files and scripts to share parameters between the stacks. To launch the service, execute the specific template by choosing the name of the service and releasing a change

D. Use Aws Step Functions to define a new service. Create a new AWS CloudFormation template for each service. Alter the existing templates to use cross-stack references to eliminate passing arameters to each template. Call each required stack for the application as a nested stack from the new service template. Configure AWS Step Functions to call the service template directly. In the AWS Step Functions console, execute the step

E. Create a new portfolio for the services in AWS Service Catalog. Create a new AWS CloudFormation template for each service. Alter the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Create a product for each application. Add the service template to the product. Add each new product to the portfolio. Deploy the product from the portfolio to deploy the service with the necessary parameters only to start the deployment

答案：CE

61.A company is migrating its marketing website and content management system from an on-premises data center to AWS. The company wants the AWS application to be deployed in a VPC with Amazon EC2

instances used for the web servers and an Amazon RDS instance for the database.
The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers. After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.
How can the application and environment be deployed and automated in AWS, while allowing for future changes?
A. Update the runbook to describe how to create the VPC, the EC2 instances, and the RDS instance for the application by using the AWS Console. Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration
B. Write a Python script that uses the AWS API to create the VPC, the EC2 instances, and the RDS instance for the application. Write shell scripts that implement the rest of the steps in the runbook. Have the python script copy and run the shell scripts on the newly created instances to complete the installation
C. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration
D. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Include EC2 user data in the AWS CloudFormation template to install and configure the software
答案：D

62.An internal security audit of AWS resources within a company found that a number of Amazon EC2 instances running Microsoft Windows workloads were missing several important operating system-level patches. A Solutions Architect has been asked to fix existing patch deficiencies, and to develop a workflow to ensure that future patching requirements are identified and taken care of quickly. The Solutions Architect has decided to use AWS Systems Manager. It is important that EC2 instance reboots do not occur at the same time on all Windows workloads to meet organizational uptime requirements.
Which workflow will meet these requirements in an automated manner?
A. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline to the Windows Servers patch group. Define an AWS Systems Manager maintenance window, conduct patching within it, and associate it with the Windows Servers patch group. Register instances with the maintenance window using associated subnet IDs. Assign the AWS-Run Patch Baseline document as a task within each maintenance window
B. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the Aws-Windows Patch Baseline to the Windows Servers patch group. Create an Amazon CloudWatch Events rule configured to use a cron expression to schedule the execution of patching using the AWS Systems Manager run command. Assign the AWS-RunwindowsPatchBaseline document as a task associated with the windows Servers patch group, Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution
C. Add a Patch Group tag with a value of either Windows Servers 1 or Windows Servers2 to all existing EC2 instances Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline with both Windows Servers patch groups.Define two non-overlapping AWS Systems Manager maintenance windows, conduct atching within them, and associate each with a different patch group. Register targets with specific maintenance indows using the Patch Group tags. Assign the AWs-Run Patch Baseline document as a task within each maintenance window

D. Add a Patch Group tag with a value of either Windows servers 1 or Windows servers2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the Aws-WindowsPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Assign the AWS-RunWindowsPatchBaseline document as a task within each maintenance window. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution

答案：C

63.A Solutions Architect has created an AWS CloudFormation template for a three-tier application that contains an Auto Scaling group of Amazon EC2 instances running a custom AMI .

The Solutions Architect wants to ensure that future updates to the custom AMI can be deployed to a running stack by first updating the template to refer to the new AMI, and then invoking Updatestack to replace the EC2 instances with instances launched from the new AMI.

How can updates to the AMI be deployed to meet these requirements?

A. Create a change set for the new version of the template,view the changes to the running EC2 instances to ensure that the AMI is correctly updated, and then execute the change set

B. Edit the aws::AutoScaling::LaunchConfiguration resource in the template, changing its Deletion Policy to Replace

C. Edit the AWS::Autoscaling::AutoScalingGroup resource in the template, inserting an Update Policy attribute

D. Create a new stack from the updated template. Once it is successfully deployed, modify the DNS records to the new stack and delete the old stack

答案：C

64.A company operating a website on AWS requires high levels of scalability, availability,and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage. Amazon CloudFront is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution.

Which solution is the MOST cost-effective at scale?

A. Implement Multi-AZ and Auto Scaling for all EC2 instances in the current configuration. Ensure that all EC2 instances are purchased as reserved instances.Implement new elastic Amazon EBS volumes for the data tier.

B. Design and implement a Docker-based containerized solution for the application using Amazon ECS.Migrate to an Amazon Aurora MySQL Multi-AZ cluster.Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow the Aurora My SQL storage, as necessary. Ensure that Multi-AZ architectures are implemented

C. Ensure that EC2 instances are right-sized and behind an Elastic Load Balancing load balancer. Implement Auto Scaling with EC2 instances.Ensure that reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand.Migrate to an Amazon Aurora My SQL Multi-AZ cluster.Ensure that Multi-AZ architectures are implemented

D. Ensure that EC2 instances are right-sized behind an Elastic Load Balancer.Implement Auto Scaling with EC2 instances. Ensure that Reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand. Migrate to an Amazon Aurora My SQL Multi-AZ cluster Implement storage checks for Aurora My SQL storage utilization and an AWS Lambda function to grow Aurora MySQL storage, as necessary. Ensure Multi-AZ architectures are implemented

答案：C

65.A company wants to replace its call center system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the callers and handle basic tasks, reducing the need to speak to an agent. The solution should also be able to query business applications and provide relevant information back to callers as requested

Which services should the Solutions Architect use to build this solution？（Select THREE ）

A. Amazon Rekognition to identify who is calling

B. Amazon Connect to create a cloud-based contact center

C Amazon Alexa for Business to build conversational interfaces

D. AWS Lambda to integrate with intemal systems

E. Amazon Lex to recognize the intent of the caller

F. Amazon SQS to add incoming callers to a queue

答案：BDE

66.A company needs to run a software package that has a license that must be run on the same physical host for the duration of its use. The software package is only going to be used for 90 days. The company requires patching and restarting of all instances every 30 days.

How can these requirements be met using AWS?

A. Run a dedicated instance with auto-placement disabled

B. Run the instance on a dedicated host with Host Affinity set to Host

C. Run an On-Demand Instance with a Reserved Instance to ensure consistent placement

D. Run the instance on a licensed host with termination set for 90 days

答案：B

67.A company runs a video processing platform. Files are uploaded by users who connect to a web server, which stores them on an Amazon EFS share. This web server is running on a single Amazon EC2 instance. A different group of instances, running in an Auto Scaling group, scans the EFS share directory structure for new files to process and generates new videos（thumbnails, different resolution, compression, etc. ）according to the instructions file, which is uploaded along with the video files. A different application running on a group of instances managed by an Auto Scaling group processes the video files and then deletes them from the EFS share. The results are stored in an S3 bucket. Links to the processed video files are emailed to the customer.

The company has recently discovered that as they add more instances to the Auto Scaling Group, many files are processed twice, so image processing speed is not improved. The maximum size of these video files is 2GB.

What should the Solutions Architect do to improve reliability and reduce the redundant processing of video files?

A. Modify the web application to upload the video files directly to Amazon S3. Use Amazon CloudWatch Events to trigger an AWS Lambda function every time a file is uploaded, and have this Lambda function put a message into an Amazon SQS queue. Modify the video processing application to read from the SQS queue for new files and use the queue depth metric to scale instances in the video processing Auto Scaling group

B. Set up a cron job on the web server instance to synchronize the contents of the EFS share into Amazon S3. Trigger an AWS Lambda function every time a file is uploaded to process the video file and store the results in Amazon S3. Using Amazon Cloud Watch Events, trigger an Amazon SES job to send an email to the customer containing the link to the processed file

C. Rewrite the web application to run directly from Amazon S3 and use Amazon API Gateway to upload the video files to an S3 bucket. Use an S3 trigger to run an AWS Lambda function each time a file is uploaded to process and store new video files in a different bucket. Using CloudWatch Events, trigger an SES job to send an email to the customer containing the link to the processed file

D. Rewrite the web application to run from Amazon S3 and upload the video files to an S3 bucket. Each time a new file is uploaded, trigger an AWS Lambda function to put a message in an SQS queue containing the link and the instructions. Modify the video processing application to read from the SQS queue and the S3 bucket. Use the queue depth metric to adjust the size of the Auto Scaling group for video processing instances

答案：D

68.A company is using AWS for production and development workloads. Each business unit has its own AWS account for production, and a separate AWS account to develop and deploy its applications. The Information Security department has introduced new security policies that limit access for terminating certain Amazon EC2 instances in all accounts to a small group of individuals from the Security team.

How can the Solutions Architect meet these requirements?

A. Create a new IAM policy that allows access to those EC2 instances only for the Security team. Apply this policy to the AWS Organizations master account.

B. Create a new tag-based IAM policy that allows access to these EC2 instances only for the Security team. Tag the instances appropriately, and apply this policy in each account.

C. Create an organizational unit under AWS Organizations. Move all the accounts into this organizational unit and use SCP to apply a whitelist policy to allow access to these EC2 instances for the Security team only

D. Set up SAML federation for all accounts in AWS. Configure SAML so that it checks for the service API call before authenticating the user. Block SAML from authenticating API calls if anyone other than the security team accesses these Instances

答案：B

69. A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The Quality Assurance（QA）department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the Manager of the department using an AWS CloudFormation template. To launch the stack, the Manager uses a role with permission to use CloudFormation, EC2, and Auto Scaling APIs. The Manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user.

Which set up would achieve these goals?

A. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the Managers role and add a policy that restricts the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console

B. Create an AWS Service Catalog product from the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the template from the Aws Service Catalog console

C. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permissions to the template and the resources it creates. Train users to launch the template from the Cloud Formation console

D. Create an AWS Elastic Beanstalk application from the environment template. Give users in the QA department permission to use Elastic Beanstalk permissions only. Train users to launch Elastic Beanstalk environments with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role

答案：D

70.A company receives clickstream data files to Amazon S3 every five minutes. A Python script runs as a cron joblonce a day on an Amazon EC2 instance to process each file and load it into a database hosted on Amazon RDS. The cron job takes 15 to 30 minutes to process 24 hours of data. The data consumers ask for the data be available as soon as possible.
Which solution would accomplish the desired outcome?
A. Increase the size of the instance to speed up processing and update the schedule to run once an hour
B. Convert the cron job to an AWS Lambda function and trigger this new function using a cron job on an EC2 instance.
C. Convert the cron job to an AWS Lambda function and schedule it to run once an hour using Amazon CloudWatch Events
D. Create an AWS Lambda function that runs when a file is delivered to Amazon S3 using S3 event notifications
答案：D

71. A company is running a commercial Apache Hadoop cluster on Amazon EC2. This cluster is being used daily to query large files on Amazon S3. The data on Amazon S3 has been curated and does not require any additional transformation steps. The company is using a commercial business intelligence（BI） tool on Amazon EC2 to run queries against the Hadoop cluster and visualize the data
The company wants to reduce or eliminate the overhead costs associated with managing the Hadoop cluster and the Bl tool. The company would like to move to a more cost-effective solution with minimal effort. The visualization is simple and requires performing some basic aggregation steps only .
Which option will meet the company's requirements?
A. Lunch a transient Amazon EMR cluster daily and develop an Apache Hive script to analyze the files on Amazon S3. Shut down the Amazon EMR cluster when the job is complete. Then use Amazon Quick Sight to connect to Amazon EMR and perform the visualization
B. Develop a stored procedure invoked from a MySQL database running on Amazon EC2 to analyze the files in Amazon S3
Then use a fast in-memory BI tool running on Amazon EC2 to visualize the data
C. Develop a script that uses Amazon Athena to query and analyze the files on Amazon S3.Then use Amazon QuickSight to connect to Athena and perform the visualization
D. Use a commercial extract, transform, load（ETL） tool that runs on Amazon EC2 to prepare the data for processing. Then switch to a faster and cheaper Bl tool that runs on Amazon EC2 to visualize the data from Amazon S3.
答案：C

72.A company runs a Windows server host in a public subnet that is configured to allow a team of administrators to connect over RDP to troubleshoot issues with hosts in a private subnet. The host must be available at all times outside of a scheduled maintenance window, and needs to receive the latest operating system updates within 3 days of release.
What should be done to manage the host with the LEAST amount of administrative effort?
A. Run the host in a single-instance AWS Elastic Beanstalk environment. Configure the environment with a custom AMI to use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch Manager
B. Run the host on AWS Work Spaces. Use Amazon Work Spaces Application Manager（WAM）to harden the host. Configure Windows automatic updates to occur every 3 days
C. Run the host in an Auto Scaling group with a minimum and maximum instance count of 1. Use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch

Manager
D. Run the host in AWS OpsWorks Stacks, Use a Chef recipe to harden the AMI during instance launch. Use an AWS Lambda scheduled event to run the Upgrade Operating System stack command to apply system updates
答案：B

73.A company is migrating a subset of its application APIs from Amazon EC2 instances to run on a serverless infrastructure. The company has set up Amazon API Gateway, AWS Lambda, and Amazon DynamoDB for the new application. The primary responsibility of the Lambda function is to obtain data from a third-party Software as a Service（SaaS） provider. For consistency, the Lambda function is attached to the same virtual private cloud （VPC）as the original EC2 instances.
Test users report an inability to use this newly moved functionality, and the company is receiving 5xx errors from API Gateway. Monitoring reports from the SaaS provider shows that the requests never made it to its systems. The company notices that Amazon CloudWatch Logs are being generated by the Lambda functions. When the same functionality is tested against the EC2 systems, it works as expected.
What is causing the issue?
A. Lambda is in a subnet that does not have a NAT gateway attached to it to connect to the SaaS provider
B. The end-user application is misconfigured to continue using the endpoint backed by EC2 instance
C. The throttle limit set on API Gateway is too low and the requests are not making their way through
D. API Gateway does not have the necessary permissions to invoke Lambda
一家公司正在将其应用程序 API 的一个子集从 Amazon EC2 实例迁移到无服务器基础结构上运行。该公司为新应用程序设置了 Amazon API Gateway、 AWS Lambda 和 Amazon DynamoDB. Lambda 函数主要用于从第三方软件即服务（SaaS）供应商处获取数据。为了保持一致性， Lambda 函数附加到与原始 EC2 实例相同的虚拟私有云（VPC）上。
测试用户报告无法使用这个新移动的功能，且公司从 API Gateway 接收到 5xx 错误。来自 SaaS 供应商的监控报告显示，请求从未成功发送到其系统。公司注意到 Amazon CloutWatch 日志是由 Lambda 函数生成的。当在 EC2 系统上测试相同的功能时，它按照预期工作.
什么导致了这个问题?
A. Lambda 位于子网中，子网没有连接到 SaaS 供应商的 NAT 网关。
B. 终端用户应用程序被错误配置为继续使用 EC2 实例支持的端点。
C. API 网关上设置的节流阀限制太低，请求无法通过
D. API 网关没有调用 Lambda 所需的权限。
答案：A

74.A company must deploy multiple independent instances of an application. The front-end application is internet accessible. However corporate policy stipulates that the backends are to be isolated from each other and the internet, yet accessible from a centralized administration server. The application setup should be automated to minimize the opportunity for mistakes as new instances are deployed
Which option meets the requirements and MINIMIZES costs?
A. Use an AWS CloudFormation template to create identical IAM roles for each region. Use AWS CloudFormation StackSets to deploy each application instance by using parameters to customize for each instance, and use security groups to isolate each instance while permitting access to the central server
B. Create each instance of the application IAM roles and resources in separate accounts by using AWS CloudFormation StackSets. Include a VPN connection to the VPN gateway of the central administration server
C. Duplicate the application IAM roles and resources in separate accounts by using a single AWS CloudFormation template Include VPC peering to connect the VPC of each application instance to a central VPC

D. Use the parameters of the AWS CloudFormation template to customize the deployment into separate accounts. Include a NAT gateway to allow communication back to the central administration server
答案：B

75.A three-tier web application runs on Amazon EC2 instances. Cron daemons are used to trigger scripts that collect the web server, application, and database logs and send them to a centralized location every hour. Occasionally, scaling events or unplanned outages have caused the instances to stop before the latest logs were collected and the log files were lost.
Which of the following options is the MOST reliable way of collecting and preserving the log files?
A. Update the cron jobs to run every 5 minutes instead of every hour to reduce the possibility of log messages being lost in an outage
B. Use Amazon CloudWatch Events to trigger Amazon Systems Manager Run Command to invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage
C. Use the Amazon CloudWatch Logs agent to stream log messages directly to CloudWatch Logs. Configure the agent with a batch count of 1 to reduce the possibility of log messages being lost in an outage
D. Use Amazon CloudWatch Events to trigger AWS Lambda to SSH into each running instance, and invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage
答案：C

76. A company stores sales transaction data in Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes to the items stored in the DynamoDB tables must be logged within 30 minutes Which solution meets the requirements?
A. Copy the DynamoDB tables into Apache Hive tables on Amazon EMR every hour and analyze them for anomalous behaviors Send Amazon SNS notifications when anomalous behaviors are detected
B. Use AWS Cloud Trail to capture all the APIs that change the DynamoDB tables Send SNS notifications when anomalous behaviors are detected using Cloud Trail event filtering
C. Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda. Create a Lambda function to output records to Amazon Kinesis Data Streams. Analyze any anomalies with Amazon Kinesis Data Analytics. Send SNS notifications when anomalous behaviors are detected
D. Use event patterns in Amazon CloudWatch Events to capture DynamoDB API call events with an AWS Lambda function as a target to analyze behavior. Send SNS notifications when anomalous behaviors are detected
答案：C

77. A company's data center is connected to the AWS Cloud over a minimally used 10 Gbps AWS Direct Connect connection with a private virtual interface to its virtual private cloud （VPC）. The company internet connection is 200 Mbps, and the company has a 150 TB dataset that is created each Friday. The data must be transferred and available in Amazon S3 on Monday morning
Which is the LEAST expensive way to meet the requirements while allowing for data transfer growth?
A. Order two 80 TB AWS Snowball appliances Offload the data to the appliances and ship them to AWS. AWS will copy the data from the snowball appliances to Amazon S3
B. Create a VPC endpoint for Amazon S3. Copy the data to Amazon S3 by using the VPC endpoint, forcing the transfer to use the Direct Connect connection
C. Create a VPC endpoint for Amazon S3. Set up a reverse proxy farm behind a Classic Load Balancer in the VPC. Copy the data to Amazon S3 using the proxy
D. Create a public virtual interface on a Direct Connect connection, and copy the data to Amazon S3 over the connection
答案：D

78. A company has developed a web application that runs on Amazon EC2 instances in one AWS Region. The company has taken on new business in other countries and must deploy its application into other regions to meet low-latency requirements for its users. The regions can be segregated, and an application running in one region does not need to communicate with instances in other regions.
How should the company's Solutions Architect automate the deployment of the application so that it can be MOST efficiently deployed into multiple regions?
A. Write a bash script that uses the AWS CLI to query the current state in one region and output a JSON representation. Pass the JSON representation to the AWS CLI, specifying the --region parameter to deploy the application to other regions
B. Write a bash script that uses the AWS CLI to query the current state in one region and output an AWS CloudFormation template. Create a CloudFormation stack from the template by using the AWS CLI, specifying the --region parameter to deploy the application to other regions
C. Write a CloudFormation template describing the application s infrastructure in the resources section. Create a CloudFormation stack from the template by using the AWS CLI, specify multiple regions using the --regions parameter to deploy the application.
D. Write a Cloud Formation template describing the application's infrastructure in the Resources section. Use a CloudFormation stack set from an administrator account to launch stack instances that deploy the application to other regions
答案：D

79. A company that provides wireless services needs a solution to store and analyze log files about user activities. Currently, log files are delivered daily to Amazon Linux on an Amazon EC2 instance. A batch script is run once a day to aggregate data used for analysis by a third-party tool. The data pushed to the third-party tool is used to generate a visualization for end users. The batch script is cumbersome to maintain, and it takes several hours to deliver the ever-increasing data volumes to the third-party tool. The company wants to lower costs, and is open to considering a new tool that minimizes development effort and lowers administrative overhead. The company wants to build a more agile solution that can store and perform the analysis in near-real time, with minimal overhead. The solution needs to be cost effective and scalable to meet the company s end-user base growth.
Which solution meets the company's requirements?
A. Develop a Python script to capture the data from Amazon EC2 in real time and store the data in Amazon S3. Use a copy command to copy data from Amazon S3 to Amazon Redshift Connect a business intelligence tool running on Amazon EC2 to Amazon Redshift and create the visualizations
B. Use an Amazon Kinesis agent running on an EC2 instance in an Auto Scaling group to collect and send the data to an Amazon Kinesis Data Firehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data directly to Amazon Es. Use kibana to visualize the data
C. Use an in-memory caching application running on an Amazon EBS-optimized EC2 instance to capture the log data in near real-time. Install an Amazon ES cluster on the same EC2 instance to store the log files as they are delivered to Amazon EC2 in near real-time. Install a Kibana plugin to create the visualizations
D. Use an Amazon Kinesis agent running on an EC2 instance to collect and send the data to an Amazon Kinesis Data Firehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data to Amazon S3. Use an AWS Lambda function to deliver the data from Amazon S3 to Amazon ES. Use Kibana to visualize the data.
答案：B

80. A large global company wants to migrate a stateless mission-critical application to AWS. The application is based on IBM WebSphere (application and integration middleware), IBM MQ (messaging

middleware ）， and IBM DB2 （database software）on a z/OS operating system.
How should the Solutions Architect migrate the application to AWS?
A. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM MQ to an Amazon EC2-based MQ Re-platform the z/OS-based DB2 to Amazon RDS DB2
B. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling Re-platform the IBM MQ to an Amazon MQ. Re-platform z/OS-based DB2 to Amazon EC2-based DB2
C. Orchestrate and deploy the application by using AWS Elastic Beanstalk Re- platform the IBM MQ to Amazon SQS. Re-platform z/OS-based DB2 to Amazon RDS DB2.
D. Use the AWS Server Migration Service to migrate the IBM WebSphere and IBM DB2 to an Amazon EC2-based solution Re-platform the IBM MQ to an Amazon MQ.
答案：B

81. A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions. and also reduce the time to detect and revert when errors are identified.
How can this be accomplished?
A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function For changes to Lambda, create an AWS CloudFormation change set and deploy: if errors are triggered, revert the AWS CloudFormation change set to the previous version.
B. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version and use pre-traffic and post-traffic test functions to verify code. Rollback if Amazon CloudWatch alarms are triggered.
C. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version
D. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint
答案：B

82. A Solutions Architect must create a cost-effective backup solution for a company's 500MB source code repository of proprietary and sensitive applications. The repository runs on Linux and backs up daily to tape. Tape backups are stored for 1 year.
The current solution is not meeting the company's needs because it is a manual process that is prone to error, expensive to maintain and does not meet the need for a Recovery Point Objective（RPO）of 1 hour or Recovery Time Objective（RTO）of 2 hours. The new disaster recovery requirement is for backups to be stored offsite and to be able to restore a single file if needed.
Which solution meets the customer’s needs for RTO, RPO, and disaster recovery with the LEAST effort and expense?
A. Replace local tapes with an AWS Storage Gateway virtual tape library to integrate with current backup software. Run backups nightly and store the virtual tapes on Amazon S3 standard storage in US-EAST-1. Use cross-region replication to create a second copy in US-WEST-2. Use Amazon S3 lifecycle policies to perform automatic migration to Amazon Glacier and deletion of expired backups after 1 year.
B. Configure the local source code repository to synchronize files to an AWS Storage Gateway file Amazon

gateway to store backup copies in an Amazon S3 Standard bucket. Enable versioning on the Amazon S3 bucket. Create Amazon S3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard- Infrequent Access, then Amazon Glacier, then delete backups after 1 year .

C. Replace the local source code repository storage with a Storage Gateway stored volume. Change the default snapshot frequency to 1 hour. Use Amazon S3 lifecycle policies to archive snapshots to Amazon Glacier and remove old snapshots after 1 year . Use cross-region replication to create a copy of the snapshots in US-WEST-2.

D. Replace the local source code repository storage with a Storage Gateway cached volume. Create a snapshot schedule to take hourly snapshots. Use an Amazon CloudWatch Events schedule expression rule to run an hourly AWS Lambda task to copy snapshots from US-EAST-1 to US-WEST-2

答案：B

83. A company is running multiple applications on Amazon EC2. Each application is deployed and managed by multiple business units. All applications are deployed on a single AWS account but on different virtual private clouds（VPCs）. The company uses a separate VPC in the same account for test and development purposes. Production applications suffered multiple outages when users accidentally terminated and modified resources that belonged to another business unit. A Solutions Architect has been asked to improve the availability of the company applications while allowing the Developers access to the resources they need.

Which option meets the requirements with the LEAST disruption?

A. Create an AWS account for each business unit Move each business unit's instances to its own account and set up a federation to allow users to access their business unit’s account

B. Set up a federation to allow users to use their corporate credentials, and lock the users down to their own VPC. Use a network ACL to block each VPC from accessing other VPCs

C. Implement a tagging policy based on business units. Create an IAM policy so that each user can terminate instances belonging to their own business units only

D. Set up role- based access for each user and provide limited permissions based on individual roles and the services for which each user is responsible

答案：c

解析：C 是 ABAC 模式，使用标签来决定访问权，D 的话不是不可以，但是每个新创建的 EC2，都需要单独再修改每个人的 IAM，使用的是 RBAC，烦人度几何级增加

84.

An organization has recently grown through acquisitions. Two of the purchased companies use the same IP CIDR range. There is a new short-term requirement to allow AnyCompany A（VPC-A）to communicate with a server that has the IP address 10.0.0.77in AnyCompany B（VPC-B）。 AnyCompany A must also communicate with all resources in AnyCompany C （VPC-C） The Network team has created the VPC peer links, but it is having issues with communications between VPC-A and VPC-B. After an investigation, the team believes that the routing tables in the VPCs are incorrect

What configuration will allow AnyCompany A to communicate with AnyCompany C in addition to the database in AnyCompany B?

A. On VPC-A, create a static route for the VPC-B CIDR range（10.0.0.0/24）across VPC peer pcx-AB
Create a static route of 10.0.0.0/16 across VPC peer pcx-AC
On VPC-B, create a static route for VPC-A CIDR（172. 16.0.0/24）on peer pcx-AB
On VPC-C, create a static route for VPC-A CIDR （172. 16.0.0/24）across peer pcx-AC

B. On VPC-A, enable dynamic route propagation on pcx-AB and pcx-AC
On VPC-B, enable dynamic route propagation and use security groups to allow only the IP address 10.0.0.77/32 on VPC peer pcx-AB
On VPC-C, enable dynamic route propagation with VPC.A on peer pcx-AC

C. On VPC-A create network access control lists that block the IP address 10.0.0.77/32 on VPC peer pcx-AC.
On VPC-A, create a static route for VPC-B CIDR（10.0.0.0/24）on pcx-AB and a static route for VPC-C CIDR（10.0.0.0/24）on pcx-AC
On VPC-B, create a static route for VPC-A CIDR （172. 16.0.0/24）on peer pcx-AB
On VPC-C, create a static route for VPC-A CIDR （172. 16.0.0/24）across peer pcx-AC

D. On VPC-A, create a static route for the VPC-B（10.0.0 77/32）database across VPC peer pcx-AB
Create a static route for the VPC-C CIDR on VPC peer pcx-AC
On VPC-B, create a static route for VPC-A CIDR（172. 16.0.0/24）on peer pcx-AB
On VPC-C create a static route for VPC-A CIDR （172. 16.0 0/24） across peer pcx-AC

答案：D

85. A company has a website that enables users to upload videos. Company policy states the uploaded videos must be analyzed for restricted content. An uploaded video is placed in Amazon S3， and a message is pushed to an Amazon SQS queue with the video's location, A backend application pulls this location from Amazon SQS and analyzes the video

The video analysis is compute-intensive and occurs sporadically during the day. The website scales with demand. The video analysis application runs on a fixed number of instances. Peak demand occurs during the holidays, so the company must add instances to the application during this time. All instances used are currently on-demand Amazon EC2 T2 instances. The company wants to reduce the cost of the current solution

Which of the following solutions is MOST cost-effective?

A. Keep the website on T2 instances. Determine the minimum number of website instances required during off-peak times and use Spot Instances to cover them while using Reserved Instances to cover peak demand. Use Amazon EC2 R4 and Amazon EC2 R5 Reserved Instances in an Auto Scaling group for the video analysis application

B. Keep the website on T2 instances. Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand. Use Spot Fleet for the video analysis application comprised of Amazon EC2 C4 and Amazon EC2 C5 Spot Instances

C. Migrate the website to AWS Elastic Beanstalk and Amazon EC2 C4 instances. Determine the minimum number of website instances required during off-peak times and use On-Demand instances to cover them while using Spot capacity to cover peak demand. Use Spot Fleet for the video analysis application comprised of C4 and Amazon EC2 C5 instances.
D. Migrate the website to AWS Elastic Beanstalk and Amazon EC2 R4 instances. Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand. Use Spot Fleet for the video analysis application comprised of R4 and Amazon EC2 R5 instances.
答案：B

86. A company is implementing a multi-account strategy；however, the Management team has expressed concerns that services like DNS may become overly complex. The company needs a solution that allows private DNS to be shared among virtual private clouds （VPCs）in different accounts. The company will have approximately 50 accounts in total.
What solution would create the LEAST complex DNS architecture and ensure that each VPC can resolve all AWS resources?
A. Create a shared services VPC in a central account, and create a VPC peering connection from the shared services VPC to each of the VPCs in the other accounts Within Amazon Route 53， create a privately hosted zone in the shared services VPC and resource record sets for the domain and subdomains. Programmatically associate other VPCs with the hosted zone
B. Create a VPC peering connection among the VPCs in all accounts. Set the VPC attributes enableDnsHostnames and enableDnsSupport to "true" for each VPC. Create an Amazon Route 53 private zone for each VPC. Create resource record sets for the domain and subdomains. Programmatically associate the hosted zones in each VPC with the other VPCs.
C. Create a shared services VPC in a central account. Create a VPC peering from the VPCs in other accounts to the shared services VPC. Create an Amazon Route 53 privately hosted zone in the shared services VPC with resource record sets for the domain and subdomains. Allow UDP and TCP port 53 over the VPC peering connections
D. Set the VPC attributes enableDnsHostnames and enableDnsSupport to "false" in every VPC. Create an AWS Direct Connect connection with a private virtual interface. Allow UDP and TCP port 53 over the virtual interface. Use the on- premises DNS servers to resolve the IP addresses in each VPC on AWS
一家公司正在实施多账户策略；然而，管理团队担心像 DNS 这样的服务可能会变得过于复杂。公司需要一种解决方案，允许在不同帐户中的虚拟私有云（VPC）之间共享私有 DNS。该公司将总共有大约 50 个账户
什么解决方案可以创建复杂度最低的 DNS 架构并确保每个 VPC 可以解析所有的 AWS 资源?
A. 在中央帐户中创建共享服务 VPC，并创建从共享服务 VPC 到其他帐户中每个 VPC 的 VPC 对等连接。在 Amazon Route53 内，在共享服务 VPC 中创建一个私有托管区域，并为域和子域创建资源记录集。以编程方式将其他 VPC 与托管区域相关联
B. 在所有帐户中的 VPC 之间创建 VPC 对等连接。为每个 VPC 将 VPC 属性 enab1eDnsHthames 和 enableDnsSupport 设置为“true”。为每个 VPC 创建一 Amazon Route53 私有区域。为域和子域创建资源记录集。以编程方式将每个 VPC 中的托管区域与其他 VPC 相关联.
C. 在中央帐户中创建共享服务 VPC。创建从其他帐户中的 VPC 到共享服务 VPC 的 VPC 对等连接。在共享服务 VPC 中创建 Amazon Rσute53 私有托管区域，并为域和子域创建资源记录集。通过 VPC 对等连接允许 UDP 和 TCP 端口 53。
D. 在每个 VPC 中将 VPC 属性 enab1eDnsHostnames 和 enab1eDnsSupport 设置为“ false”。使用专用虚拟接口创建 AWS Direct Connect 连接。通过虚拟接口允许 UDP 和 TCP 端口 53.使用本地 DNS 服务器来解析 AWS 上每 VPC 中的 IP 地址
答案：A

87. A Solutions Architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements:

- Consolidate all accounts into one organization
- Allow full access to the Amazon EC2 service from the master account and the secondary accounts
- Minimize the effort required to add additional secondary accounts

Which combination of steps should be included in the solution？ （Select TWO）

A. Create an organization from the master account. Send invitations to the secondary accounts from the master account Accept the invitations and create an OU

B. Create an organization from the master account. Send a join request to the master account from each secondary account Accept the requests and create an OU

C. Create a VPC peering connection between the master account and the secondary accounts. Accept the request for the VPC peering connection

D. Create a service control policy（SCP）that enables full EC2 access, and attach the policy to the OU

E. Create a full EC2 access policy and map the policy to a role in each account. Trust every other account to assume the role

答案：AD

88. The company Security team requires that all data uploaded into an Amazon S3 bucket must be encrypted. The encryption keys must be highly available and the company must be able to control access on a per-user basis, with different users having access to different encryption keys.

Which of the following architectures will meet these requirements？ （Select TWO）

A. Use Amazon S3 server-side encryption with Amazon S3-managed keys Allow Amazon S3 to generate an AWS/S3 master key, and use lAM to control access to the data keys that are generated.

B. Use Amazon S3 server-side encryption with AWS KMS-managed keys, create multiple customer master keys, and use key policies to control access to them.

C. Use Amazon S3 server-side encryption with customer-managed keys, and use AWS CloudHSM to manage the keys. Use CloudHSM client software to control access to the keys that are generated.

D. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use the CloudHSM client software to control access to the keys that are generated.

E. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use lAM to control access to the keys that are generated in CloudHSM.

答案：BD

89. A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier.

Company policy requires IT to durably store nightly backups of all its data in at least two locations production and disaster recovery The locations must be in different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location. All backup processes must be fully automated.

What is the MOST cost-effective backup solution that will meet all requirements？

A. Back up all the data to a large Amazon EBS volume attached to the backup media server in the production region. Run automated scripts to snapshot these volumes nightly, and copy these snapshots to the disaster recovery region

B. Back up all the data to Amazon S3 in the disaster recovery region. Use a lifecycle policy to move this data to Amazon Glacier in the production region immediately. Only the data is replicated remove the data from

the S3 bucket in the disaster recovery region.
C. Back up all the data to Amazon Glacier in the production region. Set up cross-region replication of this data to Amazon Glacier in the disaster recovery region. Set up a lifecycle policy to delete any data older than 60 days.
D. Back up all the data to Amazon S3 in the production region, Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier
答案：D

90. A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.
Which service will meet the requirements for storing the session information in the MOST cost-effective way?
A. Amazon ElastiCache with the Memcached engine
B. Amazon S3
C. Amazon RDS MySQL
D. Amazon ElastiCache with the Redis engine
答案：D

91. A company is migrating its on-premises build artifact server to an AWS solution. The current system consists of an Apache HTTP server that serves artifacts to clients on the local network, restricted by the perimeter firewall. The artifact consumers are largely build automation scripts that download artifacts via anonymous HTTP, which the company will be unable to modify within its migration timetable.
The company decides to move the solution to Amazon S3 static website hosting The artifact consumers will be migrated to Amazon EC2 instances located within both public and private subnets in a virtual private cloud（VPC）.
Which solution will permit the artifact consumers to download artifacts without modifying the existing automation scripts?
A. Create a NAT gateway within a public subnet of the VPC. Add a default route pointing to the NAT gateway into the route table associated with the subnets containing consumers. Configure the bucket policy to allow the s3：ListBucket and s3：GetObject actions using the condition IpAddress and the condition key aws: Source Ip matching the elastic IP address of the NAT gateway
B. Create a VPC endpoint and add it to the route table associated with subnets containing consumers. Configure the bucket policy to allow s3：ListBucket and s3：GetObject actions using the condition stringEquals and the condition key aws: sourceVpce matching the identification of the VPC endpoint
C. Create an lAM role and instance profile for Amazon EC2 and attach it to the instances that consume build artifacts Configure the bucket policy to allow the s3：ListBucket and s3：GetObjects actions for the principal matching the lAM role created
D. Create a VPC endpoint and add it to the route table associated with subnets containing consumers. Configure the bucket policy to allow s3：ListBucket and s3：GetObject actions using the condition IpAddress and the condition key aws:SourceIp matching the VPC CIDR block.
答案：B

92. A company operates a group of imaging satellites. The satellites stream data to one of the company's ground stations where processing creates about 5 GB of images per minute. This data is added to

network-attached storage, where 2 PB of data are already stored.
The company runs a website that allows its customers to access and purchase the images over the internet. This website is also running in the ground station Usage analysis shows that customers are most likely to access images that have been captured in the last 24 hours.
The company would like to migrate the image storage and distribution system to AWS to reduce costs and increase the number of customers that can be served.
Which AWS architecture and migration strategy will meet these requirements?
A. Use multiple AWS Snowball appliances to migrate the existing imagery to Amazon S3. Create a 1-Gb AWS Direct Connect connection from the ground station to AWS, and upload new data to Amazon S3 through the Direct Connect connection, Migrate the data distribution website to Amazon EC2 instances. By using Amazon S3 as an origin, have this website serve the data through Amazon CloudFront by creating signed URLS
B. Create a 1-Gb Direct Connect connection from the ground station to AWS. Use the AWS Command Line Interface to copy the existing data and upload new data to Amazon S3 over the Direct Connect connection. Migrate the data distribution website to EC2 instances. By using Amazon S3 as an origin, have this website serve the data through CloudFront by creating signed URLS.
C. Use multiple Snowball appliances to migrate the existing images to Amazon S3， Upload new data by regularly using Snowball appliances to upload data from the network-attached storage. Migrate the data distribution website to EC2 instances. By using Amazon S3 as an origin, have this website serve the data through CloudFront by creating signed URLs.
D. Use multiple Snowball appliances to migrate the existing images to an Amazon EFS file system. Create a 1-Gb Direct Connect connection from the ground station to AWS, and upload new data by mounting the EFS file system over the Direct Connect connection Migrate the data distribution website to EC2 instances. By using webservers in EC2 that mount the EFS file system as the origin, have this website serve the data through CloudFront by creating signed URLS.
答案：A

93. A company is running a high-user-volume media-sharing application on premises. It currently hosts about 400 TB of data with millions of video files. The company is migrating this application to AWS to improve reliability and reduce costs.
The Solutions Architecture team plans to store the videos in an Amazon S3 bucket and use Amazon CloudFront to distribute videos to users. The company needs to migrate this application to AWS within 10 days with the least amount of downtime possible. The company currently has 1 Gbps connectivity to the internet with 30 percent free capacity.
Which of the following solutions would enable the company to migrate the workload to AWS and meet all of the requirements?
A. Use a multi-part upload in Amazon S3 client to parallel-upload the data to the Amazon S3 bucket over the internet. Use the throttling feature to ensure that the Amazon S3 client does not use more than 30 percent of available internet capacity.
B. Request an AWS Snowmobile with 1 PB capacity to be delivered to the data center. Load the data into Snowmobile and send it back to have AWS download that data to the Amazon S3 bucket. Sync the new data that was generated while migration was in flight.
C. Use an Amazon S3 client to transfer data from the data center to the Amazon S3 bucket over the internet. Use the throttling feature to ensure the Amazon S3 client does not use more than 30 percent of available internet capacity.
D. Request multiple AWS Snowball devices to be delivered to the data center. Load the data concurrently into these devices and send it back. Have AWS download that data to the Amazon S3 bucket. Sync the new data that was generated while migration was in flight

答案：D

94. What combination of steps could a Solutions Architect take to protect a web workload running on Amazon EC2 from DDos and application layer attacks？（Select Two）
A. Put the EC2 instances behind a Network Load Balancer and configure AWS WAF on it
B. Migrate the DNS to Amazon Route 53 and use AWS Shield.
C. Put the EC2 instances in an Auto Scaling group and configure AWS WAF on it.
D. Create and use an Amazon CloudFront distribution and configure AWS WAF on it.
E. Create and use an internet gateway in the VPC and use AWS shield
答案：BD

95. A company has developed a new billing application that will be released in two weeks Developers are testing the application running on 10 EC2 instances managed by an Auto scaling group in subnet 172.31.0.0/24 within VPC A with CIDR block 172.31.0.0/16. The Developers noticed connection timeout errors in the application logs while connecting to an Oracle database running on an Amazon EC2 instance in the same region within VPC B with CIDR block 172.50.0.0/16. The IP of the database instance is hard-coded in the application instances.
Which recommendations should a Solutions Architect present to the Developers to solve the problem in a secure way with minimal maintenance and overhead?
A. Disable the SrcDestCheck attribute for all instances running the application and Oracle Database. Change the default route of VPC a to point ENI of the Oracle Database that has an IP address assigned within the range of 172.50.0.0/16
B. Create and attach internet gateways for both VPCs. Configure default routes to the internet gateways for both VPCs. Assign an Elastic IP for each Amazon EC2 instance in VPC A
C. Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 172.50.0.0/16
D. Create an additional Amazon EC2 instance for each VPC as a customer gateway, create one virtual private gateway （VGW） for each VPC, configure an end-to-end VPC, and advertise the routes for 172. 50.0.0/16
答案：C

96. A company has an application that runs a web service on Amazon EC2 instances and stores jpg images in Amazon S3. The web traffic has a predictable baseline, but often demand spikes unpredictably for short periods of time. The application is loosely coupled and stateless. The jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days they are seldom accessed thereafter but always need to be immediately available. The CIO has asked to find ways to reduce costs.
Which of the following options will reduce costs？（Select TWO）
A. Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes
B. Configure a lifecycle policy to move the jpg images on Amazon S3 to S3 IA after 30 days.
C. Use On-Demand instances for baseline capacity requirements and use Spot Fleet instances for the demand spikes.
D. Configure a lifecycle policy to move the jpg images on Amazon S3 to Amazon Glacier after 30 days.
E. Create a script that checks the load on all web servers and terminates unnecessary On-Demand instances.
答案：AB

97. An organization has a write-intensive mobile application that uses Amazon API Gateway, AWs Lambda, and Amazon DynamoDB. The application has scaled well; however, costs have increased exponentially

because of higher than anticipated Lambda costs. The application's use is unpredictable, but there has been a steady 20% increase in utilization every month.
While monitoring the current Lambda functions, the Solutions Architect notices that the execution-time averages 4.5 minutes. Most of the wait time is the result of a high-latency network call to a 3-TB MySQL database server that is on-premises. A VPN is used to connect to the VPC, so the Lambda functions have been configured with a five- minute timeout.
How can the solutions Architect reduce the cost of the current architecture?
A. •Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database
•Enable local caching in the mobile application to reduce the Lambda function invocation calls.
• Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.
• Offload the frequently accessed records from DynamoDB to Amazon ElastiCache.
B. •Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQl database
•Cache the API Gateway results to Amazon CloudFront.
•Use Amazon EC2 Reserved Instances instead of Lambda .
•Enable Auto Scaling on EC2， and use Spot Instances during peak times.
• Enable DynamoDB Auto Scaling to manage target utilization.
C. •Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.
•Enable caching of the Amazon API Gateway results in Amazon Cloud Front to reduce the number of Lambda function invocations.
• Monitor the Lambda function performance, gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.
• Enable DynamoDB Accelerator for frequently accessed records, and enable the DynamoDB Auto Scaling feature
D. •Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.
•Enable API caching on API Gateway to reduce the number of Lambda function invocations.
• Continue to monitor the AWS Lambda function performance, gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.
• Enable Auto Scaling in DynamoDB
答案： D

98. A company is using an Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer. The web application requires user authorization and session tracking for dynamic content. The CloudFront distribution has a single cache behavior configured to forward the Authorization, Host, and User-Agent HTTP whitelist headers and a session cookie to the origin. All other cache behavior settings are set to their default value.
A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings. The ACM certificate is also applied to the HTTPS listener for the Application Load Balancer. The CloudFront origin protocol policy is set to HTTPS only Analysis of the cache statistics report shows that the miss rate for this distribution is very high.
What can the Solutions Architect do to improve the cache hit rate for this distribution without causing the SSL/TLS handshake between CloudFront and the Application Load Balancer to fail?
A. Create two cache behaviors for static and dynamic content. Remove the User-Agent and Host HTTP headers from the whitelist headers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content.

B. Remove the User-Agent and Authorization HTTP headers from the whitelist headers section of the cache behavior. Then update the cache behavior to use presigned cookies for authorization.
C. Remove the Host HTTP header from the whitelist headers section and remove the session cookie from the whitelist. cookies section for the default cache behavior. Enable automatic object compression and use Lambda @Edge viewer request events for user authorization
D. Create two cache behaviors for static and dynamic content Remove the User-Agent HTTP header from the whitelist headers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content
答案：D

99. A company runs a memory-intensive analytics application using on-demand Amazon EC2 C5 compute optimized instances, The application is used continuously and application demand doubles during working hours. The application currently scales based on CPU usage. When scaling in occurs, a lifecycle hook is used because the instance requires 4 minutes to clean the application state before terminating.
Because users reported poor performance during working hours, scheduled scaling actions were implemented so additional instances would be added during working hours. The Solutions Architect has been asked to reduce the cost of the application.
Which solution is MOST cost-effective?
A. Use the existing launch configuration that uses C5 instances, and update the application AMI to include the Amazon CloudWatch agent. Change the Auto Scaling policies to scale based on memory utilization. Use Reserved Instances for the number of instances required after working hours, and use Spot Instances to cover the increased demand during working hours
B. Update the existing launch configuration to use R5 instances, and update the application AMI to include SSM Agent Change the Auto Scaling policies to scale based on memory utilization. Use Reserved Instances for the number of instances required after working hours, and use spot Instances with On-Demand Instances to cover the increased demand during working hours.
C. Use the existing launch configuration that uses C5 instances, and update the application AMI to include SSM Agent Leave the Auto Scaling policies to scale based on CPU utilization. Use scheduled Reserved Instances for the number of instances required after working hours, and use Spot Instances to cover the increased demand during working hours
D. Create a new launch configuration using R5 instances, and update the application AMI to include the Amazon CloudWatch agent Change the Auto Scaling policies to scale based on memory utilization. Use Reserved Instances for the number of instances required after working hours, and use Standard Reserved Instances with On-Demand Instances to cover the increased demand during working hours
答案：A

100. A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs for requests and data transfers from Amazon S3.
Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers?
A. Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Have the organizations assume and use that read role when accessing the data.
B. Ensure that all organizations in the partnership have AWS accounts. Create a bucket policy on the bucket

that owns the data. The policy should allow the accounts in the partnership read access to the bucket Enable Requester Pays on the bucket. Have the organizations use their AWS credentials when accessing the data.

C. Ensure that all organizations in the partnership have AWS accounts. Configure buckets in each of the accounts with a bucket policy that allows the institute that owns the data the ability to write to the bucket. Periodically sync the data from the institute's account to the other organizations. Have the organizations use their AWS credentials when accessing the data using their accounts.

D. Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data Enable Requester Pays on the bucket. Have the organizations assume and use that read role when accessing the data.

答案：B

101. A company prefers to limit running Amazon EC2 instances to those that were launched from AMIs pre-approved by the Information Security department. The Development team has an agile continuous integration and deployment process that cannot be stalled by the solution.

Which method enforces the required controls with the LEAST impact on the development process？（Select TWO ）

A. Use lAM policies to restrict the ability of users or other automated entities to launch EC2 instances based on a specific set of pre-approved AMIs, such as those tagged in a specific way by Information Security.

B. Use regular scans within Amazon Inspector with a custom assessment template to determine if the EC2 instance that the Amazon Inspector Agent is running on is based upon a pre-approved AMI. If it is not, shut down the instance and inform formation Security by email that this occurred.

C. Only allow launching of EC2 instances using a centralized DevOps team, which is given work packages via notifications from an internal ticketing system. Users make requests for resources using this ticketing tool, which has manual information security approval steps to ensure that EC2 instances are only launched from approved AMIs

D. Use AWS Config rules to spot any launches of EC2 instances based on non-approved AMIs, trigger an AWS Lambda function to automatically terminate the instance, and publish a message to an Amazon SNS topic to inform Information Security that this occurred

E. Use a scheduled AWS Lambda function to scan through the list of running instances within the virtual private cloud （VPC）and determine if any of these are based on unapproved AMIs. Publish a message to an SNS topic to inform Information Security that this occurred and then shut down the instance

答案：AD

102. A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics is run, and each execution takes about 4 hours to complete. The statistical analysis is not mission critical to the business, and previous data points are picked up on the next execution if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations running full time to ingest and store the streaming data in attached Amazon EBS volumes. On-Demand EC2 instances are launched each night to perform the nightly processing, accessing the stored data from NFS shares on the ingestion servers, and terminating the nightly processing servers when complete. The Reserved Instance reservations are expiring, and the company needs to determine whether to purchase new reservations or implement a new design。

Which is the most cost-effective design？

A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a fleet of On-Demand EC2 instances that launches each night to perform the batch processing of the S3 data

and terminates when the processing complete.
B. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use AWS Batch to perform nightly processing with a Spot market bid of 50% of the On-Demand price.
C. Update the ingestion process to use a fleet of EC2 Reserved Instances behind a Network Load Balancer with 3- year leases. Use Batch with Spot Instances with a maximum bid of 50% of the On-Demand price for the nightly processing.
D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use an AWS Lambda function scheduled to run nightly with Amazon CloudWatch Events to query Amazon Redshift to generate the daily statistics
答案：B

103. An online retailer needs regularly process large product catalogs, which are handled in batches. These are sent out to be processed by people using the Amazon Mechanical Turk service, but the retailer has asked its Solutions Architect to design a workflow orchestration system that allows it to handle multiple concurrent Mechanical Turk operations, deal with the result assessment process and reprocess failures.
Which of the following options gives the retailer the ability to interrogate the state of every workflow with the LEAST amount of implementation effort?
A. Trigger Amazon CloudWatch alarms based upon message visibility in multiple Amazon SQS queues （one queue per workflow stage）and send messages via Amazon SNS to trigger AWS Lambda functions to process the next step. Use Amazon ES and Kibana to visualize Lambda processing logs to see the workflow states.
B. Hold workflow information in an Amazon RDS instance with AWS Lambda functions polling RDS for status changes. Worker Lambda functions then process the next workflow steps. Amazon Quick Sight will visualize workflow states directly out of Amazon RDS.
C. Build the workflow in AWS Step Functions, using it to orchestrate multiple concurrent workflows. The status of each workflow can be visualized in the AWS Management Console, and historical data can be written to Amazon S3 and visualized using Amazon QuickSight.
D. Use Amazon SWF to create a workflow that handles a single batch of catalog records with multiple worker tasks to extract the data, transform it, and send it through mechanical Turk. Use Amazon ES and Kibana to visualize AWS Lambda processing logs to see the workflow states
答案：D

104. A company wants to ensure that the workloads for each of its business units have complete autonomy and a minimal blast radius in AWS. The Security team must be able to control access to the resources and services in the account to ensure that particular services are not used by the business units.
How can a Solutions Architect achieve the isolation requirements?
A. Create individual accounts for each business unit and add the account to an OU in AWS Organizations. Modify the OU to ensure that the particular services are blocked. Federate each account with an ldP and create separate roles for the business units and the Security team.
B. Create individual accounts for each business unit. Federate each account with an ldP and create separate roles and policies for the business units and the Security team.
C. Create one shared account for the entire company. Create separate VPCs for each business unit. Create individual IAM policies and resource tags for each business unit. Federate each account with an IdP,and create separate roles for the business units and the Security team.
D. Create one shared account for the entire company. Create individual IAM policies and resource tags for each business unit Federate the account with an ldP, and create separate roles for the business units and the Security team.
答案：A

105. A company needs to cost-effectively persist small data records (up to 1 KiB) for up to 30 days. The data is read rarely. When reading the data, a 5-minute delay is acceptable.
Which of the following solutions achieve this goal? (Select TWO)
A. Use Amazon S3 to collect multiple records in one S3 object. Use a lifecycle configuration to move data to Amazon Glacier immediately after write. Use expedited retrievals when reading the data.
B. Write the records to Amazon Kinesis Data Firehose and configure Kinesis Data Firehose to deliver the data to Amazon S3 after 5 minutes. Set an expiration action at 30 days on the S3 bucket.
C. Use an AWS Lambda function invoked via Amazon API Gateway to collect data for 5 minutes. Write data to Amazon S3 just before the Lambda execution stops.
D. Write the records to Amazon DynamoDB configured with a Time To Live (TTL) of 30 days. Read data using the GetItem or BatchGetItem call.
E. Write the records to an Amazon ElastiCache for Redis. Configure the Redis append-only file (AOF) persistence logs to write to Amazon S3. Recover from the log if the ElastiCache instance has failed.
答案: AD

106. A company has released a new version of a website to target an audience in Asia and South America. The website's media assets are hosted on Amazon S3 and have an Amazon CloudFront distribution to improve end-user performance. However, users are having a poor login experience because the authentication service is only available in the us-east-1 AWS Region.
How can the Solutions Architect improve the login experience and maintain high security and performance with minimal management overhead?
A. Replicate the setup in each new geography and use Amazon Route 53 geo-based routing to route traffic to the AWS Region closest to the users.
B. Use an Amazon Route 53 weighted routing policy to route traffic to the CloudFront distribution. Use CloudFront cached HTTP methods to improve the user login experience
C. Use Amazon Lambda@ Edge attached to the Cloud Front viewer request trigger to authenticate and authorize users by maintaining a secure cookie token with a session expiry to improve the user experience in multiple geographies.
D. Replicate the setup in each geography and use Network Load Balancers to route traffic to the authentication service running in the closest region to users
答案: C

107. A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle of least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes.
Which account creation process meets these requirements and allows for changes?
A. Create a new AWS Organizations account Create groups in Active Directory and assign them to roles in AWS to grant federated access Require each team to tag their resources, and separate bills based on tags. Control access to resources rough lAM granting the minimally required privilege.
B. Create individual accounts for each team. Assign the security account as the master account and enable consolidated billing for all other accounts. Create a cross-account role for security to manage accounts, and send logs to a bucket in the security account
C. Create a new AWS account, and use AWS Service Catalog to provide teams with the required resources. Implement a third-party billing solution to provide the Finance team with the resource use for each team based on tagging Isolate resources using lAM to avoid account sprawl, Security will control and monitor logs and permissions.
D. Create a master account for billing using Organizations, and create each team's account from that master

account. Create a security account for logs and cross-account access. Apply service control policies on each account, and grant the Security team cross-account access to all accounts, Security will create lAM policies for each account to maintain least privilege access.
答案：D

108. A company runs a public-facing application that uses a Java-based web service via a RESTful APl. It is hosted on Apache Tomcat on a single server in a data center that runs consistently at 30% CPU utilization. Use of the API is expected to increase by 10 times with a new product launch. The business wants to migrate the application to AWS with no disruption, and needs it to scale to meet demand.
The company has already decided to use Amazon Route 53 and CNAME records to redirect traffic. How can these requirements be met with the LEAST amount of effort?
A. Use AWS Elastic Beanstalk to deploy the Java web service and enable Auto Scaling. Then switch the application to use the new web service.
B. Lift and shift the Apache server to the cloud using AWS SMS. Then switch the application to direct web service traffic to the new instance
C. Create a Docker image and migrate the image to Amazon ECS. Then change the application code to direct web service queries to the ECS container.
D. Modify the application to call the web service via Amazon API Gateway, Then create a new AWS Lambda Java function to run the Java web service code. After testing, change API Gateway to use the Lambda function
答案：A

109. A company wants to allow its Marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The Team Manager must have the ability to manage users and groups, but no team members should have access to services or resources not required for the SQL queries Additionally, Administrators need to audit the queries made and receive notifications when a query violates rules defined by the Security team.
AWS Organizations has been used to create a new account and an AWS lAM user with administrator permissions for the Team Manager.
Which design meets these requirements?
A. Apply a service control policy（SCP）that allows access to lAM, Amazon RDS, and AWS Cloud Trail. Load customer records in Amazon RDS MySQL and train users to execute queries using the AWS CLl. Stream the query logs to Amazon CloudWatch Logs from the RDS database instance. Use a subscription filter with AWS Lambda functions to audit and alarm on queries against personal data.
B. Apply a service control policy（SCP） that denies access to all services except lAM, Amazon Athena, Amazon S3， and AWS CloudTrail. Store customer record files in Amazon S3 and train users to execute queries using the CLI via Athena Analyze CloudTrail events to audit and alarm on queries against personal data.
C. Apply a service control policy （SCP）that denies access to all services except lAM, Amazon DynamoDB, and AWS CloudTrail. Store customer records in DynamoDB and train users to execute queries using the AWS CLI Enable DynamoDB streams to track the queries that are issued and use an AWS Lambda function for real-time monitoring and alerting.
D. Apply a service control policy（SCP） that allows access to lAM, Amazon Athena, Amazon S3， and AWS CloudTrail. Store customer records as files in Amazon S3 and train users to leverage the Amazon S3 Select feature and execute queries using the AWS CLI. Enable S3 object-level logging and analyze CloudTrail events to audit and alarm on queries against personal data.
答案：B

110. A company currently uses Amazon EBS and Amazon RDS for storage purposes. The company intends to use a pilot light approach for disaster recovery in a different AWS Region. The company has an RTO of 6 hours and an RPO of 24 hours.
Which solution would achieve the requirements with MINIMAL cost?
A. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region .
B. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group configured in the same way as in the primary region.
C. Use Amazon ECS to handle long-running tasks to create daily EBS and RDS snapshots, and copy to the disaster recovery region Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.
D. Use EBS and RDS cross-region snapshot copy capability to create snapshots in the disaster recovery region. Use Amaze Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.
一家公司目前使用 Amazon EBS 和 Amazon RDS 进行存储。公司打算在不同的 AWS 区域使用一种试点轻型灾难恢复方法。该公司的 RTO 为 6 小时，RPO 为 24 小时。
以下哪一种解决方案将以最小的成本实现要求?
A..使用 AWS Lambda 创建每日 EBS 和 RDS 快照，并将它们复制到灾难恢复区域。使用带有主动-被动故障转移配置的 Amazon Route 53.在 Auto Scaling 组中使用 Amazon EC2，在灾难恢复区域中将容量设置为 0
B.使用 AWS Lambda 创建每日 EBS 和 RDS 快照，并将它们复制到灾难恢复区域。使用带有主动-主动故障转移配置的 Amazon Route 53。在与主区域配置相同的 Auto Sca1ing 组中使用 Amazon EC2
C.使用 Amazon ECS 处理长时运行的任务，以创建每日 EBS 和 RDS 快照，并复制到灾难恢复区域。使用带有主动-被动故障转移配置的 Amazon Route 53.在 Auto Scaling 组中使用 Amazon EC2，在灾难恢复区域中将容量设置为 0
D.使用 EBS 和 RDS 跨区域快照复制功能在灾难恢复区域创建快照。使用带有主动-主动故障转移配置的 Amazon Route 53.在 Auto Scaling 组中使用 Amazon EC2，在灾难恢复区域中将容量设置为 0。
答案：D

111. A Solutions Architect is designing the storage layer for a recently purchased application. The application will be running on Amazon EC2 instances and has the following layers and requirements:
- Data layer : A POSIX file system shared across many systems
- Service layer :Static file content that requires block storage with more than 100k IOPS

Which combination of AWS services will meet these needs? （Select TWO ）
A. Data layer-Amazon S3
B. Data layer- Amazon EC2 Ephemeral Storage
C. Data layer- Amazon EFS
D. Service layer- Amazon EBS volumes with Provisioned IOPS
E. Service layer- Amazon EC2 Ephemeral Storage
答案：CE

112. A company is designing a new highly available web application on AWS. The application requires consistent and reliable connectivity from the application servers in AWS to a backend REST API hosted in the company's on-premises environment. The backend connection between AWS and on-premises will be routed over an AWS Direct Connect connection through a private virtual interface Amazon Route 53 will be

used to manage private DNS records for the application to resolve the IP address on the backend REST API.
Which design would provide a reliable connection to the backend API?
A. Implement at least two backend endpoints for the backend REST API, and use Route 53 health checks to monitor the availability of each backend endpoint and perform DNS-level failover
B. Install a second Direct Connect connection from a different network carrier and attach it to the same virtual private gateway as the first Direct Connect connection.
C. Install a second cross connect for the same Direct Connect connection from the same network carrier, and join both connections to the same link aggregation group（LAG）on the same private virtual interface.
D. Create an IPSec VPN connection routed over the public internet from the on-premises data center to AWS and attach it to the same virtual private gateway as the Direct Connect connection
答案：B

113. A Solutions Architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month.
Which combination of steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? （Select THREE）
A. Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances
B. Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types.
C. Purchase all upfront Reserved Instances that cover 100%of the account's expected Amazon EC2 usage
D. Place conditions in the users' IAM policies that limit the number of instances they are able to launch
E. Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console
F. Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost
答案：AEF

114. A Development team is deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS Lambda, and Amazon DynamoDB resources. A Solutions Architect has been tasked with automating the future deployments of these serverless APIs.
How can this be accomplished?
A. Use AWS CloudFormation with a Lambda-backed custom resource to provision API Gateway. Use the AWS：：DynamoDB：：Table and AWS：：Lambda :: Function resources to create the Amazon DynamoDB table and Lambda functions. Write a script to automate the deployment of the CloudFormation template
B. Use the AWS Serverless Application Model to define the resources. Upload a YAML template and application files to the code repository. Use AWS CodePipeline to connect to the code repository and to create an action to build using AWS CodeBuild. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution
C. Use AWS CloudFormation to define the serverless application Implement versioning on the Lambda functions and create aliases to point to the versions. When deploying, configure weights to implement shifting traffic to the newest version, and gradually update the weights as traffic moves over
D. Commit the application code to the AWS Code Commit code repository. Use AWS Code Pipeline and connect to the CodeCommit code repository. Use AWS Code Build to build and deploy the Lambda functions using AWS CodeDeploy. Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.
答案：B

115. A company is planning the migration of several lab environments used for software testing. An

assortment of custom tooling is used to manage the test runs for each lab. The labs use immutable infrastructure for the software test runs, and the results are stored in a highly available SQL database cluster. Although completely rewriting the custom tooling is out of scope for the migration project, the company would like to optimize workloads during the migration
Which application migration strategy meets this requirement?
A Re-host
B. Re-platform
C. Re-factor/re-architect
D. Retire
一家公司正在计划迁移几个用于软件测试的实验室环境。使用了各种定制工具管理每个实验室的测试运行。这些实验室使用不可变基础结构运行软件测试，测试结果存储在高度可用的 SQL 数据库集群中，尽管完全重写定制工具超出了迁移项目的范围，但是公司希望在迁移期间优化工作负载。
以下哪个应用程序迁移策略满足此要求?
A. 主机转换（Re-host）
B. 平台更换（Re-p1atform）
C 重构/重建（Re- factor/re- architect）
D. 停用（ Retire）
答案：B

116. A company uses Amazon S3 to store documents that may only be accessible to an Amazon EC2 instance in a certain virtual private cloud（VPC）. The company fears that a malicious insider with access to this instance could also set up an EC2 instance in another VPC to access these documents.
Which of the following solutions will provide the required protection?
A. Use an S3 VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint
B. Use EC2 instance profiles and an S3 bucket policy to limit access to the role attached to the instance profile
C. Use S3 client-side encryption and store the key in the instance metadata
D. Use S3 server-side encryption and protect the key with an encryption context
答案：A

117. A company has asked a Solutions Architect to design a secure content management solution that can be accessed by API calls by external customer applications. The company requires that a customer administrator must be able to submit an API call and roll back changes to existing files sent to the content management solution, as needed.
What is the MOST secure deployment design that meets all solution requirements?
A. Use Amazon S3 for object storage with versioning and bucket access logging enabled and an lAM role and access policy for each customer application Encrypt objects using SSE-KMS Develop the content management application to use a separate AWS KMS key for each customer
B. Use Amazon Work Docs for object storage Leverage WorkDocs encryption, user access management, and version control. Use AWS CloudTrail to log all SDK actions and create reports of hourly access by using the Amazon CloudWatch dashboard. Enable a revert function in the SDK based on a static Amazon S3 webpage that shows the output of the CloudWatch dashboard
C. Use Amazon EFS for object storage, using encryption at rest for the Amazon EFS volume and a customer managed key stored in AWS KMS. Use IAM roles and Amazon EFS access policies to specify separate encryption keys for each customer application Deploy the content management application to store all new versions as new files in Amazon EFS and use a control API to revert a specific file to a previous version
D. Use Amazon S3 for object storage with versioning and enable S3 bucket access logging Use an lAM role and access policy for each customer application. Encrypt objects using client-side encryption, and distribute

an encryption key to all customers when accessing the content management application
答案：A

118. A company has a requirement that only allows specially hardened AMIs to be launched into public subnets in a VPC, and for the AMIs to be associated with a specific security group. Allowing non-compliant instances to launch into the public subnet could present a significant security risk if they are allowed to operate
A mapping of approved AMIs to subnets to security groups exists in an Amazon DynamoDB table in the same AWS account. The company created an AWS Lambda function that, when invoked, will terminate a given Amazon EC2 instance if the combination of AMI, subnet, and security group are not approved in the DynamoDB table
What should the Solutions Architect do to MOST quickly mitigate the risk of compliance deviations?
A. Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched using one of the allowed AMIs, and associate it with the Lambda function as the target.
B. For the Amazon S3 bucket receiving the AWS Cloud Trail logs, create an S3 event notification configuration with a filter to match when logs contain the ec2：RunInstances action, and associate it with the Lambda function as the target
C. Enable AWS Cloud Trail and configure it to stream to an Amazon CloudWatch Logs group Create a metric filter in CloudWatch to match when the ec2：RunInstances action occurs, and trigger the Lambda function when the metric is greater than 0
D. Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched and associate it with the Lambda function as the target
答案：D

119. A media storage application uploads user photos to Amazon S3 for processing. End users are reporting that some uploaded photos are not being processed properly. The Application Developers trace the logs and find that AWS Lambda is experiencing execution issues when thousands of users are on the system simultaneously. Issues are caused by:
- Limits around concurrent executions
- The performance of Amazon DynamoDB when saving data

Which actions can be taken to increase the performance and reliability of the application? (Select Two)
A. Evaluate and adjust the read capacity units （RCUs） for the DynamoDB tables
B. Evaluate and adjust the write capacity units （WCUs） for the DynamoDB tables
C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions
D. Configure a dead letter queue that will reprocess failed or timed-out Lambda functions
E. Use S3 Transfer Acceleration to provide lower-latency access to end users
答案：BD

120. A company with several AWS accounts is using AWS Organizations and service control policies (SCPs)。An Administrator created the following SCP and has attached it to an organizational unit （OU） that contains AWS account 1111-1111-111:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
          "Sid": "DenyCloudTrail",
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the Administrator address this problem?
A. Add S3：CreateBucket with"Allow" effect to the SCP
B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111
C. Instruct the Developers to add Amazon S3 permissions to their IAM entities
D. Remove the SCP from account 1111-1111-1111
答案：C

121. A company has a 24 TB MySQL database in its on-premises data center that grows at the rate of 10 GB per day. The data center is connected to the company's AWS infrastructure with a 50 Mbps VPN connection. The company is migrating the application and workload to AWS. The application code is already installed and tested on Amazon EC2. The company now needs to migrate the database and wants to go live on AWS within 3 weeks
Which of the following approaches meets the schedule with LEAST downtime?
A.
1. Use the VM Import/Export service to import a snapshot of the on-premises database into AWS
2. Launch a new EC2 instance from the snapshot
3. Set up ongoing database replication from on premises to the EC2 database over the VPN
4. Change the DNS entry to point to the EC2 database
5. Stop the replication
B.
1. Launch an AWS DMS instance
2. Launch an Amazon RDS Aurora MySQL DB instance
3. Configure the AWS DMS instance with on-premises and Amazon RDS MySQL database information
4. Start the replication task within AWS DMS over the VPN
5. Change the DNS entry to point to the Amazon RDS MySQL database
6. Stop the replication
C.
1. Create a database export locally using database-native tools
2. Import that into AWS using AWS Snowball
3. Launch an Amazon RDS Aurora DB instance
4. Load the data in the RDS Aurora DB instance from the export.
5. Set up database replication from the on-premises database to the RDS Aurora DB instance over the VPN
6. Change the DNS entry to point to the RDS Aurora DB instance
7. Stop the replication.
D.
1. Take the on-premises application offline
2. Create a database export locally using database-native tools
3. Import that into AWS using AWS Snowball
4. Launch an Amazon RDS Aurora DB instance

5. Load the data in the RDS Aurora DB instance from the export
6 Change the DNS entry to point to the Amazon RDS Aurora DB instance
7. Put the Amazon EC2 hosted application online
答案：C

122. A Solutions Architect must build a highly available infrastructure for a popular global video game that runs on a mobile phone platform. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The database tier is an Amazon RDS MySQL Multi-AZ instance. The entire application stack is deployed in both us-east-1 and eu-central-1 Amazon Route 53 is used to route traffic to the two installations using a latency-based routing policy. A weighted routing policy is configured in Route 53 as a fail over to another region in case the installation in a region becomes unresponsive
During the testing of disaster recovery scenarios, after blocking access to the Amazon RDS MySQL instance in eu-central-1 from all the application instances running in that region, Route 53 does not automatically failover all traffic to us-east-1
Based on this situation, which changes would allow the infrastructure to failover to us-east-1？（Select TWO）
A. Specify a weight of 100 for the record pointing to the primary Application Load Balancer in us-east- 1 and a weight of 60 for the record pointing to the primary Application Load Balancer in eu-central-1.
B. Specify a weight of 100 for the record pointing to the primary Application Load Balancer in us-east- 1 and a weight of 0 for the record pointing to the primary Application Load Balancer in eu-central-1
C. Set the value of Evaluate Target Health to Yes on the latency alias resources for both eu-central-1 and us-east-1
D. Write a URL in the application that performs a health check on the database layer. Add it as a health check within the weighted routing policy in both regions
E. Disable any existing health checks for the resources in the policies and set a weight of 0 for the records pointing to primary in both eu-central-1 and us-east-1， and set a weight of 100 for the primary Application Load Balancer only in the region that has healthy resources
答案：BC

123. A retail company is running an application that stores invoice files in an Amazon S3 bucket and metadata about the files in an Amazon DynamoDB table. The application software runs in both us-east-1 and eu-west-1. The S3 bucket and DynamoDB table are in us-east-1The company wants to protect itself from data corruption and loss of connectivity to either Region
Which option meets these requirements？
A. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1 Enable continuous backup on the DynamoDB table in us-east-1 Enable versioning on the S3 bucket
B. Create an AWS Lambda function triggered by Amazon CloudWatch Events to make regular backups of the DynamoDB table Set up S3 cross-region replication from us-east- 1 to eu-west-1. Set up MFA the S3 bucket in us-east-1
C. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1 Enable versioning on the S3 bucket Implement strict ACLs on the S3 bucket.
D. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1 Enable continuous backup on the DynamoDB table in us-east-1. Set up S3 cross-region replication from us-east- 1 to eu-west-1
答案：D

124. A company has an Amazon EC2 deployment that has the following architecture
- An application tier that contains 8 m4.xlarge instances

•A Classic Load Balancer
•Amazon S3 as a persistent data store

After one of the EC2 instances fails, users report very slow processing of their requests. A Solutions Architect must recommend design changes to maximize system reliability. The solution must minimize costs
What should the Solutions Architect recommend?

A. Migrate the existing EC2 instances to a serverless deployment using AWS Lambda functions
B. Change the Classic Load Balancer to an Application Load Balancer
C. Replace the application tier with m4. large instances in an Auto Scaling group
D. Replace the application tier with 4 m4. 2xlarge instances

答案：C

125. A Solutions Architect is designing a highly available and reliable solution for a cluster of Amazon EC2 instances
The Solutions Architect must ensure that any EC2 instance within the cluster recovers automatically after a system failure. The solution must ensure that the recovered instance maintains the same IP address
How can these requirements be met?

A. Create an AWS Lambda script to restart any EC2 instances that shut down unexpectedly
B. Create an Auto Scaling group for each EC2 instance that has a minimum and maximum size of 1
C. Create a new t2. micro instance to monitor the cluster instances. Configure the t2. micro instance to issue an AWS EC2 reboot-instances command upon failure
D. Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric, and then configure an EC2 action to recover the instance

答案：D

126. A company CFO recently analyzed the company's AWS monthly bill and identified an opportunity to reduce the cost for AWS Elastic Beanstalk environments in use. The CFO has asked a Solutions Architect to design a highly available solution that will spin up an Elastic Beanstalk environment in the morning and terminate it at the end of the day.
The solution should be designed with minimal operational overhead and to minimize costs. It should also be able to handle the increased use of Elastic Beanstalk environments among different teams, and must provide a one-stop scheduler solution for all teams to keep the operational costs low
What design will meet these requirements?

A. Set up a Linux EC2 Micro instance. Configure an IAM role to allow the start and stop of the Elastic Beanstalk environment and attach it to the instance. Create scripts on the instance to start and stop the Elastic Beanstalk environment. Configure cron jobs on the instance to execute the scripts
B. Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution role ranting Elastic Beanstalk environment start/stop permissions, and assign the role to the Lambda functions. Configure cron expression Amazon CloudWatch Events rules to trigger the Lambda functions
C. Develop an AWS Step Functions state machine with "wait" as its type to control the start and stop time. Use the activity task to start and stop the Elastic Beanstalk environment. Create a role for Step Functions to allow it to start and stop the Elastic Beanstalk environment. Invoke Step Functions daily
D. Configure a time-based Auto Scaling group. In the morning have the Auto Scaling group scale up an Amazon EC2
instance and put the Elastic Beanstalk environment start command in the EC2 instance user date. At the end of the day, scale down the instance number to 0 to terminate the EC2 instance

答案：B

127. A company runs an ordering system on AWS using Amazon SQS and AWS Lambda, with each order received as a JSON message Recently, the company had a marketing event that led to a tenfold increase in orders. With this increase, the following undesired behaviors started in the ordering system：

- •Lambda failures while processing orders lead to queue backlogs
- •The same orders have been processed multiple times

A Solutions Architect has been asked to solve the existing issues with the ordering system and add the following resiliency features

- •Retain problematic orders for analysis
- •Send notification if errors go beyond a threshold value

How should the Solutions Architect meet these requirements?

A. Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing ,increase the visibility timeout for the messages, create a dead letter queue for messages that could not be processed, create an Amazon CloudWatch alarm on Lambda errors for notification

B. Receive single messages with each Lambda invocation, put additional Lambda workers to poll the queue, delete messages after processing increase the message timer for the messages, use Amazon CloudWatch Logs for messages that could not be processed, create a CloudWatch alarm on Lambda errors for notification

C. Receive multiple messages with each Lambda invocation, use long polling when receiving the messages, log the errors from the message processing code using Amazon CloudWatch Logs, create a dead letter queue with AWS Lambda to capture failed invocations, create CloudWatch events on Lambda errors for notification

D. Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing, increase the visibility timeout for the messages, create a delay queue for messages that could not be processed, create an Amazon CloudWatch metric on Lambda errors for notification

答案：D

128. A company has implemented AWS Organizations. It has recently set up a number of new accounts and wants to deny access to a specific set of AWS services in these new accounts .

How can this be controlled MOST efficiently?

A. Create an lAM policy in each account that denies access to the services. Associate the policy with an lAM group, and add all lAM users to the group

B. Create a service control policy that denies access to the services. Add all of the new accounts to a single organizational unit（OU），and apply the policy to that OU

C. Create an IAM policy in each account that denies access to the services. Associate the policy with an IAM role, and instruct users to log in using their corporate credentials and assume the lAM role

D. Create a service control policy that denies access to the services, and apply the policy to the root of the organization

答案：B

129. A bank is re-architecting its mainframe-based credit card approval processing application to a cloud-native application on the AWS cloud.

The new application will receive up to 1,000 requests per second at peak load. There are multiple steps to each transaction, and each step must receive the result of the previous step. The entire request must return an authorization response within less than 2 seconds with zero data loss. Every request must receive a response. The solution must be Payment Card Industry Data Security Standard（PCI DSS）-compliant

Which option will meet all of the bank’s objectives with the LEAST complexity and LOWEST cost while also

meeting compliance requirements?
A. Create an Amazon API Gateway to process inbound requests using a single AWS Lambda task that performs multiple steps and returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application
B. Create an Application Load Balancer with an Amazon ECS cluster on Amazon EC2 Dedicated Instances in a target group to process incoming requests, Use Auto Scaling to scale the cluster out/in based on average CPU utilization. Deploy a web service that processes all of the approval steps and returns a JSON object with the approval status.
C. Deploy the application on Amazon EC2 on Dedicated Instances. Use an Elastic Load Balancer in front of a farm of application servers in an Auto Scaling group to handle incoming requests. Scale out/in based on a custom Amazon CloudWatch metric for the number of inbound requests per second after measuring the capacity of a single instance
D. Create an Amazon API Gateway to process inbound requests using a series of AWS Lambda processes, each with an Amazon SQS input queue. As each step completes, it writes its result to the next step's queue. The final step returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application
答案：D

130. A company is having issues with a newly deployed serverless infrastructure that uses Amazon API Gateway, Amazon Lambda, and Amazon DynamoDB.
In a steady state, the application performs as expected. However, during peak load, tens of thousands of simultaneous invocations are needed and user requests fail multiple times before succeeding. The company has checked the logs for each component, focusing specifically on Amazon CloudWatch Logs for Lambda. There are no errors logged by the services or applications.
What might cause this problem?
A. Lambda has very low memory assigned, which causes the function to fail at peak load
B. Lambda is in a subnet that uses a NAT gateway to reach out to the internet, and the function instance does not have sufficient Amazon EC2 resources in the VPC to scale with the load
C. The throttle limit set on API Gateway is very low. During peak load, the additional requests are not making their way through to Lambda.
D. DynamoDB is set up in an auto scaling mode. During peak load, DynamoDB adjusts capacity and throughput behind the scenes, which is causing the temporary downtime. Once the scaling completes, the retries go through successfully.
答案：B

131. A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content. The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB.
What can a Solutions Architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?
A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 putObject operation. Secure the API Gateway using a COGNITO_USER_POOLS authorizer. Have the browser interface use API Gateway instead of the resigned URL to upload objects.
B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy.

Configure the PUT method for this resource to expose the S3 putObject operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.

C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload API.

D. Configure an Amazon Cloud Front distribution for the destination S3 bucket Enable PUT and POST methods for the Cloud Front cache behavior. Update the Cloud Front origin to use an origin access identity （OAI）. Give the OAI user S3：PutObject permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

答案：C

132.A photo-sharing and publishing company receives 10,000 to 150，000 images daily. The company receives the images from multiple suppliers and users registered with the service. The company is moving to AWS and wants to enrich the existing metadata by adding data using Amazon Rekognition.

The following is an example of the additional data:

List celebrities【name of the personality】 wearing【color】looking 【happy, sad】near【location example Eiffel Tower in Paris】

As part of the cloud migration program, the company uploaded existing image data to Amazon S3 and told users to upload images directly to Amazon S3

What should the solutions Architect do to support these requirements?

A. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon DynamoDB to store the metadata and Amazon ES to create an index. Use a web front-end to provide search capabilities backed by Amazon ES.

B. Use Amazon Kinesis to stream data based on an S3 event. Use an application running in Amazon EC2 to extract metadata from the images. Then store the data on Amazon DynamoDB and Amazon CloudSearch and create an index. Use a web front-end with search capabilities backed by CloudSearch

C. Start an Amazon SQS queue based on S3 event notifications. Then have Amazon SQS send the metadata information to Amazon DynamoDB. An application running on Amazon EC2 extracts data from Amazon Rekognition using the API and adds data to DynamoDB and Amazon ES. Use a web front-end to provide search capabilities backed by Amazon ES.

D. Nigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon RDS My SQL Multi-AZ to store the metadata information and use Lambda to create an index. Use a web front-end with search capabilities backed by Lambda

答案：A

133. A company has a single AWS master billing account, which is the root of the AWS Organizations hierarchy. The company has multiple AWS accounts within this hierarchy, all organized into organizational units （OUs）.More OUs and AWS accounts will continue to be created as other parts of the business migrate applications to AWS. These business units may need to use different AWS services. The Security team is implementing the following requirements for all current and future AWS accounts:

- Control policies must be applied across all accounts to prohibit certain AWS services.
- Exceptions to the control policies are allowed based on valid use cases.

Which solution will meet these requirements with minimal operational overhead?

A. Use an SCP in Organizations to implement a deny list of AWS services. Apply this SCP at the root level. For any specific exceptions for an OU, create a new SCP for that OU and add the required AWS services to the allow list

B. Use an SCP in Organizations to implement an allow list of AWS services. Apply this SCP at the root level

and at each OU. Remove the default AWS managed SCP from the root level and all OU levels. For any specific exceptions, modify the SCP attached to that OU, and add the required AWS services to the allow list.
C. Use an SCP in Organizations to implement a deny list of AWS services. Apply this SCP at each OU level. Leave the default AWS managed SCP at the root level, For any specific exceptions for an OU, create a new SCP for that OU
D. Use an SCP in Organizations to implement an allow list of AWS services apply this SCP at the root level. Remove the default AWS managed SCP from the root level and all OU levels. For any specific exceptions for an OU, modify the SCP attached to that OU, and add the required AWS services to the allow list.
答案：A

134. A company's CISO has asked a Solutions Architect to re-engineer the company's current Cl/CD practices to make sure patch deployments to its application can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.
The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer. The company is currently using GitHub to host the application source code, and has configured an AWS Code Build project to build the application. The company also intends to use AWS Code Pipeline to trigger builds from GitHub commits using the existing CodeBuild project.
What Cl/CD configuration meets all of the requirements?
A. Configure CodePipeline with a deploy stage using AWS Code Deploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update.
B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.
C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks Monitor the newly deployed code, and, if there are any issues, push another code update.
D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.
答案：B

135. A company has deployed an application to multiple environments in AWS, including production and testing. The company has separate accounts for production and testing, and users are allowed to create additional application users for team members or services, as needed. The security team has asked the Operations team for better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments.
Which of the following options would MOST securely accomplish this goal?
A. Create a new AWS account to hold user and service accounts, such as an identity account. Create users and groups in the identity account. Create roles with appropriate permissions in the production and testing accounts. Add the identity account to the trust policies for the roles.
B. Modify permissions in the production and testing accounts to limit creating new lAM users to members of the Operations team. Set a strong lAM password policy on each account. Create new lAM users and groups in each account to limit developer access to just the services required to complete their job function.
C. Create a script that runs on each account that checks user accounts for adherence to a security policy. Disable any user or service accounts that do not comply.
D. Create all user accounts in the production account. Create roles for access in the production account and

testing accounts. Grant cross-account access from the production account to the testing account.
一家公司将应用程序部署在 AWS 的多个环境中，包括生产和测试环境。公司拥有独立的账户用于生产和测试，并且如果需要的话，允许用户为团队成员或服务创建额外的应用程序用户。安全团队要求运营团队通过对安全凭证的集中控制以及对环境间权限的改进来更好的隔离生产和测试环境.
以下哪一个选项能最安全的完成这一目标?
A. 创建新的 AWS 账户以保存用户和服务账户，例如身份账户。在身份账户中创建用户和组。在生产和测试账户中，创建具有适当权限的角色。为角色在信任策略中添加身份账户
B. 修改生产和测试账户中的权限，以将创建的新 IAM 用户限制为运营团队成员。在每个账户中设置强 IAM 密码策略。在每个账户中创建新的 IAM 用户和组以限制开发人员仅访问完成其工作职能所需的服务。
C. 创建运行在每个账户上的脚本，以检查用户账户是否符合安全政策。禁用任何不合规的用户或服务账户
D. 在生产账户中创建全部用户账户。创建能够访问生产账户和测试账户的角色。允许从生产账户到测试账户的跨账户访问。
答案：B

136. A Solutions Architect is designing the storage layer for data warehousing application. The data files are large, but they have statically placed metadata at the beginning of each file that describes the size and placement of the file's index. The data files are read in by a fleet of Amazon EC2 instances that store the index size, index location, and other category information about the data file in a database. That database is used by Amazon EMR to group files together for deeper analysis.
What would be the MOST cost-effective, high availability storage solution for this workflow?
A. Store the data files in Amazon S3 and use Range GET for each file's metadata, then index the relevant data.
B. Store the data files in Amazon EFS mounted by the EC2 fleet and EMR nodes
C. Store the data files on Amazon EBS volumes and allow the EC2 fleet and EMR to mount and unmount the volumes where they are needed.
D. Store the content of the data files in Amazon DynamoDB tables with the metadata, index and data as their own keys
答案：A

137. A company is planning to migrate an application from on premises to AWS. The application currently uses an Oracle database and the company can tolerate a brief downtime of 1 hour when performing the switch to the new infrastructure. As part of the migration, the database engine will be changed to MySQL. A Solutions Architect needs to determine which AWS services can be used to perform the migration while minimizing the amount of work and time required.
Which of the following will meet the requirements?
A. Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to analyze the current schema and provide a recommendation for the optimal database engine. Then, use AWS DMS to migrate to the recommended engine. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.
B. Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to begin moving data from the on-premises database to AWS. After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.
C. Use AWS DMS to help identify the best target deployment between installing the database engine on Amazon EC2 directly or moving to Amazon RDS. Then, use AWS DMS to migrate to the platform Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and

what has to be done manually
D. Use AWS DMS to begin moving data from the on-premises database to AWS. After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database, Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually
答案：B

138.A large company has increased its utilization of AWS over time in an unmanaged way. As such, they have a large number of independent AWS accounts across different business units, projects, and environments. The company has created a Cloud Center of Excellence team, which is responsible for managing all aspects of the AWS Cloud, including their AWS accounts.
Which of the following should the Cloud Center of Excellence team do to BEST address their requirements in a centralized way？(Select TWO)
A. Control all AWS account root user credentials. Assign AWS lAM users in the account of each user who needs to access AWS resources. Follow the policy of least privilege in assigning permissions to each user.
B. Tag all AWS resources with details about the business unit, project, and environment. Send all AWS Cost and Usage reports to a central Amazon S3 bucket, and use tools such as Amazon Athena and Amazon Quick Sight to collect billing details by business unit.
C. Use the AWS Marketplace to choose and deploy a Cost Management tool. Tag all AWS resources with details about the business unit, project, and environment. Send all AWS Cost and Usage reports for the AWS accounts to this tool for analysis.
D. Set up AWS Organizations. Enable consolidated billing and link all existing AWS accounts to a master billing account Tag all AWS resources with details about the business unit, project, and environment. Analyze cost and Usage reports
Using tools such as Amazon Athena and Amazon QuickSight, to collect billing details by business unit.
E. Using a master AWS account, create IAM users within the master account. Define lAM roles in the other AWS accounts which cover each of the required functions in the account. Follow the policy of least privilege in assigning permissions to each role, then enable the lAM users to assume the roles that they need to use.
答案：AD

139. An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP, Java, or Ruby web applications, are no longer actively developed, and serve little traffic.
Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs？
A. Deploy the applications to single-instance AWS Elastic Beanstalk environments without a load balancer.
B. Use AWS SMS to create AMIs for each virtual machine and run them in Amazon EC2
C. Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.
D. Use VM Import/Export to create AMIs for each virtual machine and run them in single-instance AWS Elastic Beanstalk environments by configuring a custom image.
答案：C

140. A financial services company is moving to AWS and wants to enable Developers to experiment and innovate while preventing access to production applications. The company has the following requirements
- Production workloads cannot be directly connected to the internet
- All workloads must be restricted to the us-west-2 and eu-central-1 Regions
- Notification should be sent when Developer sandboxes exceed $500 in AWS spending monthly

Which combination of actions needs to be taken to create a multi-account structure that meets the company's requirements ？ （Select THREE）

A. Create accounts for each production workload within an organization in AWS Organizations, Place the production accounts within an organizational unit （OU）. For each account, delete the default VPC. Create an SCP with a Deny rule for the attach an internet gateway and create a default VPC actions. Attach the SCP to the OU for the production accounts.

B. Create accounts for each production workload within an organization in AWS Organizations. Place the production

Accounts within an organizational unit (OU). Create an SCP with a Deny rule on the attach an internet gateway action.

Create an SCP with a Deny rule to prevent use of the default VPC. Attach the SCPs to the OU for the production

C. Create a SCP containing a Deny Effect for cloudfront:*,iam:,route 53： *,and support:* with a StringNotEquals condition on an aws: RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the SCP to the organization's root.

D. Create an lAM permission boundary containing a Deny Effect for cloudfront： *, iam:*,route53： *,and support:*with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the permission boundary to an lAM group containing the development and production users

E. Create accounts for each development workload within an organization in AWS Organizations. Place the development accounts within an organizational unit （OU）. Create a custom AWS Config rule to deactivate all lAM users when an account's monthly bill exceeds $500

F. Create accounts for each development workload within an organization in Aws Organizations. Place the development accounts within an organizational unit （OU）， Create a budget within AWS Budgets for each development account to monitor and report on monthly spending exceeding $500

答案： ACF

141.A company has a data center that must be migrated to AWS as quickly as possible. The data center has a 500 Mbps AWS Direct Connect link and a separate fully available 1 Gbps ISP connection. A Solutions Architect must transfer 20 TB of data from the data center to an Amazon S3 bucket.

What is the FASTEST way to transfer the data？

A. Upload the data to the S3 bucket using the existing DX link

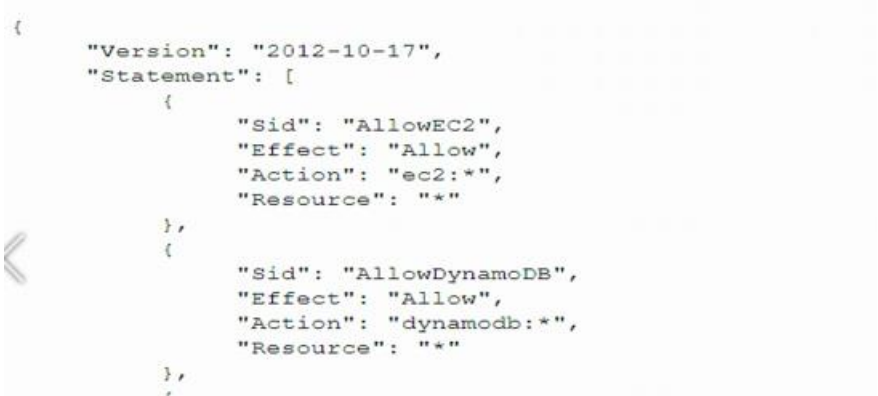
B. Send the data to AWS using the AWS Import/Export service

C. Upload the data using an 80 TB AWS Snowball device

D. Upload the data to the S3 bucket using S3 Transfer Acceleration

答案： D

142. A company is in the process of implementing AWS Organizations to constrain its Developers to use only Amazon EC2， Amazon S3.and Amazon DynamoDB. The Developers account resides in a dedicated organizational unit （OU）. The Solutions Architect has implemented the following SCP on the Developers account:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "AllowDynamoDB",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "*"
        },
```

When this policy is deployed, lAM users in the Developers account are still able to use AWS services that are not listed in the policy. What should the Solutions Architect do to eliminate the Developers' ability to use services outside the scope of this policy?

A. Create an explicit deny statement for each AWS service that should be constrained

B. Remove the FullAWSAccess SCP from the Developer account's OU

C. Modify the FullAWSAccess SCP to explicitly deny all services.

D. Add an explicit deny statement using a wildcard to the end of the SCP

答案：D

143. A company has multiple AWS accounts hosting IT applications. An Amazon CloudWatch Logs agent is installed on all Amazon EC2 instances. The company wants to aggregate all security events in a centralized AWS account dedicated to log storage.

Security Administrators need to perform near-real-time gathering and correlating of events across multiple AWS accounts.

Which solution satisfies these requirements?

A. Create a Log Audit lAM role in each application AWS account with permissions to view CloudWatch Logs, configure an AWS Lambda function to assume the Log Audit role, and perform an hourly export of CloudWatch Logs data to an Amazon S3 bucket in the logging AWS account

B. Configure CloudWatch Logs streams in each application AWS account to forward events to CloudWatch Logs in the logging AWS account. In the logging AWS account, subscribe an Amazon Kinesis Data Firehose stream to Amazon CloudWatch Events, and use the stream to persist log data in Amazon S3

C. Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to CloudWatch Logs streams in each application AWS account, configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams as its source, and persist the log data in an Amazon S3 bucket inside the logging AWS account

D. Configure CloudWatch Logs agents to publish data to an Amazon Kinesis Data Firehose stream in the logging AWS account, use an AWS Lambda function to read messages from the stream and push messages to Data Firehose, and persist the data in Amazon S3

答案：C

144. A company wants to analyze log data using date ranges with a custom application running on AWS. The application generates about 10 GB of data every day, which is expected to grow. A Solutions Architect is tasked with storing the data in Amazon S3 and using Amazon Athena to analyze the data.

Which combination of steps will ensure optimal performance as the data grows? （Select Two）

A. Store each object in Amazon S3 with a random string at the front of each key.

B. Store the data in multiple S3 buckets.

C. Store the data in Amazon S3 in a columnar format, such as Apache Parquet or Apache ORC.

D. Store the data in Amazon S3 in objects that are smaller than 10 MB.

E. Store the data using Apache Hive partitioning in Amazon S3 using a key that includes a date, such as dt=2019-02

答案：AE

145. An advisory firm is creating a secure data analytics solution for its regulated financial services users. Users will upload their raw data to an Amazon S3 bucket, where they have PutObject permissions only. Data will be analyzed by applications running on an Amazon EMR cluster launched in a VPC. The firm requires that the environment be isolated from the internet. All data at rest must be encrypted using keys controlled by the firm

Which combination of actions should the solutions Architect take to meet the user's security requirements? （Select Two）

A. Launch the Amazon EMR cluster in a private subnet configured to use an AWS KMS CMK for at-rest encryption. Configure a gateway VPC endpoint for Amazon S3 and an interface VPC endpoint for AWS KMS.

B. Launch the Amazon EMR cluster in a private subnet configured to use an AWS KMS CMK for at-rest encryption. Configure a gateway VPC endpoint for Amazon S3 and a NAT gateway to access AWS KMS.

C. Launch the Amazon EMR cluster in a private subnet configured to use an AWS CloudHSM appliance for at-rest encryption. Configure a gateway VPC endpoint for Amazon S3 and an interface VPC endpoint for CloudHSM.

D. Configure the S3 endpoint policies to permit access to the necessary data buckets only

E. Configure the S3 bucket policies to permit access using an aws: sourceVpce condition to match the S3 endpoint ID.

答案：CE

146. An enterprise company is using a multi-account AWS strategy. There are separate accounts for development, staging, and production workloads. To control costs and improve governance, the following requirements have been defined:

- The company must be able to calculate the AWS costs for each project
- The company must be able to calculate the AWS costs for each environment: development, staging, and production.
- Commonly deployed IT services must be centrally managed
- Business units can deploy pre-approved IT services only
- Usage of AWS resources in the development account must be limited.

Which combination of actions should be taken to meet these requirements ？ （Select THREE）

A. Apply environment, cost center, and application name tags to all taggable resources

B. Configure custom budgets and define thresholds using Cost Explore

C. Configure AWS Trusted Advisor to obtain weekly emails with cost-saving estimates

D. Create a portfolio for each business unit and add products to the portfolios using AWS Cloud Formation in AWS Service Catalog

E. Configure a billing alarm in Amazon CloudWatch

F. Configure SCPs in AWS Organizations to allow services available using AWS Service Catalog

答案：ABF

147. A Solutions Architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The Solutions Architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.

What should be done next to complete the update?

A. Redirect to the new environment using Amazon Route 53

B. Select the Swap Environment URLs option

C. Replace the Auto Scaling launch configuration

D. Update the DNS records to point to the green environment

答案：B

148. A Solutions Architect is redesigning an image-viewing and messaging platform to be delivered as SaaS. Currently, there is a farm of virtual desktop infrastructure（VDI）that runs a desktop image-viewing application and a desktop messaging application. Both applications use a shared database to manage user accounts and sharing. Users log in from a web portal that launches the applications and streams the view of the application on the user's machine. The Development Operations team wants to move away from using VDI and wants to rewrite the application.
What is the MOST cost-effective architecture that offers both security and ease of management?
A. Run a website from an Amazon S3 bucket with a separate S3 bucket for images and messaging data. Call AWS Lambda functions from embedded JavaScript to manage the dynamic content, and use Amazon Cognito for user and sharing management
B. Run a website from Amazon EC2 Linux servers, storing the images in Amazon S3， and use Amazon Cognito for user accounts and sharing. Create AWS CloudFormation templates to launch the application by using EC2 user data to install and configure the application
C. Run a website as an AWS Elastic Beanstalk application, storing the images in Amazon S3， and using an Amazon RDS database for user accounts and sharing. Create AWS CloudFormation templates to launch the application and perform blue/green deployments.
D. Run a website from an Amazon S3 bucket that authorizes Amazon AppStream to stream applications for a combined image viewer and messenger that stores images in Amazon S3. Have the website use an Amazon RDS database for user accounts and sharing
答案：C

149. A fleet of Amazon ECS instances is used to poll an Amazon SQS queue and update items in an Amazon DynamoDB database. Items in the table are not being updated, and the SQS queue is filling up. Amazon CloudWatch Logs are showing consistent 400 errors when attempting to update the table. The provisioned write capacity units are appropriately configured, and no throttling is occurring.
What is the LIKELY cause of the failure?
A. The ECS service was deleted
B. The ECS configuration does not contain an Auto scaling group
C. The ECS instance task execution IAM role was modified
D. The ECS task role was modified
答案：C

150. A financial company is using a high-performance compute cluster running on Amazon EC2 instances to perform market simulations DNS record must be created in an Amazon Route 53 private hosted zone when instances start The DNS record must be removed after instances are terminated.
Currently, the company uses a combination of Amazon CloudWatch Events and AWS Lambda to create the DNS record. The solution worked well in testing with small clusters, but in production with clusters containing thousands of instances, the company sees the following error in the Lambda logs:
HTTP 400 error （Bad request ）.
The response header also includes a status code element with a value of "Throttling" and a status message element with a value of "Rate exceeded."
Which combination of steps should the Solutions Architect take to resolve these issues? （Select THREE）
A. Configure an Amazon SQS FIFO queue and configure a CloudWatch Events rule to use this queue as a target. Remove the Lambda target from the CloudWatch Events rule
B. Configure an Amazon Kinesis data stream and configure a Cloud Watch Events rule to use this queue as a target Remove the Lambda target from the CloudWatch Events rule.

C. Update the CloudWatch Events rule to trigger on Amazon EC2" Instance Launch Successful" and "Instance Terminate Successful" events for the Auto Scaling group used by the cluster.
D. Configure a Lambda function to retrieve messages from an Amazon SQS queue. Modify the Lambda function to retrieve a maximum of 10 messages, then batch the messages by Amazon Route 53 API call type and submit. Delete the messages from the SQS queue after successful API calls.
E. Configure an Amazon SQS standard queue and configure the existing CloudWatch Events rule to use this queue as a target. Remove the Lambda target from the CloudWatch Events rule.
F. Configure a Lambda function to read data from the Amazon Kinesis data stream and configure the batch window to 5 minutes. Modify the function to make a single API call to Amazon Route 53 with all records read from the Kinesis data stream.
答案：ACE

151.A company is operating a large customer service call center, and stores and processes call recordings with a custom application. Approximately 2% of the call recordings are transcribed by an offshore team for quality assurance purposes. These recordings take up to 72 hours to be transcribed. The recordings are stored on an NFS share before they are archived to an offsite location after 90 days. The company uses Linux servers for processing the call recordings and managing the transcription queue. There is also a web application for the quality assurance staff to review and score call recordings.
The company plans to migrate the system to AWS to reduce storage costs and the time required to transcribe calls.
Which set of actions should be taken to meet the company's objectives?
A. Upload the call recordings to Amazon S3 from the call center. Set up an S3 lifecycle policy to move the call recordings to Amazon S3 Glacier after 90 days. Use an AWS Lambda trigger to transcribe the call recordings with Amazon Transcribe. Use Amazon S3， Amazon API Gateway, and Lambda to host the review and scoring application
B. Upload the call recordings to Amazon S3 from the call center, Set up an S3 lifecycle policy to move the call recordings to Amazon S3 Glacier after 90 days. Use an AWS Lambda trigger to transcribe the call recordings with Amazon Mechanical Turk. Use Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer to host the review and scoring application.
C. Use Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer to host the review and scoring application. Upload the call recordings to this application from the call center and store them on an Amazon EFS mount Transcribe.
D. Upload the call recordings to Amazon S3 from the call center and put the object key in an Amazon SQS queue. Set up an S3 lifecycle policy to move the call dings to Amazon S3 Glacier after 90 days. Use Amazon EC2 instances in an Auto Scaling group to send the recordings to Amazon Mechanical Turk for transcription. Use the number of objects in the queue as the scaling metric. Use Amazon S3,Amazon API Gateway ,and AWS Lambda to host the review and scoring application.
答案：C

152. An online e-commerce business is running a workload on AWS. The application architecture includes a web tier, an application tie for business logic, and a database tier for user and transactional data management. The database server has a 100 GB memory requirement. The business requires cost-efficient disaster recovery for the application with an RTO of 5 minutes and an RPO of 1 hour. The business also has a regulatory requirement for out-of-region disaster recovery with a minimum distance between the primary and alternate sites of 250 miles.
Which of the following options can the Solutions Architect design to create a comprehensive solution for this customer that meets the disaster recovery requirements?
A. Back up the application and database data frequently and copy them to Amazon S3 Replicate the

backups using S3 cross-region replication, and use AWS CloudFormation to instantiate infrastructure for disaster recovery and restore data from Amazon S3

B. Employ a pilot light environment in which the primary database is configured with mirroring to build a standby database on m4. large in the alternate region. Use AWS CloudFormation to instantiate the web servers, application servers, and load balancers in case of a disaster to bring the application up in the alternate region. Vertically resize the database to meet the full production demands, and use Amazon Route 53 to switch traffic to the alternate region

C. Use a scaled-down version of the fully functional production environment in the alternate region that includes one instance of the web server,one instance of the application server, and a replicated instance of the database server in standby mode. Place the web and the application tiers in an Auto Scaling group behind a load balancer, which can automatically scale when the load arrives to the application. Use Amazon Route 53 to switch traffic to the alternate region.

D. Employ a multi-region solution with fully functional web, application, and database tiers in both regions with equivalent capacity. Activate the primary database in one region only and the standby database in the other region. Use Amaze Route 53 to automatically switch traffic from one region to another using health check routing policies

答案：D

153. A company has an internal AWS Elastic Beanstalk worker environment inside a VPC that must access an external payment gateway API available on an HTTPS endpoint on the public internet Because of security policies, the payment gateway's Application team can grant access to only one public IP address.

Which architecture will set up an Elastic Beanstalk environment to access the company 's application without making multiple changes on the company's end?

A. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet with an outbound route to a NAT gateway in a public subnet. Associate an Elastic IP address to the NAT gateway that can be whitelisted on the payment gateway application side.

B. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet with an internet gateway. Associate an Elastic IP address to the internet gateway that can be whitelisted on the payment gateway application side

C. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet. Set an HTTPS_ PROXY application parameter to send outbound HTTPS connections to an EC2 proxy server deployed in a public subnet. Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side.

D. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet. Set the HTTPS_ PROXY and No_ PROXY application parameters to send non-VPC outbound HTTPS connections to an EC2 proxy server deployed in a public subnet. Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side

一家公司在 VPC 内有内部 AWS Elastic Beanstalk 工作者环境，该环境必须访问公共互联网上 HTTPS 端点上可用的外部支付网关 API。由于安全策略，该支付网关的应用程序团队只能授予对一个公共 IP 地址的访问权限。

哪个架构将创建 Elastic Beanstalk 环境来访问该公司的应用程序，而无需对公司端进行多次更改？

A. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在私有子网中，该私用子网具有通往公共子网中 NAT 网关的出站路由。将弹性 IP 地址与可以在支付网关应用程序端被列入白名单的 NAT 网关相关联。

B. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在具有互联网网关的公共子网中。将弹性 IP 地址与可以在支付网关应用程序端被列入白名单的互联网网关相关联。

C. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在私有子网中。设置 HTTPS_PROXY 应用程序参数，以将出站 HTTPS 连接发送到部署在公共子网中的 EC2 代理服务器。将弹性 IP 地址与可以

在支付网关应用程序端被列入白名单的 EC2 代理主机相关联。
D. 配置 Elastic Beanstalk 应用程序以将 Amazon EC2 实例放置在公共子网中。设置 HTPS_PROXY 和 NO_PROXY 应用程序参数，以将非 VPC 出站 HTTPS 连接发送到部署在公共子网中的 EC2 代理服务器。将弹性 IP 地址与可以在支付网关应用程序端被列入白名单的 EC2 代理主机相关联
答案：A

154. A Solutions Architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted
The Solutions Architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.
Which storage strategy is the MOST cost-effective and meets the design requirements?
A. Design the application to store each incoming record as a single csv file in an Amazon S3 bucket to allow for indexed retrieval: Configure a lifecycle policy to delete data older than 120 days
B. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live （TTL） feature to delete records older than 120 days
C. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that executes a query to delete any records older than 120 days
D. Design the application to batch incoming records before writing them to an Amazon S3 bucket, Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days
答案：B

155. While debugging a backend application for an IoT system that supports globally distributed devices, a Solutions Architect notices that stale data is occasionally being sent to user devices. Devices often share data, and stale data does not cause issues in most cases. However, device operations are disrupted when a device reads the stale data after an update.
The global system has multiple identical application stacks deployed in different AWS Regions. If a user device travels out of its home geographic region, it will always connect to the geographically closest AWS Region to write or read data. The same data is available in all supported AWS Regions using an Amazon DynamoDB global table.
What change should be made to avoid causing disruptions in device operations?
A. Update the backend to use strongly consistent reads. Update the devices to always write to and read from their home AWS Region
B. Enable strong consistency globally on a DynamoDB global table. Update the backend to use strongly consistent reads
C. Switch the backend data store to Amazon Aurora MySQL with cross-region replicas. Update the backend to always write to the master endpoint.
D. Select one AWS Region as a master and perform all writes in that AWS Region only Update the backend to use strongly consistent reads.
答案：A

156. A company wants to host its website on AWS using serverless architecture design patterns for global customers. The company has outlined its requirements as follows:
- The website should be responsive.
- The website should offer minimal latency

• The website should be highly available
• Users should be able to authenticate through social identity providers such as Google, Facebook, and Amazon
• There should be baseline DDoS protections for spikes in traffic
How can the design requirements be met?
A. Use Amazon CloudFront with Amazon ECS for hosting the website, Use AWS Secrets Manager to provide user management and authentication functions. Use ECS Docker containers to build an APl
B. Use Amazon Route 53 latency routing with an Application Load Balancer and AWS Fargate in different regions for hosting the website. Use Amazon Cognito to provide user management and authentication functions. Use Amazon EKS containers to build an API
C. Use Amazon CloudFront with Amazon S3 for hosting static web resources. Use Amazon Cognito to provide user management and authentication functions. Use Amazon API Gateway with AWS Lambda to build an API
D. Use AWS Direct Connect with Amazon CloudFront and Amazon S3 for hosting static web resources. Use Amazon Cognito to provide user management and authentication functions. Use AWS Lambda to build an API
答案：C

157. A company has a legacy application running on servers on premises. To increase the application's reliability, the company wants to gain actionable insights using application logs. A Solutions Architect has been given following requirements for the solution:
•Aggregate logs using AWS
•Automate log analysis for errors
•Notify the Operations team when errors go beyond a specified threshold.
What solution meets the requirements?
A. Install Amazon Kinesis Agent on servers, send logs to Amazon Kinesis Data Streams and use Amazon Kinesis Data Analytics to identify errors, create an Amazon CloudWatch alarm to notify the Operations team of errors
B. Install an AWS X-Ray agent on servers, send logs to AWS Lambda and analyze them to identify errors, use Amazon CloudWatch Events to notify the Operations team of errors
C. Install Logstash on servers, send logs to Amazon S3 and use Amazon Athena to identify errors, use sendmail to notify the Operations team of errors
D. Install the Amazon CloudWatch agent on servers, send logs to Amazon CloudWatch Logs and use metric filters to identify errors, create a CloudWatch alarm to notify the Operations team of errors
答案：D

158. An auction website enables users to bid on collectible items. The auction rules require that each bid is processed only once and in the order it was received. The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis Data Streams. A single t2. instance has a cron job that runs the bid processor, which reads incoming bids from Kinesis Data Streams and processes each bid. The auction site is growing in popularity, but users are complaining that some bids are not registering.
Troubleshooting indicates that the bid processor is too slow during peak demand hours, sometimes crashes while processing, and occasionally loses track of which record is being processed.
What changes should make the bid processing more reliable?
A. Refactor the web application to use the Amazon Kinesis Producer Library （KPL） when posting bids to Kinesis Data Streams, Refactor the bid processor to flag each record in Kinesis Data Streams as being unread, processing, and processed. At the start of each bid processing run, scan Kinesis Data Streams for

unprocessed records
B. Refactor the web application to post each incoming bid to an Amazon SNS topic in place of Kinesis Data Streams Configure the SNS topic to trigger an AWS Lambda function that processes each bid as soon as a user submits it
C. Refactor the web application to post each incoming bid to an Amazon SQS FIFO queue in place of Kinesis Data Streams Refactor the bid processor to continuously consume the SQS queue. Place the bid processing EC2 instance in an Auto Scaling group with a minimum and a maximum size of 1
D. Switch the EC2 instance type from t2. large to a larger general compute instance type. Put the bid processor EC2
stances in an Auto Scaling group that scales out the number of EC2 instances running the bid processor, based on the IncomingRecords metric in Kinesis Data Streams
答案：C

159. A company currently runs a secure application on Amazon EC2 that takes files from on-premises locations through AWS Direct Connect processes them and uploads them to a single Amazon S3 bucket The application uses HTTPS for encryption in transit to Amazon S3， and S3 server-side encryption to encrypt at rest.
Which of the following changes should the Solutions Architect recommend to make this solution more secure without impeding the application’s performance?
A. Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the NAT gateway's Elastic IP address only
B. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required Amazon S3 buckets only.
C. Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the source public IP address of the on-premises network only.
D. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required S3 buckets only Implement an S3 bucket policy that allows communication from the VPC endpoint only
答案：D

160. A manufacturing company is growing exponentially and has secured funding to improve its IT infrastructure and ecommerce presence. The company's ecommerce platform consists of：
- Static assets primarily comprised of product images stored in Amazon S3
- Amazon DynamoDB tables that store product information, user information, and order information
- Web servers containing the application’s front-end behind Elastic Load Balancers

The company wants to set up a disaster recovery site in a separate Region
Which combination of actions should the Solutions Architect take to implement the new design while meeting all the requirements ? (Select THREE).
A. Enable Amazon Route 53 health checks to determine if the primary site is down, and route traffic to the disaster recovery site if there is an issue.
B. Enable Amazon S3 cross-Region replication on the buckets that contain static assets
C. Enable multi-Region targets on the Elastic Load Balancer and target Amazon EC2 instances in both Regions
D. Enable DynamoDB global tables to achieve a multi-Region table replication.
E. Enable Amazon CloudWatch and create CloudWatch alarms that route traffic to the disaster recovery site when application latency exceeds the desired threshold.
F. Enable Amazon S3 versioning on the source and destination buckets containing static assets to ensure

there is a rollback version available in the event of data corruption
答案：BEF

161. A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in a single AWS Region. The fully qualified domain names（FQDNS）of all of the applications are made available through HTTPS using Application Load Balancers （ALBs）. The ALBs are configured to use public SSL/TLS certificates.
A Solutions Architect needs to migrate the web applications to a multi-region architecture. All HTTPS services should continue to work without interruption.
Which approach meets these requirements?
A. Request a certificate for each FQDN using AWS KMS. Associate the certificates with the ALBs in the primary AWS Region Enable cross-region availability in AWS KMS for the certificates and associate the certificates with the ALBs in the secondary AWS Region
B. Generate the key pairs and certificate requests for each FQDN using AWS KMS. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
C. Request a certificate for each FQDN using AWS Certificate Manager. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
D. Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manager Associate the certificates with the corresponding ALBs in each AWS Region
答案：D

162. A public retail web application uses an Application Load Balancer（ALB） in front of Amazon EC2 instances running across multiple Availability Zones（AZs）in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page Auto Scaling is configured to maintain the web fleet size based on the ALB health check.
Recently, the application experienced an outage Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load. resulting in severely elevated query response time.
Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? （Select TWO）
A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails
D. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier
答案：BE

163. A company uses an Amazon EMR cluster to process data once a day. The raw data comes from Amazon S3， and the resulting processed data is also stored in Amazon S3. The processing must complete within 4 hours, currently, it only takes 3 hours. However, the processing time is taking 5 to 10 minutes longer each

week due to an increasing volume of raw data.
The team is also concerned about rising costs as the compute capacity increases. The EMR cluster is currently running on three m3. xlarge instances （one master and two core nodes）
Which of the following solutions will reduce costs related to the increasing compute needs?
A. Add additional task nodes, but have the team purchase an all-upfront convertible Reserved Instance for each additional node to offset the costs
B. Add additional task nodes. but use instance fleets with the master node in on-Demand mode and a mix of on-Demand and Spot Instances for the core and task nodes. Purchase a scheduled Reserved Instance for the master node C. Add additional task nodes, but use instance fleets with the master node in Spot mode and a mix of on-Demand and Spot Instances for the core and task nodes. Purchase enough scheduled Reserved Instances to offset the cost of running any On-Demand Instances.
D. Add additional task nodes, but use instance fleets with the master node in on-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase a standard all-upfront Reserved Instance for the master node
答案：B

164. A company runs an loT platform on AWS .loT sensors in various locations send data to the company's Node. js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.
The number of sensors the company has deployed in the field has increased over time， and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency.
Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned， while keeping this platform cost-efficient? （Select TWO.）
A. Resize the My SQL General Purpose SSD storage to 6 TB to improve the volume’s IOPS
B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas
C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load
E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance
答案：CE

165. A company is developing a new service that will be accessed using TCP on a static port. A Solutions Architect must ensure that the service is highly available， has redundancy across Availability Zones， and is accessible using the DNS name my service. com， which is publicly accessible. The service must use fixed address assignments so other companies can add the addresses to their allow lists
Assuming that resources are deployed in multiple Availability Zones in a single Region， which solution will meet these requirements?
A. Create Amazon EC2 instances with an Elastic IP address for each instance. Create a Network Load Balancer （NLB） and expose the static TCP port Registe EC2 instances with the NLB. Create a new name server record set named my。 service. Com，and assign the Elastic IP addresses of the EC2 instances to the record set. Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists。
B. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP addresses for the ECS cluster. Create a Network Load Balancer （NLB） and expose the TCP port. Create a target group and assign the ECS cluster name to the NLB. Create a new A record set named my service. com，and assign the public IP addresses of the ECS cluster to the record set. Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.
C. Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone.

Create a Network Load Balancer（NLB）and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone，Create a target group and register the EC2 instances with the NLB. Create a new A（alias）record set named my service. com，and assign the NLB DNS name to the record set.

D. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP address for each host in the cluster，Create an Application Load Balancer (ALB）and expose the static TCP port. Create a target group and assign the ECS service definition name to the ALB. Create a new CNAME record set and associate the public IP addresses to the record set. Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists

答案：C

166. A Solutions Architect is building a containerized NET Core application that will run in AWS Fargate. The backend of the application requires Microsoft SQL Server with high availability. All tiers of the application must be highly available. The credentials used for the connection string to SQL Server should not be stored on disk within the NET Core front-end containers.

Which strategies should the Solutions Architect use to meet these requirements?

A. Set up SQL Server to run in Fargate with Service Auto Scaling. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server running in Fargate. Specify the ARN of the secret in AWS Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones

B. Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the. NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

C. Create an Auto Scaling group to run SQL Server on Amazon EC2. Create a secret in AWS Secrets Manager for the credentials to SQL Server running on EC2. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL. Server on EC2. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the.NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones

D. Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database Create non-persistent empty storage for the. NET Core containers in the Fargate task definition to store the sensitive information. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be written to the non-persistent empty storage on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

答案：B

167.To abide by industry regulations, a Solutions Architect must design a solution that will store a company’s critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located he Solutions Architect is required to provide access to the data stored in AWS to

the company's global WAN network. The security team mandates that no traffic accessing this data should traverse the public interne.
How should the Solutions Architect design a highly available solution that meets the requirements and is cost-effective?
A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data
B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
C. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions
答案：B
解析：D 太贵，多了 dx 网关的费用比 vpc 对等贵，C 走的是公网

168.A company has an existing on-premises three-tier web application. The Linux web servers serve content from a centralized file share on a NAS server because the content is refreshed several times a day from various sources. The existing infrastructure is not optimized and the company would like to move to AWS in order to gain the ability to scale resources up and down in response to load On-premises and AWS resources are connected using AWS Direct Connect.
How can the company migrate the web infrastructure to AWS without delaying the content refresh process?
A. Create a cluster of web server Amazon EC2 instances behind a Classic load Balancer on AWS Share an Amazon EBS volume among all instances for the content, Schedule a periodic synchronization of this volume and the NAS server.
B. Create an on-premises file gateway using AWS Storage Gateway to replace the NAS server and replicate content to AWS On the AWS side, mount the same Storage Gateway bucket to each web server Amazon EC2 instance to serve the content
C. Expose an Amazon EFS share to on-premises users to serve as the NAS server. Mount the same EFS share to the web server Amazon EC2 stances to serve the content
D. Create web server Amazon EC2 instances on AWS in an Auto Scaling group. Configure a nightly process where the web server instances are updated from the NAS server
答案：C

169. A company is refactoring an existing web service that provides read and write access to structured data. The service must respond to short but significant spikes in the system load. The service must be fault tolerant across multiple AWS Regions.
Which actions should be taken to meet these requirements?
A. Store the data in Amazon DocumentDB. Create a single global Amazon Cloud Front distribution with a custom origin built on edge-optimized Amazon API Gateway and AWS Lambda Assign the company's domain as an alternate domain for the distribution， and configure Amazon Route 53 with an alias to the Cloud Front distribution
B. Store the data in replicated Amazon S3 buckets in two Regions. Create an Amazon Cloud Front distribution in each Region, with custom origins built on Amazon API Gateway and AWS Lambda launched

in each Region，Assign the company's domain as an alternate domain for both distributions， and configure Amazon Route 53 with a failover routing policy between them.

C. Store the data in an Amazon DynamoDB global table in two Regions using on-demand capacity. In both Regions， run the web service as Amazon ECS Fargate tasks in an Auto Scaling ECS service behind an Application Load Balancer（ALB）.In Amazon Route 53，configure an alias record in the company’s domain and a Route 53 latency-based routing policy with health checks to distribute traffic between the two ALBs.

D. Store the data in Amazon Aurora global databases. Add Auto Scaling replicas to both Regions. Run the web service on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer in each Region. Configure the instances to download the web service code in the user data. In Amazon Route 53，configure an alias record for the company’s domain and a multi-value routing policy

答案：C

170. A group of research institutions are partnering to study 2 PB of genomic data that changes regularly. The primary institution that owns the data is storing it in an Amazon S3 bucket in its AWS account. All of the secondary institutions in the partnership have their own AWS accounts and require read access to the data The institute that owns the data does not want to pay for the data transfer costs associated with allowing the secondary institutes access to the data.

Which of the following solutions will meet the requirements?

A. In the primary account， create a cross-account AWS lAM role for each secondary account that allows read access to the data. Have the secondary institutions assume the role when accessing the data.

B. In the primary account，create an S3 bucket policy to give read access to each secondary account. Enable Requester Pays on the S3 bucket. Have the secondary institutions use their own AWS credentials with read permissions to the S3 bucket， when accessing the data.

C. Create an S3 bucket in each of the secondary accounts with a S3 bucket policy that gives write access to the primary account. Periodically synchronize the S3 buckets from the primary account to each secondary account. Have the secondary institutions use their own AWS credentials when accessing the data.

D. In the primary account， create a cross-account AWS IAM role for each secondary account that allows read access to the data. Enable Requester Pays on the S3 bucket. Have the secondary institutions assume the role when accessing the data.

答案：B

171. A company is running an email application across multiple AWS Regions. The company uses Ohio （us-east-2）as the primary Region and Northern Virginia（us-east-1）as the Disaster Recovery（DR）Region. The data is continuously replicated from the primary Region to the DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time， but it affects the application’s RPO. Which of the following solutions should help remediate this performance problem? （Select TWO.）

A. Increase the size of the instances

B. Have the instance in the primary Region write the data to an Amazon SQS queue in the primary Region instead， and have the instance in the DR Region poll from this queue.

C. Use multiple instances on the primary and DR Regions to send and receive the replication data

D. Change the DR Region to Oregon （us-west-2） instead of the current DR Region

E. Attach an additional elastic network interface to each of the instances in both Regions and set up load balancing between the network interfaces

答案：BC

172. A company is testing Amazon Elastic File Service（EFS） in its Development VPC and would like to

extend this test on-premises. EFS is running in us-east-1 and the corporate network is currently connected to this Region through a site-to-Site VPN. All on-premises computers and servers are required to have all DNS traffic resolved by their on-premises DNS servers. The on-premises users would like to connect to the EFS using a DNS name instead of an IP address.
What collection of steps must be taken to meet this requirement? (select Two.)
A. Create a new Amazon Route 53 Private Hosted Zone with a domain name of awscloud. example. com and associate the Development VPC to this zone. Create a CNAME record and point this to the EFS endpoint .
B. Create a new Amazon route 53 Public Hosted Zone with a domain name of awscloud. example. com and associate the Development VPC to this zone. Create a CNAME record and point this to the EFS endpoint .
C. Create a conditional forwarder rule in the on-premises DNS servers to forward requests for awscloud. example. com to the Amazon Route 53 Resolver inbound endpoints
D. Create a conditional forwarder rule in the on-premises DNS servers to forward requests for awscloud. example. com to the Amazon Route 53 Resolver outbound endpoints
E. Create a conditional forwarder rule in the on-premises DNS servers to forward requests for awscloud. example. com to the Amazon-provided DNS server
答案: BC

173.A company wants to launch an online shopping website in multiple countries and must ensure that customers are protected against potential "man-in-the-middle" attacks.
Which architecture will provide the MOST secure site access?
A. Use Amazon Route 53 for domain registration and DNS services. Enable DNSSEC for all Route 53 requests. Use AWS Certificate Manager (ACM) to register TLS/SSL certificates for the shopping website, and use Application Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all client requests to the site.
B. Register 2048-bit encryption keys from a third-party certificate service. Use a third-party DNS provider that uses the customer managed keys for DNSSec Upload the keys to ACM, and use ACM to automatically deploy the certificates for secure web services to an EC2 front-end web server fleet by using NGINX. Use the server Name Identification extension in all client requests to the site.
C. Use Route 53 for domain registration. Register 2048-bit encryption keys from a third-party certificate service. Use a third-party DNS service that supports DNSSEC for DNS requests that use the customer managed keys. Import the customer managed keys to ACM to deploy the certificates to Classic Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all client requests to the site.
D. Use Route 53 for domain registration, and host the company DNS root servers on Amazon EC2 instances running Bind. Enable DNSSEC for DNS requests. Use ACM to register TLS/SSL certificates for the shopping website, and use Application Load Balancers configured with those TLS/SSL certificates for the site. Use the server Name Identification extension in all client requests to the site
答案: A

174. A company is using multiple AWS accounts and has multiple DevOps teams running production and non-production workloads in these accounts. The company would like to centrally-restrict access to some of the AWS services that the DevOps teams do not use. The company decided to use AWS Organizations and successfully invited all AWS accounts into the Organization. They would like to allow access to services that are currently in-use and deny a few specific services. Also they would like to administer multiple accounts together as a single unit.
What combination of steps should the Solutions Architect take to satisfy these requirements? (Select THREE.)

A. Use a Deny list strategy
B. Review the Access Advisor in AWS lAM to determine services recently used
C. Review the AWS Trusted Advisor report to determine services recently used
D. Remove the default FullAWSAccess SCP
E. Define organizational units (OUs) and place the member accounts in the OUs.
F. Remove the default DenyAWSAccess SCP
答案：ACE

175. An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's ClO has asked a Solutions Architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays.
Which of the following is the MOST reliable approach to meet the requirements?
A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them
B. Receive the orders in an Amazon SQS queue and trigger an AWS Lambda function to process them
C. Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container to process them
D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them
答案：B

176.A bank is designing an online customer service portal where customers can chat with customer service agents. The portal is required to maintain a 15-minute RPO and RTO in case of a regional disaster.
Banking regulations require that all customer service chat transcripts must be preserved on durable storage for at least 7 years, chat conversations must be encrypted in-flight, and transcripts must be encrypted at rest. The Data Loss Prevention team requires that data at rest must be encrypted using a key that the team controls. rotates. and revokes
Which design meets these requirements?
A. The chat application logs each chat message into Amazon CloudWatch Logs. A scheduled AWS Lambda function invokes a CloudWatch Logs Create Export Task every 5 minutes to export chat transcripts to Amazon S3. The S3 bucket is configured for cross-region replication to the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the S3 bucket
B. The chat application logs each chat message into two different Amazon CloudWatch Logs groups in two different regions, with the same AWS KMS key applied. Both CloudWatch Logs groups are configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy with a KMS key specified
C. The chat application logs each chat message into Amazon CloudWatch Logs. A subscription filter on the CloudWatch Logs group feeds into an Amazon Kinesis Data Firehose which streams the chat messages into an Amazon S3 bucket in the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Kinesis Data Firehose.
D. The chat application logs each chat message into Amazon CloudWatch Logs. The CloudWatch Logs group is configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy Glacier cross-region replication mirrors chat archives to the backup region. Separate AWS KMS keys are specified for the Cloud Watch Logs group and the Amazon Glacier vault
答案：C

177. A hybrid network architecture must be used during a company's multi-year data center migration from multiple private data centers to AWS. The current data centers are linked together with private fiber. Due to unique legacy applications, Network Address Translation （NAT） cannot be used. During the migration

period, many applications will need access to other applications in both the data centers and AWS.
Which option offers a hybrid network architecture that is secure and highly available, that allows for consistent high bandwidth and a multi-region deployment post-migration?
A. Use an AWS Direct Connect connection to each data center from different providers, and configure routing to failover to the other data center's Direct Connect connection if one fails. Ensure that no VPC CIDR blocks overlap one another or the on-premises network
B. Use multiple hardware VPN connections to AWS from the on-premises data center. Route different subnet traffic through different VPN connections. Ensure that no VPC CIDR blocks overlap one another or the on-premises network C. Use a software VPN with clustering both in AWS and the on-premises data center, and route traffic through the cluster. Ensure that no VPC CIDR blocks overlap one another or the on-premises network
D. Use a single AWS Direct Connect connection and a VPN as backup, and configure both to use the same virtual private gateway and Border Gateway Protocol（BGP）。 Ensure that no VPC CIDR blocks overlap one another or the on-premises network
答案： D

178. A Solutions Architect needs to migrate an on-premises legacy application to AWS. The application runs on two servers behind a load balancer. The application requires a license file that is associated with the MAC address of the server's network adapter. It takes the software vendor 12 hours to send new license files. The application also uses configuration files with a static IP address to access a database server; host names are not supported.
Given these requirements, which combination of steps should be taken to enable highly available architecture for the application servers in AWS? （Select Two）
A. Create a pool of ENIs. Request license files from the vendor for the pool, and store the license files in Amazon S3. Create a bootstrap automation script to download a license file and attach the corresponding ENI to an Amazon EC2 instance
B. Create a pool of ENIs. Request license files from the vendor for the pool, store the license files on an Amazon EC2 instance. Create an AMI from the instance and use this AMI for all future EC2 instances
C. Create a bootstrap automation script to request a new license file from the vendor. When the response is received, apply the license file to an Amazon EC2 instance
D. Edit the bootstrap automation script to read the database server IP address from the AWS Systems Manager Parameter Store, and inject the value into the local configuration files
E. Edit an Amazon EC2 instance to include the database server IP address in the configuration files and re-create the AMI to use for all future EC2 instances
答案： AE

179. A Developer would like to implement multi-account access for AWS Systems Manager and plans to use two member accounts within their AWS Organization The Developer has delegated an IAM Role that allows Systems Manager（SSM）
Parameter Store and Document resources to be trusted by the member accounts. While testing access from a member account, a user receives "Access Denied" errors when performing any SSM related operations. The Solutions Architect confirms that SSM operations are not denied in any of the Organization's Service Control Policies（SCP）。 Both member accounts are moved into a test OU which is not associated with any deny SCPs, however the user is still receiving an access denied error.
What changes should the Solutions Architect make to provide access while maintaining least privileges?
A. Create a new SCP which allows SSM operations and specify the ARNs for each SSM Parameter Store and Document. Apply the new SCP to the test OU that the member accounts were moved into.
B. Create a new SCP that allows full access to AWS resources. Apply the new SCP to the test OU that the

member accounts were moved into.
C. Remove both member accounts from the current Organization. Create a new Organization, with the account holding the SSM resources as the new master account and the other account as a member to the new Organization. Create a new SCP which allows full access to AWS resources.
D. Remove both member accounts from the current Organization. Create a new Organization, with the account holding the SSM resources as the new master account and the other account as a member to the new Organization. Create a new SCP which allows SSM operations and specify the ARNs for each SSM Parameter Store and Document within the new master account.
答案：D

180. A company is currently using AWS CodeCommit for its source control and AWS CodePipeline for continuous integration. The pipeline has a build stage for building the artifacts, which is then staged in an Amazon S3 bucket.
The company has identified various improvement opportunities in the existing process and a Solutions Architect has been given the following requirements:
- Create a new pipeline to support feature development.
- Support feature development without impacting production applications.
- Incorporate continuous testing with unit tests.
- Isolate development and production artifacts.
- Support the capability to merge tested code into production code.

How should the Solutions Architect achieve these requirements?
A. Trigger a separate pipeline from CodeCommit feature branches. Use AWS CodeBuild for running unit tests. Use CodeBuild to stage the artifacts within an S3 bucket in a separate testing account.
B. Trigger a separate pipeline from CodeCommit feature branches Use AWS Lambda for running unit tests. Use AWS CodeDeploy to stage the artifacts within an S3 bucket in a separate testing account
C. Trigger a separate pipeline from CodeCommit tags. Use Jenkins for running unit tests. Create a stage in the pipeline with S3 as the target for staging the artifacts within an S3 bucket in a separate testing account.
D. Create a separate Code Commit repository for feature development and use it to trigger the pipeline. Use AWS Lambda for running unit tests Use AWS CodeBuild to stage the artifacts within different S3 buckets in the same production account.
答案：A

181. A company hosts a community forum site using an Application Load Balancer （ALB） and a Docker application hosted in an Amazon ECS cluster. The site data is stored in Amazon RDS for MySQL and the container image is stored in ECR. The company needs to provide their customers with a disaster recovery SLA with an RTO of no more than 24 hours and RPO of no more than 8 hours
Which of the following solutions is the MOST cost-effective way to meet the requirements?
A. Use AWS Cloud Formation to deploy identical ALB, EC2,ECs and RDS resources in two regions. Schedule RDS snapshots every 8 hours. Use RDS multi-region replication to update the secondary region's copy of the database. In the event of a failure, restore from the latest snapshot, and use an Amazon Route 53 DNS failover policy to automatically redirect customers to the ALB in the secondary region
B. Store the Docker image in ECR in two regions. Schedule RDS snapshots every 8 hours with snapshots copied to the secondary region. In the event of a failure, use AWS CloudFormation to deploy the ALB, EC2，ECs and RDS resources in the secondary region, restore from the latest snapshot, and update the DNS record to point to the ALB in the secondary region
C. Use AWS Cloud Formation to deploy identical ALB, EC2,ECS, and RDS resources in a secondary region. Schedule hourly RDS MySQL backups to Amazon S3 and use cross-region replication to replicate data to a bucket in the secondary region. In the event of a failure, import the latest Docker image to Amazon ECR in

the secondary region, deploy to the EC2 instance restore the latest MySQL backup, and update the DNS record to point to the ALB in the secondary region

D. Deploy a pilot light environment in a secondary region with an ALB and a minimal resource EC2 deployment for Docker in an AWS Auto Scaling group with a scaling policy to increase instance size and number of nodes. Create a cross-region read replica of the RDS data. In the event of a failure, promote the replica to primary, and update the DNS record to point to the ALB in the secondary region

答案：C

182. A mobile gaming application publishes data continuously to Amazon Kinesis Data Streams. An AWS Lambda function processes records from the data stream and writes to an Amazon DynamoDB table. The DynamoDB table has an auto scaling policy enabled with the target utilization set to 70%

For several minutes at the start and end of each day, there is a spike in traffic that often exceeds five times the normal load. The company notices the GetRecords Iterator AgeMilliseconds metric of the Kinesis data stream temporarily spikes to over a minute for several minutes. The AWS Lambda function writes Provisioned ThroughputExceededException messages to Amazon Cloud Watch Logs during these times, and some records are redirected to the dead letter queue. No exceptions are thrown by the Kinesis producer on the gaming application.

What change should the company make to resolve this issue?

A. Use Application Auto Scaling to set a scaling schedule to scale out write capacity on the DynamoDB table during predictable load spikes.

B. Use Amazon CloudWatch Events to monitor the dead letter queue and invoke a Lambda function to automatically retry failed records

C. Reduce the DynamoDB table auto scaling policy's target utilization to 20% to more quickly respond to load spikes

D. Increase the number of shards in the Kinesis data stream to increase throughput capacity

答案：B

解析：瓶颈在于 ddb 扩展的时候，速度跟不上突发的流量，所以导致一部分流量来不及被处理就过期了，所以我们增加 kinesis 的吞吐量不能解决问题，因为只丢失了一部分，所以让 lambda 重传一下就行

183. A company is planning to deploy a new business analytics application that requires 10，000 hours of compute time each month. The compute resources can have flexible availability, but must be as cost-effective as possible. The company will also provide a reporting service to distribute analytics reports, which needs to run at all times。

How should the Solutions Architect design a solution that meets these requirements?

A. Deploy the reporting service on a Spot Fleet. Deploy the analytics application as a container in Amazon ECS with AWS Fargate as the compute option. Set the analytics application to use a custom metric with Service Auto Scaling

B. Deploy the reporting service on an On-Demand Instance. Deploy the analytics application as a container in AWS Batch with AWS Fargate as the compute option. Set the analytics application to use a custom metric with Service Auto Scaling.

C. Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option. Deploy the analytics application on a Spot Fleet. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the Spot Fleet.

D. Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option. Deploy the analytics application on an On-Demand Instance and purchase a Reserved Instance with a 3-year term. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the On-Demand Instance

答案：B

184. A retail company processes point-of-sale data on application servers in its data center and writes outputs to an Amazon DynamoDB table. The data center is connected to the company's VPC with an AWS Direct Connect（DX）connection, and the application servers require a consistent network connection at speeds greater than 2 Gbps.
The company decides that the DynamoDB table needs to be highly available and fault tolerant. The company policy states that the data should be available across two regions.
What changes should the company make to meet these requirements?
A. Establish a second DX connection for redundancy. Use DynamoDB global tables to replicate data to a second Region. Modify the application to fail over to the second Region.
B. Use an AWS managed VPN as a backup to DX. Create an identical DynamoDB table in a second Region. Modify the application to replicate data to both Regions.
C. Establish a second DX connection for redundancy. Create an identical DynamoDB table in a second Region. Enable DynamoDB auto scaling to manage throughput capacity. Modify the application to write to the second Region
D. Use AWS managed VPN as a backup to DX. Create an identical DynamoDB table in a second Region. Enable DynamoDB streams to capture changes to the table Use AWS Lambda to replicate changes to the second Region
答案：D

185. A company developed a Java application and deployed it to an Apache Tomcat server that runs on Amazon EC2 instances. The company's Engineering team has implemented AWS Cloud Formation and Chef Automate to automate the provisioning of and updates to the infrastructure and configuration of the application in the development, test, and production environments. These implementations have led to significantly improved reliability in releasing changes. The Engineering team reports there are frequent service disruptions due to unexpected errors when updating the application or the Apache Tomcat server.
Which solution will increase the reliability of all releases?
A. Implement a blue/green deployment methodology
B. Implement the canary release methodology
C. Configure Amazon Cloud Front to serve all requests from the cache while deploying the updates
D. Implement the all at once deployment methodology.
答案：A

186. During an audit, a Security team discovered that a Development team was putting IAM user secret access keys in their code and then committing it to an AWS CodeCommit repository. The security team wants to automatically find and remediate instances of this security vulnerability.
Which solution will ensure that the credentials are appropriately secured automatically?
A. Run a script nightly using AWS Systems Manager Run Command to search for credentials on the development instances. If found, use AWS Secrets Manager to rotate the credentials.
B. Use a scheduled AWS Lambda function to download and scan the application code from Code Commit If credentials are found, generate new credentials and store them in AWS KMS.
C. Configure Amazon Macie to scan for credentials in Code commit repositories. If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user.
D. Configure a Code Commit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.
答案：D
解析：macie 是检测 pii 的

187. A company has a Microsoft SQL Server database in its data center and plans to migrate data to Amazon Aurora MySQL. The company has already used the AWS Schema Conversion Tool to migrate triggers, stored procedures, and other schema objects to Aurora MySQL. The database contains 1 TB of data and grows less than 1 MB per day. The company ‘s data center is connected to AWS through a dedicated 1 Gbps AWS Direct Connect connection.
The company would like to migrate data to Aurora MySQL and perform reconfigurations with minimal downtime to the applications.
Which solution meets the company' s requirements?
A. Shut down applications over the weekend. Create an AWS DMS replication instance and task to migrate existing data from SQL Server to Aurora MySQL. Perform application testing and migrate the data to the new database endpoint.
B. Create an AWS DMS replication instance and task to migrate existing data and ongoing replication from SQL Server to Aurora MySQL. Perform application testing and migrate the data to the new database endpoint.
C. Create a database snapshot of SQL Server on Amazon S3. Restore the database snapshot from Amazon S3 to Aurora MySQL. Create an AWS DMS replication instance and task for ongoing replication from SQL Server to Aurora MySQL Perform application testing and migrate the data to the new database endpoint.
D. Create a SQL Server native backup file on Amazon S3. Create an AWS DMS replication instance and task to restore the SQL Server backup file to Aurora MySQL. Create another AWS DMS task for ongoing replication from SQL Server to Aurora MySQL. Perform application testing and migrate the data to the new database endpoint
答案：C

188. A company has been using a third-party provider for its content delivery network and recently decided to switch to Amazon CloudFront. The development team wants to maximize performance for the global user base. The company uses a content management system（CMS）that serves both static and dynamic content. The CMS is behind an Application Load Balancer（ALB）which is set as the default origin for the distribution. Static assets are served from an Amazon S3 bucket. The Origin Access Identity（OAI）was created properly and the S3 bucket policy has been updated to allow the GetObject action from the OAI, but static assets are receiving a 404 error.
Which combination of steps should the solutions architect take to fix the error? （Select Two）
A. Add another origin to the CloudFront distribution for the static assets
B. Add a path-based rule to the ALB to forward requests for the static assets
C. Add an RTMP distribution to allow caching of both static and dynamic content
D. Add a behavior to the CloudFront distribution for the path pattern and the origin of the static assets
E. Add a host header condition to the ALB listener and forward the header from CloudFront to add traffic to the allow list
答案：BE

189. A company has several teams, and each team has their own Amazon RDS database that totals 100 TB. The company is building a data query platform for business intelligence analysts to generate a weekly business report. The new system must run ad-hoc SQL queries.
What is the most cost-effective solution?
A. Create a new Amazon Redshift cluster. Create an AWS Glue ETL job to copy data from the RDS databases to the Amazon Redshift cluster. Use Amazon Redshift to run the query.
B. Create an Amazon EMR cluster with enough core nodes. Run an Apache Spark job to copy data from the RDS databases to an Hadoop Distributed File System（HDFS）. Use a local Apache Hive metastore to maintain the table definition. Use Spark SQL to run the query.

C. Use an AWS Glue ETL job to copy all the RDS databases to a single Amazon Aurora PostgreSQL database. Run SQL queries on the Aurora PostgreSQL database

D. Use an AWS Glue crawler to crawl all the databases and create tables in the AWS Glue Data Catalog. Use an AWS Glue ETL job to load data from the RDS databases to Amazon S3， and use Amazon Athena to run the queries

答案：D

190. A company is migrating its three-tier web application from on-premises to the AWS Cloud. The company has the following requirements for the migration process:

- Ingest machine images from the on-premises environment.
- Synchronize changes from the on-premises environment to the AWS environment until the production cutover
- Minimize downtime when executing the production cutover
- Migrate the virtual machines' root volumes and data volumes.

Which solution will satisfy these requirements with minimal operational overhead?

A. Use AWS Server Migration Service（SMS）to create and launch a replication job for each tier of the application. Launch instances from the AMIs created by AWS SMS. After initial testing, perform a final replication and create new instances from the updated AMIs

B. Create an AWS CLI VM Import/Export script to migrate each virtual machine. Schedule the script to run incrementally to maintain changes in the application Launch instances from the AMIs created by VM Import/Export. Once testing is done, rerun the script to do a final import and launch the instances from the AMIs

C. Use AWS Server Migration Service（SMS） to upload the operating system volumes. Use the AWS CLI import-snapshot command for the data volumes. Launch instances from the AMIs created by AWS SMS and attach the data volumes to the instances. After initial testing, perform a final replication, launch new instances from the replicated AMIs, and attach the data volumes to the instances.

D. Use AWS Application Discovery Service and AWS Migration Hub to group the virtual machines as an application. Use the AWS CLI VM Import/Export script to import the virtual machines as AMIs. Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs. After initial testing, perform a final virtual machine import and launch new instances from the AMIs

答案：A

191. A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone. The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:

- Inbound requests must be filtered for common vulnerability attacks
- Rejected requests must be sent to a third-party auditing application
- All resources should be highly available

Which solution meets these requirements?

A. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer（ALB）and select the previously created Auto Scaling group as the target. Use Amazon Inspector to monitor to the ALB and EC2 instances. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.

B. Configure an Application Load Balancer（ALB）and add the EC2 instances as targets. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.

C. Configure an Application Load Balancer（ALB）along with a target group adding the EC2 instances as

targets. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application. Create a web ACL in WAF.Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

D. Configure a Multi-AZ Auto Scaling group using the application's AMI Create an Application Load Balancer （ALB） and select the previously created Auto Scaling group as the target. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

答案： D

解析：题目中说了 3 个要求，第一个考点是 waf，第二个是 kinesis 发送到第三方，第三个就是多 az 的自动扩展组

192. A retail company has a custom. NET web application running on ASW that uses Microsoft SQL Server for the database. The application servers maintain a user's session locally.

Which combination of architecture changes are needed to ensure all tiers of the solution are highly available？ （Select THREE）

A. Refactor the application to store the user's session in Amazon ElastiCache. Use Application Load Balancers to distribute the load between application instances.

B. Set up the database to generate hourly snapshots using Amazon EBS. Configure an Amazon CloudWatch Events rule to launch a new database instance if the primary one fails.

C. Migrate the database to Amazon RDS for SQL Server. Configure the RDS instance to use a Multi-AZ deployment

D. Move the NET content to an Amazon S3 bucket. Configure the bucket for static website hosting

E. Put the application instances in an Auto Scaling group. Configure the Auto Scaling group to create new instances if an instance becomes unhealthy

F. Deploy Amazon Cloud Front in front of the application tier. Configure Cloud Front to serve content from healthy application instances only

答案： BCF

193. During a security audit of a service team’s application, a solutions architect discovers that a username and password for an Amazon RDS database and a set of AWS IAM user credentials can be viewed in the AWS Lambda function code. The Lambda function uses the username and password to run queries on the database, and it uses the lAM credentials to call AWS services in a separate management account

The solutions architect is concerned that the credentials could grant inappropriate access to anyone who can view the Lambda code. The management account and the service team’s account are in separate AWS Organizations organizational units （OUs） .

Which combination of changes should the solutions architect make to improve the solution's security ？ （Select Two）

A. Configure Lambda to assume a role in the management account with appropriate access to AWS.

B. Configure Lambda to use the stored database credentials in AWS Secrets Manager and enable automatic rotation C. Create a Lambda function to rotate the credentials every hour by deploying a new Lambda version with the updated credentials.

D. Use an SCP on the management account's OU to prevent IAM users from accessing resources in the service team’s account

E. Enable AWS Shield Advanced on the management account to shield sensitive resources from unauthorized lAM access

答案： BD

194. A solutions architect needs to design a highly available application that will allow authenticated users to stay connected to the application even when there are underlying failures.
Which solution will meet these requirements?
A. Deploy the application on Amazon EC2 instances. Use Amazon Route 53 to forward requests to the EC2 instances. Use Amazon DynamoDB to save the authenticated connection details.
B. Deploy the application on Amazon EC2 instances in an Auto Scaling group. Use an internet-facing Application Load Balancer to handle requests. Use Amazon DynamoDB to save the authenticated connection details
C. Deploy the application on Amazon EC2 instances in an Auto Scaling group. Use an internet-facing Application Load Balancer on the front end. use EC2 instances to save the authenticated connection details.
D. Deploy the application on Amazon EC2 instances in an Auto Scaling group. Use an internet-facing Application Load Balancer on the front end. Use EC2 instances hosting a MySQL database to save the authenticated connection details
答案：B

195. A company's AWS architecture currently uses access keys and secret access keys stored on each instance to access AWS services. Database credentials are hard-coded on each instance. SSH keys for command-line remote access are stored in a secured Amazon S3 bucket. The company has asked its solutions architect to improve the security posture of the architecture without adding operational complexity.
Which combination of steps should the solutions architect take to accomplish this? （Select THREE）
A. Use Amazon EC2 instance profiles with an IAM role
B. Use AWS Secrets Manager to store access keys and secret access keys
C. Use AWS Systems Manager Parameter Store to store database credentials
D. Use a secure fleet of Amazon EC2 bastion hosts for remote access
E. Use AWS KMS to store database credentials
F. Use AWS Systems Manager Session Manager for remote access
答案：ABF

196. A company is migrating its on-premises systems to AWS. The user environment consists of the following systems:
- Windows and Linux virtual machines running on VMware
- Physical servers running Red Hat Enterprise Linux

The company wants to be able to perform the following steps before migrating to AWS:
- Identify dependencies between on-premises systems
- Group systems together into applications to build migration plans
- Review performance data using Amazon Athena to ensure that Amazon EC2 instances are right-sized

How can these requirements be met?
A. Populate the AWS Application Discovery Service import template with information from an on-premises configuration management database（CMDB）. Upload the completed import template to Amazon S3，then import the data into Application Discovery Service
B. Install the AWS Application Discovery Service Discovery Agent on each of the on-premises systems. Allow the Discovery Agent to collect data for a period of time.
C. Install the AWS Application Discovery Service Discovery Connector on each of the on-premises systems and in VMware vCenter. Allow the Discovery Connector to collect data for one week
D. Install the AWS Application Discovery Service Discovery Agent on the physical on-premises servers. Install the AWS Application Discovery Service Discovery Connector in VMware vCenter. Allow the Discovery Agent to collect data for a period of time

答案：B

197. An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit（OU）that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access

What is the MOST efficient way to design an architecture to meet these requirements?

A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all lAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy

B. Create an lAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.

C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.

D. Create an IAM role named procurement-manager-role in the AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization

答案：C

198. A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPS in the root of the organization to manage access to restricted services.

The company recently acquired a new business unit and invited the new unit' s existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company’s policies Which option will allow administrators to make changes and continue to enforce the current policies.

Which option will allow administrators to make changes and continue the current policies without introducing additional long-term maintenance?

A. Remove the organization’s root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.

B. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the new account to the Production OU when adjustments to AWS Config are complete

C. Convert the organization’s root SCPs from deny list SCPs to allow list SCPs to allow the required services only. Temporarily apply an SCP to the organization’s root that allows AWS Config actions for principals only in the new account

D. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to

allow AWS Config actions. Move the organization's root SCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete
答案：B

199.A company needs to move its on-premises resources to AWS. The current environment consists of 100 virtual machines（VMs）with a total of 40 TB of storage. Most of the VMs can be taken offline because they support functions during business hours only, however, some are mission critical. so downtime must be minimized.
The administrator of the on-premises network provisioned 10 Mbps of internet bandwidth for the migration. The on-premises network throughput has reached capacity and would be costly to increase. A solutions architect must design a migration solution that can be performed within the next 3 months.
Which method would fulfill these requirements?
A. Set up a 1 Gbps AWS Direct Connect connection. Then, provision a private virtual interface, and use AWS Server Migration Service（SMS）to migrate the VMs into Amazon EC2
B. Use AWS Application Discovery Service to assess each application, and determine how to refactor and optimize each using AWS services or AWS Marketplace solutions
C. Export the VMs locally, beginning with the most mission-critical servers first Use AWS Transfer for SFTP to securely upload each VM to Amazon S3 after they are exported. Use VM Import/Export to import the VMs into Amazon EC2
D. Migrate mission-critical VMs with AWS SMS. Export the other VMs locally and transfer them to Amazon S3 using AWS Snowball. Use VM Import/Export to import the VMs into Amazon EC2
答案：D

200. A utility company wants to collect usage data every 5 minutes from its smart meters to facilitate time-of-use metering. When a meter sends data to AWS, the data is sent to Amazon API Gateway, processed by an AWS Lambda function, and stored in an Amazon DynamoDB table. During the pilot phase, the Lambda functions took from 3 to 5 seconds to complete
As more smart meters are deployed, the engineers notice the Lambda functions are taking from 1 to 2 minutes to complete. The functions are also increasing in duration as new types of metrics are collected from the devices. There are many ProvisionedThroughputExceededException errors while performing PUT operations on DynamoDB, and there are also many TOOManyRequestsException errors from Lambda.
Which combination of changes will resolve these issues? （Select TWO）
A. Increase the write capacity units to the Dynamo DB table
B. Increase the memory available to the Lambda functions
C. Increase the payload size from the smart meters to send more data
D. Stream the data into an Amazon Kinesis data stream from API Gateway and process the data in batches
E. Collect data in an Amazon SQS FIFO queue, which triggers a Lambda function to process each message
答案：BE

201. A company provides AWS solutions to its users with AWS CloudFormation templates. Users launch the templates in their accounts to have different solutions provisioned for them. The users want to improve the deployment strategy for solutions while retaining the ability to do the following:

- Add their own features to a solution for their specific deployments
- Run unit tests on their changes
- Turn features on and off for their deployments
- Automatically update with code changes
- Run security scanning tools for their deployments

Which strategies should the solutions architect use to meet the requirements?

A. Allow users to download solution code as docker images. Use AWS CodeBuild and AWS CodePipeline for the CI/CD pipeline. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use AWS CodeDeploy to run unit tests and security scans, and for deploying and updating a solution with changes

B. Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use AWS Amplify plugins for different solution features and user prompts to turn features on and off. Use AWS Lambda to run unit tests and security scans, and AWS CodeBuild for deploying and updating a solution with changes

C. Allow users to download solution code artifacts in their Amazon S3 buckets. Use Amazon S3 and AWS CodePipeline for the CI/CD pipelines. Use CloudFormation StackSets for different solution features and to turn features on and off. Use AWS Lambda to run unit tests and security scans, and CloudFormation for deploying and updating a solution with changes.

D. Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use the AWS Cloud Development Kit constructs for different solution features, and use the manifest file to turn features on and off. Use AWS CodeBuild to run unit tests and security scans, and for deploying and updating a solution with changes

答案：D

202. A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?

A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function

B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions

C. Run a script that puts a private ACL on all of the objects in the bucket

D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket

答案：D

203. A company needs to create a centralized logging architecture for all of its AWS accounts. The architecture should provide near-real-time data analysis for all AWS CloudTrail logs and VPC Flow Logs across all AWS accounts. The company plans to use Amazon Elasticsearch Service（Amazon ES） to perform log analyses in the logging account.

Which strategy should a solutions architect use to meet these requirements?

A. Configure CloudTrail and VPC Flow Logs in each AWS account to send data to a centralized Amazon S3 bucket in the logging account. Create an AWS Lambda function to load data from the S3 bucket to Amazon ES in the logging account

B. Configure CloudTrail and VPC flow Logs to send data to a log group in Amazon CloudWatch Logs in each AWS account Configure a CloudWatch subscription filter in each AWS account to send data to Amazon Kinesis Data Firehose in the logging account Load data from Kinesis Data Firehose into Amazon ES in the logging account

C. Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket in each AWS account. Create an AWS Lambda function triggered by S3 events to copy the data to a centralized logging bucket. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging

account
D. Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch Logs in each AWS account. Create AWS Lambda functions in each AWS account to subscribe to the log groups and stream the data to an Amazon S3 bucket in the logging account. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.
答案：B

204.A company has an internal application running on AWS that is used to track and process shipments in the company's warehouse. Currently, after the system receives an order, it emails the staff the information needed to ship a package. Once the package is shipped, the staff replies to the email and the order is marked as shipped.
The company wants to stop using email in the application and move to a serverless application model.
Which architecture solution meets these requirements?
A. Use AWS Batch to configure the different tasks required to ship a package. Have AWS Batch trigger an AWS Lambda function that creates and prints a shipping label. Once that label is scanned, as it leaves the warehouse, have another Lambda function move the process to the next step in the AWS Batch job.
B. When a new order is created, store the order information in Amazon SQS. Have AWS Lambda check the queue every 5 minutes and process any needed work. When an order needs to be shipped, have Lambda print the label in the warehouse. Once the label has been scanned, as it leaves the warehouse, have an Amazon EC2 instance update Amazon SQS.
C. Update the application to store new order information in Amazon DynamoDB. When a new order is created, trigger an AWS Step Functions workflow, mark the orders as "in progress, "and print a package label to the warehouse. Once the label has been scanned and fulfilled, the application will trigger an AWS Lambda function that will mark the order as shipped and complete the workflow.
D. Store new order information in Amazon EFS. Have instances pull the new information from the NFS and send that information to printers in the warehouse. Once the label has been scanned, as it leaves the warehouse, have Amazon API Gateway call the instances to remove the order information from Amazon EFS
答案：C

205.A company is running a web application with On-Demand Amazon EC2 instances in Auto Scaling groups that scale dynamically based on custom metrics. After extensive testing, the company determines that the m5. 2xlarge instance size is optimal for the workload. Application data is stored in db.r4. 4xlarge Amazon RDS instances that are confirmed to be optimal. The traffic to the web application spikes randomly during the day. What other cost-optimization methods should the company implement to further reduce costs without impacting the reliability of the application?
A. Double the instance count in the Auto scaling groups and reduce the instance size to m5. large
B. Reserve capacity for the RDS database and the minimum number of EC2 instances that are constantly running
C. Reduce the RDS instance size to db.r4. xlarge and add five equivalently sized read replicas to provide reliability
D. Reserve capacity for all EC2 instances and leverage Spot Instance pricing for the RDS database
答案：D

206. A developer reports receiving an Error 403： Access Denied message when they try to download an object from an Amazon S3 bucket. The S3 bucket is accessed using an S3 endpoint inside a VPC, and is encrypted with an AWS KMS key. A solutions architect has verified that the developer is assuming the correct lAM role in the account that allows the object to be downloaded. The S3 bucket policy and the

NACL are also valid.
Which additional step should the solutions architect take to troubleshoot this issue?
A. Ensure that blocking all public access has not been enabled in the S3 bucket
B. Verify that the lAM role has permission to decrypt the referenced KMS key.
C. Verify that the IAM role has the correct trust relationship configured
D. Check that local firewall rules are not preventing access to the S3 endpoint.
答案：B

207. A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider（IdP）to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.
Which items should the solutions architect check to ensure identity federation is properly configured?（Select THREE）
A. The lAM user's permissions policy has allowed the use of SAML federation for that user.
B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.
C. Test users are not in the AWSFederatedUsers group in the company's IdP.
D. The web portal calls the AWS STS Assume With SAML API with the ARN of the SAML provider, the ARN of the IAM role. and the SAMl assertion from ldP
E. The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs
F. The company's IdP defines SAML assertions that properly map users or groups in the company to IAM roles with appropriate permissions
答案：ADF

208. A solutions architect is implementing federated access to AWS for users of the company's mobile application. Due to regulatory and security requirements, the application must use a custom-built solution for authenticating users and must use lAM roles for authorization.
Which of the following actions would enable authentication and authorization and satisfy the requirements?（Select Two）
A. Use a custom-built SAML-compatible solution for authentication and AWS SSO for authorization.
B. Create a custom-built LDAP connector using Amazon API Gateway and AWS Lambda for authentication. Store authorization tokens in Amazon DynamoDB, and validate authorization requests using another Lambda function that reads the credentials from DynamoDB .
C. Use a custom-built OpenID Connect-compatible solution with AWS SSO for authentication and authorization
D. Use a custom-built SAML-compatible solution that uses LDAP for authentication and uses a SAML assertion to perform authorization to the lAM identity provider
E. Use a custom-built OpenID Connect-compatible solution for authentication and use Amazon Cognito for authorization
答案：BE

209. A company has developed a custom tool used in its workflow that runs within a Docker container. The company must perform manual steps each time the container code is updated to make the container image available to new workflow executions. The company wants to automate this process to eliminate manual effort and ensure a new container image is generated every time the tool code is updated.
Which combination of actions should a solutions architect take to meet these requirements? （Select

THREE）
A. Configure an Amazon ECR repository for the tool. Configure an AWS CodeCommit repository containing code for the tool being deployed to the container image in Amazon ECR
B. Configure an AWS CodeDeploy application that triggers an application version update that pulls the latest tool container image from Amazon ECR, updates the container with code from the AWS CodeCommit repository, and pushes the updated container image to Amazon ECR.
C. Configure an AWS CodeBuild project that pulls the latest tool container image from Amazon ECR, updates the container with code from the source AWS CodeCommit repository, and pushes the updated container image to Amazon ECR
D. Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeDeploy application update.
E. Configure an Amazon EventBridge rule that triggers on commits to the AWS CodeCommit repository for the tool. Configure the event to trigger an update to the tool container image in Amazon ECR. Push the updated container image to Amazon ECR
F. Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeBuild build
答案：BCE

210. A company is migrating its applications to AWS. The applications will be deployed to AWS accounts owned by business units. The company has several teams of developers who are responsible for the development and maintenance of all applications. The company is expecting rapid growth in the number of users.
The company's chief technology officer has the following requirements:
- •Developers must launch the AWS infrastructure using AWS CloudFormation
- •Developers must not be able to create resources outside of CloudFormation
- •The solution must be able to scale to hundreds of AWS accounts

Which of the following would meet these requirements？ （Select Two）
A. Using CloudFormation, create an lAM role that can be assumed by CloudFormation that has permissions to create all the resources the company needs. Use CloudFormation StackSets to deploy this template to each AWS account
B. In a central account, create an IAM role that, can be assumed by developers, and attach a policy that allows interaction with CloudFormation. Modify the AssumeRdhePolicyDocument action to allow the lAM role to be passed to CloudFormation
C. Using CloudFormation, create an IAM role that can be assumed by developers, and attach policies that allow interaction with and passing a role to CloudFormation. Attach an inline policy to deny access to all other AWS services. Use CloudFormation StackSets to deploy this template to each AWS account.
D. Using CloudFormation, create an IAM role for each developer, and attach policies that allow interaction with CloudFormation. Use CloudFormation StackSets to deploy this template to each AWS account
E. In a central AWS account, create an IAM role that can be assumed by CloudFormation that has permissions to create the resources the company requires. Create a CloudFormation stack policy that allows the lAM role to manage resources. Use CloudFormation StackSets to deploy the CloudFormation stack policy to each AWS account
答案：BE

211. A company is running a two-tier web application on Amazon EC2. The web tier consists of an Application Load Balancer（ALB）backed by a Auto Scaling group of web server instances spanning multiple Availability Zones. The database tier is using Amazon Aurora MySQL. The company's security team has deployed AWS WAF and integrated it with the ALB to prevent SQL injection attacks against the application.

Recently, a security breach was reported in which the attacker was able to gain access to an individual web server and the company's database from random IP addresses. The security team was eventually able to write a better rule to match the SQL injection technique that the attacker had used. However, this process took about an hour from when the third-party security agent running on the EC2 instances successfully detected the attack. Which strategy allows the security team to protect the database and overall infrastructure?

A. Add an Amazon CloudFront layer to the existing architecture. Modify the AWS WAF association to integrate with CloudFront instead of the ALB. Change the web tier's security groups to allow IP addresses from Cloud Front only. Use Lambda@Edge to perform request inspection and block repetitive suspicious requests.

B. Configure the third-party security agent to invoke an AWS Lambda function. The Lambda function should first check the web tier's Auto Scaling group to ensure there is more than one running instance, and if so, then stop and quarantine the compromised web server instance.

C. Enable Amazon Macie and turn on its integrations with Amazon EC2 and the Aurora MySQL database. Create a visual dashboard for the security team. Configure automated alerts and define AWS Lambda functions to automatically block detected attacks by modifying security groups within the VPC.

D. Deploy Amazon GuardDuty to analyze VPC Flow Logs. Configure an Amazon EventBridge rule that triggers an AWS Lambda function upon a GuardDuty alert Configure the Lambda function to automatically block detected attacks by modifying security groups within the VPC

答案：A

212. A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in. NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200，000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer（NLB）in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB

B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer（ALB）in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB

C. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer（ALB）in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions

D. Use AWS Cloud Formation to launch a stack containing an Application Load Balancer（ALB）in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB

答案：B

213. A large company with hundreds of AWS accounts has a newly established centralized internal process for purchasing new or modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement or

execution. Previously, business units would directly purchase or modify Reserved Instances in their own respective AWS accounts autonomously.
Which combination of steps should be taken to proactively enforce the new process in the MOST secure way possible? (Select TWO)
A. Ensure all AWS accounts are part of an AWS Organizations structure operating in all features mode
B. Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2: PurchaseReservedInstancesOffering and ec2: Modify ReservedInstances actions
C. In each AWS account, create an IAM policy with a DENY rule to the ec2: PurchaseReservedInstancesOffering and ec2: ModifyReservedInstances actions
D. Create an SCP that contains a deny rule to the ec2: PurchaseReservedInstancesOffering and ec2: ModifyReservedInstances actions. Attach the SCP to each organizational unit (ou) of the AWS Organizations structure
E. Ensure that all AWS accounts are part of an AWS Organizations structure operating in consolidated billing features mode
答案: AD

214. An ecommerce company has an order processing application it wants to migrate to AWS. The application has inconsistent data volume patterns, but needs to be available at all times. Orders must be processed as they occur and in the order that they are received.
Which set of steps should a solutions architect take to meet these requirements.
A. Use AWS Transfer for SFTP and upload orders as they occur. Use On-Demand Instances in multiple Availability Zones for processing
B. Use Amazon SNS with FIFO and send orders as they occur. Use a single large Reserved Instance for processing
C. Use Amazon SQS with FIFO and send orders as they occur. Use Reserved Instances in multiple Availability Zones for processing
D. Use Amazon SQS with FIFO and send orders as they occur. Use Spot Instances in multiple Availability Zones for processing
答案: C

215. A company has an application that runs on a fleet of Amazon EC2 instances and stores 70 GB of device data for each instance in Amazon S3. Recently, some of the S3 uploads have been failing. At the same time, the company is seeing an unexpected increase in storage data costs. The application code cannot be modified.
What is the MOST efficient way to upload the device data to Amazon S3 while managing storage costs?
A. Upload device data using a multipart upload. Use the AWS CLI to list incomplete parts to address the failed S3 uploads. Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating.
B. Upload device data using S3 Transfer Acceleration. Use the AWS Management Console to address the failed S3 upload. Use the Multi-Object Delete operation nightly to delete the old uploads.
C. Upload device data using a multipart upload. Use the AWS Management Console to list incomplete parts to address the failed S3 uploads. Configure a lifecycle policy to archive continuously to Amazon S3 Glacier.
D. Upload device data using S3 Transfer Acceleration. Use the AWS Management Console to list incomplete parts to address the failed S3 uploads. Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating
答案: D

216. A company hosts a legacy application that runs on an Amazon EC2 instance inside a VPC without

internet access. Users access the application with a desktop program installed on their corporate laptops. Communication between the laptops and the VPC flows through AWS Direct Connect（DX）. A new requirement states that all data in transit must be encrypted between users and the VPC.
Which strategy should a solutions architect use to maintain consistent network performance while meeting this new requirement?
A. Create a client VPN endpoint and configure the laptops to use an AWS client VPN to connect to the VPC over the internet.
B. Create a new public virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX public virtual interface.
C. Create a new Site-to-Site VPN that connects to the VPC over the internet.
D. Create a new private virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX private virtual interface
答案：A

217. A company's main intranet page has experienced degraded response times as its user base has increased, although there are no reports of users seeing error pages. The application uses Amazon DynamoDB in read-only mode.
Amazon DynamoDB latency metrics for successful requests have been in a steady state even during times when users have reported degradation. The development team has correlated the issue to ProvisionedThroughputExceeded exceptions in the application logs when doing scan and read operations. The team also identified an access pattern of steady spikes of read activity on a distributed set of individual data items.
The chief technology officer wants to improve the user experience.
Which solutions will meet these requirements with the LEAST amount of changes to the application ?（Select TWO）
A. Change the data model of the DynamoDB tables to ensure that all scan and read operations meet DynamoDB best practices of uniform data access, reaching the full request throughput provisioned for the DynamoDB tables.
B. Enable DynamoDB auto scaling to manage the throughput capacity as table traffic increases. Set the upper and lower limits to control costs, and set a target utilization given the peak usage and how quickly the traffic changes.
C. Provision Amazon ElastiCache for Redis with cluster mode enabled. The cluster should be provisioned with enough shards to spread the application load and provision at least one read replica node for each shard
D. Implement the DynamoDB Accelerator（DAX）client and provision a DAX cluster with the appropriate node types to sustain the application load. Tune the item and query cache configuration for an optimal user experience
E. Remove error retries and exponential backoffs in the application code to handle throttling errors
答案：BD

218. A company currently has data hosted in an IBM Db2 database. A web application calls an API that runs stored procedures on the database to retrieve user information data that is read-only. This data is historical in nature and changes on a daily basis. When a user logs in to the application, this data needs to be retrieved within 3 seconds. Each time a user logs in, the stored procedures run. Users log in several times a day to check stock prices.
Running this database has become cost-prohibitive due to Db2 CPU licensing. Performance goals are not being met. Timeouts from Db2 are common due to long-running queries.
Which approach should a solutions architect take to migrate this solution to AWS?

A. Rehost the Db2 database in Amazon Fargate. Migrate all the data. Enable caching in Fargate. Refactor the API to use the Fargate Db2 database Implement Amazon API Gateway and enable API caching.
B. Use AWS DMS to migrate data to Amazon DynamoDB using a continuous replication task. Refactor the API to use the DynamoDB data. Implement the refactored API in Amazon API Gateway and enable API caching.
C. Create a local cache on the mainframe to store query outputs. Use SFTP to sync to Amazon S3 on a daily basis. Refactor the API to us e Amazon EFS. Implement Amazon API Gateway and enable API caching.
D. Extract data daily and copy the data to AWS Snowball for storage on Amazon S3. Sync daily Refactor the API to use the S3
答案：B

219. A financial services company logs personally identifiable information to its application logs stored in Amazon S3. Due to regulatory compliance requirements, the log files must be encrypted at rest. The security team has mandated that the company's on-premises hardware security modules （HSMs）be used to generate the CMK material.
Which steps should the solutions architect take to meet these requirements?
A. Create an AWS CloudHSM cluster. Create a new CMK in AWS KMS using AWS_CloudHSM as the source for the key material and an origin of AWS_ CLOUDHSM. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket that disallows uploads of unencrypted data and requires that the encryption source be AWS KMS
B. Provision an AWS Direct Connect connection, ensuring there is no overlap of the RFC 1918 address space between on-premises hardware and the VPCs. Configure an AWS bucket policy on the logging bucket that requires all objects to be encrypted. Configure the logging application to query the on-premises HSMs from the AWS environment for the encryption key material, and create a unique CMK for each logging event.
C. Create a CMK in AWS KMS with no key material and an origin of EXTERNAL. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AWS. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.
D. Create a new CMK in AWS KMS with AWS-provided key material and an origin of AWS_ KMS. Disable this CMK, and overwrite the key material with the key material from the on-premises HSM using the public key and import token provided by AWS. Re-enable the CMK. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS
答案：C

220. A company with multiple accounts is currently using a configuration that does not meet the following security governance policies:
•Prevent ingress from port 22 to any Amazon EC2 instance.
•Require billing and application tags for resources
•Encrypt all Amazon EBS volumes
A solutions architect wants to provide preventive and detective controls, including notifications about a specific resource, if there are policy deviations.
Which solution should the solutions architect implement?
A. Create an AWS CodeCommit repository containing policy-compliant AWS CloudFormation templates. Create an AWS Service Catalog portfolio. Import the CloudFormation templates by attaching the CodeCommit repository to the portfolio. Restrict users across all accounts to items from the AWS Service Catalog portfolio. Use AWS Config managed rules to detect deviations from the policies. Configure an Amazon CloudWatch Events rule for deviations, and associate a CloudWatch alarm to send notifications

when the TriggeredRules metric is greater than zero
B. Use AWS Service Catalog to build a portfolio with products that are in compliance with the governance policies in a central account. Restrict users across all accounts to AWS Service Catalog products. Share a compliant portfolio to other accounts. Use AWS Config managed rules to detect deviations from the policies. Configure an Amazon CloudWatch Events rule to send a notification when a deviation occurs.
C. Implement policy-compliant AWS CloudFormation templates for each account, and ensure that all provisioning is completed by CloudFormation. Configure Amazon Inspector to perform regular checks against resources. Perform policy validation and write the assessment output to Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter to increment a metric when a deviation occurs. Configure a CloudWatch alarm to send notifications when the configured metric is greater than zero.
D. Restrict users and enforce least privilege access using AWS lAM. Consolidate all AWS CloudTrail logs into a single account. Send the CloudTrail logs to Amazon Elasticsearch Service（Amazon ES）. Implement monitoring, alerting, and reporting using the Kibana dashboard in Amazon ES and with Amazon SNS
答案：D

221. A company's lease of a colocated storage facility will expire in 90 days. The company wants to move to AWS to avoid signing a contract extension. The company's environment consists of 200 virtual machines and a NAS with 40 TB of data. Most of the data is archival, yet instant access is required when data is requested. Leadership wants to ensure minimal downtime during the migration. Each virtual machine has a number of customized configurations. The company's existing 1 Gbps network connection is mostly idle, especially after business hours.
Which combination of steps should the company take to migrate to AWS while minimizing downtime and operational impact？（Select TWO）
A. Use new Amazon EC2 instances and reinstall all application code.
B. Use AWS SMS to migrate the virtual machines
C. Use AWS Storage Gateway to migrate the data to cloud-native storage.
D. Use AWS Snowball to migrate the data
E. Use AWS SMS to copy the infrequently accessed data from the NAS
答案：DE

222. A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:
- The database must use strong, randomly generated passwords stored in a secure AWS managed service
- The application resources must be deployed through AWS CloudFormation
- The application must rotate credentials for the database every 90 days.

A solutions architect will generate a CloudFormation template to deploy the application.
Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead？
A. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
B. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days
C. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every go days

D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days
答案：B

223. A company has a web-based application deployed in the ap-southeast-2 Region behind an Application Load Balancer（ALB）. AWS Certificate Manager（ACM）has issued a TLS certificate for example. com. This certificate is deployed to the ALB. There is a record set in Amazon Route 53 for example. com associated to the ALB.
Due to increased load on the application, the company wants to use Amazon CloudFront. This transition cannot cause application downtime.
Which combination of actions can achieve this？（Choose THREE.）
A. Create a new ACM certificate in the ap-southeast-2 Region for origin. example. com and example. com. Associate this certificate to the existing ALB. Add a DNS entry in Route 53 for origin. example. com associated with the existing ALB.
B. Create a CloudFront distribution and use the existing certificate associated with the ALB in the ap-southeast-2 Region. Set origin. example. com as the custom origin.
C. Create a new ACM certificate in the us-east-1 Region for example. com. Create a CloudFront distribution and use the ACM certificate in the us-east-1 Region. Set origin. example. com as the custom origin
D. Update Route 53 for example. com to the alias record of the CloudFront distribution.
E. Create a new ACM certificate in the us-east-1 Region for example. com. Create a new ALB in the us-east-1 Region as the origin of the CloudFront distribution. Attach the security group associated with the AlB to the CloudFront distribution
F. Update the ALB security group to allow access from the CloudFront Edge locations only.
答案：BCD

224. A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:
- High availability within an AWS Region.
- Able to fail over in 1 minute to another AWS Region for disaster recovery
- Provide the most efficient solution while minimizing the impact on the user experience

Which combination of steps will meet these requirements ？（Select THREE）
A. Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live（TTL）to 1 hour
B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live（TTL）to 30 seconds
C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
D. Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region. Have a script import the data into DynamoDB in a disaster recovery scenario
E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.
F. Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.
答案：BCE

225. A company experienced a breach of highly confidential personal information due to permissions issues on an Amazon S3 bucket. The information security team has tightened the bucket policy to restrict access. Additionally, to be better prepared for future attacks, these requirements must be met:

- Identify remote IP addresses that are accessing the bucket objects
- Receive alerts when the security policy on the bucket is changed
- Remediate the policy changes automatically

Which strategies should the solutions architect use?

A. Use Amazon CloudWatch Logs with CloudWatch filters to identify remote IP addresses. Use CloudWatch Events rules with AWS Lambda to automatically remediate S3 bucket policy changes. Use Amazon SES with CloudWatch Events rules for alerts

B. Use Amazon Athena with S3 access logs to identify remote IP addresses. Use AWS Config rules with AWS Systems Manager Automation to automatically remediate S3 bucket policy changes. Use Amazon SNS with AWS Config rules for alerts

C. Use S3 access logs with Amazon Elasticsearch Service and Kibana to identify remote IP addresses. Use an Amazon Inspector assessment template to automatically remediate S3 bucket policy changes. Use Amazon SNS for alerts.

D. Use Amazon Macie with an S3 bucket to identify access patterns and remote IP addresses. Use AWS Lambda with Macie to automatically remediate S3 bucket policy changes. Use Macie automatic alerting capabilities for alerts

答案：B

226. A company is planning on hosting its ecommerce platform on AWS using a multi-tier web application designed for a NoSQL database. The company plans to use the us-west-2 Region as its primary Region. The company want to ensure that copies of the application and data are available in a second Region, us-west-1, for disaster recovery. The company wants to keep the time to fail over as low as possible. Failing back to the primary Region should be possible without administrative interaction after the primary service is restored. Which design should the solutions architect use?

A. Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outage. Use Amazon DynamoDB global tables for the database tier

B. Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outage. Deploy an Amazon Aurora global database for the database tier

C. Use AWS Service Catalog to deploy the web and application servers in both Regions. Asynchronously replicate static content between the two Regions using Amazon S3 cross-Region replication. Use Amazon Route 53 health checks to identify a primary Region failure and update the public DNS entry listing to the secondary Region in the event of an outage. Use Amazon RDS for MySQL with cross-Region replication for the database tier.

D. Use AWS CloudFormation StackSets to create the stacks in both Regions using Auto Scaling groups for the web and application tiers. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use Amazon CloudFront with static files in Amazon S3， and multi-Region origins for the front-end web tier. Use Amazon DynamoDB tables in each Region with scheduled backups to Amazon S3.

答案：A

227. A software as a service（SaaS）company offers a cloud solution for document management to private law firms and the public sector.
A local government client recently mandated that highly confidential documents cannot be stored outside the country. The company ClO asks a solutions architect to ensure the application can adapt to this new requirement. The CIO also wants to have a proper backup plan for these documents, as backups are not currently performed.
What solution meets these requirements?
A. Tag documents that are not highly confidential as regular in Amazon S3. Create individual S3 buckets for each user. Upload objects to each user's bucket Set S3 bucket replication from these buckets to a central S3 bucket in a different AWS account and AWS Region. Configure an AWS Lambda function triggered by scheduled events in Amazon CloudWatch to delete objects that are tagged as secret in the S3 backup bucket.
B. Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Create a cross-region S3 bucket in a separate AWS account. Set proper IAM roles to allow cross-region permissions to the S3 buckets. Configure an AWS Lambda function triggered by Amazon CloudWatch scheduled events to copy objects that are tagged as secret to the S3 backup bucket and objects tagged as normal to the cross-region S3 bucket.
C. Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to an S3 bucket in a different AWS Region. Configure an AWS Lambda function that triggers when new S3 objects are created in the main bucket to replicate only documents tagged as secret into the S3 bucket in the same AWS Region.
D. Tag highly confidential documents as secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to a different AWS Region. Create an Amazon CloudWatch Events rule for new S3 objects tagged as secret to trigger an AWS Lambda function to replicate them into a separate bucket in the same AWS Region
答案：B

228. A web application is hosted in a dedicated VPC that is connected to a company's on-premises data center over a Site-to-Site VPN connection. The application is accessible from the company network only. This is a temporary non-production application that is used during business hours. The workload is generally low with occasional surges.
The application has an Amazon Aurora MySQL provisioned database cluster on the backend. the VPC has an internet gateway and a NAT gateways attached. The web servers are in private subnets in an Auto Scaling group behind an Elastic Load Balancer. The web servers also upload data to an Amazon S3 bucket through the internet.
A solutions architect needs to reduce operational costs and simplify the architecture.
Which strategy should the solutions architect use?
A. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Use 3-year scheduled Reserved Instances for the web server EC2 instances. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket.
B. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket,

then update the network routing and security rules and policies related to the changes.
C. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway from the VPC, and use an Aurora Serverless database. Set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes
D. Use 3-year scheduled Reserved Instances for the web server Amazon EC2 instances. Remove the NAT gateways from the VPC, and set up a VPC endpoint for the S3 bucket. Use Amazon CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours only. Update the network routing and security rules and policies related to the changes
答案：B

229. A company has several Amazon EC2 instances in both public and private subnets within a VPC that is not connected to the corporate network. A security group associated with the EC2 instances allows the company to use the windows remote desktop protocol（RDP）over the internet to access the instances. The security team has noticed connection attempts from unknown sources. The company wants to implement a more secure solution to access the EC2 instances.
Which strategy should a solutions architect implement?
A. Deploy a Linux bastion host on the corporate network that has access to all instances in the VPC
B. Deploy AWS Systems Manager Agent on the EC2 instances. Access the EC2 instances using Session Manager, restricting access to users with permission.
C. Deploy a Linux bastion host with an Elastic IP address in the public subnet. Allow access to the bastion host from 0.0.0.0/0.
D. Establish a Site-to-Site VPN connecting the corporate network to the VPC. Update the security groups to allow access from the corporate network only
答案：B

230. A company is deploying a public-facing global application on AWS using Amazon CloudFront. The application communicates with an external system. A solutions architect needs to ensure the data is secured during end-to-end transit and at rest.
Which combination of steps will satisfy these requirements ？ （Select THREE）
A. Create a public certificate for the required domain in AWS Certificate Manager and deploy it to CloudFront, an Application Load Balancer, and Amazon EC2 instances.
B. Acquire a public certificate from a third-party vendor and deploy it to CloudFront, an Application Load Balancer, and Amazon EC2 instances.
C. Provision Amazon EBS encrypted volumes using AWS KMS and ensure explicit encryption of data when writing to Amazon EBS.
D. Provision Amazon EBS encrypted volumes using AWS KMS.
E. Use SSL or encrypt data while communicating with the external system using a VPN.
F. Communicate with the external system using plaintext and use the VPN to encrypt the data in transit
答案：BCE

231. A company has multiple lines of business（LOBs）that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements:
•Produce a single AWS invoice for all of the AWS accounts used by its LOBs.
•The costs for each LOB account should be broken out on the invoice.
•Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy.
•Each LOB account should be delegated full administrator permissions, regardless of the governance

policy. Which combination of steps should the solutions architect take to meet these requirements? (Select Two)

A. Use AWS Organizations to create an organization in the parent account for each LOB. Then invite each LOB account to the appropriate organization

B. Use AWS Organizations to create a single organization in the parent account. Then, invite each LOB's AWS account to join the organization.

C. Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB, as appropriate.

D. Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts

E. Enable consolidated billing in the parent account's billing console and link the LOB accounts

答案：AD

232. A company has a mobile app with users in Europe. When the app is used, it downloads a configuration file that is device- and app version-specific. The company has the following architecture:

•Configuration files are stored in Amazon S3 in the eu-west-1 Region and served to the users using Amazon CloudFront

•Lambda @Edge is used to extract the device and version information from the app requests. It then updates the requests to load the correct configuration.

The company uses the configuration file load time as a key performance metric, and targets a response time of 100 ms or less. The app recently launched in the ap-southeast-2 Region, and the latency for requests from users in Australia is significantly above the 100 ms target. A solutions architect needs to recommend a solution. Which solution will reduce latency for users in Australia?

A. Create an S3 bucket in the ap-southeast-2 Region. Use cross-Region replication to synchronize from the bucket in the eu-west-1 Region. Modify Lambda @Edge to access Amazon S3 in the Region that is closest to the user.

B. Configure S3 Transfer Acceleration on the bucket. Modify Lambda@ Edge to access Amazon S3 using the Transfer Acceleration endpoint in the Region that is closest to the user.

C. Configure S3 Transfer Acceleration on the bucket. Add the Transfer Acceleration Edge endpoints for Australia and Europe as CloudFront origins. Modify Lambda@Edge to update the origin of the request to be the Transfer Acceleration endpoint in the Region that is closest to the user.

D. Create an S3 bucket in the ap-southeast-2 Region. Use cross-Region replication to synchronize from the bucket in the eu-west-1 Region. Create an Amazon Route 53 hosted zone with latency-based routing configured for both buckets. Modify Lambda@Edge to update the origin of the request to be the Route 53 hosted zone that is closest to the user.

答案：C

233. A fitness tracking company serves users around the world, with its primary markets in North America and Asia. The company needs to design an infrastructure for its read-heavy user authorization application with the following requirements:

•Be resilient to problems with the application in any Region.
•Write to a database in a single Region
•Read from multiple Regions
•Support resiliency across application tiers in each Region
•Support the relational database semantics reflected in the application

Which combination of steps should a solutions architect take? (Select TWO)

A. Use an Amazon Route 53 geoproximity routing policy combined with a multivalue answer routing policy.

B. Deploy web, application, and MySQL database servers to Amazon EC2 instances in each Region. Set up the application so that reads and writes are local to the Region. Create snapshots of the web, application,

and database servers and store the snapshots in an Amazon S3 bucket in both Regions. Set up cross-Region replication for the database layer.

C. Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy.

D. Set up web, application, and Amazon RDS for MySQL instances in each Region. Set up the application so that reads are local and writes are partitioned based on the user. Set up a Multi-AZ failover for the web, application, and database servers. Set up cross-Region replication for the database layer.

E. Set up active-active web and application servers in each Region. Deploy an Amazon Aurora global database with clusters in each Region. Set up the application to use the in-Region Aurora database endpoints. Create snapshots of the web and application servers and store them in an Amazon S3 bucket in both Regions

答案：CE

234. A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their image uploads.

How can a solutions architect improve the performance of the image upload process?

A. Redeploy the application to use S3 multipart uploads

B. Create an Amazon CloudFront distribution and point to the application as a custom origin

C. Configure the buckets to use S3 Transfer Acceleration

D. Create an Auto Scaling group for the EC2 instances and create a scaling policy

答案：C

235. A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database

Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.

Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? （Select THREE.）

A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs

B. Implement the AWS x-ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the x-Ray SDK for Java

C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis

D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs

E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora

F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-RAY

答案：ADE

236. A financial services company has an on-premises environment that ingests market data feeds from stock exchanges, transforms the data, and sends the data to an internal Apache Kafka cluster. Management wants to leverage AWS services to build a scalable and near-real-time solution with consistent network

performance to provide stock market data to a web application.
Which steps should a solutions architect take to build the solution？ （Select THREE.）
A. Establish an AWS Direct Connect connection from the on-premises data center to AWS
B. Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Consumer Library to put the data into an Amazon Kinesis data stream
C. Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Kinesis Produce Library to put the data into a Kinesis data stream.
D. Create a WebSocket API in Amazon API Gateway, create an AWS lambda function to process an Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.
E. Create a GraphQL API in AWS AppSync, create an AWS Lambda function to process the Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.
F. Establish a Site-to-Site VPN from the on-premises data center to AWS
解析：ACD

237. A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones（AZ）with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size of the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:
VPC C|DR：10.0.0.0/23
AZ1 subnet CIDR：10.0.0.0/24
AZ2 subnet CIDR：100.10/24
Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime
Which solution will meet these requirements?
A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space. Adjust the Auto Scaling group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.
B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.
D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the precious address space. Adjust the Auto Scaling group to also use the AZ1 subnet again, When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address. Space from the original AZ1 subnet Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all new subnets.
答案：D

238. A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The

company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location Which solutions will meet these requirements?

A. Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package

B. Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group. Publish the game download URL for users to download the package

C. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Use Amazon CloudFront for the website. Publish the game download URL for users to download the package.

D. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Set Requester Pays for the S3 bucket. Publish the game download URL for users to download the package.

解析：C

239. A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region

Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer（ALB）spanning multiple Availability Zones（AZs）to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB

B. Deploy an Application Load Balancer（ALB）spanning multiple Availability Zones（AZs）to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions

C. Create a VPC in the us-west- 1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer（ALB）that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB

D. Deploy an Application Load Balancer（ALB）spanning multiple Availability Zones（AZs）to the VPC in the us-east-1 Region Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions

答案：B

240. An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine’s dynamic website currently uses an Application Load Balancer in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only.

The magazine is expecting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch

Which combination of steps should a solutions architect take to reduce system response times for a global audience? （Select Two）

A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region. Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode
B. Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection. Deploy the web and application tiers in Regions across the world.
C. Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers-web application, and database-are in private subnets
D. Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication for static content and resources. Deploy the web and application tiers in Regions across the world
E. Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups
答案：DE

241. A media company has a static web application that is generated programmatically. The company has a build pipeline that generates HTML content that is uploaded to an Amazon S3 bucket served by Amazon CloudFront. The build pipeline runs inside a Build Account. The S3 bucket and CloudFront distribution are in a Distribution Account. The build pipeline uploads the files to Amazon S3 using an IAM role in the Build Account. The S3 bucket has a bucket policy that only allows CloudFront to read objects using an origin access identity（OAI）. During testing, all attempts to access the application using the CloudFront URL result in an HTTP 403 Access Denied response
What should a solutions architect suggest to the company to allow access the objects in Amazon S3 through CloudFront?
A. Modify the S3 upload process in the Build Account to add the bucket-owner-full-control ACL to the objects at upload.
B. Create a new cross-account IAM role in the Distribution Account with write access to the S3 bucket. Modify the build pipeline to assume this role to upload the files to the Distribution Account
C. Modify the S3 upload process in the Build Account to set the object owner to the Distribution Account
D. Create a new IAM role in the Distribution Account with read access to the S3 bucket. Configure CloudFront to use this new role as its OAI. Modify the build pipeline to assume this role when uploading files from the Build Account
解析：D

242. A company runs a popular public-facing ecommerce website. Its user base is growing quickly from a local market to a national market. The website is hosted in an on-premises data center with web servers and a MySQL database. The company wants to migrate its workload to AWS. A solutions architect needs to create a solution to:
-Improve security
-Improve reliability
-Improve availability
-Reduce latency
-Reduce maintenance
Which combination of steps should the solutions architect take to meet these requirements? （Select THREE.）
A. Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer
B. Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster
C. Use Amazon EC2 instances in two Availability Zones to host a highly available MySQL database cluster
D. Host static website content in Amazon S3. Use S3 Transfer Acceleration to reduce latency while serving

webpages. Use AWS WAF to Improve website security
E. Host static website content in Amazon S3. Use Amazon CloudFront to reduce latency while serving webpages. Use AWS WAF to Improve website security
F. Migrate the database to a single-AZ Amazon RDS for MySQL DB Instance
答案：ABE

243. A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events. The database is unable to scale due to heavy ingestion and it frequently runs out of storage. The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:
-Managed AWS services to minimize operational complexity
-A buffer that automatically scales to match the throughput of data and requires no ongoing administration
-A visualization tool to create dashboards to observe events in near-real time
-Support for semi-structured JSON data and dynamic schemas
Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements？（Select TWO）
A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events
B. Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events
C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards
D. Configure Amazon Elasticsearch Service（Amazon ES）to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards
E. Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards
答案：BD

244. An ecommerce website running on AWS uses an Amazon RDS for MySQL DB instance with General Purpose SSD storage. The developers chose an appropriate instance type based on demand, and configured 100 GB of storage with a sufficient amount of free space.
The website was running smoothly for a few weeks until a marketing campaign launched. On the second day of the campaign, users reported long wait times and time outs. Amazon CloudWatch metrics indicated that both reads and writes to the DB instance were experiencing long response times. The CloudWatch metrics show 40% to 50% CPU and memory utilization, and sufficient free storage space is still available. The application server logs show no evidence of database connectivity issues
What could be the root cause of the issue with the marketing campaign？
A. It exhausted the I/O credit balance due to provisioning low disk storage during the setup phase
B. It caused the data in the tables to change frequently, requiring indexes to be rebuilt to optimize queries C. It exhausted the maximum number of allowed connections to the database instance
D. It exhausted the network bandwidth available to the RDS for MySQL DB instance
答案：A

245. A solutions architect is designing a network for a new cloud deployment. Each account will need autonomy to modify route tables and make changes. Centralized and controlled egress internet connectivity is also needed. The cloud footprint is expected to grow to thousands of AWS accounts
Which architecture will meet these requirements？
A. A centralized transit VPC with a VPN connection to a standalone VPC in each account. Outbound internet

traffic will be controlled by firewall appliances
B. A centralized shared VPC with a subnet for each account. outbound internet traffic will controlled through a fleet of proxy servers
C. A shared services VPC to host central assets to include a fleet of firewalls with a route to the internet. Each spoke VPC will peer to the central VPC
D. A shared transit gateway to which each VPC will be attached. Outbound internet access will route through a fleet of VPN-attached firewalls
答案：D

246. A company has a media metadata extraction pipeline running on AWS Notifications containing a reference to a file in Amazon S3 are sent to an Amazon Simple Notification Service（Amazon SNS）topic. The pipeline consists of a number of AWS Lambda functions that are subscribed to the SNS topic. The Lambda functions extract the S3 file and write metadata to an Amazon RDS Postgre SQL DB instance
Users report that updates to the metadata are sometimes slow to appear or are lost. During these times, the CPU utilization on the database is high and the number of failed Lambda invocations increases
Which combination of actions should a solutions architect take to help resolve this issue？（Select TWO）
A. Enable message delivery status on the SNs topic. Configure the sns topic delivery policy to enable retries with exponential backoff
B. Create an Amazon Simple Queue Service（Amazon SQS）FIFo queue and subscribe the queue to the SNS topic. Configure the Lambda functions to consume messages from the SQS queue
C. Create an RDS proxy for the RDS instance. Update the Lambda functions to connect to the RDS instance using the proxy
D. Enable the RDS Data API for the RDS instance, Update the Lambda functions to connect to the RDS instance using the Data API
E. Create an Amazon Simple Queue Service（Amazon SQS）standard queue for each Lambda function and subscribe the queues to the SNS topic. Configure the Lambda functions to consume messages from their respective SQS queue
答案：CE

247.A financial services company receives a regular data feed from its credit card servicing partner Approximately 5,000 records are sent every 15 minutes in plaintext delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption. This feed contains sensitive credit card primary account number（PAN）data. The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing. The company also needs to remove and merge specific fields, and then transform the record into JSON format Additionally, extra feeds are likely to be added in the future, so any design needs to be easily expandable
Which solutions will meet these requirements？
A. Trigger an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Trigger another Lambda function when new messages arrive in the SQS queue to process the records, writing the results to a temporary location in Amazon S3. Trigger a final Lambda function once the SQS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing
B. Trigger an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Configure an AWS Fargate container application to automatically scale to a single instance when the SQS queue contains messages. Have the application process each record, and transform the record into JSON format. When the queue is empty, send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance
C. Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table

definition to match. Trigger an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, have the ETL job send the results to another S3 bucket for internal processing

D. Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match. Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL Job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON Once complete, send the results to another S3 bucket for internal processing and scale down the EMR cluster

答案：A

248. A solutions architect needs to migrate 50 TB of NFS data to Amazon S3. The files are on several NFS file servers on a corporate network. These are dense file systems containing tens of millions of small files. The system operators have configured file interface on an AWS Snowball Edge device and are using a shell script to copy data

Developers report that copying the data to the snowball Edge device is very slow. The solutions architect suspects this may be related to the overhead of encrypting all the small files and transporting them over the network

Which changes can be made to speed up the data transfer?

A. Cluster two Snowball Edge devices together to increase the throughput of the devices.

B. Change the solution to use the S3 Adapter instead of the file interface on the Snowball Edge device.

C. Increase the number of parallel copy jobs to increase the throughput of the Snowball Edge device

D. Connect directly to the USB interface on the Snowball Edge device and copy the files locally

答案：A

249. A company has a web application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB A recent marketing campaign has increased demand. Monitoring software reports that many requests have significantly longer response times than before the marketing campaign

A solutions architect enabled Amazon CloudWatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests. In CloudWatch the Lambda function Throttles metric represents 1% of the requests and the Errors metric represents 10% of the requests. Application logs indicate that, when errors occur, there is a call to DynamoDB

What change should the solutions architect make to improve the current response times as the web application becomes more popular?

A. Increase the concurrency limit of the Lambda function

B. Implement DynamoDB auto scaling on the table

C. Increase the API Gateway throttle limit

D. Re-create the DynamoDB table with a better-partitioned primary index

答案：B

250. A company has a VPC with two domain controllers running Active Directory in the default configuration. The VPC DHCP options set is configured to use the IP addresses of the two domain controllers. There is a VPC interface endpoint defined, but instances within the VPC are not able to resolve the private endpoint addresses

Which strategies would resolve this issue? （Select TWO）

A. Define an outbound Amazon route 53 Resolver. set a conditional forward rule for the Active Directory domain to the Active Directory servers. Update the VPC DHCP options set to AmazonProvidedDNS

B. Update the DNS service on the Active Directory servers to forward all non-authoritative queries to the

VPC Resolver
C. Define an inbound amazon route 53 resolver. set a conditional forward rule for the Active Directory domain to the Active Directory servers. Update the VPC DHCP options set to Amazon ProvidedDNS
D. Update the DNS service on the client instances to split DNS queries between the Active Directory servers and the VPC Resolver.
E. Update the DNS service on the Active Directory servers to forward all queries to the VPC resolver
答案：AB

251. A company uses AWS Organizations to manage one parent account and nine member accounts. The number of member accounts is expected to grow as the business grows. A security engineer has requested consolidation of AWS CloudTrail logs into the parent account for compliance purposes. Existing logs currently stored in Amazon S3 buckets in each individual member account should not be lost. Future member accounts should comply with the logging strategy
Which operationally efficient solution meets these requirements?
A. Create an AWS Lambda function in each member account with a cross-account role. Trigger the Lambda functions when new CloudTrail logs are created and copy the CloudTrail logs to a centralized S3 bucket. Set up an Amazon CloudWatch alarm to alert if CloudTrail is not configured properly
B. Configure CloudTrail in each member account to deliver log events to a central S3 bucket. Ensure the central S3 bucket policy allows PutObject access from the member accounts. Migrate existing logs to the central S3 bucket. Set up an Amazon CloudWatch alarm to alert if CloudTrail is not configured properly
C. Configure an organization-level CloudTrail in the parent account to deliver log events to a central S3 bucket. Migrate the existing CloudTrail logs from each member account to the central S3 bucket. Delete the existing CloudTrail and logs in the member accounts
D. Configure an organization-level CloudTrail in the parent account to deliver log events to a central S3 bucket. Configure CloudTrail in each member account to deliver log events to the central S3 bucket
答案：C

252. A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management There are various accounts associated with AWS Organizations including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances
Which strategy should the solutions architect provide to meet these requirements?
A. Use Tag Editor to tag existing resources Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources
B. Use an AWS Config rule to alert the finance team of untagged resources Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role
C. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID Use SCPs to restrict resource creation that de not have the cost center and project ID on the resource
D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost Center and project ID on the resource
答案：B

253. A company wants to run a serverless application on AWS. The company plans to provision its

application in Docker containers running in an Amazon ECS cluster. The application requires a MySQL database and the company plans to use Amazon RDS. The company has documents that need to be accessed frequently for the first 3 months, and rarely after that. The documents must be retained for 7 years

What is ine MOST cost-effective solution to meet these requirements?

A. Create an ECS cluster using On-Demand Instances Provision the database and its read replicas in Amazon RDS using Spot Instances. Store the documents in an encrypted EBS volume, and create a cron job to delete the documents after 7 years

B. Create an ECS cluster using a fleet of Spot Instances, with Spot Instance draining enabled. Provision the database and its read replicas in Amazon RDS using Reserved Instances. Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier. then delete the documents from Amazon S3 Glacier that are more than 7 years old

C. Create an ECS cluster using On-Demand Instances Provision the database and its read replicas in Amazon RDS using On-Demand Instances. Store the documents in Amazon EFS. Create a cron job to move the documents that are older than 3 months to Amazon S3 Glacier. Create an AWS Lambda function to delete the documents in S3 Glacier that are older than 7 years

D. Create an ECS cluster using a fleet of Spot Instances with Spot Instance Rendering draining enabled Provision the database and its read replicas in Amazon RDS On-Demand Instances: Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier, then delete the documents in Amazon S3 Glacier after 7 years.

答案：B

254. A multimedia company with a single AWS account is launching an application for a global user base. The application storage and bandwidth requirements are unpredictable. The application will use Amazon EC2 instances behind an Application Load Balancer as the web tier and will use Amazon DynamoDB as the database tier. The environment for the application must meet the following requirements:

-Low latency when accessed from any part of the world

-Web Socket support

-End-to-end encryption

-Protection the latest security threats

-Managed layer 7 DDoS protection

Which actions should the solutions architect take to meet these requirements？（Select Two.）

A. Use Amazon Route 53 and Amazon CloudFront for content distribution. Use Amazon S3 to store static content

B. Use Amazon Route 53 and AWs Transit Gateway for content distribution. Use an Amazon Elastic Block Store（Amazon EBS）volume to store static content

C. Use AWS WAF with AWS Shield Advanced to protect the application

D. Use AWS WAF and Amazon Detective to protect the application

E. Use Aws Shield Standard to protect the application

答案：AC

255. A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes. The solutions architecture team is forecasting that the database will store approximately 10 TB of data. As part of the design, they are looking for a database solution that will provide the company with the ability to fail over to a secondary Region

Which solution will meet these business requirements at the LOWEST cost?

A. Deploy an Amazon Aurora DB cluster and take snapshots of the cluster every 5 minutes. Once a snapshot is complete, copy the snapshot to a secondary Region to serve as a backup in the event of a failure

B. Deploy an Amazon RDS instance with a cross-Region read replica in a secondary Region. In the event of a failure, promote the read replica to become the primary
C. Deploy an Amazon Aurora DB cluster in the primary Region and another in a secondary Region. Use AWS DMS to keep the secondary Region in sync
D. Deploy an Amazon RDS instance with a read replica in the same Region. In the event of a failure, promote the read replica to become the primary
答案：B

256. A company is manually deploying its application to production and wants to move to a more mature deployment pattern. The company has asked a solutions architect to design a solution that leverages its current Chef tools and knowledge. The application must be deployed to a staging environment for testing and verification before being deployed to production, Any new deployment must be rolled back in 5 minutes if errors are discovered after a deployment
Which AWS service and deployment pattern should the solutions architect use to meet these requirements?
A. Use AWS Elastic Beanstalk and deploy the application using a rolling update deployment strategy
B. Use AWS Code Pipeline and deploy the application using a rolling update deployment strategy
C. Use AWS Code Build and deploy the application using a canary deployment strategy
D. Use AWS OpsWorks and deploy the application using a blue/green deployment strategy
答案：D

257. An enterprise company's data science team wants to provide a safe cost-effective way to provide easy access to Amazon SageMaker. The data scientists have limited AWS knowledge and need to be able to launch a Jupyter notebook instance. The notebook instance needs to have a preconfigured AWS KMS key to encrypt data at rest on the machine learning storage volume without exposing the complex setup requirements
Which approach will allow the company to set up a self- service mechanism for the data scientists to launch Jupyter notebooks in its AWS accounts with the LEAST amount of operational overhead?
A. Create a serverless front end using a static Amazon S3 website to allow the data scientists to request a Jupyter notebook instance by filling out a form, Use Amazon API Gateway to receive requests from the S3 website and trigger a central AWS Lambda function to make an API call to Amazon SageMaker that will launch a notebook instance with a preconfigured KMS key for the data scientists. Then call back to the front-end website to display the URL to the notebook instance
B. Create an AWS CloudFormation template to launch a Jupyter notebook instance using the AWS. Sage Maker:: NotebookInstance resource type with a preconfigured KMS key Add a user-friendly name to the CloudFormation template. Display the URL to the notebook using the Outputs section. Distribute the CloudFormation template to the data scientists using a shared Amazon S3 bucket
C. Create an AWS CloudFormation template to launch a Jupyter notebook instance using the AWS. SageMaker NotebookInstance resource type with a preconfigured KMS key Simplify the parameter names, such as the instance size, by mapping them to Small, Large, and X-Large using the Mappings section in CloudFormation. Display the URL to the notebook using the Outputs section, then upload the template into an AWS Service Catalog product in the data scientist's portfolio and share it with the data scientist's lAM role
D. Create an AWS CLI script that the data scientists can run locally. Provide step-by-step instructions about the parameters to be provided while executing the AWS CLI script to launch a Jupyter notebook with a preconfigured KMS key Distribute the CLI script to the data scientists using a shared Amazon S3 bucket
答案：C

258. A large financial company is deploying applications that consist of Amazon EC2 and Amazon RDS instances to the AWS Cloud using AWS CloudFormation The CloudFormation stack has the following stack policy:

```
{
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" : ["Update:*"],
            "Principal": "*",
            "Resource" : "*"
        }
    ]
}
```

The company wants to ensure that developers do not lose data by accidentally removing or replacing RDS instances when updating the CloudFormation stack. Developers also still need to be able to modify or remove EC2 instances as needed.
How should the company change the stack policy to meet these requirements?
A. Modify the statement to specify "Effect": "Deny", "Action": 【Update:*"】for all logical RDS resources
B. Modify the statement to specify"Effect": "Deny", "Action":【Update Delete"】for all logical RDS resources
C. Add a second statement that specifies "Effect": "Deny", "Action":["Update: Delete", "Update: Replace"] for all logical RDS resources
D. Add a second statement that specifies "Effect": "Deny", "Action": 【"Update:*"】 for all logical RDS resources
答案: C

259. A solutions architect is designing a publicly accessible web application that is on an Amazon Cloud Front distribution with an Amazon S3 website endpoint as the origin. When the solution is deployed, the website returns an Error 403: Access Denied message
Which steps should the solutions architect take to correct the issue? (Select TWO)
A. Remove the S3 block public access option from the S3 bucket
B. Remove the requester pays option from the S3 bucket
C. Remove the origin access identity (OAI) from the CloudFront distribution
D. Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA)
E. Disable S3 object versioning
答案: AB

260. A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold
Which solution is the MOST cost-effective way to meet these requirements?
A. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in each account to create monthly reports for each business unit
B. Configure AWS Budgets in the organizations master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's master account to create monthly reports for each business

unit
C. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit
D. Enable AWS Cost and Usage Reports in the organization's master account and configure reports grouped by application, environment, and owner. Create an AWS Lambda function that processe LS AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business units email list
答案：B

261. A company's service for video game recommendations has just gone viral. The company has new users from all over the world. The website for the service is hosted on a set of Amazon EC2 instances in an Auto Scaling group behind an Application Balancer（ALB）. The website consists of static content with different resources being loaded depending on the device type.
Users recently reported that the load time for the website has increased. Administrators are reporting high loads on the EC2 instances that host the service
Which set actions should a solutions architect take to improve response times?
A. Create separate Auto Scaling groups based on device types. Switch to a Network Load Balancer（NLB）. Use the User-agent Http header in the NLB to route to a different set of EC2 instances
B. Move content to Amazon S3 Create an Amazon Cloud Front distribution to serve content out of the S3 bucket Use Lambda @ Edge to load different resources based on the User-agent Http header
C. Create a separate ALB for each device type Create one Auto Scaling group behind each ALB. Use Amazon Route 53 to route to different ALBs depending on the User-agent Http header
D. Move content to Amazon S3 Create an Amazon CloudFront distribution to serve content out of the S3 bucket Use the User-agent Http header to load different content
答案：B

262. A company plans to migrate to AWS. A solutions architect uses AWS Application Discovery Service over the fleet and discovers that there is an Oracle data warehouse and several PostgreSQL databases.
Which combination of migration patterns will reduce licensing costs and operational overhead? （Select TWO）
A. Lift and shift the Oracle data warehouse to Amazon EC2 using AWS DMS
B. Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS DMS
C. Lift and shift the PostgreSQL databases to Amazon EC2 using AWS DMS
D. Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS
E. Migrate the Oracle data warehouse to an Amazon EMR managed cluster using AWS DMS
答案：DE

263. A solutions architect is implementing infrastructure as code for a two-tier web application in an AWS CloudFormation template. The web frontend application will be deployed on Amazon EC2 instances in an Auto Scaling group. The backend database will be an Amazon RDS for MySQL DB instance. The databaII password will be rotated every 60 days
How can the solutions architect MOST securely manage the configuration of the applications database credentials?
A. Provide the database password as a parameter in the CloudFormation template. Create an initialization script in the Auto Scaling group's launch configuration UserData property to reference the password parameter using the Ref intrinsic function. Store the password on the EC2 instances. Reference the parameter for the value of the Master UserPassword property in the AWS:: RDS::DBInstance resource using the Ref intrinsic function

B. Create a new AWS Secrets Manager secret resource in the CloudFormation template to be used as the database password. Configure the application to retrieve the password from Secrets Manager when needed. Reference the secret resource for the value of the MasterUserPassword property in the AWS:: RDS::DBInstance resource using a dynamic reference

C. Create a new AWS Secrets Manager secret resource in the CloudFormation template to be used as the database password. Create an initialization script in the Auto Scaling group's launch configuration UserData property to reference the secret resource using the Ref intrinsic function Reference the secret resource for the value of the MasterUserPassword property in the AWS:: RDS:: DBInstance resource using the Ref intrinsic function

D. Create a new AWS Systems Manager Parameter Store parameter in the CloudFormation template to be used as the database password. Create an initialization script in the Auto Scaling group's launch configuration UserData property to reference the parameter Reference the parameter for the value of the MasterUserPassword property in the AWS::RDS:: DBInstance resource using the Fn::GetAtt intrinsic function

答案： B

264. A company is using AWS Organizations to manage multiple AWS accounts For security purposes, the company requires the creation of an Amazon Simple Notification Service（Amazon SNS） topic that enables integration with a third-party alerting system in all the Organizations member accounts

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation Stack Sets in all AWS accounts?

A. Create a stack set in the Organizations member accounts. Use service-managed permissions Set deployment options to deploy to an organization Use CloudFormation stack Sets drift detection

B. Create stacks in the Organizations member accounts Use self-service permissions Set deployment options to deploy to an organization. Enable the CloudFormation Stack Sets automatic deployment

C. Create a stack set in the Organizations master account. Use service-managed permissions Set deployment options to deploy to the organization. Enable CloudFormation Stack Sets automatic deployment

D. Create stacks in the Organizations master account. Use service-managed permissions Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection

答案： C

265. An enterprise company is building an infrastructure services platform for its users. The company has the following requirements ：

-Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services

-Use a central account to manage the creation of infrastructure services

-Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations

-Provide the ability to enforce tags on any infrastructure that is started by users

Which combination of actions using AWS services will meet these requirements? （Select THREE）

A. Develop infrastructure services using AWS CloudFormation templates. Add the templates to a central Amazon S3 bucket and add the IAM roles or users that require access to the S3 bucket policy.

B. Develop infrastructure services using AWS CloudFormation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.

C. Allow user IAM roles to have AWSCloudFormationFullAccessand AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS

CloudFormation and Amazon S3.
D. Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption, assign users access, and apply launch constraints
E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company Apply the TagOption to AWS Service Catalog products or portfolios
F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any Cloud Formation templates that will be created for user
答案：BCE

266. A company is using multiple AWS accounts. The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A The company ' s applications and databases are running in Account B
A solutions architect will deploy a two-tier application in a new VPC. To simplify the configuration, the db. example. com CNAME record set for the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.
During deployment, the application failed to start. Troubleshooting revealed that db. example. com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53
Which combination of steps should the solutions architect take to resolve this issue？ （Select Two）
A. Deploy the database on a separate EC2 instance in the new VPC. Create a record set for the instance's private IP in the private hosted zone
B. Use SSH to connect to the application tier EC2 instance. Add an RDS endpoint IP address to the /etc/resolv. conf file.
C. Create an authorization to associate the private hosted zone in Account a with the new VPC in Account B
D. Create a private hosted zone for the example. com domain in Account B. Configure Route 53 replication between AWS accounts
E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A
答案：CE

267. A company is designing a data processing platform to process a large number of files in an Amazon S3 bucket and store the results in Amazon DynamoDB. These files will be processed once and must be retained for 1 year. The company wants to ensure that the original files and resulting data are highly available in multiple AWS Regions.
Which solution will meet these requirements？
A. Create an S3 CreateObject event notification to copy the file to Amazon Elastic Block Store（Amazon EBS）. Use AWS DataSync to sync the files between EBS volumes in multiple Regions. Use an Amazon EC2 Auto Scaling group in multiple Regions to attach the EBS volumes. Process the files and store the results in a DynamoDB global table in multiple Regions. Configure the S3 bucket with an S3 Lifecycle policy to move the files to S3 Glacier after 1 year
B. Create an S3 CreateObject event notification to copy the file to Amazon Elastic File System（Amazon EFS）. Use AWS DataSync to sync the files between EFS volumes in multiple Regions. Use an AWS Lambda function to process the EFS files and store the results in a DynamoDB global table in multiple Regions. Configure the S3 buckets with an S3 Lifecycle policy to move the files to S3 Glacier after 1 year
C. Copy the files to an S3 bucket in another Region by using cross-Region replication. Create an S3 Create Object event notification on the original bucket to push S3 file paths into Amazon EventBridge （Amazon CloudWatch Events ）. Use an AWS Lambda function to poll EventBridge（CloudWatch Events） to process each file and store the results in a DynamoDB table in each Region. Configure both S3 buckets to use the S3

Standard-Infrequent Access（S3 Standard-IA） storage class and an S3 Lifecycle policy to delete the files after 1 year.

D. Copy the files to an S3 bucket in another Region by using cross-Region replication. Create an S3 Create Object event notification on the original bucket to execute an AWS Lambda function to process each file and store the results in a DynamoDB global table in multiple Regions. Configure both S3 buckets to use the S3 Standard-Infrequent Access（S3 Standard-IA） storage class and an S3 Lifecycle policy to delete the files after 1 year.

答案：D

268. A new startup is running a serverless application using AWS Lambda as the primary source of compute. New versions of the application must be made available to a subset of users before deploying changes to all users. Developers should also have the ability to abort the deployment and have access to an easy rollback mechanism. A solutions architect decides to use AWS CodeDeploy to deploy changes when a new version is available

Which Code Deploy configuration should the solutions architect use?

A. A blue/green deployment

B. A linear deployment

C. A canary deployment

D. An all-at-once deployment

答案：A

269. A company has a photo sharing social networking application. To provide a consistent experience for users, the company performs some image processing on the photos uploaded by users before publishing on the application. The image processing is implemented using a set of Python libraries.

The current architecture is as follows：

-The image processing Python code runs in a single Amazon EC2 instance and stores the processed images in an Amazon S3 bucket named ImageBucket

-The front-end application, hosted in another bucket, loads the images from ImageBucket to display to users.

With plans for global expansion, the company wants to implement changes in its existing architecture to be able to scale for increased demand on the application and reduce management complexity as the application scales

Which combination of changes should a solutions architect make? （Select TWO）

A. Place the image processing EC2 instance into an Auto Scaling group

B. Use AWS Lambda to run the image processing tasks

C. Use Amazon Rekognition for image processing

D. Use Amazon CloudFront in front of Image Bucket

E. Deploy the applications in an Amazon ECS cluster and apply Service Auto Scaling

答案：BD

270. A company has several development teams collaborating on multiple projects. Developers frequently move between projects, and each project requires access to a different set of AWS resources.

There are current projects for web, mobile, and database development. However, the set of projects may change over time. Developers should have full control over the resources for the project to which they are assigned, and read-only access to resources for all other projects

When developers are assigned to a different project or new AWS resources are added, the company wants to minimize policy maintenance

What type of control policy should a solutions architect recommend?

A. Create a policy document for each project with specific project tags and allow full control of the resources with a matching tag. Allow read-only access for all other resources. Attach the project-specific policy document to the IAM role for that project. Change the role assigned to the developer's IAM user when they change projects. Assign a specific project tag to new resources when they are created
B. Create an IAM role for each project that requires access to AWS resources. Attach an inline policy document to the role that specifies the IAM users that are allowed to assume the role, with full control of the resources that belong to a project and read-only access for all other resources within the account Update the policy document when the set of resources changes or developers change projects
C. Create a customer managed policy document for each project that requires access to AWS resources Specify full control of the resources that belong to a project and read-only access for all other resources within the account. Attach the project-specific policy document to the developer's IAM user when they change projects. Update the policy document when the set of resources changes
D. Create a customer managed policy document for each project that requires access to AWS resources Specify full control of the resources that belong to a project and read-only access for all other resources within the account, Attach the project-specific policy document to an IAM group. Change the group membership when developers change projects Update the policy document when the set of resources changes.
答案：D

271. A company has multiple AWS accounts as part of an organization created with AWS Organizations. Each account has a VPC in the us-east-2 Region and is used for either production or development workloads. Amazon EC2 instances across production accounts need to communicate with each other, and EC2 instances across development accounts need to communicate with each other, but production and development instances should not be able to communicate with each other.
To facilitate connectivity, the company created a common network account. The company used AWS Transit Gateway to create a transit gateway in the us-east-2 Region in the network account and shared the transit gateway with the entire organization by using AWS Resource Access Manager Network administrators then attached VPCs in each account to the transit gateway, after which the EC2 instances were able to communicate across accounts. However, production and development accounts were also able to communicate with one another
Which set of steps should a solutions architect take to ensure production traffic and development traffic are completely isolated?
A. Modify the security groups assigned to development EC2 instances to block traffic from production EC2 instances. Modify the security groups assigned to production EC2 instances to block traffic from development EC2 instances
B. Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached Using the Network Manager feature of AWS Transit Gateway, create policies that restrict traffic between VPCs based on the value of this tag.
C. Create separate route tables for production and development traffic. Delete each account's association and route propagation to the default AWS Transit Gateway route table. Attach development VPCs the development AWS Transit Gateway route table and production VPCs to the production route table, and enable automatic route propagation on each attachment
D. Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached Modify the AWS Transit Gateway routing table to route production tagged attachments to one another and development tagged attachments to one another.
答案：C

272. A solutions architect is migrating an existing workload to AWS Fargate. The task can only run in a

private subnet within the VPC where there is no direct connectivity from outside the system to the application. When the Fargate task is launched, the task fails with the following error:

```
CannotPullContainerError: API error (500): Get https://111122223333.dkr.ecr.us-east-
1.amazonaws.com/v2/: net/http: request canceled while waiting for connection
```

How should the solutions architect correct this error?

A. Ensure the task is set to ENABLED for the auto-assign public IP setting when launching the task

B. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the public subnet in the VPC to route requests to the internet

C. Ensure the task is set to DISABLED for the auto-assign public setting when launching the task Configure a NAT gateway in the private subnet in the VPC to route requests to the internet

D. Ensure the network mode is set to bridge in the Fargate task definition

答案：B

273. A company is planning a large event where a promotional offer will be introduced. The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance. The website explains the promotion and includes a sign-up page that collects user information and preferences. Management expects large and unpredictable volumes of traffic periodically, which will create many database writes. A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database

Which solutions meets these requirements?

A. Immediately before the event, scale up the existing DB instance to meet the anticipated demand. Then scale down after the event

B. Use Amazon SQS to decouple the application and database layers. Configure an AWS Lambda function to write items from the queue into the database

C. Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling

D. Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance

答案：B

274. A European online newspaper service hosts its public-facing WordPress site in a colocated data center in London. The current WordPress infrastructure consists of a load balancer, two web servers, and one MySQL database server. A solutions architect is tasked with designing a solution with the following requirements:

-Improve the websites performance.

-Make the web tier scalable and stateless

-Improve the database server performance for read-heavy loads

-Reduce latency for users across Europe and the US

-Design the new architecture with a goal of 99. 9% availability

Which solution meets these requirements while optimizing operational efficiency?

A. Use an Application Load Balancer（ALB）in front of an Auto Scaling group of WordPress Amazon EC2 instances in one AWS Region and three Availability Zones. Configure an Amazon ElastiCache cluster in front of a Multi-AZ Amazon Aurora MySQL DB cluster. Move the WordPress shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes the US and Europe

B. Use an Application Load Balancer（ALB） in front of an Auto Scaling group of WordPress Amazon EC2 instances in two AWS Regions and two Availability Zones in each Region. Configure an Amazon Elasticache cluster in front of a global Amazon Aurora MySQL database. Move the Word Press shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes the US and Europe. Configure EFS cross-Region replication

C. Use an Application Load Balancer（ALB）in front of an Auto Scaling group of WordPress Amazon EC2

instances in one AWS Region and three Availability Zones. Configure an Amazon DocumentDB table in front of a Multi-AZ Amazon Aurora MySOL DB Cluster Move the WordPress shared files to Amazon EFS Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes all global locations
D. Use an Application Load Balancer (ALB) IN FRONT OF AN Auto Scaling group of Wordpress Amazon EC2 instances in two AWS Regions and three Availability Zones in each Region. Configure an Amazon ElastiCache cluster in front of a global Amazon Aurora MYSQL database. Move the wordpress shared files to amazon FSx with cross-Region synchronization Configure amazon cloudfront with the ALB as the origin and a price class that includes the US and Europe.
答案： B

275. A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC. In a peered VPC, the company launched an EC2 Linux instance that serves as a bastion host. The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host. The security group of the bastion host allows access to TCP port 22 from 0.0.0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices.
While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world. The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:
-Eliminate brute-force SSH login attempts
-Retain a log of commands run during an SSH session
-Retain the ability to forward ports
Which solution meets these requirements for remote access to the application instances?
A. Configure the application instances to communicate with AWS Systems Manager Grant access to the system administrators to use Session Manager to establish a session with the application instances. Terminate the bastion host
B. Update the security group of the bastion host to allow traffic from only the public IP addresses of the branch offices
C. Configure an AWS Client VPN endpoint and provision each system administrator with a certificate to establish a VPN connection to the application VPC. Update the security group of the application instances to allow traffic from only the client VPN IPV4 CIDR. Terminate the bastion host
D. Configure the application instances to communicate with AWS Systems Manager Grant access to the system administrators to issue commands to the application instances by using Systems Manager Run Command. Terminate the bastion host
答案： A

276. A company's security compliance requirements state that all Amazon EC2 images must be scanned for vulnerabilities and must pass a CVE assessment. A solutions architect is developing a mechanism to create security-approved AMIs that can be used by developers. Any new AMIs should go through an automated assessment process and be marked as approved before developers can use them. The approved images must be scanned every 30 days to ensure compliance
Which combination of steps should the solutions architect take to meet these requirements while following best practices? （Select TWO.）
A. Use the AWS Systems Manager EC2 agent to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned
B. Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems Manager Parameter Store. Use Amazon EventBridge to trigger an AWS Systems Manager Automation document on all EC2 instances every 30 days

C. Use Amazon Inspector to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned
D. Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems Manager Parameter Store. Use a managed AWS Config rule for continuous scanning on all EC2 instances, and use AWS Systems Manager Automation documents for remediation
E. Use AWS CloudTrail to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned
答案：AB

277. A company wants to host a global web application on AWS. It has the following design requirements:
-The access pattern must allow for fetching data from multiple data sources
-Minimize the cost of API calls
-Keep page load times to within 50 ms
-Provide user authentication and authorization and manage data access for different user personas（for example, administrator manager, or engineer）
Use a serverless design
Which set of strategies should a solutions architect use?
A. Use Amazon CloudFront with Amazon S3 to host the web application. Use Amazon API Gateway to build the application APIs with AWS Lambda for the custom authorizer Authorize data access by performing user lookup in Simple AD
B. Use Amazon CloudFront with AWS WAF to host the web application. Use AWS App Sync to build the application APIs. Use IAM groups for each user persona. Authorize data access by leveraging IAM groups in AWS App Sync resolvers
C. Use Amazon CloudFront with Amazon S3 to host the web application Use Aws AppSync to build the application APIs. Use Amazon Cognito groups for each user persona. Authorize data access by leveraging Amazon Cognito groups in AWS AppSync resolvers
D. Use AWS Direct Connect with Amazon S3 to host the web application Use Amazon API Gateway to build the application APIs. Use AWS Lambda for custom authentication and authorization Authorize data access by leveraging IAM roles
答案：A

278. A solutions architect must enable an AWS CloudHSM M of N access control-also named a quorum authentication mechanism-to allow security officers to make administrative changes to a hardware security module（HSM）. The new security policy states that at least three of the five security officers must authorize any administrative changes to CloudHSM
Which well-architected design ensures the security officers can authenticate as a quorum?
A. Create a static website on Amazon S3 integrated with Amazon API Gateway to allow an officer to initiate a quorum request. Use Amazon SNS to notify the officers of a quorum request. Allow the officers to download the CloudHSM quorum token, sign the token offline, and upload the signed token through the website Use Amazon DynamoDB to store the quorum token and additional officer responses with their signed quorum tokens. Configure an Aws Step Functions workflow to orchestrate officer notifications, count signed tokens in Amazon DynamoDB, and notify the initiating officer once at least three officers have signed the token. Use the signed quorum token to administer CloudHSM
B. Create a static website on Amazon S3 integrated with Amazon API Gateway to allow an officer to initiate a quorum request. Use the website to redirect the officers to sign to CloudHSM with their federated identity credentials. Once at least three officers are signed in to CloudHSM, initiate a synchronous quorum token signing process. Use the signed quorum token to administer CloudHSM
C. Create a quorum signing application hosted on multiple Amazon EC2 instances behind an Application

Load Balancer to allow an officer to initiate a quorum request Require officers to log in to the application with their federated identity credentials. Each officer will then use the application to approve the quorum signing request. Configure the application to use AWS STS to sign the CloudHSM quorum token on behalf of the officers. Once at least three officers have approved the quorum signing request, use EC2 IAM service roles to administer CloudHSM with the signed quorum token

D. Create an Amazon Cognito-authenticated Amazon API Gateway API endpoint with an AWS Lambda proxy Integration Allow an officer to create a CloudHSM quorum token and post it to the API Gateway API after signing in with Amazon Cognito. Configure the Lambda function to perform a signing procedure on the quorum token using the officer's Amazon Cognito IAM role and store the signed token in Amazon DynamoDB Once at least three officers have signed the quorum token, allow a POST method to administer CloudHSM with the signed token

答案：C

279. A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization

The website contains static content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2 instances running in an Auto Scaling group to process an Amazon SQS queue. The company wants to re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software

Which solution meets these requirements?

A. Use Amazon ECS containers for the web application and spot Instances for the Auto scaling group that processes the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos

B. Store the uploaded videos in Amazon EFS and mount the system to the EC2 instances for the web application Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.

C. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3 Use S3 event notifications to publish events to the SQS queue Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos

D. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos

答案：C

280. A mobile app has become very popular, and usage has gone from a few hundred to millions of users. Users capture and upload images of activities within a city, and provide ratings and recommendations. Data access patterns are unpredictable. The current application is hosted on Amazon EC2 instances behind an Application Load Balancer（ALB）. The application is experiencing slowdowns and costs are growing rapidly

Which changes should a solutions architect make to the application architecture to control costs and improve performance?

A. Create an Amazon CloudFront distribution and place the ALB behind the distribution. Store static content in Amazon s3 in an Infrequent Access storage class

B. Store static content in an Amazon s3 bucket using the Intelligent Tiering storage class. Use an Amazon CloudFront distribution in front of the s3 bucket and the ALB

C. Place AWS Global Accelerator in front of the ALB Migrate the static content to Amazon EFS, and then run an AWS Lambda function to resize the images during the migration procees

D. Move the application code to AWS Fargate containers and swap out the EC2 instances with the Fargate

containers
答案：B

281. A company has many services running in its on-premises data center. The data center is connected to Aws using AWS Direct Connect（DX） and an IPSec VPN. The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using Aws
Which solution will meet these requirements ?
A. Create a VPC Endpoint Service that accepts TCP traffic, host it behind a Network Load Balancer, and make the service available over DX
B. Create a VPC Endpoint Service that accepts Http or Https traffic host it behind an Application Load Balancer and make the service available over DX
C. Attach an internet gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic
D. Attach a NAT gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic
答案：A

282. A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to Aws public services. Upon testing the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints
Which step should the solutions architect take to resolve this issue?
A. Update the subnet route table with a route to the interface endpoint
B. Enable the private DNS option on the VPC attributes
C. Configure the security group on the interface endpoint to allow connectivity to the Aws services
D. Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application
答案：B

283. A company is running a two-tier web-based application in an on-premises data center. The application layer consists of a single server running a stateful application. The application connects to a postgreSQL database running on a separate server. The application's user base is expected to grow significantly, so the company is migrating the application and database to Aws. The solution will use Amazon Aurora PostgreSQL, Amazon EC2 Auto Scaling and Elastic Load Balancing
Which solution will provide a consistent user experience that will allow the application and database tiers to scale?
A. Enable Aurora Auto Scaling for Aurora Replicas. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled
B. Enable Aurora Auto Scaling for Aurora writers Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled
C. Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled
D. Enable Aurora Auto Scaling for Aurora writers Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled
答案：C

284. A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling

group. All Aws resources a defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon s3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the CloudFormation templates have caused unplanned downtime

How should a solutions architect improve the Cl/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

A. Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to execute in a non-production environment before approving the change for production

B. Implement automated testing using AWs CodeBuild in a test environment. Use Cloud Formation change sets to evaluate changes before deployment. Use AWs Code Deploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed

C. Use plugins for the integrated development environment（IDE） to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and execute a manual test plan before approving the change for production

D. Use AWS Code Deploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected

答案：B

285. A company wants to migrate its on-premises data center to the Aws Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MySQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration

Which tools or services should the solutions architect use to plan the cloud migration？（Select THREE）

A. AWS Application Discovery Service

B. AWS SMS

C. AWS X-Ray

D. AWS Cloud Adoption Readiness TOOl （CART）

E. Amazon Inspector

F. AWS Migration Hub

答案：ADF

286. A company hosts a web application on Aws that uses Amazon RDs for MySQL Multi-AZ DB instances. Usage of the web application has increased recently. Users have indicated that dynamic reports in the application load slowly

Which configuration change will improve application performance while ensuring the database is highly available for data operations?

A. Add a read replica and configure the application to direct read requests to it

B. Configure the application to direct read requests to the primary and standby DB instances

C. Create two read replicas in the same Availability Zone as the primary DB instance. Use Amazon Route 53 to evenly distribute read requests to the replicas

D. Migrate to Amazon Aurora MySQL with two Aurora Replicas in different Availability Zones. Configure the application to direct read requests to the reader endpoint

答案：D

287. A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MySQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2 and has configured Amazon Route 53 health
Which additional step should the solutions architect take?
A. Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2
B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2
C. Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment
D. Create a MySQL standby database on an Amazon EC2 instance in us-west-2
答案：B

288. A healthcare company runs a production workload on AWS that stores highly sensitive personal information. The security team mandates that, for auditing purposes, any AWS API action using AWS account root user credentials must automatically create a high-priority ticket in the company's ticketing system. The ticketing system has a monthly 3-hour maintenance window when no tickets can be created.
To meet security requirements, the company enabled AWS Cloud Trail logs and wrote a scheduled Aws Lambda function that uses Amazon Athena to query API actions performed by the root user. The Lambda function submits any actions found to the ticketing system API. During a recent security audit, the security team discovered that several tickets were not created because the ticketing system was unavailable due to planned maintenance
Which combination of steps should a solutions architect take to ensure that the incidents are reported to the ticketing system even during planned maintenance? (Select TWO)
A. Create an Amazon SNS topic to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to invoke the Lambda function
B. Create an Amazon SQS queue to which Amazon Cloudwatch alarms will be published Configure a Cloudwatch alarm to publish to the SQS queue
C. Modify the Lambda function to be triggered by messages published to an Amazon SNS topic. Update the existing application code to retry every 5 minutes if the ticketing system's API endpoint is unavailable
D. Modify the Lambda function to be triggered when there are messages in the Amazon SQS queue and to return successfully when the ticketing system API has processed the request
E. Create an Amazon EventBridge rule that triggers on all API events where the invoking user identity is root. Configure the EventBridge rule to write the event to an Amazon SQS queue
答案：BD

289. An AWS partner company is building a service in AWS Organizations using its organization named org 1. This service requires the partner company to have access to Aws resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account
What is the MOST secure way to allow org 1 to access resources in org2?
A. The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks
B. The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks

C. The customer should create an IAM role and assign the required permissions to the IAM user. The customer should then use the IAM role's Amazon Resource Name （ARN ） When permiss questing access to perform the required tasks.

D. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name （ARN）， including the external ID in the lAM role's trust policy, when requesting access to perform the required tasks

答案： D

290. A software company hosts an application on Aws with resources in multiple Aws accounts and regions. The application runs on a group of Amazon EC2 instances in an application VPC located in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a different Aws account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses Aws Cloud Formation to attempt to peer the application VPC with the shared services VPC, an error message indicates a peering failure

Which factors could cause this error？ （Select Two）

A. The IPv4 CIDR ranges of the two VPCs overlap

B. The VPCs are not in the same Region

C. One or both accounts do not have access to an internet gateway

D. One of the VPCs was not shared through AWs Resource Access Manager

E. The IAM role in the peer accepter account does not have the correct permissions

答案：AE

291. A company is using an existing orchestration tool to manage thousands of Amazon EC2 Instances. A recent penetration test found a vulnerability in the company's software stack. This vulnerability has prompted the company to perform a full evaluation of its current production environment. The analysis determined that the following vulnerabilities exist within the environment

-Operating systems with outdated libraries and known vulnerabilities are being used in production

-Relational databases hosted and managed by the company are running unsupported versions with known vulnerabilities

-Data stored in databases is not encrypted

The solutions architect intends to use AWS Config to continuously audit and assess the compliance of the company's AWS resource configurations with the company's policies and guidelines. What additional steps will enable the company to secure its environments and track resources while adhering to best practices ？

A. Use AWS Application Discovery Service to evaluate all running EC2 instances. Use the AWS CLI to modify each instance, and use EC2 user data to install the AWS Systems Manager Agent during boot. Schedule patching to run as a Systems Manager Maintenance Windows task, Migrate all relational databases to Amazon RDS and enable AWS KMS encryption

B. Create an AWS CloudFormation template for the EC2 instances Use EC2 user data in the CloudFormation template to install the AWS Systems Manager Agent, and enable AWS KMS encryption on all Amazon EBS volumes Have CloudFormation replace all running instances. Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to execute AWS-RunPatchBaseline using the patch baseline

C. Install the Aws Systems Manager Agent on all existing instances using the company's current orchestration tool. Use the Systems Manager Run Command to execute a list of commands to upgrade software on each instance using operating system-specific tools. Enable Aws KMS encryption on all Amazon EBS volumes

D. Install the AWS Systems Manager Agent on all existing instances using the company's current

orchestration tool. Migrate all relational databases to amazon RDS and enable AWS KMS encryption. Use Systems Manager Patch Manager to establish a patch baseline and deploy a systems manager maintenance windows task to execute aws-runpatchbaseline using the patch baseline.
答案：A

292. A company has multiple AWS accounts and manages these accounts with AWS Organizations. a developer was given IAM user credentials to access Aws resources. The developer should have read-only access to all Amazon s3 buckets in the account. However, when the developer tries to access the S3 buckets from the console, they receive an access denied error message with no buckets listed
A solutions architect reviews the permissions and finds that the developer's IAM user is listed as having read-only access to all S3 buckets in the account
Which additional steps should the solutions architect take to troubleshoot the issue？ （Select Two）
A. Check the bucket policies for all s3 buckets
B. Check the ACLs for all s3 buckets
C. Check the SCPs set at the organizational units （OUs）
D. Check for the permissions boundaries set for the IAM user.
E. Check if an appropriate lAM role is attached to the lAM user.
答案：BE

293. A company has a complex web application that leverages Amazon Cloud Front for global scalability and performance. Over time, users report that the web application is slowing down
The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters
Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible？
A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function
B. Update the CloudFront distribution to disable caching based on query string parameters
C. Deploy a reverse proxy after the load balancer to post-process the emitted URLS in the application to force the URL strings to be lowercase
D. Update the CloudFront distribution to specify casing-insensitive query string processing
答案：B

294. A company hosts an application on Amazon EC2 instances and needs to store files in Amazon s3. The files should never traverse the public internet, and only the application EC2 instances are granted access to a specific Amazon s3 bucket. A solutions architect has created a VPC endpoint for Amazon s3 and connected the endpoint to the application VPC
Which additional steps should the solutions architect take to meet these requirements？
A. Assign an endpoint policy to the endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint. Add the gateway prefix list to a NACL of the instances to limit access to the application EC2 instances only
B. Attach a bucket policy to the s3 bucket that grants access to application EC2 instances only using the aws: Sourcelp condition. Update the VPC route table so only the application EC2 instances can access the VPC endpoint
C. Assign an endpoint policy to the VPC endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint Assign an lAM role to the application EC2 instances and only allow access to this role in the S3 bucket's policy

D. Assign an endpoint policy to the VPC endpoint that restricts access to S3 in the current Region Attach a bucket policy to the S3 bucket that grants access to the VPC private subnets only Add the gateway prefix list to a NACL to limit access to the application EC2 Instances only

答案：D

295. A company standardized its method of deploying applications to Aws using AWs CodePipeline and Aws CloudFormation. The applications are in Type Script and Python. The company has recently acquired another business that deploys applications to Aws using Python scripts

Developers from the newly acquired company are hesitant to move their applications under Cloud Formation because it would require that they learn a new domain-specific language and eliminate their access to language features, such as looping

How can the acquired applications quickly be brought up to deployment standards while addressing the developers' concerns?

A. Create CloudFormation templates and re-use parts of the Python scripts as instance user data. Use the Aws Cloud Development Kit（AWS CDK ）to deploy the application using these templates. Incorporate the Aws CDK into CodePipeline and deploy the application to AWs using these templates.

B. Use a third- party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired company Orchestrate the CodeBuild job using CodePipeline.

C. Standardize on AWS OpsWorks. Integrate OpsWorks with CodePipeline Have the developers create Chef recipes to deploy their applications on AWS

D. Define the AWS resources using Type Script or Python. Use the Aws Cloud Development Kit （AWS CDK）to create CloudFormation templates from the developers’ code, and use the Aws CDK to create CloudFormation stacks Incorporate the Aws CDK as a CodeBuild job in CodePipeline

答案：D

296. A company is using Amazon Aurora MySQL for a customer relationship management （CRM）application. The application requires frequent maintenance on the database and the Amazon EC2 instances on which the application runs. For Aws Management Console access, the system administrators authenticate against Aws Identity and Access Management（IAM）using an internal identity provider For database access, each system administrator has a user name and password that have previously been configured within the database

A recent security audit revealed that the database passwords are not frequently rotated. The company wants to replace the passwords with temporary credentials using the company's existing Aws access controls

Which set of options will meet the company’s requirements?

A. Create a new AWS Systems Manager Parameter Store entry for each database password. Enable parameter expiration to invoke an AWs Lambda function to perform password rotation by updating the parameter value. Create an IAM policy allowing each system administrator to retrieve their current password from the Parameter Store. Use the Aws CLI to retrieve credentials when connecting to the database

B. Create a new Aws Secrets Manager entry for each database password. Configure password rotation for each secret using an Aws Lambda function in the same VPC as the database cluster. Create an IAM policy allowing each system administrator to retrieve their current password. Use the Aws CLI to retrieve credentials when connecting to the database

C. Enable lAM database authentication on the database. Attach an lAM policy to each system administrator's role to map the role to the database user name. Install the Amazon Aurora SSL certificate bundle to the system administrators’ certificate trust store. Use the AWs CLI to generate an authentication token used when connecting to the database.

D. Enable IAM database authentication on the database. Configure the database to use the IAM identity provider to map the administrator roles to the database user. Install the Amazon Aurora ssL certificate bundle to the system administrators' certificate trust store. Use the AWs CLI to generate an authentication token used when connecting to the database
答案：B

297. A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint Each of the six partners will access the API once per day to post daily sales figures
After initial deployment, the company observes 1 000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic Is originating from a botnet and wants to secure its API while minimizing cost
Which approach should the company take to secure its API?
A. Create an Amazon CloudFront distribution with the API as the origin Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day Associate the web ACL with the CloudFront distribution Configure CloudFront with an origin access identity （OAI） and associate it with the distribution. Configure API Gateway to ensure only the OAI can execute the POST method
B. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the Cloud Front distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method
C. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners Associate the web ACL With the API. Create a resource policy with a request limit and associate it with the API Configure the API to require an API Key on the POST method
D. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners Associate the web ACL With the API. Create a usage plan with a request limit and associate it with the API. Create an API key and add it to the usage plan
答案：B

298. A company wants to use Amazon Workspaces in combination with thin client devices to replace aging desktops. Employees use the desktops to access applications that work with clinical trial data. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch office in the next 6 months.
Which solution meets these requirements with the MOST operational efficiency?
A. Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IP access control group with the Workspaces directory
B. Use Aws Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office locations. Associate the web ACL with the Work spaces directory
C. Use Aws Certificate Manager（ACM）to issue trusted device certificates to the machines deployed in the branch office locations. Enable restricted access on the Workspaces directory
D. Create a custom WorkSpace image with Windows Firewall configured to restrict access to the public addresses of the branch offices. Use the image to deploy the Workspaces
答案：C

299. A company is running a web application on Amazon EC2 instances in a production AWS account. The company requires all logs generated from the web application to be copied to a central AWS account for analysis and archiving. The company's AWS accounts are currently managed independently Logging agents are configured on the EC2 instances to upload the log files to an Amazon S3 bucket in the central AWS

account
A solutions architect needs to provide access for a solution that will allow the production account to store log files in the central account. The central account also needs to have read access to the log files
What should the solutions architect do to meet these requirements?
A. Create a cross-account role in the central account. Assume the role from the production account when the logs are being copied
B. Create a policy on the s3 bucket with the production a as the principal. Account ID as the principal. Allow S3 access from a delegated user
C. Create a policy on the S3 bucket with access from only the CIDR range of the EC2 instances in the production account. Use the production account ID as the principal
D . Create a cross-account role in the production account. Assume the role from the production account when the logs are being copied
答案: C

300. A company is launching a web-based application in multiple regions around the world. The application consists of both static content stored in a private Amazon s3 bucket and dynamic content hosted in Amazon ECS containers behind an Application Load Balancer（ALB）. The company requires that the static and dynamic application content be accessible through Amazon CloudFront only
Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? （Select THREE）
A. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB.
B. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution
C. Configure CloudFront to add a custom header to origin requests
D. Configure the ALb to add a custom header to Http requests.
E. Update the S3 bucket ACL to allow access from the CloudFront distribution only
F. Create a CloudFront Origin Access Identity（OAI）and add it to the CloudFront distribution. Update the s3 bucket policy to allow access to the OAl only.
答案: BCF

301. A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app Is rarely used at any other time A user is notified when image processing is complete
Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load? （Select THREE.）
A. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue
B. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service（Amazon SQS）standard queue
C. Invoke an AWS Lambda function to perform image processing when a message Is available in the queue.
D. Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue
E. Send a push notification to the mobile app by using Amazon Simple Notification Service（Amazon SNS）when processing is complete
F. Send a push notification to the mobile app by using Amazon Simple Email Service （Amazon SES） When processing is complete
答案: BCE

302. A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud. example. com for the resources stored within VPCS
The company has the following DNS resolution requirements:
-On-premises systems should be able to resolve and connect to cloud. example. com
-All VPCs should be able to resolve cloud. example. com
There is already an AWS Direct Connect connection between the on-premises corporate network and AwS Transit Gateway
Which architecture should the company use to meet these requirements with the HIGHEST performance?
A. Associate the private hosted zone to all the VPCS. Create a Route 53 inbound resolver in the shared services VPC. Attach all Vpcs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
B. Associate the private hosted zone to all the VPCs Deploy an Amazon EC2 conditional forwarder in the shared services VPC. Attach all VPCs to transit gateway and create forwarding rules in the on-premises DNS server for cloud. example. com that point to the conditional forwarder
C. Associate the private hosted zone to the shared services VPC. Create a Route 53 outbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud. example. com that point to the outbound resolver.
D. Associate the private hosted zone to the shared services VPC. Create a Route 53 inbound resolver in the shared services VPC. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
答案：A

303. A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region. The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon CloudFront
The company recently expanded to serve users in the us-east-1 Region, and these new users report that viewing their respective weather maps is slow from time to time
Which combination of steps will resolve the us-east-1 performance issues? （Select Two）
A. Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1 Configure endpoint groups for TCP ports 80 and 443 in us-east-1
B. Create a new S3 bucket in us-east-1 Configure S3 cross-Rogion replication to synchronize from the S3 bucket in eu-west-1
C. Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1
D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1
E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution Use Lambda@Edge to modify requests from North America to use the new origin
答案：BE

304. An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation the company wants to migrate its application and database to Aws to increase the reliability of its architecture
Which solution should provide the HIGHEST level of reliability?
A. Migrate the database to an Amazon RDS MysQL Multi-AZ DB instance Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune

B. Migrate the database to Amazon Aurora MysQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer Store sessions in an Amazon Elasticache for Redis replication group.

C. Migrate the database to Amazon DocumentDB（with MongoDB compatibility）. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data firehose

D. Migrate the database to an Amazon RDS MariaDB Multh-Az DB instance Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Elasticache for Memcached

答案：B

305. A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift. Major updates to the sales data occur on the final calendar day of the month. for the remainder of the month, the data warehouse only receives minor daily updates and is primarily used for reading and reporting. Because of this, the migration process must start on the first day of the month and must be complete before the next set of updates occur. This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse. Because the migration cannot impact normal business network operations, the bandwidth allocated to the migration for moving data over the internet is 50 Mbps. The company wants to keep data migration costs low

Which steps will allow the solutions architect to perform the migration within the specified timeline?

A. Install Oracle database software on an Amazon EC2 instance. Configure VPN connectivity between Aws and the company's data center. Configure the Oracle database running on Amazon EC2 to join the Oracle Real Application Clusters（RAC）. When the Oracle database on Amazon EC2 finishes synchronizing, create an AWS DMs ongoing replication task to migrate the data from the Oracle database on Amazon EC2 to Amazon Redshift. verify the data migration is complete and perform the cut over to Amazon Redshift

B. Create an AWs Snowball import job. Export a backup of the Oracle data warehouse. Copy the exported data to the Snowball device. Return the snowball device to Aws. Create an Amazon RDS for oracle database and restore the backup file to that RDs instance. Create an aws DMs task to migrate the data om the rds for Oracle database to Amazon Redshift. Copy daily incremental backups from Oracle in the data center to the RDs for Oracle database over the internet. Verify the data migration is complete and perform the cut over to Amazon Redshift

C. Install Oracle database software on an Amazon EC2 instance. To minimize the migration time, configure VPN connectivity between Aws and the company ' s data center by provisioning a 1 Gbps Aws Direct Connect connection. Configure the Oracle database running on Amazon EC2 to be a read replica of the data center Oracle database. Start the synchronization process between the company's on-premises data center and the Oracle database on Amazon EC2. When the Oracle database on Amazon EC2 is synchronized with the on-premises database, create an AWS DMS ongoing replication task to migrate the data from the Oracle database read replica that is running on Amazon EC2 to Amazon redshift Verify the data migration is complete and perform the cut over to Amazon Redshift.

D. Create an AwS Snowball import job Configure a server in the company's data center with an extraction agent. Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema. Create a new project in AWS SCT using the registered data extraction agent. Create a local task and an AWS DMS task in AWS SCT with replication of ongoing changes. Copy data to the Snowball device and return the Snowball device to AwS. Allow AWS DMS to copy data from Amazon S3 to Amazon Redshift. Verify that the data migration Is complete and perform the cut over to Amazon Redshift

答案：D

306. A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers. The data platform must meet the following requirements:
-Provide near-real-time analytics of the inbound genomic data
-Ensure the data is flexible, parallel, and durable
-Deliver results of processing to a data warehouse
Which strategy should a solutions architect use to meet these requirements?
A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance
B. Use Amazon kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift cluster using Amazon EMR
C. Use Amazon S3 to collect the inbound device data. analyze the data from Amazon SQS with Kinesis and save the results to an Amazon Redshift cluster
D. Use an Amazon API Gateway to put requests into an Amazon SQS queue analyze the data with an Aws Lambda function and save the results to an Amazon Redshift cluster using Amazon EMR
答案： B

307. A financial company needs to create a separate Aws account for a new digital wallet application. The company uses AWs Organizations to manage its accounts. A solutions architect uses the lAM user Support1 from the master account to create a new memberaccountwithfinance1@example.com as the email address What should the solutions architect do to create lam users in the new member account?
A. Sign in to the Aws Management Console with Aws account root user credentials by using the 64-character password from the initial Aws Organizations email sent to finance1@example.com. Set up the IAM users as required
B. From the master account, switch roles to assume the OrganizationAccountAccessRole role with the account ID of the new member account Set up the IAM users as required
C. Go to the AWS Management Console sign-in page Choose “Sing in using root account credentials” sign in in by using the email address finance1@example.com and the master account root password. Set up the IAM user as required.
D. Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials. Set up the IAM users as required.
答案： D

308. A company wants to improve cost awareness for its Amazon EMR platform. The company has allocated budgets for each team’s Amazon EMR usage. When a budgetary threshold is reached, a notification should be sent by email to the budget office's distribution list. Teams should be able to view their EMR cluster expenses to date. A solutions architect needs to create a solution that ensures this policy is proactively and centrally enforced in a multi-account environment.
Which combination of steps should the solutions architect take to meet these requirements? （Select Two.）
A. Update the Aws CloudFormation template to include the Aws：：Budgets::Budget resource with the NotificationsWithSubscribers property
B. Implement Amazon CloudWatch dashboards for Amazon EMR usage
C. Create an EMR bootstrap action that runs at startup that calls the cost Explorer api to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscribers actions.
D. Create an AWS Service Catalog portfolio for each team. Add each team's Amazon EMR cluster as an Aws CloudFormation template to their Service Catalog portfolio as a Product

E. Create an Amazon Cloud Watch metric for billing Create a custom alert when costs exceed the budgetary threshold
答案：AD

309. A company has an application that sends newsletters through email to users. The application runs on two Amazon EC2 instances in a VPC. The first EC2 instance contains the email application that sends email directly to users. The second EC2 instance contains a MySQL database that is heavily dependent upon relational data. Each EC2 instance is controlled by its own Auto Scaling group with a minimum and maximum of one instance. Management wants improved application reliability and support for personalized email
Which set of steps should a solutions architect take to meet these requirements?
A. Migrate the database to Amazon DynamoDB global tables. Reconfigure the email application to use Amazon Simple Email Service（Amazon SES）to send email
B. Migrate the database to an Amazon Aurora MySQL DB cluster with Aurora Replicas. Reconfigure the email application to use Amazon Simple Notification Service（Amazon SNS）to send email
C. Increase the minimum number of EC2 instances in the Scaling group to three. Reconfigure the email application to use Amazon Simple Notification Service（Amazon SNS）to d email Migrate the database to send email
D. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance Reconfigure the email application to use Amazon Pinpoint to send email
答案：C

310. A company is planning to host a three-tier application in the Aws Cloud. The application layer will use Amazon EC2 in an Auto Scaling group. A custom EC2 role named AppServer will be created and associated with the application instances. The entire application stack will be deployed using AWS CloudFormation. The company's security team requires encryption of all AMI snapshots and Amazon Elastic Block Store（Amazon EBS） volumes with an Aws Key Management Service （AWs KMS） CMK
Which action will deploy the stack correctly after the AMI snapshot is encrypted with the KMs key?
A. Update the KMs key policy to provide the required permissions to the App server role
B. Update the KMs key policy to provide the required permissions to the AwsserviceRoleForAutoScaling service-linked role
C. Update the AppServer role to have the required permissions to access the KMS key
D. Update the CloudFormation stack role to have the required permissions to access the KMS key
答案：D

311. An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service（Amazon ECS）cluster in an Auto Scaling group behind an Application Load Balancer（ALB）. A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the applications authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the failed login attempts from overwhelming the authentication service
Which solution meets these requirements with the MOST operational efficiency?
A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses
B. Create an AWS WAF web ACL with a rate- based rule and set the rule action to Block. Connect the web ACL to the ALB
C. Use Aws Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges

D. Create an AWS WAF web ACL with an IP set match rule and set the rule action to Block. Connect the web ACL to the ALB
答案：B

312. A financial company is building a system to generate monthly, immutable bank account statements for its users. Statements are stored in Amazon S3. Users should have immediate access to their monthly statements for up to 2 years. Some users access their statements frequently, whereas others rarely access their statements. The company's security and compliance policy requires that the statements be retained for at least 7 years
What is the MOST cost-effective solution to meet the company's needs?
A. Create an S3 bucket with Object Lock disabled. Store statements in S3 Standard. Define an S3 Lifecycle policy to transition the data to S3 Standard-Infrequent Access（S3 Standard-IA）after 30 days. Define another S3 Lifecycle policy to move the data to S3 Glacier Deep Archive after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old
B. Create an S3 bucket with versioning enabled Store statements in S3 Intelligent-Tiering Use same-Region replication to replicate objects to a backup S3 bucket. Define an S3 Lifecycle policy for the backup S3 bucket to move the data to S3 Glacier. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old
C. Create an S3 bucket with Object Lock enabled Store statements in S3 Intelligent-Tiering Enable compliance mode with a default retention period of 2 years. Define an 53 Lifecycle policy to move the data to S3 Glacier after 2 years Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old
D. Create an S3 bucket with versioning disabled Store statements in S3 One Zone-Infrequent Access（S3 One Zone-IA）Define an S3 Lifecycle policy to move the data to S3 Glacier Deep Archive after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.
答案：A

313. A company recently completed a large-scale migration to AWS. Development teams that support various business units have their own accounts in AWS Organizations. A central cloud team is responsible for controlling which services and resources can be accessed, and for creating operational strategies for all teams within the company. Some teams are approaching their account service quotas. The cloud team needs to create an automated and operationally efficient solution to proactively monitor service quotas. Monitoring should occur every 15 minutes and send alerts when a team exceeds 80% utilization
Which solution will meet these requirements?
A. Create a scheduled AWS Config rule to trigger an AWS Lambda function to call the GetServiceQuota API. If any service utilization is above 80%, publish a message to an Amazon Simple Notification Service（Amazon SNS）topic to alert the cloud team. Create an AWS CloudFormation template and deploy the necessary resources to each account
B. Create an Amazon Event Bridge（Amazon CloudWatch Events ）rule that triggers an AWS Lambda function to refresh the AWS Trusted Advisor service limits checks and retrieve the most current utilization and service limit data. If the current utilization is above 80%, publish a message to an Amazon Simple Notification Service（Amazon SNS）topic to alert the cloud team Create AWS CloudFormation StackSets that deploy the necessary resources to all Organizations accounts.
C. Create an Amazon CloudWatch alarm that triggers an AWS Lambda function to call the Amazon CloudWatch GetinsightRuleReport API to retrieve the most current utilization and service limit data. If the current utilization is above 80%, publish an Amazon Simple Email Service（Amazon SES）notification to alert the cloud team. Create AWS CloudFormation StackSets that deploy the necessary resources to all Organizations accounts

D. Create an Amazon EventBnidge（Amazon Cloud Watch Events）rule that triggers an AWS Lambda function to refresh the AWS Trusted Advisor service limits checks and retrieve the most current utilization and service limit data. If the current utilization is above 80%, use Amaznon Pinpoint to send an alert to the cloud team. Create an AWS CloudFormation template and deploy the necessary resources to each account.
答案：B

314. A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions, and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors. Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events.
The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution
Which strategy meets these requirements?
A. Convert the API Gateway Regional endpoint to an edge-optimized endpoint Enable caching in the production stage
B. Implement an Amazon ElastiCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache
C. Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory
D. Enable throttling in the API Gateway production stage. Set the rate and burst values to limit the incoming calls
答案：A

315. A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored in central file storage. Backend services use different API keys for throttling and to distinguish between live and test traffic.
The load on the game backend varies throughout the day. During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player session data. Management has asked a solutions architect to present a cloud architecture that can handle the game's varying load and provide low-latency data access. The API model should not be changed
Which solution meets these requirements?
A. Implement the REST API using a Network Load Balancer（NLB）. Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless
B. Implement the REST API using an Application Load Balancer（ALB）. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
C. Implement the REST API using Amazon API Gateway. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity
D. Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda Store player session data in Amazon Aurora Serverless
答案：C

316. A company is using AWS CloudFormation as its deployment tool for all applications. It stages all application binaries and templates within Amazon S3 buckets with versioning enabled. Developers have access to an Amazon EC2 instance that hosts the integrated development environment（IDE）. The

developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and upload the binaries to an S3 bucket after running the unit tests locally. The developers want to improve the existing deployment mechanism and implement CI/CD using AWS CodePipeline
The developers have the following requirements:
-Use AWS Code Commit for source control
-Automate unit testing and security scanning
-Alert the developers when unit tests fail
-Turn application features on and off, and customize deployment dynamically as part of CI/CD
-Have the lead developer provide approval before deploying an application
Which solution will meet these requirements？？
A. Use AWS CodeBuild to run unit tests and security scans. Use an Amazon EventBridge rule to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Cloud Development Kit （AWS CDK） constructs for different solution features, and use a manifest file to turn features on and off in the AWS CDK application. Use a manual approval stage in the pipeline to allow the lead developer to approve applications
B. Use AWS Lambda to run unit tests and security scans. Use Lambda in a subsequent stage in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Amplify plugins for different solution features and utilize user prompts to turn features on and off. Use Amazon SES in the pipeline to allow the lead developer to approve applications.
C. Use Jenkins to run unit tests and security scans Use an Amazon Event Bridge rule in the pipeline to send Amazon SES alerts to the developers when unit tests fail. Use AWS CloudFormation nested stacks for different solution features and parameters to turn features on and off. Use AWS Lambda in the pipeline to allow the lead developer to approve applications
D. Use AWS CodeDeploy to run unit tests and security scans. Use an Amazon CloudWatch alarm in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use a manual approval stage in the pipeline to allow the lead developer to approve applications
答案：A

317. A company has implemented an ordering system using an event-driven architecture. During initial testing, the system stopped processing orders. Further log analysis revealed that one order message in an Amazon Simple Queue Service（Amazon SQS）standard queue was causing an error on the backend and blocking all subsequent order messages. The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages
Which step should the solutions architect take to meet these requirements?
A. Increase the backend processing timeout to 30 seconds to match the visibility timeout
B. Reduce the visibility timeout of the queue to automatically remove the faulty message
C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages
D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages
答案：D

318. A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily
The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS
Which data migration strategy should the company use?

A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway
B. Use AWS Data Sync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx
C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System （Amazon EFS）
D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System （Amazon EFS）
答案：B

319. A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3
What is the next step in the transfer process?
A. Deploy an AWS Data Sync agent and configure a task to transfer the images to the S3 bucket
B. Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration
C. Use an AWS Snowball device to transfer the images with the S3 bucket as the target
D. Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload
答案：C

320. A company is configuring connectivity to a multi-account AWS environment to support application workloads that serve users in a single geographic region. The workloads depend on a highly available, on-premises legacy system deployed across two locations. It is critical for the AWS workloads to maintain connectivity to the legacy system, and a minimum of 5 Gbps of bandwidth is required. All application workloads within AWS must have connectivity with one another.
Which solution will meet these requirements?
A. Configure multiple AWs Direct Connect （DX） 10 Gbps dedicated connections from a DX partner for each on-premises location. Create private virtual interfaces on each connection for each AWS account VPC. Associate the private virtual interface with a virtual private gateway attached to each VPC
B. Configure multiple AWS Direct Connect （DX） 10 Gbps dedicated connections from two DX partners for each on-premises location. Create and attach a virtual private gateway for each AWS account VPC. Create a DX gateway in a central network account and associate it with the virtual private gateways. Create a public virtual interface on each DX connection and associate the interface with the DX gateway
C. Configure multiple AWS Direct Connect （DX） 10 Gbps dedicated connections from two DX partners for each on-premises location. Create a transit gateway and a DX gateway in a central network account. Create a transit virtual interface for each DX interface and associate them with the DX gateway. Create a gateway association between the DX gateway and the transit gateway
D. Configure multiple AWS Direct Connect （DX） 10 Gbps dedicated connections from a DX partner for each on-premises location. Create and attach a virtual private gateway for each AWS account VPC. Create a transit gateway in a central network account and associate it with the virtual private gateways. Create a transit virtual interface on each DX connection and attach the interface to the transit gateway
答案：C

321. A company runs an application in Amazon VPC. The application requires that all traffic to three different third-party networks be connection. The network traffic between the application and the third-party networks is expected to be no more than 500 Mbps for each connection. To facilitate network

connectivity, a solutions architect has created a transit gateway and attached the application VPC.
Which set of actions should the solutions architect perform to complete the solution while MINIMIZING costs?

A. Use AWS Certificate Manager (ACM) to generate three public/private key pairs. Install the private keys on a public-facing Application Load Balancer (ALB). Have each third-party network connect to the ALB using HTTPS/TLS. Update the transit gateway route table to route traffic between the application and the third-party networks through the ALB

B. Create an AWS Direct Connect connection between each third-party network and a Direct Connect gateway. Associate the Direct Connect gateway with the transit gateway. Encrypt the Direct Connect connection with each third-party network using a different encryption key

C. Use AWS Marketplace to deploy three different public-facing Amazon EC2 instances running software VPN appliances Establish VPN connections between each appliance and the third-party networks. Update the transit gateway route table to send encrypted traffic to each third-party network using the appropriate VPN appliance.

D. Create a transit gateway VPN attachment to each third-party network. Use separate preshared keys for each VPN attachment. Share those keys with the third-party networks. Update the transit gateway route table by creating a separate route to each third-party network using the appropriate transit gateway attachment

答案：A

322. A solutions architect is designing a solution that consists of a fleet of Amazon EC2 Reserved Instances (RIs) in an Auto Scaling group that will grow over time as usage increases. The solution needs to maintain 80% RI coverage to maintain cost control with an alert to the DevOps team using an email distribution list when coverage drops below 80%. The solution must also include the ability to generate a report to easily track and manage coverage. The company has a policy that allows only one workload for each AWS account.
Which set of steps should the solutions architect take to create the report and alert the DevOps team?

A. Create an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the DevOps email distribution list. Enable cost allocation tags and ensure instances populate a customer-managed cost allocation tag at startup. Use the AWS Billing and Cost Management console to create a budget for RI coverage, filter using the customer-managed cost allocation tag and set the threshold to 80%, and link to the SNS topic created in the alert configuration.

B. Create an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the DevOps email distribution list. Use the Cost Explorer console to configure the report for RI utilization, set the utilization target to 80%, and link to the SNS topic created in the alert configuration

C. Use the AWS Billing and cost Management console to create a reservation budget for RI utilization, set the utilization to 80%, and enter the email distribution list in the alert configuration

D. Enable cost allocation tags and ensure instances populate a customer-managed cost allocation tag at startup. Use the Cost Explorer console to configure the report for RI coverage, filter using the customer-managed cost allocation tag and set the threshold to 80%, and enter the email distribution list in the alert configuration.

答案：D

323. A company is planning to migrate an existing high performance computing (HPC) solution to the AWS Cloud. The existing solution consists of a 12-node cluster running Linux with high-speed interconnectivity deployed on a single rack. A solutions architect needs to optimize the performance of the HPC cluster
Which combination of steps will meet these requirements? (Select TWO)

A. Deploy instances across at least three Availability Zones

B. Deploy Amazon EC2 instances in a placement group

C. Use Amazon EC2 instances that support Elastic Fabric Adapter （EFA）
D. Use Amazon EC2 instances that support burstable performance
E. Enable CPU hyperthreading
答案：BC

324. A startup company recently migrated a large ecommerce website to AWS. The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The DevOps team is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue
The software engineers have decided to use AWS CodePipeline to manage their build and deployment process
Which solution will meet these requirements?
A. Use GitHub websockets to trigger the Code Pipelinepipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.
B. Use GitHub webhooks to trigger the Code Pipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
C. Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds Deploy in a blue/green deployment using AWS CodeDeploy.
D. Use GitHub webhooks to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.
答案：B

325. A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.
In each AWS account with a client, an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer（NLB）are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.
Which combination of steps should a solutions architect take to resolve this issue? （Select TWO）
A. Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances
B. Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances
C. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets
D. Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients.
E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets
答案：AC

326. A company operates an on-premises software-as-a-service（SaaS）solution that ingests several files

daily. The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers. The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic. Changes to the SFTP endpoint IP addresses are not permitted.
The company wants to migrate the SaaS solution to AWS and decrease the operational overhead of the file transfer service.
Which solution meets these requirements?
A. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint. Use AWS Transfer to store the files in Amazon S3
B. Add a subnet containing the customer-owned block of IP addresses to a VPC. Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer（ALB）. Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB. Store the files in attached Amazon Elastic Block Store（Amazon EBS）volumes.
C. Register the customer-owned block of IP addresses with Amazon Route 53. Create alias records in Route 53 that point to a Network Load Balancer（NLB）. Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB. Store the files in Amazon S3
D. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an Amazon S3 VPC endpoint Enable SFTP support on the S3 bucket
答案：D

327. A solutions architect is evaluating the reliability of a recently migrated application running on AWS. The front end is hosted on Amazon S3 and accelerated by Amazon CloudFront. The application layer is running in a stateless Docker container on an Amazon EC2 On-Demand Instance with an Elastic IP address. The storage layer is a MongoDB database running on an EC2 Reserved Instance in the same Availability Zone as the application layer
Which combination of steps should the solutions architect take to eliminate single points of failure with minimal application code changes? （Select TWO）.
A. Create a REST API in Amazon API Gateway and use AWS Lambda functions as the application layer
B. Create an Application Load Balancer and migrate the Docker container to AWS Fargate.
C. Migrate the storage layer to Amazon DynamoDB
D. Migrate the storage layer to Amazon DocumentDB（with MongoDB compatibility）
E. Create an Application Load Balancer and move the storage layer to an EC2 Auto Scaling group
答案：AB

328. A company uses multiple AWS accounts in a single AWS Region. A solutions architect is designing a solution to consolidate logs generated by Elastic Load Balancers（ELBs） in the AppDev, App Test, and App Prod accounts. The logs should be stored in an existing Amazon S3 bucket named s3-elb-logs in the central AWS account. The central account is used for log consolidation only and does not have ELBs deployed. ELB logs must be encrypted at rest
Which combination of steps should the solutions architect take to build the solution? （Select Two.）
A. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3：PutBucketLogging action for the central AWS account ID
B. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3：PutObject and s3：DeleteObject actions for the AppDev, AppTest, and AppProd account IDs.
C. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3. PutObject action for the AppDev, AppTest, and AppProd account IDs.

D. Enable access logging for the ELBs. Set the S3 location to the s3-elb-logs bucket
E. Enable Amazon S3 default encryption using server-side encryption with S3 managed encryption keys （SSE-S3） for the s3-elb-logs S3 bucket
答案：BD

329. A company built an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release. Which solution will meet these requirements?
A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load
B. Deploy the application into a new CloudFormation stack. Use an Amazon Route 53 weighted routing policy to distribute the load
C. Create a version for every new deployed Lambda function. Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load
D. Configure AWS CodeDeploy and use CodeDeployDefault. OneAtATime in the Deployment configuration to distribute the load
答案：A

330. A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows:
GET/posts/{postId}:to get post details
GET /users/{userid}:to get user details
GET /comments/{commentId}:to get comments details
The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by making the comments appear in real time.
Which design should be used to reduce comment latency and improve user experience?
A. Use edge-optimized API with Amazon CloudFront to cache API responses
B. Modify the blog application code to request GET/comments/{commentId} every 10 seconds
C. Use AWS AppSync and leverage WebSockets to deliver comments
D. Change the concurrency limit of the Lambda functions to lower the API response time
答案：D

331. A company that tracks medical devices in hospitals wants to migrate its existing storage solution to the AWS cloud. The company equips all of its devices with sensors that collect location and usage information. This sensor data is sent in unpredictable patterns with large spikes. The data is stored in a MySQL database running on premises at each hospital. The company wants the cloud storage solution to scale with usage
The company's analytics team uses the sensor data to calculate usage by device type and hospital. The team needs to keep analysis tools running locally while fetching data from the cloud. The team also needs to use existing Java application and SQL queries with as few changes as possible.
How should a solutions architect meet these requirements while ensuring the sensor data is secure?
A. Store the data in an Amazon Aurora Serverless database. Serve the data through a Network Load Balancer （NLB） Authenticate users using the NLB with credentials stored in AWS Secrets Manager
B. Store the data in an Amazon S3 bucket. Serve the data through Amazon QuickSight using an IAM user authorized with AWS Identity and Access Management （IAM） with the S3 bucket as the data source
C. Store the data in an Amazon Aurora serverless database. serve the data through the aurora data API using an IAM user authorized with AWS Identity and Access Management （IAM） and the AWS Secrets

Manager ARN
D. Store the data in an Amazon S3 bucket. Serve the data through Amazon Athena using AWS PrivateLink to secure the data in transit
答案：B

332. A company has an application that sells tickets online and experiences bursts of demand every 7 days. The application has a stateless presentation layer running on Amazon EC2，an Oracle database to store unstructured data catalog information, and a backend API layer. The front-end layer uses an Elastic Load Balancer to distribute the load across nine On-Demand Instances over three Availability Zones（AZs）. The Oracle database is running on a single EC2 instance. The company is experiencing performance issues when running more than two concurrent campaigns. A solutions architect must design a solution that meets the following requirements:
-Address scalability issues
-Increase the level of concurrency
-Eliminate licensing costs.
-Improve reliability
Which set of steps should the solutions architect take?
A. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the Oracle database into a single Amazon RDS reserved DB instance
B. Create an Auto Scaling group for the front end with a combination of on-Demand and spot Instances to reduce costs. Create two additional copies of the database instance, then distribute the databases in separate AZs
C. Create an Auto Scaling group for the front end with a combination of on-Demand and spot Instances to reduce costs. Convert the tables in the Oracle database into Amazon DynamoDB tables
D. Convert the On-Demand Instances into Spot Instances to reduce costs for the front end. Convert the tables in the Oracle database into Amazon Dynamo DB tables
答案：C

333. A company has built a high performance computing（HPC）cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.
Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? （Select THREE.）
A. Ensure the HPC cluster is launched within a single Availability Zone
B. Launch the EC2 instances and attach elastic network interfaces in multiples of four
C. Select EC2 instance types with an Elastic Fabric Adapter（EFA）enabled
D. Ensure the cluster is launched across multiple Availability Zones
E. Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array
F. Replace Amazon EFS with Amazon FSx for Lustre
答案：ACF

334. A government agency is building a forms submission portal using AWS to allow citizens to submit and retrieve sensitive documents. The solution was built using a serverless architecture, with the front-end code developed using HTML and JavaScript and the backend architecture using Amazon API Gateway and Amazon S3
The portal must meet the following security requirements:
-Requests to the backend infrastructure should be allowed only if they originate from a specific country.

-Requests to the backend infrastructure should prevent brute force attacks from individual IP addresses by not allowing more than 3，000 requests per 5 minutes（or 10 requests per second）for each IP address.
-All access attempts to the backend infrastructure must be logged
Which steps should a solutions architect take to meet these requirements？（Select TWO）
A. Configure the API Gateway API with a custom rule condition that allows APIs to be called from the authorized country only. Then enable default method throttling, setting the rate limit to 10 requests per second
B. Create an AWS WAF web ACL with a custom rule condition that allows access attempts from the authorized country only, and a rate-based rule with a rate limit of 3，000 requests per 5 minutes. Then associate the web ACL with the API Gateway API
C. Configure Amazon CloudFront with a geographical restriction that allows access attempts from the authorized country only, and a rate-based rule with a rate limit of 3，000 requests per 5 minutes. Then add the API Gateway API as a custom origin
D. Configure the AWS WAF web ACL to log to an Amazon Kinesis Data Firehose delivery stream with Amazon Elasticsearch Service（Amazon ES）as the destination. Configure API Gateway to log to an Amazon CloudWatch Logs group
E. Configure the AWS WAF web ACL to log to an Amazon CloudWatch Logs group. Configure API Gateway to log to an Amazon CloudWatch Logs group
答案：BD

335. A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours
What is the MOST cost-effective migration recommendation？
A. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket
B. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.
C. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS
D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket
答案：D

336. A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting, database API services, and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs
Which solution will meet these requirements？
A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple

Queue Service（Amazon SQS） for order queuing. Use Amazon Elastic Container Service（Amazon ECS） for business logic with Amazon SQS long polling for retaining failed orders

B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders C. Use Amazon S3 for web hosting with AWS AppSync for database API services. Use Amazon Simple Queue Service（Amazon SQS）for order queuing. Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders

D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service(Amazon SES）for order queuing. Use Amazon Elastic Kubernetes service（Amazon EKS） for business logic with Amazon Elasticsearch Service （Amazon ES）for retaining failed orders

答案：A

337. A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance. A solutions architect is designing a disaster recovery（DR）solution with an RPO of 5 minutes

Which solution will meet the company s requirements?

A. Configure AWS Backup to perform cross-Region backups of all servers every 5 minutes. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster

B. Maintain another running copy of the web and application server stack in the DR Region using AWS Cloud Formation drift detection. Configure cross-Region snapshots of the DB instance to the DR Region every 5 minutes. In the event of a disaster, restore the DB instance using the snapshot in the DR Region

C. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Regions. Create a cross-Region read replica of the DB instance in the DR Region. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS Cloud Formation using the AMIs

D. Create AMIs of the web and application servers in the DR Region. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region. In the event of a disaster, switch to the DB instance in the DR Region and reprovision the servers with AWS Cloud Formation using the AMIs

答案：A

338. A company runs an application in the cloud that consists of a database and a website. Users can post data to the website, have the data processed, and have the data sent back to them in an email Data is stored in a MySQL database running on an Amazon EC2 instance. The database is running in a VPC with two private subnets. The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet. There is a single VPC peering connection between the database and website VPC.

The website has suffered several outages during the last month due to high traffic

Which actions should a solutions architect take to increase the reliability of the application? （Select THREE.）

A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.

B. Provision an additional VPC peering connection

C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica

D. Provision two NAT gateways in the database VPC

E. Move the Tomcat server to the database VPC

F. Create an additional public subnet in a different Availability Zone in the website VPC

答案：ACF

339. A solutions architect works for a government agency that has strict disaster recovery requirements. All

Amazon Elastic Block Store（Amazon EBS） snapshots are required to be saved in at least two additional Aws Regions. The agency also is required to maintain the lowest possible operational overhead
Which solution meets these requirements?
A. Configure a policy in Amazon Data Lifecycle Manager（Amazon DLM）to run once daily to copy the EBS snapshots to the additional Regions
B. Use Amazon EventBridge（Amazon CloudWatch Events）to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
C. Set up AWS Backup to create the EBS snapshots. Configure Amazon S3 cross-Region replication to copy the EBS snapshots to the additional Regions
D. Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions
答案：B

340. A solutions architect needs to provide AWS Cost and Usage Report data from a company's AWS Organizations master account. The company already has an Amazon S3 bucket to store the reports. The reports must be automatically ingested into a database that can be visualized with other tools
Which combination of steps should the solutions architect take to meet these requirements? （Select THREE.）
A. Create an Amazon EventBridge（Amazon CloudWatch Events） rule that a new object creation in the S3 bucket will trigger.
B. Create an AWS Cost and Usage Report configuration to deliver the data into the S3 bucket
C. Configure an AWS Glue crawler that a new object creation in the S3 bucket will trigger
D. Create an AWS Lambda function that a new object creation in the s3 bucket will trigger.
E. Create an AWS Glue crawler that the AWS lambda function will trigger to crawl objects in the S3 bucket
F. Create an AWS Glue crawler that the Amazon EventBridge（Amazon CloudWatch Events） rule will trigger to crawl objects in the S3 bucket
答案：ABD

341. A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.
Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?
A. Migrate the backend services to AWS Lambda Increase the read and write capacity of DynamoDB
B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables
C. Use Auto Scaling groups for the backend services Use DynamoDB auto scaling
D. Use Auto Scaling groups for the backend services Use Amazon Simple Queue Service（Amazon SQS）and an AWS Lambda function to write to DynamoDB
答案：C

342. A software company has deployed a web application on AWS in a VPC. The application uses an Application Load Balancer and Amazon EC2 instances in an Auto Scaling group for the application tier. The EC2 instances access an IBM Db2 database that is hosted on separate EC2 instances. Db2 credentials are stored in the configuration file on the application tier and are deployed with AWS AppConfig
The company has a new requirement to prove that the team in charge of the operations of the platform cannot access the cleartext data that is stored in Db2. a solutions architect must implement a solution to meet this requirement with the least possible redevelopment needed
Which combination of steps should the solutions architect take? （Select TWO）

A. Use an AWS managed CMK to ensure that EBS disks for the EC2 instances are encrypted. Edit the key policy to ensure that only the roles provided to the EC2 instances in the application tier are allowed to use the key B. Use a customer managed CMK to ensure that EBS disks for the EC2 instances are encrypted. Edit the key policy to ensure that only the roles provided to the EC2 instances in the application tier are allowed to use the key

C. Use AWS Certificate Manager（ACM） to implement mutual authentication between the application and the database

D. Use AWS Secrets Manager to ensure that a password is not stored in the application configuration

E. Use client-side encryption in the application

答案：AD

343. A company manages hundreds of AWS accounts centrally in an organization in AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs. not on the internet.

What is the MOST operationally efficient way to enforce this requirement?

A. Set the S3 access point resource policy to deny the s3：Create Access Point action unless the s3: Access PointNetworkorigin condition key evaluates to VPC

B. Create an SCP at the root level in the organization to deny the s3：Create Access Point action unless the S3：AccessPointNetworkorigin condition key evaluates to VPC

C. Use AWS Cloud Formation Stack Sets to create a new lam policy in each AWS account that allows the s3：CreateAccessPoint action only if the s3 AccessPointNetworkorigin condition key evaluates to VPC

D. Set the S3 bucket policy to deny the s3：CreateAccessPoint action unless the s3：AccessPointNetwork Origin condition key evaluates to VPC

答案：B

344. A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function

To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application

Which combination of steps should the solutions architect take to implement this solution？（Select Two）

A. Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the applications VPC. Update the bucket policy to require access from an access point

B. Create an interface endpoint for Amazon S3 in each applications VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint

C. Create a gateway endpoint for Amazon S3 in each application’s VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point

D. Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket Configure each access point to be accessible only from the applications VPC. Update the bucket policy to require access from an access point

E. Create a gateway endpoint for Amazon S3 in the data lake's VPC Attach an endpoint policy to allow access to the S3 bucket. specify the route table that is used to access the bucket.

答案：AC

345. A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instance. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded,

uses 2 GB of RAM, and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution
Which strategy should the solutions architect use?
A. Use AWS Lambda to run the application Use Amazon Cloud Watch logs to invoke the lambda function every 4 hours
B. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS batch job every 4 hours
C. Use AWS Fargate to run the application. Use Amazon EventBridge（Amazon CloudWatch Events） to invoke the Fargate task every 4 hours
D. Use Amazon EC2 Spot Instances to run the application. Use AWS Code Deploy to deploy and run the application every 4 hours
答案：C

346. A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS
Which solution meets these requirements MOST cost-effectively?
A. Create a new S3 bucket Deploy an Aws Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share
B. Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSX file system. Enable nightly backups
C. Create an Amazon FSx for Windows File server Multi-AZ file system within the VPC that is connected to the direct Connect Connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system Enable nightly backups
D. Create a new S3 bucket Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.
答案：D

347. A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer（ALB）in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region
What should a solutions architect do to meet these requirements?
A. Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary
B. Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs Set the Evaluate Target Health value to Yes
C. Create two Amazon Cloud Front distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes
D. Create an Amazon Route 53 health check for each ALB. Create a Route 53 late key alias record pointing to the two ALBs Set the Evaluate Target health value to Yes
答案：C

348. A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0.0.0.0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway

A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet

What should the solutions architect do to meet these requirements?

A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway

B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for::/0 to the NAT gateway

C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Create an egress-only internet gateway. Update the VPC route tables for all private subnets, and add a route for ::/0 to the egress-only internet gateway

D. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPv6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6 enabled NAT gateway

答案：D

349. A development team has created a new flight tracker application that provides near-real-time data to users. The application has a front end that consists of an Application Load Balancer（ALB）in front of two large Amazon EC2 instances in a single Availability Zone Data is stored in a single Amazon RDS MySQL DB instance. An Amazon Route 53 DNS record points to the ALB

Management wants the development team to improve the solution to achieve maximum reliability with the least amount of operational overhead

Which set of actions should the team take?

A. Create RDS My SQL read replicas. Deploy the application to multiple AWS Regions. Use a route 53 latency- based routing policy to route to the application

B. Configure the DB instance as Multi-AZ. Deploy the application to two additional EC2 instances in different Availability Zones behind an ALB

C. Replace the DB instance with Amazon DynamoDB global tables. Deploy the application in multiple AWS Regions. Use a Route 53 latency-based routing policy to route to the application

D. Replace the DB instance with Amazon Aurora with Aurora Replicas. Deploy the application to multiple smaller EC2 instances across multiple Availability Zones in an Auto Scaling group behind an ALB

答案：C

350. A multimedia company needs to deliver its video-on-demand（VOD）content to its subscribers in a cost-effective way. The video files range in size from 1-15 GB and are typically viewed frequently for the first 6 months after creation, and then access decreases considerably. The company requires all video files to remain immediately available for subscribers. There are now roughly 30，000 files and the company anticipates doubling that number over time

What is the MOST cost-effective solution for delivering the company's VOD content?

A. Store the video files in an Amazon S3 bucket using S3 Intelligent-Tiering Use Amazon Cloud Front to deliver the content with the s3 bucket as the origin

B. Use AWS Elemental Media Convert and store the adaptive bitrate video files in Amazon S3. Configure an AWS elemental MediaPackage endpoint to deliver the content from Amazon S3

C. Store the video files in Amazon Elastic File System（Amazon EFS）Standard. Enable EFS lifecycle management to move the video files to EFS Infrequent Access after 6 months. Create an Amazon EC2 Auto

Scaling group behind an Elastic Load Balancer to deliver the content from amazon EFS
D. Store the video files in Amazon S3 Standard Create S3 Lifecycle rules to move the video files to S3 Standard-Infrequent Access（S3 Standard-IA） after 6 months and to S3 Glacier Deep Archive after 1 year. Use Amazon CloudFront to deliver the content with the S3 bucket as the origin
答案：A

351. A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer（NLB）for scalability Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC, and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only
Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?
A. Create an AWS Transit Gateway. Attach the shared VPC and the authorized business unit VPCs to the transit gateway Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway
B. Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service Accept authorized endpoint requests from the endpoint service console
C. Create a VPC peering connection from each business unit VPC to the shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection
D. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCS. Establish a site-to-Site VPN connection from the business unit VPCs to the shared VPC. configure VPC routing tables to send traffic to the VPN Connection
答案：A

352. A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer（ALB）. Only users from a specific country are allowed to access the application. the company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance
Which solution meets these requirements?
A. Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet Associate the rule with the web ACL Associate the web ACL with the ALB
B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country Associate the rule with the web ACL. associate the web ACL with the ALB
C. Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB
D. Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB
答案：B

353.A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network（SAN）， and then the data is

processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days.
The company has a high-speed AWS Direct Connect connection Sequencers will generate around 200 GB of data for each genome and individual jobs can take several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day
Which solution meets these requirements?
A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data
B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data
C. Use AWS Data Sync to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow Store the Docker images in Amazon Elastic Container Registry（Amazon ECR）and trigger AWs Batch to run the container and process the sequencing data
D. Use an Aws Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data
答案：B

354. A company is running several workloads in a single AWS account. a new company policy states that engineers can provision only approved resources and that engineers must use AWS CloudFormation to provision these resources. A solutions architect needs to create a solution to enforce the new restriction on the lAM role that the engineers use for access
What should the solutions architect do to create the solution
A. Upload AWS Cloud Formation templates that contain approved resources to an Amazon S3 bucket. Update the lAM policy for the engineers' lAM role to only allow access to Amazon S3 and AWS CloudFormation. Use AWS CloudFormation templates to provision resources
B. Update the lAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation. Use AWS CloudFormation templates to create stacks with approved resources
C. Update the IAM policy for the engineers' lAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new lAM service role. Assign the lAM service role to AWS Cloud Formation during stack creation
D. Provision resources in AWS CloudFormation stacks. Update the lAM policy for the engineers' lAM role to only allow access to their own AWS cloud Formation stack
答案：C

355. A company hosts a large on-premises MySQL database at its main office that supports an issue tracking system used by employees around the world. The company already uses AWS for some workloads and has created an Amazon Route 53 entry for the database endpoint that points to the on-premises database Management is concerned about the database being a single point of failure and wants a solutions architect to migrate the database to AWS without any data loss or downtime
Which set of actions should the solutions architect implement?
A. Create an Amazon Aurora DB cluster Use AWS Database Migration Service（ AWS DMS）to do a full load from the on-premises database to Aurora. Update the Route 53 entry for the database to point to the

aurora cluster endpoint, and shut down the on-premises database

B. During nonbusiness hours, shut down the on-premises database and create a backup. Restore this backup to an amazon Aurora DB cluster. When the restoration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database

C. Create an Amazon Aurora DB cluster Use AWS Database Migration Service（AWS DMS）to do a full load with continuous replication from the on-premises database to Aurora. When the migration is complete, update the Route 53 entry for the database to point to the aurora cluster endpoint and shut down the on-premises database

D. Create a backup of the database and restore it to an amazon aurora multi-master cluster. This aurora cluster will be in a master-master replication configuration with the on-premises database Update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database

答案：C

356. A company wants to migrate its corporate data center from on premises to the AWs Cloud The data center includes physical servers and VMs that use VMware and Hyper-V. An administrator needs to select the correct services to collect data for the initial migration discovery process. The data format should be supported by Aws Migration Hub. The company also needs the ability to generate reports from the data Which solution meets these requirements?

A. Use the AWS Agentless Discovery Connector for data collection on physical servers and all VMs. Store the collected data in Amazon S3. Query the data with S3 Select Generate reports by using Kibana hosted on Amazon EC2

B. Use the AWS Application Discovery Service agent for data collection on physical servers and all VMs. Store the collected data in Amazon Elastic File System（Amazon EFS）Query the data and generate reports with Amazon Athena

C. Use the AWS Application Discovery Service agent for data collection on physical servers and Hyper-V. Use the Aws Agentless Discovery Connector for data collection on VMware Store the collected data in Amazon S3. Query the data with Amazon Athena Generate reports by using Amazon QuickSight

D. Use the AWS Systems Manager agent for data collection on physical servers Use the AWS Agentless Discovery Connector for data collection on all VMs. Store, query, and generate reports from the collected data by using Amazon Redshift

答案：B

357. The following AWs Identity and Access Management（IAM）customer managed policy has been attached

to an IAM user:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::prod-data",
                "arn:aws:s3:::prod-data/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::prod-data",
                "arn:aws:s3:::prod-data/*"
            ]
        }
    ]
}
```

Which statement describes the access that this policy provides to the user?
A. This policy grants access to all Amazon S3 actions, including all actions in the prod-data S3 bucket
B. This policy denies access to all Amazon S3 actions, excluding all actions in the prod-data S3 bucket
C. This policy denies access to the Amazon S3 bucket and objects not having prod -data in the bucket name
D. This policy grants access to all Amazon S3 actions in the prod-data S3 bucket, but explicitly denies access to all other AWS services
答案：C

358. A large company in Europe plans to migrate its applications to the AWS Cloud. The company uses multiple AWS accounts for various business groups. a data privacy law requires the company to restrict developers access to AWS European Regions only
What should the solutions architect do to meet this requirement with the LEAST amount of management overhead?
A. Create IAM users and lAM groups in each account. Create IAM policies to limit access to non-European Regions Attach the IAM policies to the lAM groups
B. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions Create SCPs to limit access to non-European Regions and attach the policies to the OUs
C. Set up AWs Single Sign-On and attach Aws accounts. Create permission sets with policies to restrict access to non-European Regions Create lAM users and lAM groups in each account
D. Enable AWS Organizations, attach the AWs accounts, and create OUs for European Regions and non-European Regions Create permission sets with policies to restrict access to non-European Regions. Create IAM users and lAM groups in the primary account
答案：B

359. A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts
The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network. Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets. Which combination of actions should the solutions architect perform to meet these requirements? （Select Two）
A. Create a transit gateway in the infrastructure account
B. Enable resource sharing from the AWS Organizations management account
C. Create VPCs in each AWS account within the organization in AWS Organizations. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account. Peer the VPCs in each individual account with the VPC in the infrastructure account
D. Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each subnet to associate with the resource share
E. Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each prefix list to associate with the resource share
答案：BD

360. A company is using AWS Organizations to manage 15 AWS accounts. A solutions architect wants to run advanced analytics on the company's cloud expenditures. The cost data must be gathered and made available from an analytics account. The analytics application runs in a VPC and must receive the raw cost data each night to run the analytics

The solutions architect has decided to use the Cost Explorer API to fetch the raw data and store the data in Amazon S3 in JSON format Access to the raw cost data must be restricted to the analytics application. The solutions architect has already created an AWS Lambda function to collect data by using the Cost Explorer API

Which additional actions should the solutions architect take to meet these requirements?

A. Create an IAM role in the Organizations master account with permissions to use the Cost Explorer API, and establish trust between the role and the analytics account. Update the Lambda function role and add sts: AssumeRole permissions. Assume the role in the master account from the Lambda function code by using the AWS Security Token Service（AWS STS）Assume Role API call. Create a gateway endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the S3 endpoint.

B. Create an IAM role in the analytics account with permissions to use the Cost Explorer APl. Update the Lambda function and assign the new role. Create a gateway endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the analytics VPC by using the aws: SourceVpc condition

C. Create an IAM role in the Organizations master account with permissions to use the Cost Explorer API, and establish trust between the role and the analytics account. Update the Lambda function role and add sts: AssumeRole permissions. Assume the role in the master account from the Lambda function code by using the AWS Security Token Service（AWS STS）Assume Role API call Create an interface endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the analytics VPC private CIDR range by using the aws: Sourcelp condition

D. Create an IAM role in the analytics account with permissions to use the Cost Explorer API. Update the Lambda function and assign the new role. Create an interface endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the S3 endpoint

答案：C

361. A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company’s resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC

A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions

Which solution meets these requirements?

A. Provision a Direct Connect gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC

B. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC

C. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the new connection, and connect the new public virtual interface to the single VPC.

D. Provision a transit gateway. Delete the existing private virtual interface from the existing connection.

Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC

答案：D

362. A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS for PostgreSQL. The company expects a significant increase of orders on its platform when a new version of its flagship product is released

What changes to the current architecture will reduce operational overhead and support the product release?

A. Create an EC2 Auto Scaling group behind an Application Load Balancer Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams Store and serve static content directly from Amazon S3

B. Create an EC2 Auto Scaling group behind an Application Load Balancer Deploy the DB instance in Multi-AZ mode and enable storage auto scaling Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3

C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster Store static content in Amazon S3 behind an Amazon Cloud Front distribution

D. Deploy the application on Amazon Elastic Kubernetes Service（Amazon EKS）with AWS Fargate and enable auto scaling behind an Application Load Balancer Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon Cloud Front distribution

答案：D

363. A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account The company is using AWS Organizations and created an account for the security team

How should a solutions architect meet these requirements?

A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the lAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access

B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the lAM role to gain access

C. Ask the security team to use AWS Security Token Service（AWS STS）to call the Assume Role API for the OrganizationAccountAccessRole IAM role in the master account from the security account. Use the generated temporary credentials to gain access

D. Ask the security team to use AWS Security Token Service（AWS STS）to call the Assume Role API for the OrganizationAccountAccessRole lAM role in the member account from the security account. Use the generated temporary credentials to gain access

答案：C

364. A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account.

Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.
Which combination of steps will meet these requirements ？ （Select TWO）
A. From the master account, share the transit gateway with member accounts by using AWS Resource Access Manager
B. From the master account, share the transit gateway with member accounts by using AWS Organizations SCP.
C. Lunch an AWS CloudFormation stack set from the master account that automatically creates a new VPC and a VPC transit gateway attachment in a member account. Associate the attachment with the transit gateway in the master account by using the transit gateway ID
D. Launch an AWS Cloud Formation stack set from the master account that automatically creates a new VPC and a peering transit gateway attachment in a member account. Share the attachment with the transit gateway in the master account by using a transit gateway service-linked role
E. From the master account, share the transit gateway with member accounts by using AWS Service Catalog
答案：BD

365. A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching Management requires a single report showing the patch status of all the servers and instances
Which set of actions should a solutions architect take to meet these requirements?
A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances Use Systems Manager to generate patch compliance ports
B. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances Use Amazon Quick Sight integration with OpsWorks to generate patch compliance reports
C. Use an Amazon EventBridge（Amazon CloudWatch Events）rule to apply patches by scheduling an AWS Systems Manager patch remediation job. Use Amazon Inspector to generate patch compliance reports
D. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports
答案：C

366. An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list.
The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer（ALB）in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets
How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?
A. Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC
B. Register a block of customer-owned public IP addresses in the AWS account Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC
C. Create Elastic IP addresses from the block of customer-owned IP addresses Assign the static Elastic IP addresses to the ALB
D. Register a block of customer-owned public IP addresses in the AWS account Set up AWS Global Accelerator to use Elastic IP addresses from the address block Set the ALB as the accelerator endpoint

答案：B

367. A company maintains a restaurant review website. The website is a single-page application where files are stored in Amazon S3 and delivered using Amazon CloudFront. The company receives several fake postings every day that are manually removed
The security team has identified that most of the fake posts are from bots with IP addresses that have a bad reputation within the same global region. The team needs to create a solution to help restrict the bots from accessing the website
Which strategy should a solutions architect use?
A. Use AWS Firewall Manager to control the CloudFront distribution security settings. Create a geographical block rule and associate it with Firewall Manager.
B. Associate an AWS WAF web ACL with the Cloud Front distribution. Select the managed Amazon IP reputation rule group for the web ACL with a deny action
C. Use AWS Firewall Manager to control the CloudFront distribution security settings. Select the managed Amazon IP reputation rule group and associate it with Firewall Manager with a deny action
D. Associate an AWS WAF web ACL with the Cloud Front distribution. Create a rule group for the web ACL with a geographical match statement with a deny action
答案：D

368. A company is running an Apache Hadoop cluster on Amazon EC2 instances. The Hadoop cluster stores approximately 100 TB of data for weekly operational reports and allows occasional access for data scientists to retrieve data. The company needs to reduce the cost and operational complexity for storing and serving this data
Which solution meets these requirements in the MOST cost-effective manner?
A. Move the Hadoop cluster from EC2 instances to Amazon EMR Allow data access patterns to remain the same
B. Write a script that resizes the EC2 instances to a smaller instance type during downtime and resizes the instances to a larger instance type before the reports are created
C. Move the data to Amazon S3 and use Amazon Athena to query the data for reports Allow the data scientists to access the data directly in Amazon S3
D. Migrate the data to Amazon DynamoDB and modify the reports to fetch data from DynamoDB Allow the data scientists to access the data directly in DynamoDB
答案：D

369. A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT.
The company wants to allow only the launch of t3. small EC2 instances by developers in the project's account These EC2 instances must be restricted to the us-east-2 Region
What should a solutions architect do to meet these requirements?
A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company’s organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity
B. Create an SCP that denies the launch of all EC2 instances except t3 small EC2 instances in us-east-2 Attach the SCP to the projects account
C. Create and purchase a t3. small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag
D. Create an IAM policy than allows the launch of only t3. small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the projects account
答案：B

370. A company has a serverless application that is deployed on AWS . The application uses an Amazon API Gateway REST API and AWS Lambda to receive and process requests from other applications within the company's on-premises network. The application uses a preshared API key as the authentication method
A recent security review showed that the application was accessible from anywhere on the internet. The company's security policy states that requests can be accepted only from the company's on-premises network
What should a solutions architect recommend to meet this requirement?
A. Configure a security group with rules to allow traffic only from within the company's public IP address range. Attach the security group to the API Gateway API, and redeploy the API
B. Create a Lambda function to inspect the requests and deny the execute-api：Invoke action if the request is not from within the company's public IP address range. Configure the Lambda function as a custom authorizer for the API Gateway API. Redeploy the API
C. Create a resource policy with a statement to deny the execute-api：Invoke action if the AWS ：Sourcelp attribute is not from within the company's public IP address range. Attach that resource policy to the API Gateway API Redeploy the API
D. Configure a request validator for API Gateway to inspect the requests and deny the execute-api: Invoke action if the AWS :Sourcelp attribute is not from within the company's public IP address range. Redeploy the API Gateway API
答案：B

371. A company is running a distributed application on a set of Amazon EC2 instances in an Auto Scaling group. The application stores large amounts of data on an Amazon Elastic File System（Amazon EFS）file system, and new data is generated monthly. The company needs to back up the data in a secondary AWS Region to restore from in case of a performance problem in its primary Region. The company has an RTO of 1 hour. A solutions architect needs to create a backup strategy while minimizing the extra cost
Which backup strategy should the solutions architect recommend to meet these requirements?
A. Create a pipeline in AWS Data Pipeline. Copy the data to an EFS file system in the secondary Region. Create a lifecycle policy to move files to the EFS One Zone-Infrequent Access storage class
B. Set up automatic backups by using AWS Backup. Create a copy rule to copy backups to an Amazon S3 bucket in the secondary Region. Create a lifecycle policy to move backups to the S3 Glacier storage class
C. Set up AWS DataSync and continuously copy the files to an Amazon S3 bucket in the secondary Region. Create a lifecycle policy to move files to the S3 Glacier Deep Archive storage class
D. Turn on EFS Cross-Region Replication and set the secondary Region as the target. Create a lifecycle policy to move files to the EFS Infrequent Access storage class in the secondary Regio
答案：A

372. A company has an on-premises website application that provides real estate information for potential renters and buyers. The website uses a Java backend and a NoSQL MongoDB database to store subscriber data. The company needs to migrate the entire application to AWS with a similar structure. The application must be deployed for high availability, and the company cannot make changes to the application.
Which solution will meet these requirements?
A. Use an Amazon Aurora DB cluster as the database for the subscriber data Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application
B. Use MongoDB on Amazon EC2 instances as the database for the subscriber data. Deploy EC2 instances in an Auto Scaling group in a single Availability Zone for the Java backend application
C. Configure Amazon DocumentDB（with MongoDB compatibility）with appropriately sized instances in multiple Availability Zones as the database for the subscriber data Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application
D. Configure Amazon DocumentDB （with MongoDB compatibility） in on-demand capacity mode in multiple

Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application

答案：D

373. A startup company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI The company's engineers rely heavily on SSH access to the instances for troubleshooting

The company's existing architecture includes the following:

-A VPC with private and public subnets, and a NAT gateway

-Site-to-Site VPN for connectivity with the on-premises environment

-EC2 security groups with direct SSH access from the on-premises environment

The company needs to increase security controls around SSH access and provide auditing of commands executed by the engineers

Which strategy should a solutions architect use?

A. Install and configure EC2 Instance Connect on the fleet of EC2 instances. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI

B. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs

C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices Enable AWS Config for EC2 security group resource changes Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules

D. Create an IAM role with the AmazonSSMManagedInstance Core managed policy attached. Attach the IAM role to all the EC2 instances. Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager.

答案：D

374. A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests

Which combination of steps meets these requirements while minimizing operational overhead? （Select TWO）

A. Deploy the application to Amazon EC2 On-Demand Instances with load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays

B. Deploy the application in a container using Amazon Elastic Container Service（Amazon ECS） with load balancing across multiple Availability Zones. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays

C. Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration

D. Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source

E. Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source

答案：CE

375. A travel company built a web application that uses Amazon Simple Email Service（Amazon SES）to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The

company also needs the ability to do searches that are based on recipient, subject, and time sent.
Which combination of steps should a solutions architect take to meet these requirements? （Select TWO） A. Create an Amazon SES configuration set with Amazon Kinesis Data Firehose as the destination. Choose to send logs to an Amazon S3 bucket
B. Enable AWS CloudTrail logging Specify an Amazon S3 bucket as the destination for the logs
C. Use Amazon Athena to query the logs in the Amazon S3 bucket for recipient, subject and time sent
D. Create an Amazon CloudWatch log group. Configure Amazon SES to send logs to the log group
E. Use Amazon Athena to query the logs in Amazon CloudWatch for recipient, subject, and time sent
答案：BC

376. A company is planning to host a web application on AWS and wants to load balance the traffic across a group of Amazon EC2 instances. One of the security requirements is to enable end-to-end encryption in transit between the client and the web server.
Which solution will meet this requirement?
A. Place the EC2 instances behind an Application Load Balancer（ALB）Provision an SSL certificate using AWS Certificate Manager（ACM），and associate the SSL certificate with the ALB. Export the SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances
B. Associate the EC2 instances with a target group. Provision an SSL certificate using AWS Certificate Manager（ACM）. Create an Amazon CloudFront distribution and configure it to use the SSL certificate. Set Cloud Front to use the target group as the origin server
C. Place the EC2 instances behind an Application Load Balancer（ALB）. Provision an SSL certificate using AWS Certificate Manager（ACM），and associate the SSL certificate with the ALB. Provision a third-party SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances
D. Place the EC2 instances behind a Network Load Balancer（NLB）Provision a third-party SSL certificate and install it on the NLB and on each EC2 instance. Configure the NLB to listen on port 443 and to forward traffic to port 443 on the instances.
答案：A

377. A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10，000 users worldwide will upload their images. The service will then overlay text on the uploaded images, which will then be published on the company website
Which design should a solutions architect implement?
A. Store the uploaded images in Amazon Elastic File System（Amazon EFS）Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in another directory in Amazon EFS Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet
B. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service（Amazon SNS）. Create a fleet of Amazon EC2 instances behind an Application Load Balancer（ALB）to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System（Amazon EFS） Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances
C. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service（Amazon SQS ）queue. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images
D. Store the uploaded images on a shared Amazon Elastic Block Store（Amazon EBS）volume mounted to a fleet of

Amazon EC2 Spot instances. Create an Amazon Dynamo DB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge（Amazon CloudWatch Events）rule to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances
答案：C

378. A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration
What should a solutions architect do to meet these requirements?
A. Create an AWS Config ule in the specific member accounts to limit Regions and apply a tag policy
B. From the AWS Billing and Cost Management console, in the master account, disable Regions for the specific member accounts and apply a tag policy on the root
C. Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions
D. Associate the specific member accounts with a new OU Apply a tag policy an SCP using conditions to limit Regions
答案：D

379. A company's solutions architect is designing a disaster recovery（DR）solution for an application that runs on AWS . The application uses PostgreSQL 11.7 as its database. The company has an RPO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the failover database in the us-west-2 Region
What should the solutions architect do to meet these requirement s with minimum appl cation change?
A. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica in us-west-2 Set the managed RPO for the RDS database to 30 seconds
B. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2. Set the managed RPO for the RDS database to 30 seconds
C. Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2 Set the managed RPO for the Aurora database to 30 seconds D. Migrate the database to Amazon DyramoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2
答案：D

380. A company uses an AWS CloudFormation template to deploy an Amazon Elastic Container Service（Amazon ECS）service into a production environment. The template includes an Amazon S3 bucket that is named by using a common prefix with the Cloud Formation stack name
The company uses the same template to create temporary environments for development and continuous integration. Developers can create environments successfully, but they receive errors from CloudFormation when they attempt to delete the environments. The developers often need to delete and recreate stacks with the same names as part of the development and testing process
Which combination of steps should a solutions architect take to modify the solution to resolve this issue? （Select Two）
A. Associate an AWS Lambda function with a CloudFormation custom resource to delete all keys that are present in a given S3 bucket. Implement this custom resource as part of the application's CloudFormation template
B. Modify the S3 bucket resource in the CloudFormation template by specifying Delete for the DeletionPolicy attribute. specify the CAPABILITY_DELETE_NONEMPTY capability to process CloudFormation delete operation
C. Modify the S3 bucket resource in the CloudFormation template by specifying Retain for the DeletionPolicy

attribute. Configure an AWS Config custom rule to run every 24 hours to identify empty, and delete buckets that are no longer owned by a CloudFomation stack

D. Ensure that CloudFormation operations are being invoked by a role that has s3：DeleteObject permissions on all objects in the bucket

E. Modify the S3 bucket resource in the Cloud Formation template to configure a bucket policy that grants s3：DeleteObject permissions on all objects in the bucket

答案：CD

381. A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account

A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. the solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account

What should the solutions architect do next to meet these requirements?

A. Create the OrganizationAccountAccess IAM group in each member account. Include the necessary IAM roles for each administrator

B. Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access

C. Create the OrganizationAccountaccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role

D. Create the OrganizationAccountaccessRole IAM role in the management account. Attach the administrator Access AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account

答案：C

382. A company wants to retire its Oracle Solaris NFS storage arrays. The company requires rapid data migration over its internet network connection to a combination of destinations for Amazon S3，Amazon Elastic File System（Amazon EFS），and Amazon FSx for Windows File server. The company also requires a full initial copy, as well as incremental transfers of changes until the retirement of the storage arrays. All data must be encrypted and checked for integrity

What should a solutions architect recommend to meet these requirements?

A. Configure CloudEndure Create a project and deploy the CloudEndure agent and token to the storage array. Run the migration plan to start the transfer

B. Configure AWS Data Sync. Configure the DataSync agent and deploy it to the local network. Create a transfer task and start the transfer

C. Configure the AWS S3 sync command. Configure the AWS client on the client side with credentials. Run the sync command to start the transfer

D. Configure AWS Transfer for FTP. Configure the FTP client with credentials. Script the client to connect and sync to start the transfer

答案：C

383. A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account

Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? （Select THREE）

A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization

B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API

C. From each developer account, remove the account from the old organization using the Remove AccountFromOrganization operation in the Organizations API

D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration

E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts

F. Have each developer sign in to their account and confirm to join the new developer organization

答案：BDE

384. A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized Row Columnar（OCR）files in the Hadoop Distributed File System（HDFS）on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in Apache Presto deployed on the same EMR cluster Queries scan large amounts of data, always run for less than 15 minutes, and run only between 5 PM and 10 PM

The company is concerned about the high cost associated with the current solution. A solutions architect must propose the most cost-effective solution that will allow SQL data queries

Which solution will meet these requirements?

A. Store data in Amazon S3. Use Amazon Redshift Spectrum to query data

B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data

C. Store data in EMR File System（EMRFS）Use Presto in Amazon EMR to query data

D. Store data in Amazon Redshift. Use Amazon Redshift to query data

答案：B

385. A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts. AWS Site-to-Site VPN connections are configured between all of the company's global offices and the transit account. The company has AWS Config enabled on all of its accounts

The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices. Developers will reference this list to gain access to their applications securely

Which solution meets these requirements with the LEAST amount of operational overhead?

A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges. Configure an Amazon Simple Notification Service（Amazon SNS）topic in each of the accounts that can be invoked when the json file is updated. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with the updated IP address ranges

B. Create a new AWS Config managed rule that contains all of the internal IP address ranges. Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges. Configure the rule to automatically remediate any noncompliant security group that is detected

C. In the transit account, create a VPC　prefix list with all of the internal IP address ranges Use AWS Resource Access Manager to share the prefix list with all of the other accounts. Use the shared prefix list to configure security group rules in the other accounts

D. In the transit account, create a security group with all of the internal IP address ranges. Configure the security groups in the other accounts to reference the transit accounts security group by using a nested security group reference of “<transit-account-id>/sg-1a2b3c4d”

答案：B

386. A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet

of a VPC . After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp. example. com through the use of Amazon Route 53
What should a solutions architect do to improve the reliability and scalability of the SFTP solution?
A. Move the EC2 instance into an Auto Scaling group. Place the EC2 instance behind an Application Load Balancer（ALB）. Update the DNS record sftp. example. com in Route 53 to point to the ALB
B. Migrate the SFTP server to AWS Transfer for SFTP. Update the DNS record sftp. example. com in Route 53 to point to the server endpoint hostname
C. Migrate the SFTP server to a file gateway in AWS Storage Gateway. Update the DNS record sftp. example. com in Route 53 to point to the file gateway endpoint
D. Place the EC2 instance behind a Network Load Balancer (NLB) Update the DNS record sftp. example. com in Route 53 to point to the NLB
答案：A

387. A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS . The application data is stored on a shared file system on premises and the application servers connect to the shared file system through SMB
A solutions architect must implement a solution that uses an Amazon S3 bucket for shared storage. Until the application is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB. The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data
Which solution will meet these requirements?
A. Create a new Amazon FSX for Windows File Server file system Configure AWS DataSync with one location for the on-premises file share and one location for the new Amazon FSx file system. Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system
B. Create an S3 bucket for the application, Copy the data from the on-premises storage to the S3 bucket
C. Deploy an AWS Server Migration Service（AWS SMS）VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance
D. Create an S3 bucket for the application Deploy a new AWS Storage Gateway file gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the file gateway. Copy the data from the on-premises storage to the new file gateway endpoint
答案：D

388. A solutions architect uses AWS Organizations to manage several AWS accounts for a company. The full Organizations feature set is activated for the organization. All production AWS accounts exist under an OU that is named "production" Systems operators have full administrative privileges within these accounts by using IAM roles
The company wants to ensure that security groups in all production accounts do not allow inbound traffic for TCP port 22. All noncompliant security groups must be remediated immediately, and no new rules that allow port 22 can be created
Which solution will meet these requirements
A. Write an SCP that denies the CreateSecurityGroup action with a condition of ec2：Ingress rule with value 22. Apply the SCP to the "production" OU
B. Configure an AWS Cloud Trail trail for all accounts. Send Cloud Trail logs to an Amazon S3 bucket in the Organizations management account. Configure an AWS Lambda function on the management account with permissions to assume a role in all production accounts to describe and modify security groups. Configure Amazon S3 to invoke the Lambda function on every Putobject event on the S3 bucket. Configure the Lambda function to analyze each CloudTrail event for noncompliant security group actions and to automatically remediate any issues
C. Create an Amazon EventBridge（Amazon CloudWatch Events ）event bus in the Organizations management account. Create an AWS CloudFormation template to deploy configurations that send CreateSecurityGroup events to

the event bus from all production accounts. Configure an AWS Lambda function in the management account with permissions to assume a role in all production accounts to describe and modify security groups. Configure the event bus to invoke the Lambda function. Configure the Lambda function to analyze each event for noncompliant security group actions and to automatically remediate any issues

D. Create an AWS CloudFormation template to turn on AWS Config. Activate the INCOMING_SSH_DISABLED AWS Config managed rule. Deploy an AWS Lambda function that will run based on AWS Config findings and will remediate noncompliant resources. Deploy the CloudFormation template by using a StackSet that is assigned to the "production" ou. Apply an SCP to the OU to deny modification of the resources that the CloudFormation template provisions

答案：B

389. A company is deploying a new cluster for big data analytics on AWS . The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.

All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX) , and must accommodate high levels of throughput

Which storage solution will meet these requirements?

A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket. Mount the NFS file share on each EC2 instance in the cluster

B. Provision a new Amazon Elastic File System（Amazon EFS）file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster

C. Provision a new Amazon Elastic Block Store（Amazon EBS）volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster

D. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode. Mount the EFS file system on each EC2 instance in the cluster.

答案：B

390. A company that designs multiplayer online games wants to expand its user base outside of Europe. The company transfers a significant amount of UDP traffic to keep all the live and interactive sessions of the games. The company has plans for rapid expansion and wants to build its architecture to provide an optimized online experience to its users

Which architecture will meet these requirements with the LOWEST latency for users?

A. Set up a Multi-AZ environment in a single AWS Region. Use Amazon CloudFront to cache user sessions

B. Set up environments in multiple AWS Regions. Create an accelerator in AWS Global Accelerator, and add endpoints from different Regions to it

C. Set up environments in multiple AWS Regions Use Amazon Route 53，and select latency-based routing

D. Set up a Multi-AZ environment in a single AWS Region. Use AWS Lambda@ Edge to update sessions closer to the users

答案：C

391. A company has several applications running in an on-premises data center. The data center runs a mix of windows and Linux VMs managed by VMware vCenter. a solutions architect needs to create a plan to migrate the applications to AWS . However the solutions architect discovers that the documentation for the applications is not up to date and that there are no complete infrastructure diagrams. The company's developers lack time to discuss their applications and current usage with the solutions architect

What should the solutions architect do to gather the required information?

A. Deploy the AWS Server Migration Service（AWS SMS）connector using the OVA image on the VMware cluster to collect configuration and utilization data from the VMS

B. Use the AWS Migration Portfolio Assessment (MPA) tool to connect to each of the VMs to collect the configuration and utilization data

C. Install the AWS Application Discovery Service on each of the VMs to collect the configuration and utilization data

D. Register the on-premises VMs with the AWS Migration Hub to collect configuration and utilization data

答案：C

392. A new application is running on Amazon Elastic Container Service (Amazon ECS) with AWS Fargate. The application uses an Amazon Aurora MySQL database. The application and the database run in the same subnets of a VPC with distinct security groups that are configured

The password for the database is stored in AWS Secrets Manager and is passed to the application through the DB_PASSWORD environment variable. The hostname of the database is passed to the application through the DB_HOST environment variable. The application is failing to access the database

Which combination of actions should a solutions architect take to resolve this error? (Select THREE)

A. Ensure that the container has the environment variable with name "DB_PASSWORD" specified with a "ValueFrom" and the ARN of the secret

B. Ensure that the container has the environment variable with name "DB_PASSWORD" specified with a " ValueFrom" and the secret name of the secret

C. Ensure that the Fargate service security group allows inbound network traffic from the Aurora MysSQL database on the MySQL TCP port 3306

D. Ensure that the Aurora MySQL database security group allows inbound network traffic from the Fargate service on the MySQL TCP port 3306

E. Ensure that the container has the environment variable with name "DB_HOST" specified with the hostname of a DB instance endpoint

F. Ensure that the container has the environment variable with name "DB_HOST" specified with the hostname of the DB cluster endpoint

答案：ADE

393. A company is migrating its data center from on premises to the AWS Cloud. The migration will take several months to complete. The company will use Amazon route 53 for private DNS zones

During the migration, the company must keep its AWS services pointed at the VPC 's Route 53 Resolver for DNS. The company also must maintain the ability to resolve addresses from its on-premises DNS server. A solutions architect must set up DNS SO that Amazon EC2 instances can use native Route 53 endpoints to resolve on-premises DNS queries

Which configuration will meet these requirements?

A. Configure the VPC DHCP options set to point to on-premises DNS server IP addresses. Ensure that security groups for EC2 instances allow outbound access to port 53 on those DNS server IP addresses

B. Launch an EC2 instance that has DNS BIND installed and configured. Ensure that the security groups that are attached to the EC2 instance can access the on-premises DNS server IP address on port 53. Configure BIND to forward DNS queries to on-premises DNS server IP addresses. Configure each migrated EC2 instance's DNS settings to point to the BIND server IP address

C. Create a new outbound endpoint in Route 53, and attach the endpoint to the VPC . Ensure that the security groups that are attached to the endpoint can access the on-premises DNS server IP address on port 53. Create a new Route 53 Resolver rule that routes on-premises designated traffic to the on-premises DNS server

D. Create a new private DNS zone in Route 53 with the same domain name as the on-premises domain. Create a single wildcard record with the on-premises DNS server IP address as the record's address

答案：C

394. A company plans to refactor a monolithic application into a modern application design deployed on AWS . The

CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements:
-It should allow changes to be released several times every hour
-It should be able to roll back the changes as quickly as possible
Which design will meet these requirements?
A. Deploy a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances
B. Specify AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/ CD pipeline of the application. To deploy, swap the staging and production environment URLs.
C. Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment
D. Roll out the application updates as part of an Auto Scaling event using prebuilt AMIs. Use new versions of the AMIs to add instances, and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event
答案：B

395. A solutions architect is designing a data processing system that will use Amazon EC2 instances. Data that needs to be processed will wait in an Amazon Simple Queue Service（Amazon SQS ）queue. At least two data processing instances must run at all times
Which combination of actions will meet these requirements MOST cost-effectively? （Select TWO.）
A. Create a Spot Fleet with a target scaling policy that targets the acceptable backlog per instance Request two On-Demand Instances for minimum capacity. Use Spot Instances for additional capacity
B. Purchase two Reserved Instances for the target platform and instance type in the target AWS Region
C. Create On-Demand Capacity Reservations for two instances for the target platform and instance type in the target AWS Region
D. Create an Auto Scaling group that uses Spot Instance requests. Configure the scaling policy to scale with the size of the SQS queue. Set the minimum value to 2
E. Provision two Dedicated Hosts. Configure AWS Batch to use Spot Instances to supply additional capacity
答案：BD

396. A company manages an on-premises Java Script front-end web application. The application is hosted on two servers secured with a corporate Active Directory. The application calls a set of Java-based microservices on an application server and stores data in a clustered MySQL database. The application is heavily used during the day on weekdays. It is lightly used during the evenings and weekends
Daytime traffic to the application has increased rapidly, and reliability has diminish ed as a result. The company wants to migrate the application to AWS with a solution that eliminates the need for server maintenance, with an API to securely connect to the microservices
Which combination of actions will meet these requirements ？（Select THREE ）
A. Host the web application on Amazon S3. Use Amazon Cognito identity pools（federated identities）with SAML for authentication and authorization
B. Host the web application on Amazon EC2 with Auto Scaling. Use Amazon Cognito federation and Login with Amazon for authentication and authorization
C. Create an API layer with Amazon API Gateway Rehost the microservices on AWS Fargate containers
D. Create an API layer with Amazon API Gateway Rehost the microservices on Amazon Elastic Container Service （Amazon ECS）containers
E. Replatform the database to Amazon RDS for MySQL
F. Replatform the database to Amazon Aurora MySQL Serverless

答案：ACF

397. A solutions architect must analyze a company's Amazon EC2 instances and amazon Elastic Block Store（Amazon EBS）volumes to determine whether the company is using resources efficiently. The company is running several large, high-memory EC2 instances to host database clusters that are deployed in active/passive configurations. The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern

The solutions architect must analyze the environment and take action based on the findings

Which solution meets these requirements MOST cost-effectively?

A. Create a dashboard by using AWS Systems Manager OpsCenter Configure visualizations for Amazon Cloud Watch metrics that are associated with the EC2 instances and their EBS volumes. Review the dashboard periodically, and identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics

B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes. Create and review a dashboard that is based on the metrics. Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics

C. Install the Amazon CloudWatch agent on each of the EC2 instances. Turn on AWS Compute Optimizer, and let it run for at least 12 hours. Review the recommendations from Compute optimizer, and rightsize the EC2 instances as directed

D. Sign up for the AWS Enterprise Support plan. Turn on AWS Trusted Advisor. Wait 12 hours. Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed

答案：C

398. A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for 4 hours daily. sales traffic is lower outside of those peak hours

The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based on Amazon DynamoDB. The database table uses provisioned throughput mode with 100,000 RCUs and 80， 000 WCUs to match known peak resource consumption

The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff Which solution meets these requirements MOST cost-effectively?

A. Reduce the provisioned RCUs and WCUs

B. Change the DynamoDB table to use on-demand capacity

C. Enable Dynamo DB auto scaling for the table

D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day

答案：C

399. A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune dB cluster. The Neptune DB cluster is located in three subnets in a VPC

Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? （Select Two）

A. Create three public subnets in the Neptune VPC , and route traffic through an internet gateway Host the Lambda functions in the three new public subnets.

B. Create three private subnets in the Neptune VPC , and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets

C. Host the Lambda functions outside the VPC . Update the Neptune security group to allow access from the IP ranges of the Lambda functions

D. Host the Lambda functions outside the VPC . Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint

E. Create three private subnets in the Neptune VPC . Host the Lambda functions in the three new isolated subnets. Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint
答案：DE

400. A company is creating a sequel for a popular online game.A large number of users from all over the world will play the game within the first week after launch. Currently, the game consists of the following components deployed in a single AWS Region:
-Amazon S3 bucket that stores game assets
-Amazon DynamoDB table that stores player scores
A solutions architect needs to design a multi-Region solution that will reduce latency, improve reliability, and require the least effort to implement
What should the solutions architect do to meet these requirements?
A. Create an Amazon Cloud Front distribution to serve assets from the S3 bucket. Configure S3 Cross-Region Replication. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables
B. Create an Amazon Cloud Front distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication Create a new DynamoDB table in a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service（AWS DMS）with change data capture（CDC）
C. Create another S3 bucket in a new Region, and configure S3 Cross-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region
D. Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. Create an Amazon Cloud Front distribution and configure origin failover with two origins accessing the S3 buckets. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables
答案：C

401. A solutions architect needs to deploy an application on a fleet of Amazon EC2 Instances. The EC2 instances run in private subnets in an auto Scaling group. the application is expected to generate logs at a rate of 100 MB each second on each of the EC2 instances.
The logs must be stored in an Amazon S3 bucket so that an Amazon EMR cluster can consume them for further processing. The logs must be quickly accessible for the first 90 days and should be retrievable within 48 hours thereafter
What is the MOST cost-effective solution that meets these requirements?
A. Set up an S3 copy job to write logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a NAT instance within the private subnets to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier
B. Set up an S3 sync job to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive
C. Set up an S3 batch operation to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a NAT gateway with the private subnets to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive
D. Set up an S3 sync job to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier
答案：D

402. A company is running an application in the AWS Cloud. The application consists of microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. The company recently added a new REST API that was implemented in Amazon API Gateway. Some of the older microservices that run on EC2 instances need to call this new API

The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet

What should a solutions architect do to meet these requirements?

A. Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway. Use API Gateway to generate a unique API key for each microservice Configure the API methods to require the key

B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private

C. Modify the API Gateway to use IAM authentication. Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway. Move the API Gateway into a new VPC . Deploy a transit gateway and connect the VPCs

D. Create an accelerator in AWS Global Accelerator, and connect the accelerator to the API Gateway. Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication

答案：B

403. A company has deployed its corporate website in a VPC on two Amazon EC2 instances behind an Application Load Balancer（ALB）. The EC2 instances are deployed in private subnets. The ALB is in a public subnet. A route to an internet gateway exists in the public subnet route table. The company has deployed an Amazon CloudFront distribution with the ALB as the origin

The company's security team recently identified that malicious traffic is accessing the ALB directly. The company must deploy security controls to prevent common attack techniques, including cross-site scripting, and to protect against volumetric denials of service

Which strategy should a solutions architect recommend to meet these requirements?

A. Migrate the ALB to a private subnet. Associate an AWS WAF web ACL with the ALB. Update inbound rules on the ALB security group to allow traffic on port 443 only from CloudFront IP addresses

B. Associate an AWS WAF web ACL with the Cloud Front distribution. Configure an origin access identity （OAI）on the ALB to drop access attempts that do not originate from CloudFront.

C. Associate an AWS WAF web ACL with the CloudFront distribution. Configure CloudFront to add a custom header to the requests that are sent to the ALB. Configure advanced routing on the ALB to only forward requests that include the custom header that is set by CloudFront

D. Associate an AWS WAF web ACL with the Cloud Front distribution. Configure AWS WAF to add a custom header to the requests that are sent to the ALB. Configure advanced routing on the ALB to only forward requests that include the custom header that is set by CloudFront

答案：D

404. A company wants to host a new global website that consists of static content. A solutions architect is working on a solution that uses amazon Cloud front with an origin access identity（OAI）to access website content that is stored in a private Amazon S3 bucket

During testing, the solutions architect receives 404 errors from the S3 bucket. Error messages appear only for attempts to access paths that end with a forward slash, such as example. com/path/. These requests should return the existing S3 object path/index. html. Any potential solution must not prevent CloudFront from caching the content

What should the solutions architect do to resolve this problem?

A. Change the CloudFront origin to an Amazon API Gateway proxy endpoint. Rewrite the S3 request URL by using an

AWS Lambda function

B. Change the CloudFront origin to an Amazon API Gateway endpoint. Rewrite the S3 request URL in an AWS service integration

C. Change the CloudFront configuration to use an AWS Lambda @Edge function that is invoked by a viewer request event to rewrite the S3 request URL

D. Change the Cloud Front configuration to use an AWS Lambda @Edge function that is invoked by an origin request event to rewrite the S3 request URL.

答案：A

405. A company is running a data-intensive application on AWS . The application runs on a cluster of hundreds of Amazon EC2 instances. a shared file system also runs on several EC2 instances that store 200 TB of data. The application reads and modifies the data on the shared file system and generates a report. The job runs once monthly, reads a subset of the files from the shared file system, and takes about 72 hours to complete The compute instances scale in an auto Scaling group, but the instances that host the shared file system run continuously. The compute and storage instances are all in the same AWS Region

A solutions architect needs to reduce costs by replacing the shared file system instances. The file system must provide high performance access to the needed data for the duration of the 72-hour run

Which solution will provide the LARGEST overall cost reduction while meeting these requirements?

A. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Intelligent-Tiering storage class. Before the job runs each month, use Amazon FSX for Lustre to create a new file system with the data from Amazon S3 by using lazy loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete

B. Migrate the data from the existing shared file system to a large Amazon Elastic Block Store（Amazon EBS）volume with Multi-Attach enabled. Attach the EBS volume to each of the instances by using a user data script in the auto scaling group launch template. Use the EBS volume as the shared storage for the duration of the job. Detach the EBS volume when the job is complete

C. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Standard storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using batch loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete

D. Migrate the data from the existing shared file system to an Amazon S3 bucket. Before the job runs each month use AWS Storage Gateway to create a file gateway with the data from Amazon S3. Use the file gateway as the shared storage for the job. Delete the file gateway when the job is complete

答案：C

406. A company is running a large containerized workload in the AWS Cloud. The workload consists of approximately 100 different services. The company uses Amazon Elastic Container Service（Amazon ECS）to orchestrate the workload Recently, the company's development team started using AWS Fargate instead of Amazon EC2 instances in the ECS cluster. In the past, the workload has come close to running the maximum number of EC2 instances that are available in the account. The company is worried that the workload could reach the maximum number of ECS tasks that are allowed. A solutions architect must implement a solution that will notify the development team when Fargate reaches 80% of the maximum number of tasks

What should the solutions architect do to meet this requirement?

A. Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster. Set an alarm for when the math expression sample count/SERVICE_QUOTA（service）*100 is greater than 80 Notify the development team by using Amazon Simple Notification Service（Amazon SNS）

B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS / Usage metric namespace. Set an alarm for when the math expression metric/SERVICE QUOTA（metric）*100 is greater than 80 Notify the

development team by using Amazon Simple Notification Service（Amazon SNS）
C. Create an AWS Lambda function to poll detailed metrics from the ECS cluster. When the number of running Fargate tasks is greater than 80，invoke Amazon Simple Email Service（Amazon SES）to notify the development team
D. Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service（Amazon SES）to notify the development team when the AWS Config rule is not compliant
答案：A

407. A company has multiple business units. Each business unit has its own AWS account and runs a single website within that account. The company also has a single logging account. Logs from each business unit website are aggregated into a single Amazon S3 bucket in the logging account. The S3 bucket policy provides each business unit with access to write data into the bucket and requires data to be encrypted The company needs to encrypt logs uploaded into the bucket using a single AWS Key Management Service（AWS KMS）CMK. The CMK that protects the data must be rotated once every 365 days
Which strategy is the MOST operationally efficient for the company to use to meet these requirements?
A. Create a customer managed CMK in the logging account. Update the CMK key policy to provide access to the logging account only Manually rotate the CMK every 365 days
B. Create a customer managed CMK in the logging account. Update the CMK key policy to provide access to the logging account and business unit accounts. Enable automatic rotation of the CMK
C. Use an AWS managed CMK in the logging account. Update the CMK key policy to provide access to the logging account and business unit accounts. Manually rotate the CMK every 365 days
D. Use an AWS managed CMK in the logging account. Update the CMK key policy to provide access to the logging account only Enable automatic rotation of the CMK
答案：D

408. A company that runs applications on AWS recently subscribed to a new software-as-a-service（SaaS）data vendor. The vendor provides the data by way of a REST API that the vendor hosts in its AWS environment. The vendor offers multiple options for connectivity to the API and is working with the company to find the best way to connect
The company's AWS account does not allow outbound internet access from its AWS environment. The vendor's services run on AWS in the same AWS Region as the company's applications
A solutions architect must implement connectivity to the vendor's API so that the API is highly available in the company's VPC
Which solution will meet these requirements?
A. Connect to the vendor's public API address for the data service
B. Connect to the vendor by way of a VPC　peering connection between the vendor's VPC　and the company's VPC
C. Connect to the vendor by way of a VPC　endpoint service that uses AWS PrivateLink
D. Connect to a public bastion host that the vendor provides. Tunnel the API traffic
答案：B

409. A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services（AD Ds）on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC　must be accessible through a VPN. Multi-factor authentication（MFA）must be used for access to a VPN
What should a solutions architect do to meet these requirements?
A. Create an AWS Site-to-Site VPN connection. Configure integration between a VPN and AD DS. Use an Amazon Work Spaces client with MFA support enabled to establish a VPN connection
B. Create an AWS Client VPN endpoint. Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector. Use AWS Client VPN to establish a VPN connection

C. Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub Configure integration between AWS VPN CloudHub and AD DS. Use AWS Copilot to establish a VPN connection
D. Create an Amazon WorkLink endpoint Configure integration between Amazon WorkLink and AD ds. Enable MFA in Amazon WorkLink Use AWS Client VPN to establish a VPN connection
答案：B

410. A company's site reliability engineer is performing a review of Amazon FSx for Windows File server deployments within an account that the company acquired. Company policy states that all amazon FSx file systems must be configured to be highly available across Availability Zones
During the review, the site reliability engineer discovers that one of the Amazon FSx file systems used a deployment type of Single-AZ 2. A solutions architect needs to minimize downtime while aligning this Amazon FSx file system with company policy.
What should the solutions architect do to meet these requirements?
A. Reconfigure the deployment type to Multi-AZ for this Amazon FSX file system
B. Create a new Amazon FSx file system with a deployment type of Multi-AZ Use AWS Data Sync to transfer data to the new Amazon FSx file system. Point users to the new location
C. Create a second Amazon FSx file system with a deployment type of Single-AZ 2. Use AWS Data Sync to keep the data in sync. Switch users to the second Amazon FSx file system in the event of failure
D. Use the AWS Management Console to take a backup of the Amazon FSx file system. Create a new Amazon FSx file system with a deployment type of Multi-AZ Restore the backup to the new Amazon FSX file system. Point users to the new location
答案：B
411. A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPC s in either of those Regions. The company also needs to support traffic that is routed directly between VPC s in those Regions. No single points of failure can exist on the network
The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region
Which solution will meet these requirements?
A. Create a private VIF from the DX-A connection into a Direct Connect gateway. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway. peer the transit gateways with each other to support cross-Region routing
B. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Associate the eu-west-1 transit gateway with this Direct Connect gateway. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway Associate the us-east-1 transit gateway with this separate Direct Connect gateway. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing
C. Create a transit VIF from the DX-A connection into a Direct Connect gateway Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east.1 transit gateways with his Direct Connect gateway. Configure the Direct Connect gateway to route traffic between the transit gateways
D. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west- 1 and us-east-1 transit gateways with his Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing
答案：D

412. A video processing company has a fleet of Amazon EC2 Spot Instances. The company uses an Auto Scaling group to launch the EC2 instances. The fleet runs a custom processing service that requires a high amount of CPU for a short amount of time to modify a proprietary video format

The EC2 instances are configured by a user data script that runs the required service at launch and downloads the required video file from Amazon S3. The launch template uses burstable instance types in unlimited mode. The processing of each request takes an average of 20 minutes to complete

A solutions architect must review the existing architecture to determine whether the company is using resources properly

What should the solutions architect recommend to reduce the company s operational costs?

A. Replace the EC2 instances with an Amazon Elastic Transcoder pipeline. Invoke the pipeline by using Amazon S3 Event Notifications

B. Create a new version of the launch template. Edit the configuration options to change to burstable instance types in standard mode Change the Auto Scaling group to use the new launch template version

C. Create an AWS Batch job that uses the launch template that the Auto Scaling group uses Configure the job to use compute optimized instances on a Dedicated Host

D. Copy the custom application into a container image Upload the container image to Amazon Elastic Container Registry（Amazon ECR）. Create an AWS Lambda function to run the custom container image

答案：B

413. A company manages multiple AWS accounts by using AWS Organizations. Under the root ou, the company has two ous: Research and DataOps

Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types

A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance

Which combination of steps will meet these requirements? （Select TWO）

A. Create an IAM role in one account under the DataOps OU Use the ec2：InstanceType condition key in an inline policy on the role to restrict access to specific instance types

B. Create an IAM user in all accounts under the root ou. Use the AWS . RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1

C. Create an SCP. Use the AWS : RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU

D. Create an SCP. Use the ec2 Region condition key to restrict access to all AWS Regions except ap-northeast-1 Apply the SCP to the root ou, the DataOps ou, and the Research ou

E. Create an SCP. Use the ec2：Instance Type condition key to restrict access to specific instance types. Apply the SCP to the DataOps ou

答案：AE

414. A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances

Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

A. Create a script to copy log files to Amazon S3，and store the script in a file on the EC2 instance. Create an Auto Scaling lifecycle hook and an Amazon EventBridge（Amazon CloudWatch Events）rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling: EC2_INSTANCE_ TERMINATING

transition to send ABANDON to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK

B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3 Create an Auto Scaling lifecycle hook and an amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group Invoke an AWS Lambda function on the autoscaling EC2_INSTANCE_ TERMINATING transition to call the AWS Systems Manager API Send command operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance

C. Change the log delivery rate to every 5 minutes. Create a script to copy log files to Amazon S3，and add the script to EC2 instance user data. Create an Amazon Event Bridge（Amazon CloudWatch Events）rule to detect EC2 instance termination Invoke an AWS lambda function from the EvenBridge (CloudWatch Events）rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance

D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3 Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service（Amazon SNS） topic. From the SNS notification, call the AWS Systems Manager API Send Command operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance

答案：B

415. A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region, The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant

Which solution will meet these requirements?

A. Launch five new EC2 instances into a cluster placement group. Ensure that the EC2 instance type supports enhanced networking

B. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance O

C. Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking

D. Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance

答案：A

416. A company runs a software-as-a-service（SaaS）application on AWS . The application consists of AWS Lambda functions and an Amazon RDS for MySQL Multi-AZ database. During market events, the application has a much higher workload than normal. Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database

Which solution meets these requirements?

A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold

B. Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function

C. Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records D. Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools

答案：A

417. A company has a policy that all Amazon EC2 instances that are running a database must exist within the same subnets in a shared VPC . Administrators must follow security compliance requirements and are not allowed to directly log in to the shared account. All company accounts are members of the same organization in AWS

Organizations. The number of accounts will rapidly increase as the company grows
A solutions architect uses AWS Resource Access Manager to create a resource share in the shared account What is the MOST operationally efficient configuration to meet these requirements?
A. Add the VPC to the resource share. Add the account IDs as principals
B. Add all subnets within the VPC to the resource share. Add the account IDs as principals
C. Add all subnets within the VPC to the resource share. Add the organization as a principal
D. Add the VPC to the resource share. Add the organization as a principal
答案：C

418. A company wants to migrate its data analytics environment from on premises to AWS . The environment consists of two simple Node.js applications. One of the applications collects sensor data and loads it into a MySQL database. The other application aggregates the data into reports. When the aggregation jobs run, some of the load jobs fail to run correctly.
The company must resolve the data loading issue. The company also needs the migration to occur without interruptions or changes for the company's customers
What should a solutions architect do to meet these requirements?
A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer（NLB），and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced disable the replication job and restart the Aurora Replica as the primary instance, Point the collector DNS record to the NLB
B. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service（AWS DMS）to perform continuous data replication from the on-premises database to Aurora the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer（ALB）as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS
C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service（AWS DMS）to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer（ALB），and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS .
D. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database, and the aggregation jobs to run against the Aurora Replica Set up collection endpoints as an amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream
答案：C

419. A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration
What should the solutions architect do to meet these requirements
A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2
B. Use the VMware vSphere client to export the application as an image in Open Virtualization Format（OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command

C. Configure AWS Storage Gateway for files service to export a Common Internet File System（CIFS）share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI
D. Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI Launch an EC2 instance that is based on the AMI
答案：A

420. A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and in internet gateway. Each public subnet also contains a NAT gateway. Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets.
A solutions architect must review the infrastructure. The solutions architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-other category is consistently high. A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category
What should the solutions architect do to meet these requirements?
A. Enable VPC Flow Logs Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs
B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC . Ensure that applications have the correct IAM permissions to use the interface VPC endpoint
C. Enable VPC Flow Logs and Amazon Detective Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic
D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC . Ensure that the VPC endpoint policy allows traffic from the applications
答案：D

421. A company wants to use a hybrid cloud architecture between an on-premises data center and AWS . The company already has deployed a multi-account structure in AWS Organizations while following the AWS Well-Architected Framework. Due to strict security requirements, connectivity between the data center and AWS must be encrypted in transit. Only a single entry point into AWS is permitted from the data center. The data center must be able to access all the AWS accounts.
Which solution meets these requirements?
A. Connect the AWS accounts with AWS Transit Gateway. Establish an AWS Site-to-Site VPN connection with the data center, and attach the connection to the transit gateway. Route traffic from the data center to all AWS accounts
B. Connect the AWS accounts with VPC peering Establish an AWS Site-to-Site VPN connection with the data center. Route traffic from the data center to all AWS accounts
C. Connect the AWS accounts with VPC peering. Establish an AWS Direct Connect connection to the closest AWS Region. Route traffic from the data center to all AWS accounts
D. Connect the AWS accounts with AWS Transit Gateway. Establish an AWS Direct Connect connection to the closest AWS Region, and attach the connection to the transit gateway Route traffic from the data center to all AWS accounts
答案：A

422. A company is running an application distributed over several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The security team requires that all application access attempts be made available for analysis. Information about the client IP address, connection type, and user agent must be included
Which solution will meet these requirements?
A. Enable EC2 detailed monitoring, and include network logs. Send all logs through Amazon Kinesis Data Firehose to

an Amazon Elasticsearch Service（Amazon ES）cluster that the security team uses for analysis
B. Enable VPC　Flow Logs for all EC2 instance network interfaces. Publish VPC　Flow Logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs
C. Enable access logs for the Application Load Balancer, and publish the logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs
D. Enable Traffic Mirroring and specify all EC2 instance network interfaces as the source. Send all traffic information through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis
答案：C

423. A company is running multiple workloads in the AWS Cloud. The company has separate units for software development. The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources in their AWS accounts. The development units each deploy their production workloads into a common production account
Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a similar incident from happening in the future. The solution also must allow developers the possibility to manage the instances used for their workloads
Which strategy will meet these requirements?
A. Create separate ous in AWS Organizations for each development unit. Assign the created ous to the company AWS accounts. Create separate SCPs with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU
B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service（AWS STS）session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and AWS : PrincipalTag/ DevelopmentUnit
C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service（AWS STS）session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and AWS :PrincipalTag/ DevelopmentUnit. Assign the SCP to the root OU
D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service（AWS STS）to assign the IAM policy and match the development unit name to the assumed IAM role
答案：A

424. A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode. Once each day at midnight, a few million new records are loaded into the table. Application read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB
Which strategy should a solutions architect recommend to meet this requirement?
A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table
B. Deploy DynamoDB Accelerator (DAX) . Configure DynamoDB auto scaling. Purchase Savings Plans in Cost Explorer
C. Use provisioned capacity mode. Purchase Savings Plans in Cost Explorer
D. Deploy DynamoDB Accelerator（DAX）. Use provisioned capacity mode. Configure DynamoDB auto scaling
答案：B

425. A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance. The DB instance is expected to receive many more reads than writes. The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available

Which steps should the solutions architect take to meet these requirements? (Select THREE)
A. Create multiple read replicas and put them into an Auto Scaling group
B. Create multiple read replicas in different Availability Zones
C. Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy
D. Create an Application Load Balancer（ALB）and put the read replicas behind the ALB
E. Configure an Amazon CloudWatch alarm to detect a failed read replica. Set the alarm to directly invoke an AWS Lambda function to delete its Route 53 record set
F. Configure an Amazon Route 53 health check for each read replica using its endpoint
答案：BCE

426. A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application the instances that run in the Auto Scaling group are constantly changing because of scaling events
When the company deploys new application code versions the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours
What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?
A. Configure Amazon EventBridge（Amazon CloudWatch Events）to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group
B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches Resume Amazon EC2 Auto Scaling operations
C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure Code Build to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation
D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling groups launch template to use the new AMI. Associate the Code Deploy deployment group with the Auto Scaling group instead of the EC2 instances
答案：C

427. A large company is running a popular web application. The application runs on several Amazon EC2 Linux instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the instances in the auto Scaling group in the private subnet. AWS Systems Manager Session Manager is configured, and AWS Systems Manager Agent is running on all the EC2 instances
The company recently released a new version of the application. Some EC2 instances are now being marked as unhealthy and are being terminated. As a result, the application is running at reduced capacity. A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are inconclusive
How should the solutions architect gain access to an EC2 instance to troubleshoot the issue?
A. Suspend the Auto Scaling group's Health Check scaling process. Use Session Manager to log in to an instance that is marked as unhealthy
B. Enable EC2 instance termination protection Use Session Manager to log in to an instance that is marked as unhealthy
C. Set the termination policy to Oldestinstance on the Auto Scaling group Use Session Manager to log in to an instance that is marked as unhealthy

D. Suspend the Auto Scaling group's Terminate process Use Session Manager to log in to an instance that is marked as unhealthy
答案：B

428. A company wants to control its cost of Amazon Athena usage. The company has allocated a specific monthly budget for Athena usage. A solutions architect must design a solution that will prevent the company from exceeding the budgeted amount Which solution will meet these requirements?
A. Use AWS Budgets. Create an alarm for when the cost of Athena usage reaches the budgeted amount for the month. Configure AWS Budgets actions to deactivate Athena until the end of the month
B. Use Cost Explorer to create an alert for when the cost of Athena usage reaches the budgeted amount for the month. Configure Cost Explorer to publish notifications to an Amazon Simple Notification Service（Amazon SNS）topic
C. Use AWS Trusted Advisor to track the cost of Athena usage. Configure an Amazon EventBridge（Amazon CloudWatch Events）rule to deactivate Athena until the end of the month whenever the cost reaches the budgeted amount for the month
D. Use Athena workgroups to set a limit on the amount of data that can be scanned. Set a limit that is appropriate for the monthly budget and the current pricing for Athena
答案:A

429. A company wants to migrate a 30 TB Oracle data warehouse from on premises to Amazon Redshift. The company used the AWS Schema Conversion Tool（AWS SCT）to convert the schema of the existing data warehouse to an Amazon Redshift schema. The company also used a migration assessment report to identify manual tasks to complete
The company needs to migrate the data to the new Amazon Redshift cluster during an upcoming data freeze period of 2 weeks. The only network connection between the on-premises data warehouse and AWS is a 50 Mbps internet connection
Which migration strategy meets these requirements?
A. Create an AWS Database Migration Service (AWS DMS) replication instance. Authorize the public IP address of the replication instance to reach the data warehouse through the corporate firewall. Create a migration task to run at the beginning of the data freeze period
B. Install the AWS SCT extraction agents on the on-premises servers. Define the extract, upload, and copy tasks to send the data to an Amazon S3 bucket. Copy the data into the Amazon Redshift cluster. Run the tasks at the beginning of the data freeze period
C. Install the AWS SCT extraction agents on the on-premises servers.Create a Site-to-Site VPN connection. Create an AWS Database Migration Service（AWS DMS）replication instance that is the appropriate size Authorize the IP address of the replication instance to be able to access the on-premises data warehouse through the VPN connection
D. Create a job in AWS Snowball Edge to import data into Amazon S3. Install AWS SCT extraction agents on the on-premises servers. Define the local and AWS Database Migration Service（AWS DMS）tasks to send the data to the Snowball Edge device. When the Snowball Edge device is returned to AWS and the data is available in Amazon S3, run the AWS DMS subtask to copy the data to Amazon Redshift
答案：D

430. A company is serving files to its customers through an SFTP server that is accessible over the internet. The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached. Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses
A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure

management, and minimize the disruption to customers who access files. The solution must not change the way customers connect

Which solution will meet these requirements?

A. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket

B. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC -hosted, internet-facing endpoint Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket

C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System（Amazon EFS）file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer（NLB）in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server Associate IP address with the NLB. Sync all files from the SFTP server to the S3 bucket

D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store（Amazon EBS）volume to be used for SFTP file hosting. Create a Network Load Balancer（NLB）with the Elastic IP address attached Create an Auto Scaling group with EC2 instances that run an SFTP server, Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume Configure the Auto Scaling group to automatically add stances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto scaling group launches, Sync all files from the SFTP server to the new multi-attach EBS volume

答案：B

431. A company is building a hybrid solution between its existing on-premises systems and a new backend in AWS . The company has a management application to monitor the state of its current IT infrastructure and automate responses to issues. The company wants to incorporate the status of its consumed AWS services into the application. The application uses an Https endpoint to receive updates

Which approach meets these requirements with the LEAST amount of operational overhead?

A. Configure AWS Systems Manager OpsCenter to ingest operational events from the on-premises systems. Retire the on-premises management application and adopt OpsCenter as the hub

B. Configure Amazon EventBridge（Amazon CloudWatch Events）to detect and react to changes for AWS Health events from the AWS Personal Health Dashboard. Configure the EventBridge（CloudWatch Events）event to publish a message to an Amazon Simple Notification Service（amazon SNS）Topic and subscribe the topic to the HTTPS endpoint of the management application

C. Modify the on-premises management application to call the AWS Health API to poll for status events of AWS services

D. Configure Amazon EventBridge（Amazon CloudWatch Events）to detect and react to changes for AWS Health events from the AWS Service Health Dashboard. Configure the EventBridge（CloudWatch Events）event to publish a message to an Amazon Simple Notification Service（Amazon SNS）topic and subscribe the topic to an HTTPS endpoint for the management application with a topic filter corresponding to the services being used

答案：D

432.A solutions architect is migrating a legacy Oracle database from an on-premises server to AWS . Initially, the database will be deployed to an existing Amazon Elastic Block Store（Amazon EBS）-backed Amazon EC2 instance

that has several EBS volumes
As part of the migration, the solutions architect must create a new EBS volume and must attach the EBS volume to the EC2 instance. This EBS volume will be used solely by an application that stores historical customer order data that is accessed frequently. Cost-effectiveness is more important than performance for this data
Which solution meets these requirements MOST cost-effectively?
A. Migrate the database by using AWS Server Migration Service（AWS SMS）. Use a Provisioned IOPS SSD（io2）EBS volume
B. Migrate the database by using AWS Database Migration Service（ AWS DMS）. Use a General Purpose SSD (gp2) EBS volume
C. Migrate the database by using AWS Server Migration Service（AWS SMS）. Use a Provisioned IOPS SSD （io1）EBS volume
D. Migrate the database by using AWS Database Migration Service（AWS DMS）. Use a Throughput Optimized HDD （st1）EBS volume
答案：B

433. A scientific company needs to process text and image data from an Amazon S3 bucket. The data is collected from several radar stations during a live, time-critical phase of a deep space mission. The radar stations upload the data to the source S3 bucket. The data is prefixed by radar station identification number. The company created a destination S3 bucket in a second account Data must be copied from the source S3 bucket to the destination S3 bucket to meet a compliance objective. This replication occurs through the use of an S3 replication rule to cover all objects in the source S3 bucket
One specific radar station is identified as having the most accurate data. Data replication at this radar station must be monitored for completion within 30 minutes after the radar station uploads the objects to the source S3 bucket
What should a solutions architect do to meet these requirements?
A. Set up an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge（Amazon CloudWatch Events）rule to trigger an alert if this status changes
B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge（Amazon CloudWatch Events）rule to trigger an alert when the time exceeds the desired threshold
C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge（Amazon CloudWatch Events）rule to trigger an alert if this status changes D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data Enable S3 Replication Time Control（S3 RTC）Monitor the maximum replication time to the destination. Create an Amazon EventBrdge（Amazon CloudWatch Events）rule to trigger an alert when the time exceeds the desired threshold
答案：D

434. A company is running a line-of-business（LOB）application on AWS to support its users. The application runs in one VPC , with a backup copy in a second VPC in a different AWS Region for disaster recovery. The company has a single AWS Direct Connect connection between its on-premises network and AWS . The connection terminates at a Direct Connect gateway
All access to the application must originate from the company's on-premises network, and traffic must be encrypted in transit through the use of IPsec. The company is routing traffic through a VPN tunnel over the Direct Connect connection to provide the required encryption

A business continuity audit determines that the Direct Connect connection represents a potential single point of failure for access to the application. The company needs to remediate this issue as quickly as possible
Which approach will meet these requirements?
A. Order a second Direct Connect connection to a different Direct Connect location. Terminate the second Direct Connect connection at the same Direct Connect gateway
B. Configure an AWS Site-to-Site VPN connection over the internet. Terminate the VPN connection at a virtual private gateway in the secondary Region
C. Create a transit gateway. Attach the VPC s to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to-Site VPN connection, and terminate it at the transit gateway
D. Create a transit gateway. Attach the VPC s to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Order a second Direct Connect connection, and terminate it at the transit gateway
答案：C

435. A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances
A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPC s
Which steps should the solutions architect recommend to meet these requirements? (Select THREE)
A. Deploy two firewall appliances into the shared services VPC , each in a separate Availability Zone
B. Create a new Network Load Balancer in the shared services VPC . Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group
C. Create a new Gateway Load Balancer in the shared services VPC . Create a new target group, and attach it to the new Gateway Load Balancer. Add each of the firewall appliance instances to the target group
D. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPC s
E. Deploy two firewall appliances into the shared services VPC , each in the same Availability Zone
F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPC s
答案：ACF

436. A software company has deployed an application that consumes a REST API by using Amazon API Gateway, AWS Lambda functions, and an Amazon DynamoDB table. The application is showing an increase in the number of errors during PUT requests. Most of the Put calls come from a small number of clients that are authenticated with specific API keys
A solutions architect has identified that a large number of the PUT requests originate from one client. The API is noncritical, and clients can tolerate retries of unsuccessful calls. However, the errors are displayed to customers and are causing damage to the API's reputation
What should the solutions architect recommend to improve the customer experience?
A. Implement retry logic with exponential backoff and irregular variation in the client application. Ensure that the errors are caught and handled with descriptive error messages
B. Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error
C. Turn on API caching to enhance responsiveness for the production stage. Run 10-minute load tests. Verify that the cache capacity is appropriate for the workload
D. Implement reserved concurrency at the Lambda function level to provide the resources that are needed during sudden increases in traffic

答案：B

437. A media company uses Amazon DynamoDB to store metadata for its catalog of movies that are available to stream. Each media item contains user-facing content that includes a description of the media, a list of searchable tags, and other similar data. In addition, media items include a list of Amazon S3 key names that relate to movie files. The company stores these movie files in a single S3 bucket that has versioning enabled. The company uses Amazon CloudFront to serve these movie files

The company has 100,000 media items, and each media item can have many different S3 objects that represent different encodings of the same media. S3 objects that belong to the same media item are grouped together under the same key prefix. Which is a random unique ID.

Because of an expiring contract with a media provider, the company must remove 2,000 media items. The company must completely delete all DynamoDB keys and movie files on Amazon S3 that are related to these media items within 36 hours. The company must ensure that the content cannot be recovered

Which combination of actions will meet these requirements ?

A. Configure the DynamoDB table with a TTL field. Create and invoke an AWS Lambda function to perform a conditional update. Set the TTL field to the time of the contract's expiration on every affected media item

B. Configure an S3 Lifecycle object expiration rule that is based on the contract's expiration date

C. Write a script to perform a conditional delete on all the affected DynamoDB records

D. Temporarily suspend versioning on the S3 bucket. Create and invoke an AWS Lambda function that deletes affected objects. Reactivate versioning when the operation is complete.

E. Write a script to delete objects from Amazon S3. Specify in each request a NoncurrentVersionExpiration property with a NoncurrentDays attribute set to 0

答案：AE

438. A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us-east-1 Region. The files range in size from 1 GB to 10 GB

Users who access the app from Australia have experienced uploads that take long periods of time. Sometimes the files fail to completely upload for these users. A solutions architect must improve the app's performance for these uploads

Which solutions will meet these requirements? （Select TWO）

A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads

B. Configure an S3 bucket in each Region to receive the uploads. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket

C. Set up amazon route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region D. D.Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3

E. Modify the app to add random prefixes to the files before uploading

答案：AD

439. A large company has a business-critical application that runs in a single AWS Region. The application consists of multiple Amazon EC2 instances and an Amazon RDS Multi-AZ DB instance. The EC2 instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones

A solutions architect is implementing a disaster recovery（DR）plan for the application. The solutions architect has created a pilot light application deployment in a new Region, which is referred to as the DR Region. The DR environment has an Auto Scaling group with a single EC2 instance and a read replica of the RDS DB instance

The solutions architect must automate a failover from the primary application environment to the pilot light environment in the RD Region

Which solution meets these requirements with the MOST operational efficiency?

A. Publish an application availability metric to Amazon CloudWatch in the DR Region from the application environment in the primary Region. Create a Cloud Watch alarm in the DR Region that is invoked when the application availability metric stops being delivered. Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service（Amazon SNS）topic in the DR Region. Add an email subscription to the SNS topic that sends messages to the application owner. Upon notification, instruct a systems operator to sign in to the AWS Management Console and initiate failover operations for the application
B. Create a cron task that runs every 5 minutes by using one of the application's EC2 instances in the primary Region. Configure the cron task to check whether the application is available Upon failure, the cron task notifies a systems operator and attempts to restart the application services
C. Create a cron task that runs every 5 minutes by using one of the application's EC2 instances in the primary Region. Configure the cron task to check whether the application is available. Upon failure, the cron task modifies the DR environment by promoting the read replica and by adding EC2 instances to the Auto scaling group
D. Publish an application availability metric to Amazon Cloud Watch in the DR Region from the application environment in the primary Region. Create a CloudWatch alarm in the DR Region that is invoked when the application availability metric stops being delivered. Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service（Amazon SNS）topic in the DR Region. Use an AWS Lambda function that is invoked by Amazon SNS in the DR Region to promote the read replica and to add EC2 instances to the Auto Scaling group
答案：D

440.A solutions architect is importing a VM from an on-premises environment by using the Amazon EC2 VM Import feature of AWS Import/Export. The solutions architect has created an AMI and has provisioned an Amazon EC2 instance that is based that AMI. The EC2 instance runs inside a public subnet in a VPC and has a public IP address assigned
The EC2 instance does not appear as a managed instance in the AWS Systems Manager console
Which combination of steps should the solutions architect take to troubleshoot this issue? （Select Two.）
A.Verfy that Systems Manager Agent is installed on the instance and is running
B.Verify that the instance is assigned an appropriate IAM role for Systems Manager
C.verity the existence of a VPC endpoint on the VPC
D.Verify that the AWS Application Discovery Agent is configured
E. Verify the correct configuration of service-linked roles for Systems Manager
答案：AB

441. A greeting card company recently advertised that customers could send cards to their favorite celebrities through the company 's platform. Since the advertisement was published, the platform has received constant traffic from 10, 000 unique each er（ALB） The instances run in an Auto Scaling group and use a custom AMI that is based on Amazon Linux. The platform uses a highly available amazo Aurora My SQL DB cluster that uses primary and reader endpoints, The platform also uses an Amazon Elasti Cache for Redis cluster that uses its cluster endpoint
The platform generates a new process for each customer and holds open database connections to My SQL for the duration of each customers session. However, resource usage for the platform is low
Many customers are reporting errors when they connect to the platform. Logs show that connections to the aurora database are failing. Amazon Cloudwatch metrics show that the CPU load is low across the platfom and that connections to the platform successful through the ALB
Which solution will remediate the errors MOST cost-effectively?
A.Set up an Amazon CloudFront distribution. Set the ALB as the origin. Move all customer traffic to the CloudFront distribution endpoint
B.Use Amazon RDS Proxy Reconfigure the database connections to use the proxy

C. Increase the number of reader nodes in the Aurora MySQL cluster
D.Increase the number of nodes in the ElastiCache for Redis cluster
答案：C
解析:
出错的日志显示连接到 aurora 出错，是后端达到上限了，需要添加新的 Read rep

442. A company has a new security policy. The policy requires the company to log any event that retrieves data from Amazon S3 buckets. The company must save these audit logs in a dedicated s3 bucket.
The company created the audit logs s3 bucket in an AWS account that is designated for centralized logging. The S3 bucket has a bucket policy that allows write-only cross-account access
A solutions architect must ensure that all S3 object-level is being logged for current S3 buckets and ture S3 buckets
Which solution will meet these requirements?
A. Enable server access logging for all current S3 buckets. Use the audit logs S3 bucket as a destination for audit logs
B.Enable replication between all current S3 buckets and the audit logs S3 bucket Enable S3 Versioning in the audit logs S3 bucket
C. Configure S3 Event Notifications for all current S3 buckets to invoke an AWS Lambda function every time objects are accessed. Store Lambda logs in the audit logs S3 bucket.
D.Enable AWS CloudTrail, and use the audit logs S3 bucket to store logs. Enable data event logging for S3 event sources, current S3 buckets, and future S3 buckets
答案：c

443. A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts.
A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts
Which solution meets these requirements?
A. Create an AWS Cost and Usage Report （ CUR）for each OU by using AWS Resource Access Manager, Allow each team to visualize the CUR through an Amazon QuickSight dashboard
B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard
C. Create an AWS Cost and Usage Report（CUR） in each AWS Organizations member account Allow each team to visualize the CUR through an AmazonQuickSight dashboard
D. Create an AWS Cost and Usage Report （ CUR）by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager Ops Center dashboards
答案：B

444. A company is migrating applications from to the AWS Cloud. These applications power the company's intemal web forms. These web forms collect data for specific events several times each quarter. The web forms use simple SQL statements to save the data to a local relational database
Data collection occurs for each event, and the on premises servers are idle most of the time. The company needs to minimize the amount of idle infrastructure that supports the web forms
which solution will meet these requirements?
A. Use Amazon EC2 Image Builder to create AMIs for the legacy servers Use the AMIs to provision EC2 instances to recreate the applications in the AWS Cloud, Place an Application Load Balancer（ALB）in front of the EC2 instances Use Amazon Route 53 to point the dNs names of the web forms to the ALB.
B. Create one Amazon DynamoDB table to store data for all the data input. Use the application form name as the table key to distinguish data items. Create an Amazon Kinesis data stream to receive the data input and store the input in DynamoDB Use Amazon Route 53 to point the DNS names of the web forms to the Kinesis data streams

endpoint

C. Create Docker images for each server of the legacy web form applications. Create an Amazon Elastic Container Service（Amazon ECS）cluster on AWS Fargate Place an Application Load Balancer in front of the Ecs cluster Use Fargate task storage to store the web form data

D. Provision an Amazon Aurora Serverless cluster. Build multiple schemas for each web forms data storage. Use Amazon API Gateway and an AWS Lambda function to recreate the data input forms Use Amazon route 53 to point the dNS names

答案：B

445.A health insurance stores personally identifiable information（PII）in an Amazon S3 bucket. The company uses server-side encryption with s3 managed encryption keys （ssE-S3） to encrypt the objects. According to a new requirement, all and future objects in the s3 bucket must be encrypted by keys that the company's se am manages The s3 bucket does not have versioning enabled Which solution will meet these requirements

A. In the s3 bucket properties, change the default encryption to ssE-S3 with a customer managed key. Use the AWS CLI to re-upload all objects in the S3 bucket Set an S3 bucket policy to deny unencrypted Putobject requests

B. the S3 bucket properties change the default encryption to server- side encryption with AWS KMS managed encryption keys（SSE KMS） Set an S3 bucket policy to deny unencrypted Putobject requests Use the AWS CLI to re-upload all objects

C. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys （SSE-KMS） Set an s3 bucket policy to automatically encrypt objects on getobject and Putobject requests

D. the S3 bucket properties, change the default encryption to AES-256 with a customer managed key. Attach a policy to deny unencrypted Putobject requests to any entities that access the s3 bucket Use the AWS CLI to re-upload all objects in

答案：c

446. A company is using an Amazon EMR cluster to run its big data jobs. The cluster's jobs are invoked by AWS Step Functions Express workflows that consume various Amazon Simple Queue Service（Amazon SQS ）queues. The workload of this solution is variable and unpredictable. Amazon CloudWatch metrics show that the cluster“s peak utilization is only 25% at times and that the cluster sits idle the rest of the time.

A solutions architect must optimize the costs of the cluster without negatively impacting the time it takes to run the various jobs

What is the MosT cost-effective solution that meets these requirements?

A.Modify the EMR cluster by turning on automatic scaling of the core nodes and task nodes with a custom policy that is based on cluster utilzation. Purchase Reserved Instance capacity to cover the master node

B.Modify the EMR cluster to use an instance fleet of Dedicated On-Demand Instances for the master node and core nodes, and to use Spot Instances for the task nodes Define target capacity for each node type to cover the load

C.Purchase Reserved Instances for the master node and core nodes. Terminate all existing task nodes in the EMR cluster.

D.Modify the EMR cluster to use capacity-optimized Spot Instances and a diversified task fleet. Define target capacity for each node type with a mix of On-Demand Instances and Spot Instances

答案：B

447. A company has multiple AWS accounts. The company recently had a security audit that revealed many unencrypted Amazon Elastic Block Store（Amazon EBS） volumes to Amazon EC2 instances

A solutions architect must encrypt the unencrypted volumes and ensure that unencrypted volumes will be detected automatically in the future. Additionally, the company wants a solution that can centrally manage multiple AWS accounts with a focus on compliance and security

Which combination of steps should the solutions architect take to meet these requirements? (Select TwO)

A.Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended guardrails, Join all accounts to the organization. Categorize the AWS accounts into ous

B.Use the AWS CLI to list all the unencrypted volumes in all the AWS accounts Run a script to encrypt all the unencrypted volumes in place

C.Create a snapshot of each unencrypted volume. Create a new encrypted volume from the unencrypted snapshot Detach the existing volume, and replace it with the encrypted volume

D. Create an organization in AWS Organizations Set up AWS Control Tower, and turn on the mandatory guardrails. Join all accounts to the organization. Categorize the AWS accounts into ous

E.Turn on AWS CloudTrail Configure an Amazon EventBridge (Amazon CloudWatch Events) rule to detect and automatically encrypt unencrypted volumes

答案：AE

448. A company is migrating an application to the AWS Cloud. The application runs in an on-premises data center and writes thousands of images into a mounted NFs file system each night After the company migrates the applicatio the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system company has established an AWS Direct Connect connection to AWS . Before the migration cutover, a solutions architect must build a process that will replicate the newly created on-premises images to the EFS file system

What is the MOsT operationally efficient way to replicate the images

A.Cofigure a penodic process to run the AWS s3 sync command from the on-premises file system to Amazon s3. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon s3 to the EFS

B.Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point

C.Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an S3 bucket by using a public VIF. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system

D. Deploy an AWS DataSync agent to an on premises server that has access to the NFS file system. Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Configure a Data Sync scheduled task to send the images to the EFS file system every 24 hours

答案：D

449. A solutions architect is designing a solution to connect a compan's on-premises network with all the company's current and future VPC s on AWS . The company is running VPC s in five different AWS Regions and has at least 15 VPC s in each Region must be able to communicate with each other

The solution must maximize scalability and ease of management

Which solution meets these requirements

A. Set up a transit gateway in each Region. Establish a redundant AWS Site-to-Site VPN connection between the on-premises firewalls and the transit gateway in the Region that is closest to the on-premises network. Peer with each other. Connect all the VPC s to the transit gateway in their Region

B. Create an AWS CloudFormation template for a redundant AWS Site- to- Site vPn tunnel to the on-premises network. Deploy the CloudFormation template for each VPC . Set up VPC peering between all the VPC s for VPC -to-VPC communication

C. Set up a transit gateway in each Region. Establish a redundant AWS Site to- Site VPN connection between the on-premises firewalls and each transit gateway Route traffic between the different Regions through the company's on-premises firewalls. Connect all the VPC s to the transit gateway in their Region

D. Create an AWS CloudFormat plate for a redundant AWS Site- to Site VPN tunnel to the on-premises network. Deploy the CloudFormation template for each VPC . Route traffic between the different Regions through the

company s on-premises firewalls
答案：C

450. A software is using three AWS accounts for each of its 10 development teams. The company has developed an AWS CloudFomation standard VPC template that includes three NaT gateways. The template is added to each account for each team. The company is concerned that network costs will increase each time a new development team is added. A solutions architect must maintain the reliability of the company s solutions and minimize operational complexity
What should the solutions architect do to reduce the network costs while meeting these requirements?
A. ate a single VPC with three NAT gateways in a shared services account Configure each account VPC with a default route through a transit gateway to the nat gateway in the shared services account VPC . Remove all NAT gateways from the andard VPC template
B. Create a single VPC with three nat gateways in a shared services account Configure each account VPC with a default route through a VPC peering connection to the nat gateway in the shared services account VPC . Remove all NAT gateways from the standard VPC template
C. Remove two NaT gateways from the standard VPC template Rely on the nat gateway SLA to cover reliability for the remaining NAT gateway
D. Create a single VPC with three naT gateways in a shared services account Configure a Site-to-Site vPN connection from each account to the shared services account. Remove all NaT gateways from the standard VPC template
答案：A

451. A company runs a servertess application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to ar Amazon Simple Queue Service (Amazon SQS) queue. An AWS Lambda function uses the queue as an event source and processes the URLs from the queue. Results are saved to an Amazon S3 bucket
The company wants to process each URL in other Regions to compare possible differences in site localization, URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region
Which combination of changes will produce multi-Region deployment that meets these requirements ? (Select Two)
A.Deploy the SQS queue with the Lambda function to other Regions
B.Subscribe the SNS topic in each Region to the SQS queue
C.Subscribe the SQS queue in each Region to the SNS topic
D.Configure the SQS queue to publish URLs to SNS topics in each Regio
E.Deploy the SNS topic and the Lambda function to other Regions
答案：CE
解析:
D 没什么用，这题的顺序是用各区的 SNS 发布消息到每个区的 SQS ， 然后用 Lambda 去处理

452. A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose.
The solutions architect created the following IAM policy and attached it to an IAM role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DownloadUpload",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::BucketName/*"
        },
        {
            "Sid": "KMSAccess",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:kms:Region:Account:key/Key ID"
        }
    ]
```

During tests, the solutions architect was able to successfully get existing test objects in the s3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden

Which action must the solutions architect add to the IAM policy to meet all the requirements?

A.Kms:Generate DataKey

B.kms :GetKey policy

C.kms:GetPublicKey

D.kms:sign

答案：A

解析：

A 生成 CSE 需要 GenerateDataKey

453. A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWs managed database service. A solutions architect must design a heterogeneous database migration on AWS

Which solution will meet these requirements?

A.Migrate the SQL Server databases to Amazon RDS for My SQL by using backup and restore utilities

B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDs for My sQL Use s3 integration with SQL Server features, such as BULK INSERT

C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MysQL Then use AWS Database Migration Service（AWS DMS）to migrate the data from on-premises databases to Amazon RDS

D. Use AWS datasync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDs for MysQL Use s3 integration with SQL Server features, such as BULK INSERT

答案：c

解析：

SQL Server 迁移变成 Mysql 需要 SCT 转换，所以选 C

454. A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health,

accepting user requests.distributing user requests to worker nodes, and sending an aggregate response back to a client Worker nodes communicate with each other to replicate data partitions
The company requires the lowest possible networking latency to achieve maximum performance
Which solution will meet these requirements?
A.Launch memory optimized EC2 instances in a partition placement group
B.Launch compute optimized EC2 instances in a partition placement group
C.Launch memory optimized EC2 instances in a cluster placement group
D. Launch compute optimized EC2 instances in a spread placement group
答案：C
解析:
C 需要最短延时，需要集群模式置放群组

455. A large company runs workloads in VPC s that are deployed across hundreds of AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones. nat gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets
A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPC s must route traffic to the internet through an egress VPC . The solutions architect already has deployed a nat gateway in an egress VPC in a central AWS account
Which set of additional steps should the solutions architect take to meet these requirements
A. Create peering connections between the egress VPC and the spoke VPC s. Configure the required routing to allow access to the internetCreate peering connections between the egress VPC and the spoke VPC s. Configure the required routing to allow access to the internet
B. Create a transit gateway, and share it with the existing AWS accounts, Attach existing VPC s to the transit gateway Configure the required routing to allow access to the internet
C. Create a transit gateway in every account. Attach the NAT gateway to the transit gateways. Configure the required routing to allow access to the internet
D. Create an AWS PrivateL ink connection between the egress VPC and the spoke VPC s, Configure the required routing to allow access to the internet
答案：B

456. A retail company runs a business-critical web service on an Amazon Elastic Container Service（Amazon ECS）cluster that runs on Amazon EC2 instances. The web service receives PoST requests from end users and writes data to a My SQL database that runs on a separate EC2 instance. The company needs to ensure that data loss does not occur.
The current code deployment process includes manual updates of the ECS service. During a recent deployment, end users encountered intermittent 502 Bad Gateway errors in response to vald web requests
The company wants to implement a reliable solution to prevent this issue from recurring. The company also wants to automate code deployments. The solution must be highly available and must optimize cost-effectiveness.
Which combination of steps will meet these requirements? （Select THREE)
A.Run the web service on an ECS cluster that has a Fargate launch type Use AWS CodePipeline and AWS CodeDeploy to perform a bluegreen deployment with validation testing to update the ECS service
B.Migrate the My SQL database to run on an Amazon RDS for My SQL Multi-AZ DB instance that uses Provisioned IOPS SSD（i02）storage
C.Configure an Amazon Simple Queue Service（Amazon SQS ）queue as an event source to receive the POST requests from the web service. Configure an AWS Lambda function to poll the queue. Write the data to the database
D.Run the web service on an ECS cluster that has a Fargate launch type Use AWS Code Pipeline and AWS Code Deploy to perform a canary deployment to update the ECS service
E.Configure an Amazon Simple Queue Service（Amazon SQS ）queue. Install the SQS agent on the containers

that run in the ECS cluster to poll the queue. Write the data to the database

F.Migrate the MySQL database to run on an Amazon RDS for MySQL Multi-AZ DB instance that uses General Purpose SSD （gp3）storage

答案：ACF

457. a data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The cluster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report. The quenes to generat the report are complex read quenes and are CPU intensive.

Business requirements dictate that the cluster must be able to service read and write queries at all times. a solutions architect must devise a solution that accommodates the bursts of usage

Which solution meets these requirements MOST cost-effectively?

A. Provision an Amazon EMR cluster Offload the complex data processing tasks

B. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the clusters CPU metrics in Amazon CloudWatch reach 80%

C. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using an elastic resize operation when the clusters CPU metrics in Amazon CloudWatch reach 80%

D. Turn on the Concurrency Scaling feature for the Amazon Redshift cluster

答案：C

458. A retail company needs to provide a series of data files to another company, which is its business partner. These files are saved in an Amazon S3 bucket under Account a, which belongs to the retail company. The business partner company wants one of its LAM users, User Data Processor, to access the files from its own AWS account （Account B）

Which combination of steps must the companies take so that User_ DataProcessor can access the s3 bucket successfully? （Select TwO）

A. Turn on the cross-origin resource sharing（CORS）feature for the S3 bucket in AccountA

B. In Account A, set the s3 bucket policy to the following

```
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```

C. In Account A, set the S3 bucket policy to the following

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
    },
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::AccountABucketName/*"
    ]
}
```

D. In Account B, set the permissions of User_ Data Processor to the following

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
    },
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::AccountABucketName/*"
    ]
}
```

答案：AC

459. A company plans to migrate a 2 TB MysQL database from an on-premises data center to Amazon Aurora. The database has hundreds of updates every minute. The on-premises database server is not accessible through the intemet. The company ants the migration to begin immediately and to minimize downtime
Which solution will complete the migration with the LEAST amount of operational overhead?
A. Create a VPN tunnel connect the on-premises data center to the VPC that hosts the Aurora cluster. Create a dump of the on-premises MYSQL database by using mysqldump Upload the dump to Amazon s3 by using multipart upload. Use an Amazon EC2 instance with appropriate permissions to import the dump to the existing Aurora cluster, Connect the application to the Aurora endpoints
B. Create a VPN tunnel to connect the on-premises data center to the VPC that hosts the Aurora cluster. Use the on-premises database as a source endpoint of AWS Database Migration Service （AWS DMS）。 Use the Aurora cluster as a target endpoint. Configure a DMS task with ongoing replication. After the initial import, check the replication status, stop the application, and connect the application to the Aurora endpoints
C. Set up an AWS Direct Connect connection to connect the on-premises data center to the VPC that hosts the Aurora cluster. Use the on-premises database as a source endpoint of AWS Database Migration Service（AWS DMS） Use the Aurora cluster as a target endpoint. Configure a DMS task with ongoing replication. After the initial import, check the replication status, stop the application, and connect the application to the Aurora endpoints
D. Set up an AWS Direc connect connection to connect the on-premises data center to the VPC that hosts the Aurora cluster. Create a dump of the on-premises My sQL database by using mysqldump, Upload the dump to Amazon S3 by using multipart upload, Use an Amazon EC2 instance with approprate permissions to import the dump to the existing Aurora cluster Set up replication bet on premises and the Aurora cluster. After the databases are in sync, stop the application and point to the new endpoint
答案：B

460. A solutions architect is reviewing a stateless microservice for improvements in cost-effectiveness. The microservice is running on Amazon Elastic Container Service（Amazon ECS）， and the default Auto Scaling group is configured for nine Amazon EC2 instances. The Auto Scaling groups launch configuration specifies general purpose On-Demand Instances that are spread evenly across three Availability Zones
The application has peak usage on weekdays between 9 AM and 5 PM, Usage is minimal outside of these hours. The application is performing optimally at peak times under the existing configuration
Which combination of steps should the solutions architect recommend to REDUCE the cost of running the application? （Select THREE）
A. Modify the Auto Scaling group to use scheduled scaling
B. Create AWS Application Auto Scaling scheduled actions that target the ECS service
C. Modify the Auto Scaling group to use launch templates instead of launch configurations
D. Configure a copy of the launch configuration to request Spot Instances
E. Modify the Auto Scaling group to use Capacity Rebalancing to request Spot Instances in addition to the

On-Demand Instances
F. Modify the Auto Scaling group selection of the ECS clusters' default capacity provider
答案：AEF

461. A company is running a containerized application in the AWS Cloud. The application is running Amazon Elastic Container Service（Amazon ECS）on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group The company uses Amazon Elastic Container Registry （Amazon ECR）to store its container images. When a new image version is uploaded, the new image version receives a unique tag
The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High sevenity findings, The solution also must notify the development team when such a deletion occurs
Which solution meets these requirements?
A. Configure scan on push on the repository. Use Amazon EventBrdge （Amazon Cloud Watch Events）to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings. Use the Step functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service（Amazon SNS）
B. Configure scan on push on the repository. Configure scan results to be pushed to an Amazon Simple Queue Service（Amazon SQS ）queue Invoke an AWS Lambda function when a new message is added to the SQS queue. Use the Lambda Function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service（Amazon SES）
C. Schedule an AWS Lambda function to start a manual image scan every hour configure Amazon Event Bridge （Amazon CloudWatch Events）to invoke another Lambda function when a scan is complete, Use the second Lambda function to delete the image tag for images that have Critical or High severity findings, Notify the development team by using Amazon Simple Notification Service（Amazon SNS）
D. Configure periodic image scan on the repository. Configure scan results to be added to an Amazon Simple Queue Service（Amazon SQS ）queue, Invoke an AWS Step Functions state machine when a new message is added to the SQS queue Use the step Functions state machine to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service（Amazon SES）
答案：A
解析：
A 更加自动化

462. A finance company is storing business-critical customer data in a database that is hosted on an Amazon RDs for MySQL DB instance. The company must be able to restore the most recent point-in-time backup within an rto window of 5 minutes, For disaster recovery purposes, the company also must replicate these backups to another AWS Region
Which solution meets these requirements?
A. Create Amazon EventBridge （Amazon CloudWatch Events）rules that invoke AWS Lambda functions every 5 minutes to take a snapshot of the DB instance. Copy the snapshot to another Region
B. Migrate from Amazon RDs for MysQL to Amazon Aurora. Create a cross-Region read replica. Restore the database from the read replica, if necessary
C. Configure AWS Backup to take Amazon RDS backups. Turn on the option for continuous backups. Replicate the backup vault to another Region
D. Launch an Amazon EC2 instance in another Region. Configure the eC2 instance to serve as a MysQL read replica of the DB instance. Restore the database from the read replica, if necessary
答案：A

463. A company has an organization that has many AWS accounts in AWS Organizations. a solutions architect must

improve how the company manages common security group rules for the AWS accounts in the organization
The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company' s on-premises network Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list
The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts.
Which solution meets these requirements with the LEAST amount of operational overhead?
A. Set up an Amazon Simple Notification Service（Amazon SNS） topic in the security teams AWS account Deploy an AWS Lambda function in each AWS account. Configure the Lambda function to run every time an sNS topic receives a message Configure the Lambda function to take an iP address as input and add it to a list of security groups in the account Instruct the security team to distribute changes by publishing messages to its SNS topic
B. Create new customer-managed prefix lists in each AWS account within the organization. Populate the prefix lsts in each account with all internal CIDR ranges. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups. Instruct the security team to share updates with each AWS account owner
C. Create a new customer-managed prefix list in the security team's AWS account Populate the customer-managed prefix list with all intemal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer- managed prefix list ID in their securty groups
D. Create an IAM role in each account in the organization. Grant permissions to update security groups. Deploy an AWS Lambda function in the security team's AWS account. Configure the Lambda function to take a list of intenal IP addresses as input, assume a role in each organization account, and add the list of iP addresses to the secunty groups in each account
答案：D

464. A retail company is operating its ecommerce application on AWS . The application runs on Amazon EC2instances behind an Application Load Balancer（ALB）。 The company uses an Amazon RDS DB instance as the database backend. Amazon Cloud Front is configured with one origin that points to the ALB Static content is cached. Amazon Route 53 is used to host all public zones
After an update of the application the Alb occasionally returns a 502 status code (bad Gateway) error. The root cause is malformed Http headers that are returned to the Alb. The webpage retuns successfully when a solutions architect reloads the webpage immediately after the error occurs
While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors
Which combination of steps will meet this requirement with the LEAST amount of operational overhead? （Select TwO）
A. Create an Amazon S3 bucket Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3
B. Create an Amazon Cloudwatch alarm to invoke an AWS Lambda function if the ALB health check response Target FailedHealth checks is greater than 0. Configure the Lambda function to modify the forwarding rule at the alb to point to a publicly
C. Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage
D. Create an Amazon Cloudwatch alarm to invoke an AWS Lambda function if the aLB health check response Elb. IntemalError is greater than 0. Configure the lambda function to modify the forwarding rule at the aLB to point to a public accessible
E. Add a custom error response by configuring a CloudFront custom error page. Modify dNS records to point to a publicly accessible web page

答案：AB
解析：
AB Target.FailedHealth 是因为遇到了 malformed 问题

465. A company has developed a web application. The company is hosting the application on of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLS. The solution must not adversely affect legitimate traffic to the application
How should a solutions architect configure the web ACLs to meet these requirements?
A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.
B. Use only rate-based rules in the web ACLs, and set the throttle limit as high as possible. Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope ite tracking
C. Set the action of the web ACL rules to Block Use only AWS managed rule groups in the web ACLs. Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs
D. Use only custom rule groups in the web ACLs, and set the action to Allow. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Allow to block
答案:B

466. A company is migrating a legacy application from an on-premises data center to AWS . The application consists of a single application server and a Microsoft SQL Server database server. Each server is deployed on a VMware VM that consumes 500 TB of data across multiple attached volumes
The company has established a 10 Gbps AWS Direct Connect connection from the closest AWS Region to its on-premises data center The Direct Connect connection is not currently in use by other services
Which combination of steps should a solutions architect take to migrate the application with the LEAST amount of downtime? （Select TwO）
A. Use an AWS Server Migration Service（AWS SMS） replication job to migrate the database server VM to AWS
B. Use VM Import Export to import the application server VM
C. Export the vm images to an AWS snowball Edge storage optimized device
D. Use an AWS Server Migration Service（AWS SMS）replication job to migrate the application server VM to AWS
E. Use an AWS Database Migration Service（AWS DMS）replication instance to migrate the database to an Amazon RDs DB instance
答案：DE

467. An AWS customer has a web application that runs on premises. The web application fetches data from a third-party APi that is behind a firewall. The third party accepts only one public CIDR block in each clients allow list
The customer wants to migrate their web applcation to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Balancer（ALB）in a VPC . The ALB is located in public subnets. The EC2 instances are located in private subnets. naT gateways provide internet access to the private subnets
How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?
A. Associate a block of customer-owned public IP addresses to the VPC . Enable public iP addressing for public subnets in the VPC .
B. Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the nat gateways in the VPC
C. Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB

D. Register a block of customer-owned public IP addresses in the AWS account Set up AWS Global Accelerator to use Elastic IP addresses from the address block Set the ALB as the accelerator endpoint.
答案：B

468. A financial services company runs a complex, multi-tier application on Amazon EC2 instances and AWS Lambda functions. The application stores temporary data in Amazon S3. The s3 objects are valid for only 45 minutes and are deleted after 24hours
The company deploys each version of the application by launching an AWS CloudFormation stack. The stack creates all resources that are required to run the application. When the company deploys and validates a new application version, the making major changes to the application 's architecture
Which solution meets these requirements?
A. Implement a Lambda function that deletes all files from a given s3 bucket Integrate this Lambda function as a custom resource into the CloudFomation stack Ensure that the custom resource has a Depends on attnbute that points to the S3 bucket's resource
B. Modify the CloudFormation template to provision an Amazon Elastic File System（Amazon EFS） file system to store the temporary files there instead of in Amazon S3. Configure the Lambda functions to run in the same VPC as the file system Mount the file system to the ec2 instances and Lambda functions
C. Modify the CloudFormation stack to create an S3 Lifecycle rule that expires all objects 45 minutes after creation. Add a depends On attnbute that points to the S3 buckets resource
D. Modify the CloudFormation stack to attach a Deletion Policy attribute with a value of Delete to the S3 bucket
答案：D

469. A large company is migrating its on-premises applications to the AWS Cloud. All the company's AWS accounts belong to an organization in AWS Organizations. Each application is deployed into its own VPC in separate AWS accounts.
The company decides to start the migration process by migrating the front-end web services while keeping the databases on premises. The databases are configured with local domain names that are specific to the on-premises environment. The local domain names must be resolvable from the migrated web services
Which solution will meet these requirements with the LEAST operational overhead?
A. Create a shared services VPC in a new AWS account:Deploy Amazon Route 53 outbound resolvers. For relevant on-premises domains, use the outbound resolver settings to create forwarding rules that point to the on premises DNS servers Share these rules with the other AWS accounts by using AWS Resource Access Manager
B. Deploy Multi-AZ Amazon Route 53 outbound resolvers in each VPC . Create forwarding rules that point to on-premises DNS servers in local outbound resolvers for each VPC
C. Create a shared services VPC in a new AWS account Deploy Amazon EC2 instances that act as conditional forwarders inside the shared services VPC . Change the DHCP options set in each VPC to point to these forwarders as DNS servers Create forwarding rules for relevant on-premises domains in these forwarders
D. Create a shared services VPC in a new AWS account Deploy Amazon Route 53 inbound resolvers, For relevant on premises domains, create forwarding rules that point to on-premises DNS servers share these rules with the other AWS accounts by using AWS Resource Access Manager.
答案:A

470. A mobile gaming company is expanding into the global market. The company s game servers run in the us-east-1 Region The game s cient application uses UDP to communicate with the game servers and needs to be able to connect to a set of static iP addresses
The company wants its game to be accessible on multiple continents The company also wants the game to maintain its network performance and global availability
Which solution meets these requirements?

A. Provision an Application Load Balancer (ALB) in front of the game servers, Create an Amazon CloudFront distnbution that has no geographical restrictions. Set the aLB as the ongin Perform DNS lookups for the cloudfront. net domain name. Use the resulting iP addresses in the games client application
B. Provision game servers in each AWS Region. Provision an Application Load Balancer in front of the game servers. Create an Amazon Route 53 latency based routing policy for the game's client application to use with DNS lookups
C. Provision game servers in each AWS Region. Provision a Network Load Balancer (NLB) in front of the game servers, Create an accelerator in AWS Global Accelerator, and configure endpoint groups in each Region, Associate the NLBs with the corresponding Regional endpoint groups Point the game client's application to the global Accelerator endpoints
D. Provision game servers in each AWS Region. Provision a Network Load Balancer(NLB) in front of the game servers. Create an Amazon CloudFront distribution that has no geographical restrictions. Set the NLB as the origin, Perform DNS lookups for the cloudfront. net domain name. Use the resulting IP addresses in the game's client application.
答案：C

471. In AWS CloudFormation, what is a circular dependency?
A. When Nested Stacks depend on each other.
B. When Resources form a Depend On loop.
C. When a Template references an earlier version of itself.
D. When a Template references a region, which references the original Template.
答案:B
解析:
Correct Answer: B
To resolve a dependency error, add a Depends On attribute to resources that depend on other resources in your template. In some cases, you must explicitly declare dependencies so that AWS CloudFormation can create or delete resources in the correct order. For example, if you create an Elastic IP and a VPC with an Internet gateway in the same stack, the Elastic IP must depend on the Internet gateway attachment. For additional information, see Depends On Attribute.
Reference:
http://docs.AWS .amazon.com/AWS CloudFormation/latest/UserGuide/troubleshooting.html#troubleshooting-errors-dependency-error
在 AWS CloudFormation 中，什么是循环依赖?
A. 当嵌套堆栈相互依赖时。
B. 当资源形成依赖循环时。
C. 当模板引用自身的早期版本时。
D. 当模板引用一个区域时，它引用了原始模板。

472. Which of the following assertions is accurate in the context of AWS CloudFormation?
A. Actual resource names are a combination of the resource ID, stack, and logical resource name.
B. Actual resource name is the stack resource name.
C. Actual resource name is the logical resource name.
D. Actual resource names are a combination of the stack and logical resource name.
答案:D
解析: Correct Answer: D
In AWS CloudFormation, actual resource names are a combination of the stack and logical resource name. This allows multiple stacks to be created from a template without fear of name collisions between AWS resources.

Reference:
https://AWS .amazon.com/cloudformation/faqs/
在 AWS CloudFormation 的上下文中，以下哪个断言是准确的?
A. 实际资源名称是资源 ID、堆栈和逻辑资源名称的组合。
B. 实际资源名称为堆栈资源名称。
C. 实际资源名称是逻辑资源名称。
D. 实际资源名称是堆栈和逻辑资源名称的组合

473. A projection in DynamoDB is_____.
A. systematic transformation of the latitudes and longitudes of the locations inside your table
B. importing data from your file to a table
C. exporting data from a table to your file
D. the set of attributes that is copied from a table into a secondary index
答案:D
解析: Correct Answer: D
In DynamoDB, a projection is the set of attributes that is copied from a table into a secondary index.
Reference:
http://docs.AWS .amazon.com/amazondynamodb/latest/developerguide/GSI.html
DynamoDB 中的投影是_____。
A. 系统变换表内位置的经纬度
B. 将文件中的数据导入到表中
C. 将数据从表导出到您的文件
D. 从表复制到二级索引的属性集

474. Amazon ElastiCache supports which of the following cache engines?
A. Amazon ElastiCache supports Memcached and Redis.
B. Amazon ElastiCache supports Redis and WinCache.
C. Amazon ElastiCache supports Memcached and Hazelcast.
D. Amazon ElastiCache supports Memcached only.
答案:A
解析: Correct Answer: A
The cache engines supported by Amazon ElastiCache are Memcached and Redis.
Reference:
http://docs.AWS .amazon.com/AmazonElastiCache/latest/UserGuide/SelectEngine.html
Amazon ElastiCache 支持以下哪些缓存引擎?
A. Amazon ElastiCache 支持 Memcached 和 Redis。
B. Amazon ElastiCache 支持 Redis 和 WinCache。
C. Amazon ElastiCache 支持 Memcached 和 Hazelcast。
D. Amazon ElastiCache 仅支持 Memcached。

475. What is a quiet push notification in Amazon Cognito?
A. It is a push message that is received by your application on a user's device that will not be seen by the user.
B. It is a push message that is received by your application on a user's device that will return the user's geolocation.
C. It is a push message that is received by your application on a user's device that will not be heard by the user.
D. It is a push message that is received by your application on a user's device that will return the user's authentication credentials.

答案:A
解析: Correct Answer: A
Amazon Cognito uses the Amazon Simple Notification Service (SNS) to send silent push notifications to devices. A silent push notification is a push message that is received by your application on a user's device that will not be seen by the user.
Reference:
http://AWS .amazon.com/cognito/faqs/
什么是 Amazon Cognito 中的安静推送通知?
A. 它是您的应用程序在用户设备上接收的推送消息，该消息不会被用户看到。
B. 它是您的应用程序在用户设备上接收的推送消息，它将返回用户的地理位置。
C. It is a push message that is received by your application on a user's device that will not be heard by the user.
D. It is a push message that is received by your application on a user's device that will return the user's authentication credentials.

476. The default cache port in Amazon ElastiCache is:
A. for Memcached 11210 and for Redis 6380.
B. for Memcached 11211 and for Redis 6380.
C. for Memcached 11210 and for Redis 6379.
D. for Memcached 11211 and for Redis 6379.
答案:D
解析: Correct Answer: D
In Amazon ElastiCache, you can specify a new port number for your cache cluster, which by default is 11211 for Memcached and 6379 for Redis.
Reference:
http://docs.AWS .amazon.com/AmazonElastiCache/latest/UserGuide/GettingStarted.AuthorizeAccess.html
Amazon ElastiCache 中的默认缓存端口是:
A. 对于 Memcached 11210 和 Redis 6380。
B. 对于 Memcached 11211 和 Redis 6380。
C. 对于 Memcached 11210 和 Redis 6379。
D. 对于 Memcached 11211 和 Redis 6379

477. Which of the following settings should the user adjust to manually scale out AWS resources using AutoScaling?
A. Current capacity
B. Desired capacity
C. Preferred capacity
D. Maximum capacity
答案:B
解析: Correct Answer: B
The Manual Scaling as part of Auto Scaling allows the user to change the capacity of Auto Scaling group. The user can add / remove EC2 instances on the fly. To execute manual scaling, the user should modify the desired capacity. AutoScaling will adjust instances as per the requirements.
Reference:
http://docs.AWS .amazon.com/AutoScaling/latest/DeveloperGuide/as-manual-scaling.html
Question #8
用户应调整以下哪些设置以使用 AutoScaling 手动扩展 AWS 资源?
A. 现有容量

B. 预期容量
C. 首选容量
D. 最大容量

478. As one of the AWS resource categories, AWS _____supports_____ environments.
A. Elastic Beanstalk; Elastic Beanstalk application
B. CloudFormation; Elastic Beanstalk application
C. Elastic Beanstalk ; CloudFormation application
D. CloudFormation; CloudFormation application
答案:B
解析：Correct Answer: B
AWS CloudFormation and AWS Elastic Beanstalk services are designed to complement each other. AWS CloudFormation supports Elastic Beanstalk application environments as one of the AWS resource types.
Reference:
http://AWS .amazon.com/cloudformation/faqs/
作为 AWS 资源类别之一，AWS _____支持_____环境。
A. 弹性豆茎；弹性 Beanstalk 应用程序
B. CloudFormation；弹性 Beanstalk 应用程序
C. 弹性豆茎；CloudFormation 应用程序
D. CloudFormation；CloudFormation 应用程序

479. Which of the following statements concerning delegating authorization to perform API calls is NOT accurate in the context of IAM roles for Amazon EC2?
A. You cannot create an IAM role.
B. You can have the application retrieve a set of temporary credentials and use them.
C. You can specify the role when you launch your instances.
D. You can define which accounts or AWS services can assume the role.
答案:A
解析: Correct Answer: A
Amazon designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.
Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows: Create an IAM role.
Define which accounts or AWS services can assume the role. Define which API actions and resources the application can use after assuming the role. Specify the role when you launch your instances. Have the application retrieve a set of temporary credentials and use them.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
在 Amazon EC2 的 IAM 角色的上下文中，以下关于委派执行 API 调用的授权的哪些陈述是不准确的?
A. 您不能创建 IAM 角色。
B. 您可以让应用程序检索一组临时凭证并使用它们。
C. 您可以在启动实例时指定角色。
D. 您可以定义哪些账户或 AWS 服务可以代入该角色。

480.Which of the following configurations should be utilized when I/O speed is more essential than fault tolerance?
A. SPAN 10

B. RAID 1
C. RAID 0
D. NFS 1
答案:C
解析:
当 I/0 速度比容错更重要时，应使用以下哪种配置?
A. 跨度 10
B. RAID 1
C. RAID 0
D. NFS 1

481. Is it necessary for your application to reside in the same VPC as the CloudHSM instance when using AWS Cloud Hardware Security Module(HSM)?
A. No, but the server or instance on which your application and the HSM client is running must have network (IP) reachability to the HSM.
B. Yes, always
C. No, but they must reside in the same Availability Zone.
D. No, but it should reside in same Availability Zone as the DB instance.
答案:A
解析: Correct Answer: A
Your application does not need to reside in the same VPC as the CloudHSM instance. However, the server or instance on which your application and the HSM client is running must have network (IP) reachability to the HSM. You can establish network connectivity in a variety of ways, including operating your application in the same VPC , with VPC peering, with a VPN connection, or with Direct Connect.
Reference:
https://AWS .amazon.com/cloudhsm/faqs/

482. Which of the following actions should you take to get started with AWS Direct Connect?
A. Complete the Cross Connect
B. Configure Redundant Connections with AWS Direct Connect
C. Create a Virtual Interface
D. Download Router Configuration
答案:c
解析: Correct Answer: C
In AWS Direct Connect, your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication, and you need to provide a private
Autonomous System Number (ASN) for that to connect to Amazon Virtual Private Cloud (VPC). To connect to public AWS products such as Amazon EC2 and
Amazon S3, you will also need to provide a public ASN that you own (preferred) or a private ASN. You have to configure BGP in the Create a Virtual Interface step.
Reference:
http://docs.AWS .amazon.com/directconnect/latest/UserGuide/getstarted.html#createvirtualinterface

483. Which of the following is not a suitable tag key/value combination when adding a tag to an instance?
A. Key : "AWS " Value:"AWS "
B. Key: "AWS :name" Value: "instanceAnswer: AWS "
C. Key: "Name :AWS " Value: "instanceAnswer: AWS "

D. Key : "nameAnswer: AWS " Value:"AWS :instance"
答案： B
解析： Correct Answer: B
In Amazon Web Services, to help manage EC2 instances as well their usage in a better way, the user can tag the instances. The tags are metadata assigned by the user which consists of a key and value. The tag key cannot have a prefix as "AWS :", although it can have only "AWS ".
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/Using_Tags.html

484. The Condition element is _____ in the context of rules and permissions in AWS IAM.
A. crucial while writing the IAM policies
B. an optional element
C. always set to null
D. a mandatory element
答案:B
解析: Correct Answer: B
The Condition element (or Condition block) lets you specify conditions for when a policy is in effect. The Condition element is optional.
Reference:
http://docs.AWS .amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

485. AWS Direct Connect connects your internal network to an AWS Direct Connect facility through which of the following Ethernet standards?
A. Single mode fiber-optic cable
B. Multi-mode fiber-optic cable
C. Shielded balanced copper cable
D. Twisted pair cable
答案:A
解析: Correct Answer: A
AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet single mode fiber-optic cable.
Reference:
http://docs.AWS .amazon.com/directconnect/latest/UserGuide/Welcome.html

486. A firm maintains a publicly available application that performs RESTful API calls to a Java-based web service. It is hosted on Apache Tomcat on a single server in a data center that consistently maintains a CPU utilization of 30%. The usage of the API is expected to increase tenfold with the release of a new product. The organization needs a smooth transfer of the program to AWS and the ability for the application to scale in response to demand.
The company has already determined that traffic will be rerouted through Amazon Route 53 and CNAME records.

How can we achieve these requirements with the MINIMUM feasible effort?
A. Create a new IAM policy that allows access to those EC2 instances only for the Security team. Apply this policy to the AWS Organizations master account.
B. Create a new tag-based IAM policy that allows access to these EC2 instances only for the Security team. Tag the instances appropriately, and apply this policy in each account.
C. Create an organizational unit under AWS Organizations. Move all the accounts into this organizational unit and use SCP to apply a whitelist policy to allow access to these EC2 instances for the Security team only.
D. Set up SAML federation for all accounts in AWS . Configure SAML so that it checks for the service API call before

authenticating the user. Block SAML from authenticating API calls if anyone other than the Security team accesses these instances.
答案:C
解析:
Correct Answer: C
Reference:
https://AWS .amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission-guardrails-across-accounts-in-your-AWS -organization/
https://docs.AWS .amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html

487. Determine a true assertion regarding user passwords in the context of AWS IAM (login profiles).
A. They must contain Unicode characters.
B. They can contain any Basic Latin (ASCII) characters.
C. They must begin and end with a forward slash (/).
D. They cannot contain Basic Latin (ASCII) characters.
答案:B
解析: Correct Answer: B
The user passwords (login profiles) of IAM users can contain any Basic Latin (ASCII)characters.
Reference:
http://docs.AWS .amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

488. Which of the following assertions about Amazon ElastiCache is correct?
A. When you launch an ElastiCache cluster into an Amazon VPC private subnet, every cache node is assigned a public IP address within that subnet.
B. You cannot use ElastiCache in a VPC that is configured for dedicated instance tenancy.
C. If your AWS account supports only the EC2-VPC platform, ElastiCache will never launch your cluster in a VPC .
D. ElastiCache is not fully integrated with Amazon Virtual Private Cloud (VPC).
答案:B
解析: Correct Answer: B
The VPC must allow non-dedicated EC2 instances. You cannot use ElastiCache in a VPC that is configured for dedicated instance tenancy.
Reference:
http://docs.AWS .amazon.com/AmazonElastiCache/latest/UserGuide/AmazonVPC .EC.html

489. By shifting to AWS , a corporation wishes to control the expenses associated with a set of twenty apps that are little utilized but remain mission-critical.
The apps are written in Java and Node.js and are distributed over many instance clusters. The organization wishes to reduce expenses while increasing standardization via the use of a single deployment approach. The majority of the programs are used as part of month-end processing procedures with a limited number of concurrent users, although they are also used at other times. The average program consumes less than 1 GB of memory, while some apps use up to 2.5 GB at peak activity. The group's most critical application is a Java-based billing report that often accesses several data sources and runs for many hours.

Which approach is the MOST cost-effective?By shifting to AWS , a corporation wishes to control the expenses associated with a set of twenty apps that are little utilized but remain mission-critical.
The apps are written in Java and Node.js and are distributed over many instance clusters. The organization wishes to

reduce expenses while increasing standardization via the use of a single deployment approach. The majority of the programs are used as part of month-end processing procedures with a limited number of concurrent users, although they are also used at other times. The average program consumes less than 1 GB of memory, while some apps use up to 2.5 GB at peak activity. The group's most critical application is a Java-based billing report that often accesses several data sources and runs for many hours.

Which approach is the MOST cost-effective?
A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.
B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch.
C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.
D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.
答案:C

490. Which status in AWS CloudFormation denotes a failure state?
A. ROLLBACK_IN_PROGRESS
B. DELETE_IN_PROGRESS
C. UPDATE_COMPLETE_CLEANUP_IN_PROGRESS
D. REVIEW_IN_PROGRESS
答案:A
解析: Correct Answer: A
ROLLBACK_IN_PROGRESS means an ongoing removal of one or more stacks after a failed stack creation or after an explicitly canceled stack creation.
DELETE_IN_PROGRESS means an ongoing removal of one or more stacks. REVIEW_IN_PROGRESS means an ongoing creation of one or more stacks with an expected StackId but without any templates or resources.
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS means an ongoing removal of old resources for one or more stacks after a successful stack update.
Reference:
http://docs.AWS .amazon.com/AWS CloudFormation/latest/UserGuide/using-cfn-describing-stacks.html

491. When creating an AMI or starting a new instance on Amazon Elastic Compute Cloud, you may define storage volumes in addition to the root device volume using_____.
A. block device mapping
B. object mapping
C. batch storage mapping
D. datacenter mapping
答案:A
解析:Correct Answer: A
When creating an AMI or launching a new instance, you can assign more than one block storage device to it.
This device will be automatically set ready for you through an automated process known as block device mapping.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/block-device-mapping-concepts.html

492. Which of the following features in DynamoDB enables you to trigger alerts when a statistic reaches a preset threshold?
A. Alarm Signal
B. DynamoDB Analyzer
C. CloudWatch
D. DynamoDBALARM
答案:C
解析: Correct Answer: C
CloudWatch allows you to set alarms when you reach a specified threshold for a metric.
Reference:
http://docs.AWS .amazon.com/amazondynamodb/latest/developerguide/MonitoringDynamoDB.html
Question #23

493. You may provide up to 3TB of storage and 30,000 IOPS per database instance with Amazon RDS for PostgreSQL. PostgreSQL can achieve over 25,000 IOPS with a workload composed of 50% writes and 50% reads running on a cr1.8xlarge instance.

However, by exceeding this restriction, you may be able to do the following:
A. higher latency and lower throughput.
B. lower latency and higher throughput.
C. higher throughput only.
D. higher latency only.
答案:B
解析: Correct Answer: B
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 lower latency and higher throughput.
Your actual realized IOPS may vary from the amount you provisioned based on your database workload, instance type, and database engine choice.
Reference:
https://AWS .amazon.com/rds/postgresql/

494. Which of the following parameters does Amazon not charge you for in relation to DynamoDB?
A. Storage cost
B. I/O usage within the same Region
C. Cost per provisioned read units
D. Cost per provisioned write units
答案:B
解析: Correct Answer: B
In DynamoDB, you will be charged for the storage and the throughput you use rather than for the I/O which has been used.
Reference:
http://AWS .amazon.com/dynamodb/pricing/
Question #25

495. With the AWS Simple Notification Service, a user has enabled thorough CloudWatch monitoring.

Which of the following statements aids the user in comprehending thorough monitoring?
A. SNS cannot provide data every minute
B. SNS will send data every minute after configuration
C. There is no need to enable since SNS provides data every minute
D. AWS CloudWatch does not support monitoring for SNS
答案:A
解析: Correct Answer: A
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute.
The AWS SNS service sends data every 5 minutes. Thus, it supports only the basic monitoring. The user cannot enable detailed monitoring with SNS.
Reference:
http://docs.AWS .amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

496. An enterprise has configured RDS using a virtual private cloud (VPC). The company desires internet access to RDS.

Which of the setups listed below is not necessary in this scenario?
A. The organization must enable the parameter in the console which makes the RDS instance publicly accessible.
B. The organization must allow access from the internet in the RDS VPC security group,
C. The organization must setup RDS with the subnet group which has an external IP.
D. The organization must enable the VPC attributes DNS hostnames and DNS resolution
答案:C
解析: Correct Answer: C
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources, such as RDS into a virtual network that the user has defined. Subnets are segments of a VPC 's IP address range that the user can designate to a group of VPC resources based on security and operational needs. A DB subnet group is a collection of subnets (generally private) that the user can create in a VPC and which the user assigns to the RDS
DB instances. A DB subnet group allows the user to specify a particular VPC when creating DB instances. If the RDS instance is required to be accessible from the internet:
The organization must setup that the RDS instance is enabled with the VPC attributes, DNS hostnames and DNS resolution.
The organization must enable the parameter in the console which makes the RDS instance publicly accessible.
The organization must allow access from the internet in the RDS VPC security group.
Reference:
http://docs.AWS .amazon.com/AmazonRDS/latest/UserGuide/USER_VPC .html

497. Each resource declaration in an AWS CloudFormation template comprises the following:
A. a logical ID, a resource type, and resource properties
B. a variable resource name and resource attributes
C. an IP address and resource entities
D. a physical ID, a resource file, and resource data
答案:A

解析: Correct Answer: A
In AWS CloudFormation, each resource declaration includes three parts: a logical ID that is unique within the template, a resource type, and resource properties.
Reference:
http://docs.AWS .amazon.com/AWS CloudFormation/latest/UserGuide/concept-resources.html

498. A business maintains an on-premises legacy application. The organization wishes to acquire meaningful insights from application logs to improve the program's dependability. The following needs have been communicated to a Solutions Architect:

- Utilize AWS to aggregate logs.
- Analyze logs for problems automatically.
- Notify the Operations team when a preset threshold of errors is exceeded.

Which solution satisfies the criteria?
A. Install Amazon Kinesis Agent on servers, send logs to Amazon Kinesis Data Streams and use Amazon Kinesis Data Analytics to identify errors, create an Amazon CloudWatch alarm to notify the Operations team of errors
B. Install an AWS X-Ray agent on servers, send logs to AWS Lambda and analyze them to identify errors, use Amazon CloudWatch Events to notify the Operations team of errors.
C. Install Logstash on servers, send logs to Amazon S3 and use Amazon Athena to identify errors, use sendmail to notify the Operations team of errors.
D. Install the Amazon CloudWatch agent on servers, send logs to Amazon CloudWatch Logs and use metric filters to identify errors, create a CloudWatch alarm to notify the Operations team of errors.
答案:D
解析: Correct Answer: D
Reference:
https://docs.AWS .amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html
https://docs.AWS .amazon.com/kinesis-agent-windows/latest/userguide/what-is-kinesis-agent-windows.html
Question #29

499. Choose the appropriate group of alternatives. These are the default security group's basic configuration settings:
A. Allow no inbound traffic, Allow all outbound traffic and Allow instances associated with this security group to talk to each other
B. Allow all inbound traffic, Allow no outbound traffic and Allow instances associated with this security group to talk to each other
C. Allow no inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
D. Allow all inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
答案:A
解析: Correct Answer: A
A default security group is named default, and it has an ID assigned by AWS . The following are the initial settings for each default security group:
Allow inbound traffic only from other instances associated with the default security group Allow all outbound traffic from the instance
The default security group specifies itself as a source security group in its inbound rules. This is what allows instances associated with the default security group to communicate with other instances associated with the default security

group.
Reference:
https://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/ec2-security-groups.html#default-%20security-group

500. "The data is ultimately consistent" in DynamoDB indicates that_____.
A. a read request immediately after a write operation might not show the latest change.
B. a read request immediately after a write operation shows the latest change.
C. a write request immediately after a read operation might cause data loss.
D. a read request immediately after a write operation might cause data loss.
答案:A
解析: Correct Answer: A
In DynamoDB, it takes time for the update to propagate to all copies. The data is eventually consistent, meaning that a read request immediately after a write operation might not show the latest change.
Reference:
http://docs.AWS .amazon.com/amazondynamodb/latest/developerguide/APISummary.html

501. How can you ensure that your AWS CloudFormation template is operationally sound?
A. To check the operational validity, you need to attempt to create the stack.
B. There is no way to check the operational validity of your AWS CloudFormation template.
C. To check the operational validity, you need a sandbox or test area for AWS CloudFormation stacks.
D. To check the operational validity, you need to use the AWS cloudformation validate-template command.

答案:A
解析: Correct Answer: A
In AWS CloudFormation, to check the operational validity, you need to attempt to create the stack. There is no sandbox or test area for AWS CloudFormation stacks, so you are charged for the resources you create during testing.
Reference:
http://docs.AWS .amazon.com/AWS CloudFormation/latest/UserGuide/using-cfn-validate-template.html

502.Every five minutes, a corporation uploads clickstream data files to Amazon S3. Each file is processed and loaded into an Amazon RDS database using a Python script that runs as a cron job once a day on an Amazon EC2 instance. The cron task processes 24 hours of data in 15 to 30 minutes. The data users request that the data be made accessible immediately.

Which option would provide the required result?

答案:D
解析: Correct Answer: D

503. How many slices does a dw2.8xlarge node have in Amazon Redshift?
A. 16
B. 8
C. 32
D. 2

答案:C

解析: Correct Answer: C
The disk storage for a compute node in Amazon Redshift is divided into a number of slices, equal to the number of processor cores on the node. For example, each DW1.XL compute node has two slices, and each DW2.8XL compute node has 32 slices.
Reference:
http://docs.AWS .amazon.com/redshift/latest/dg/t_Distributing_data.html

504. An AWS AMI has been developed by a user. The user wishes for the AMI to be accessible exclusively to his buddy.

How is this to be managed by the user?
A. Share the AMI with the community and setup the approval workflow before anyone launches it.
B. It is not possible to share the AMI with the selected user.
C. Share the AMI with a friend's AWS account ID.
D. Share the AMI with a friend's AWS login ID.

答案:C
解析: Correct Answer: C
In Amazon Web Services, if a user has created an AMI and wants to share with his friends and colleagues he can share the AMI with their AWS account ID. Once the AMI is shared the other user can access it from the community AMIs under private AMIs options.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/sharingamis-explicit.html

505. What bandwidths are presently supported by AWS Direct Connect?
A. 10Mbps and 100Mbps
B. 10Gbps and 100Gbps
C. 100Mbps and 1Gbps
D. 1Gbps and 10 Gbps

答案:D
解析: Correct Answer: D
AWS Direct Connection currently supports 1Gbps and 10 Gbps.
Reference:
http://docs.AWS .amazon.com/directconnect/latest/UserGuide/Welcome.html

506. On-premises storage on a Windows file server is used by a business. Daily, the firm generates 5 GB of fresh data. The firm relocated a portion of its Windows-based workload to AWS and requires data to be accessible through a cloud file system. Between the on-premises network and AWS , the organization has already built an AWS Direct Connect link.

Which data transfer approach should a business employ?
A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway
B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx
C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS)
D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and

Amazon Elastic File System (Amazon EFS)

答案:B
解析:

507. The _____ operation in DynamoDB may be used to get a full listing of secondary indexes on a table.
A. BatchGetItem
B. TableName
C. DescribeTable
D. GetItem

答案:C
解析: Correct Answer: C
In DynamoDB, DescribeTable returns information about the table, including the current status of the table, when it was created, the primary key schema, and any indexes on the table.
Reference:
http://docs.AWS .amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html

508. The user has used an EBS optimized instance to provision the PIOPS volume.

In general, which I/O chunk should AWS utilize to determine the user's bandwidth experience?
A. 128 KB
B. 256 KB
C. 64 KB
D. 32 KB

答案:B
解析: Correct Answer: B
IOPS are input/output operations per second. Amazon EBS measures each I/O operation per second (that is 256 KB or smaller) as one IOPS.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/ebs-io-characteristics.html

509. Will you be able to use the standard Amazon S3 APIs to retrieve EC2 snapshots?
A. Yes, you will be able to access using S3 APIs if you have chosen the snapshot to be stored in S3.
B. No, snapshots are only available through the Amazon EBS APIs.
C. Yes, you will be able to access them using S3 APIs as all snapshots are stored in S3.
D. No, snapshots are only available through the Amazon EC2 APIs.

答案:D
解析: Correct Answer: D
No, snapshots are only available through the Amazon EC2 APIs.
Reference:
https://AWS .amazon.com/ec2/faqs/

510. All Amazon EC2 images must be inspected for vulnerabilities and pass a CVE assessment as part of a company's security compliance obligations. A solutions architect is working on a technique for creating developer-friendly AMIs that are security-approved. Before developers may utilize any new AMIs, they should undergo an automated evaluation procedure and be designated as acceptable. To guarantee compliance, authorized photos must be

scanned every 30 days.

Which measures should the solutions architect do in combination to achieve these criteria while adhering to best practices? (Select two.)
A. Use the AWS Systems Manager EC2 agent to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.
B. Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems Manager Parameter Store. Use Amazon EventBridge to trigger an AWS Systems Manager Automation document on all EC2 instances every 30 days.
C. Use Amazon Inspector to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.
D. Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems Manager Parameter Store. Use a managed AWS Config rule for continuous scanning on all EC2 instances, and use AWS Systems Manager Automation documents for remediation.
E. Use AWS CloudTrail to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

答案:BC
解析:

511. A user has used the VPC wizard to construct a VPC with public and private subnets.

Which of the following claims about this circumstance is true?
A. The user has to manually create a NAT instance
B. The Amazon VPC will automatically create a NAT instance with the micro size only
C. VPC updates the main route table used with the private subnet, and creates a custom route table with a public subnet
D. VPC updates the main route table used with a public subnet, and creates a custom route table with a private subnet

答案:C
解析: Correct Answer: C
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance of a smaller or higher size, respectively. The VPC has an implied router and the VPC wizard updates the main route table used with the private subnet, creates a custom route table and associates it with the public subnet.
Reference:
http://docs.AWS .amazon.com/AmazonVPC /latest/UserGuide/VPC _Scenario2.html

512. The Database Diagnostic Pack and the Database Tuning Pack are only available with _____ in the Amazon RDS Oracle DB engine.
A. Oracle Standard Edition
B. Oracle Express Edition
C. Oracle Enterprise Edition
D. None of these

答案:C
解析: Correct Answer: C
Reference:
https://blog.pythian.com/a-most-simple-cloud-is-amazon-rds-for-oracle-right-for-you/
Question #43

513. Which stack state in AWS CloudFormation rejects UpdateStack calls?
A. UPDATE_ROLLBACK_FAILED
B. UPDATE_ROLLBACK_COMPLETE
C. UPDATE_COMPLETE
D. CREATE_COMPLETE

答案:A
解析: Correct Answer: A
When a stack is in the UPDATE_ROLLBACK_FAILED state, you can continue rolling it back to return it to a working state (to
UPDATE_ROLLBACK_COMPLETE). You cannot update a stack that is in the UPDATE_ROLLBACK_FAILED state. However, if you can continue to roll it back, you can return the stack to its original settings and try to update it again.
Reference:
http://docs.AWS .amazon.com/AWS CloudFormation/latest/UserGuide/using-cfn-updating-stacks-continueupdaterollback.html

514. What should you use for incoming traffic on an elastic network interface (ENI) to guarantee failover capabilities?
A. A Route53 A record
B. A secondary private IP
C. A secondary public IP
D. A secondary ENI

答案:B
解析: Correct Answer: B
To ensure failover capabilities on an elastic network interface (ENI), consider using a secondary private IP for incoming traffic and if a failure occurs, you can move the interface and/or secondary private IP address to a standby instance.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/using-eni.html

515. As seen below, a user has set two security groups that permit traffic: SecGrp1: 0.0.0.0/0 is inbound on port 80. 0.0.0.0/0 is in route to port 22. SecGrp2: Inbound for 10.10.10.1/32 on port 22

Which of the following assertions is true if both security groups are connected with the same instance?
A. It is not possible to have more than one security group assigned to a single instance
B. It is not possible to create the security group with conflicting rules. AWS will reject the request
C. It allows inbound traffic for everyone on both ports 22 and 80
D. It allows inbound traffic on port 22 for IP 10.10.10.1 and for everyone else on port 80

答案:C
解析: Correct Answer: C

A user can attach more than one security group to a single EC2 instance. In this case, the rules from each security group are effectively aggregated to create one set of rules. AWS uses this set of rules to determine whether to allow access or not. Thus, here the rule for port 22 with IP 10.10.10.1/32 will merge with IP
0.0.0.0/0 and open ports 22 and 80 for all.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/using-network-security.html

516. A business use Amazon Simple Storage Service to store data (S3). Data at rest must be encrypted according to the company's security policy.

Which of the following strategies is capable of doing this? (Select three.)
A. Use Amazon S3 server-side encryption with AWS Key Management Service managed keys.
B. Use Amazon S3 server-side encryption with customer-provided keys.
C. Use Amazon S3 server-side encryption with EC2 key pair.
D. Use Amazon S3 bucket policies to restrict access to the data at rest.
E. Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.
F. Use SSL to encrypt the data while in transit to Amazon S3.

答案:ABE
解析: Correct Answer: ABE
Reference:
http://docs.AWS .amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

517. When you build a table with a hash-and-range key in DynamoDB.
A. You must define one or more Local secondary indexes on that table
B. You must define one or more Global secondary indexes on that table
C. You can optionally define one or more secondary indexes on that table
D. You must define one or more secondary indexes on that table

答案:C
解析: Correct Answer: C
When you create a table with a hash-and-range key, you can optionally define one or more secondary indexes on that table. A secondary index lets you query the data in the table using an alternate key, in addition to queries against the primary key.
Reference:
http://docs.AWS .amazon.com/amazondynamodb/latest/developerguide/DataModel.html

518. What does AWS mean by elasticity?
A. The ability to scale computing resources up easily, with minimal friction and down with latency.
B. The ability to scale computing resources up and down easily, with minimal friction.
C. The ability to provision cloud computing resources in expectation of future demand.
D. The ability to recover from business continuity events with minimal friction.

答案:B
解析:

519. True or False: Redis is supported by Amazon ElastiCache.
A. True, ElastiCache supports the Redis key-value store, but with limited functionalities.
B. False, ElastiCache does not support the Redis key-value store.

C. True, ElastiCache supports the Redis key-value store.
D. False, ElastiCache supports the Redis key-value store only if you are in a VPC environment.

答案:C
解析: Correct Answer: C
This is true. ElastiCache supports two open-source in-memory caching engines: 1. Memcached - a widely adopted memory object caching system. ElastiCache is protocol compliant with Memcached, so popular tools that you use today with existing Memcached environments will work seamlessly with the service. 2. Redis - a popular open-source in-memory key-value store that supports data structures such as sorted sets and lists. ElastiCache supports Master / Slave replication and
Multi-AZ which can be used to achieve cross AZ redundancy.
Reference:
https://AWS .amazon.com/elasticache/

520. A user is setting PIOPS for MySQL RDS. What should be the user's minimum provisioned PIOPS?
A. 1000
B. 200
C. 2000
D. 500

答案:A
解析: Correct Answer: A
If a user is trying to enable PIOPS with MySQL RDS, the minimum size of storage should be 100 GB and the minimum PIOPS should be 1000.
Reference:

521. Is it possible to alter a set of DHCP options created in a VPC after they have been created?
A. Yes, you can modify a set of DHCP options within 48 hours after creation and there are no VPC s associated with them.
B. Yes, you can modify a set of DHCP options any time after you create them.
C. No, you can't modify a set of DHCP options after you create them.
D. Yes, you can modify a set of DHCP options within 24 hours after creation.

答案:C
解析: Correct Answer: C
After you create a set of DHCP options, you can't modify them. If you want your VPC to use a different set of DHCP options, you must create a new set and associate them with your VPC . You can also set up your VPC to use no DHCP options at all.
Reference:
http://docs.AWS .amazon.com/AmazonVPC /latest/UserGuide/VPC _DHCP_Options.html

522. From a web application hosted on AWS in the eu-west-1 Region, a weather service offers high-resolution weather maps. Weather maps are often updated and are kept in Amazon S3 with static HTML information. Amazon CloudFront serves as the front end for the online application.
The firm has expanded to service consumers in the us-east-1 Region, and these new users have reported experiencing intermittent slowness while viewing their individual weather maps.

Which combination of procedures will address the performance concerns with us-east-1? (Select two.)
A. Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1. Configure endpoint groups for TCP ports 80 and 443 in us-east-1.
B. Create a new S3 bucket in us-east-1. Configure S3 cross-Region replication to synchronize from the S3 bucket in eu-west-1.
C. Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.
D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1.
E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution. Use Lambda@Edge to modify requests from North America to use the new origin.
答案:BC
解析:

523. A user is producing an EBS volume snapshot.

Which of the following claims about the generation of an EBS snapshot is incorrect?
A. Its incremental
B. It is a point in time backup of the EBS volume
C. It can be used to create an AMI
D. It is stored in the same AZ as the volume

答案:D
解析: Correct Answer: D
The EBS snapshots are a point in time backup of the EBS volume. It is an incremental snapshot, but is always specific to the region and never specific to a single
AZ. Hence the statement "It is stored in the same AZ as the volume" is incorrect.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/EBSSnapshots.html

524. A business hosts an application on AWS . An AWS Lambda function authenticates against an Amazon RDS for MySQL database instance using credentials. According to a security risk assessment, these credentials are not cycled often enough. Additionally, the database instance's encryption at rest is disabled. Both of these concerns must be fixed, according to the security team.

Which security mitigation method should a solutions architect recommend?
A. Configure the Lambda function to store and retrieve the database credentials in AWS Secrets Manager and enable rotation of the credentials. Take a snapshot of the DB instance and encrypt a copy of that snapshot. Replace the DB instance with a new DB instance that is based on the encrypted snapshot.
B. Enable IAM DB authentication on the DB instance. Grant the Lambda execution role access to the DB instance. Modify the DB instance and enable encryption.
C. Enable IAM DB authentication on the DB instance. Grant the Lambda execution role access to the DB instance. Create an encrypted read replica of the DB instance. Promote the encrypted read replica to be the new primary node.
D. Configure the Lambda function to store and retrieve the database credentials as encrypted AWS Systems Manager Parameter Store parameters. Create another Lambda function to automatically rotate the credentials. Create an encrypted read replica of the DB instance. Promote the encrypted read replica to be the new primary node.

答案:D

解析: Correct Answer: D
Reference:
https://docs.AWS .amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html
Question #55

525. A business is implementing a web application using the JEE stack. The program makes use of the JBoss application server and the MySQL database. The application includes a logging module that records all actions that occur when a JEE application's business function is invoked. Due to the enormous size of the log file, the logging activity takes some time.

Which of the following solutions will assist the application in establishing a scalable infrastructure?
A. Host the log files on EBS with PIOPS which will have higher I/O.
B. Host logging and the app server on separate servers such that they are both in the same zone.
C. Host logging and the app server on the same instance so that the network latency will be shorter.
D. Create a separate module for logging and using SQS compartmentalize the module such that all calls to logging are asynchronous.

答案:D
解析: Correct Answer: D
The organization can always launch multiple EC2 instances in the same region across multiple AZs for HA and DR. The AWS architecture practice recommends compartmentalizing the functionality such that they can both run in parallel without affecting the performance of the main application. In this scenario logging takes a longer time due to the large size of the log file. Thus, it is recommended that the organization should separate them out and make separate modules and make asynchronous calls among them. This way the application can scale as per the requirement and the performance will not bear the impact of logging.
Reference:
http://www.AWS architectureblog.com/2014/03/AWS -and-compartmentalization.html

526. On Amazon EC2, a business is operating a commercial Apache Hadoop cluster. This cluster is used on a regular basis to perform queries on huge files stored on Amazon S3. Amazon S3 data has been vetted and does not need any extra changes. The organization is running queries against the Hadoop cluster and visualizing the data using a commercial business intelligence (BI) application on Amazon EC2.
The organization wishes to minimize or eliminate overhead expenses associated with administering the Hadoop cluster and the business intelligence application. The organization wishes to make a seamless transition to a more cost-effective option. The visualization is straightforward and takes just a few simple aggregation processes.

Which solution best meets the needs of the business?
A. Launch a transient Amazon EMR cluster daily and develop an Apache Hive script to analyze the files on Amazon S3. Shut down the Amazon EMR cluster when the job is complete. Then use Amazon QuickSight to connect to Amazon EMR and perform the visualization.
B. Develop a stored procedure invoked from a MySQL database running on Amazon EC2 to analyze the files in Amazon S3. Then use a fast in-memory BI tool running on Amazon EC2 to visualize the data.
C. Develop a script that uses Amazon Athena to query and analyze the files on Amazon S3. Then use Amazon QuickSight to connect to Athena and perform the visualization.
D. Use a commercial extract, transform, load (ETL) tool that runs on Amazon EC2 to prepare the data for processing. Then switch to a faster and cheaper BI tool that runs on Amazon EC2 to visualize the data from Amazon S3.

答案:C

解析:

527. An company intends to employ NoSQL DB to meet its scalable data storage requirements. The business wishes to safely host an application on an AWS VPC .

What course of action should the company take?
A. The organization should setup their own NoSQL cluster on the AWS instance and configure route tables and subnets.
B. The organization should only use a DynamoDB because by default it is always a part of the default subnet provided by AWS .
C. The organization should use a DynamoDB while creating a table within the public subnet.
D. The organization should use a DynamoDB while creating a table within a private subnet.
答案:A
解析: Correct Answer: A
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web
Services (AWS) cloud. The user has complete control over the virtual networking environment. Currently VPC does not support DynamoDB. Thus, if the user wants to implement VPC , he has to setup his own NoSQL DB within the VPC .
Reference:
http://docs.AWS .amazon.com/AmazonVPC /latest/UserGuide/VPC _Introduction.html
Question #58

528. A user is building a Volume with Provisioned IOPS.

What is the maximum ratio of Provisioned IOPS to volume size that the user should configure?
A. 30 to 1
B. 50 to 1
C. 10 to 1
D. 20 to 1
答案:B
解析: Correct Answer: B
Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. An io1 volume can range in size from 4 GiB to 16 TiB and you can provision 100 up to 20,000 IOPS per volume. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1. For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS. Any volume 400
GiB in size or greater allows provisioning up to the 20,000 IOPS maximum.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/EBSVolumeTypes.html
Question #59

529. In two regions: us-east-1 and eu-west-1, a corporation implemented a three-tier web application. The application must be operational in both areas concurrently. The application's database layer utilizes a single Amazon RDS Aurora database worldwide, with the master located in us-east-1 and a read replica located in eu-west-1. A VPN connects the two locations.
The firm wants to guarantee that the application stays online even if all of the application's components fail at the

region level. For up to one hour, the program may be in read-only mode. The corporation intends to create two separate Amazon Route 53 record sets, one for each area.

How should the business finish the setup to satisfy its needs while ensuring the application's end users experience the least amount of delay possible? (Select two.)
A. Use failover routing and configure the us-east-1 record set as primary and the eu-west-1 record set as secondary. Configure an HTTP health check for the web application in us-east-1, and associate it to the us-east-1 record set.
B. Use weighted routing and configure each record set with a weight of 50. Configure an HTTP health check for each region, and attach it to the record set for that region.
C. Use latency-based routing for both record sets. Configure a health check for each region and attach it to the record set for that region.
D. Configure an Amazon CloudWatch alarm for the health checks in us-east-1, and have it invoke an AWS Lambda function that promotes the read replica in eu- west-1.
E. Configure Amazon RDS event notifications to react to the failure of the database in us-east-1 by invoking an AWS Lambda function that promotes the read replica in eu-west-1.
答案:CE

530. A user is attempting to create a PIOPS volume.

What is the maximum PIOPS-to-volume-size ratio that the user should configure?
A. 5
B. 10
C. 20
D. 30
答案:D
解析: Correct Answer: D
Provisioned IOPS volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput. A provisioned IOPS volume can range in size from 10 GB to 1 TB and the user can provision up to 4000 IOPS per volume.
The ratio of IOPS provisioned to the volume size requested can be a maximum of 30; for example, a volume with 3000 IOPS must be at least 100 GB.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/EBSVolumeTypes.html

531. An business wishes to expand its data center by connecting it through the VPN gateway to the AWS VPC . The organization is establishing a VPN connection that is dynamically routed.

Which of the following responses is not necessary for this configuration to be set up?
A. The type of customer gateway, such as Cisco ASA, Juniper J-Series, Juniper SSG, Yamaha.
B. Elastic IP ranges that the organization wants to advertise over the VPN connection to the VPC .
C. Internet-routable IP address (static) of the customer gateway's external interface.
D. Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway.

答案:B
解析: Correct Answer: B
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a

private, isolated section of the Amazon Web
Services (AWS) cloud. The user has complete control over the virtual networking environment. The organization wants to extend their network into the cloud and also directly access the internet from their AWS VPC . Thus, the organization should setup a Virtual Private Cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with their data center network over an IPsec VPN tunnel. To setup this configuration the organization needs to use the Amazon VPC with a VPN connection. The organization network administrator must designate a physical appliance as a customer gateway and configure it. The organization would need the below mentioned information to setup this configuration:
The type of customer gateway, such as Cisco ASA, Juniper J-Series, Juniper SSG, Yamaha Internet-routable IP address (static) of the customer gateway's external interface Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway, if the organization is creating a dynamically routed VPN connection. Internal network IP ranges that the user wants to advertise over the VPN connection to the VPC .
Reference:
http://docs.AWS .amazon.com/AmazonVPC /latest/UserGuide/VPC _VPN.html

532. A business must operate software that is licensed to be executed on a single physical host for the length of its usage. The software package will be utilized for a period of 90 days. Every 30 days, the organization demands that all instances be patched and restarted.

How may AWS be used to meet these requirements?
A. Run a dedicated instance with auto-placement disabled.
B. Run the instance on a dedicated host with Host Affinity set to Host.
C. Run an On-Demand Instance with a Reserved Instance to ensure consistent placement.
D. Run the instance on a licensed host with termination set for 90 days.

答案:B
解析:

533. You're creating an IAM policy and want to establish permissions for a role. Which of the configuration formats listed below should you use?
A. An XML document written in the IAM Policy Language
B. An XML document written in a language of your choice
C. A JSON document written in the IAM Policy Language
D. JSON document written in a language of your choice
答案:C
解析: Correct Answer: C
You define the permissions for a role in an IAM policy. An IAM policy is a JSON document written in the IAM Policy Language.
Reference:
http://docs.AWS .amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html

534. The access policy and the trust policy are the two policies that you may associate with an IAM job. By adding the _____ action to the AWS Lambda account principal, the trust policy specifies who may take the position and authorizes authorization in the AWS Lambda account principle.
A. AWS :AssumeAdmin
B. lambda:InvokeAsync
C. sts:InvokeAsync
D. sts:AssumeRole

答案:D
解析: Correct Answer: D
The two policies that you attach to an IAM role are the access policy and the trust policy. Remember that adding an account to the trust policy of a role is only half of establishing the trust relationship. By default, no users in the trusted accounts can assume the role until the administrator for that account grants the users the permission to assume the role by adding the Amazon Resource Name (ARN) of the role to an Allow element for the sts:AssumeRole action.
Reference:
http://docs.AWS .amazon.com/IAM/latest/UserGuide/id_roles_manage_modify.html

535. ec2ifscan is one of the components of ec2-net-utils that is used with ENI's.

Which of the following statements regarding ec2-net-utils is incorrect?
A. ec2-net-utils generates an interface configuration file suitable for use with DHCP.
B. ec2-net-utils extends the functionality of the standard if up.
C. ec2-net-utils detaches a primary network interface from an instance.
D. ec2-net-utils identifies network interfaces when they are attached, detached, or reattached to a running instance.

答案:C
解析: Correct Answer: C
Each instance in a VPC has a default elastic network interface (the primary network interface) that is assigned a private IP address from the IP address range of your VPC . You cannot detach a primary network interface from an instance. You can create and attach additional elastic network interfaces. Amazon Linux AMIs may contain additional scripts installed by AWS , known as ec2-net-utils. One of the components that is part of ec2-net-utils used with ENI's is ec2ifscan. Its function is to check for network interfaces that have not been configured and configure them.
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/using-eni.html

536. You've deployed a sizable quantity of network gear on AWS and now need to consider monitoring it all. You determine that CloudWatch is the greatest match for your requirements, but you are unclear about CloudWatch's price structure and limits.

Which of the following claims about CloudWatch's limitations is TRUE?
A. You get 10 CloudWatch metrics, 10 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per customer per month for free.
B. You get 100 CloudWatch metrics, 100 alarms, 10,000,000 API requests, and 10,000 Amazon SNS email notifications per customer per month for free.
C. You get 10 CloudWatch metrics, 10 alarms, 1,000 API requests, and 100 Amazon SNS email notifications per customer per month for free.
D. You get 100 CloudWatch metrics, 100 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per customer per month for free.

答案:A
解析: Correct Answer: A
Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications.
CloudWatch has the following limits:
You get 10 CloudWatch metrics, 10 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per

customer per month for free.
You can assign up to 10 dimensions per metric.
You can create up to 5000 alarms per AWS account. Metric data is kept for 2 weeks.
The size of a PutMetricData request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests.
You can include a maximum of 20 MetricDatum items in one PutMetricData request. A MetricDatum can contain a single value or a StatisticSet representing many values.
Reference:
http://docs.AWS .amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_limits.html

537. A business has containerized and deployed application services on various Amazon EC2 instances with public IP addresses. On the EC2 instances, an Apache Kafka cluster has been installed. Amazon RDS for PostgreSQL has been used to migrate a PostgreSQL database. The firm anticipates a big rise in order volume on its platform after the launching of a new version of its main product.

Which improvements to the present design will result in lower operating costs and better support for the product's release?
A. Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
B. Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.
D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

答案:B
解析:

538. A fitness monitoring firm services consumers worldwide, with the majority of its revenue coming from North America and Asia. The corporation must create an infrastructure that meets the following criteria for its read-intensive user authorization application:
Be robust to application-related issues in any Region.
In a single Region, write to a database.
Read from a variety of regions.
In each Region, provide resilience across application layers.
Sustain the application's relational database semantics.

Which actions should a solutions architect do in combination? (Select two.)
A. Use an Amazon Route 53 geoproximity routing policy combined with a multivalue answer routing policy.
B. Deploy web, application, and MySQL database servers to Amazon EC2 instance in each Region. Set up the application so that reads and writes are local to the Region. Create snapshots of the web, application, and database servers and store the snapshots in an Amazon S3 bucket in both Regions. Set up cross- Region replication for the database layer.

C. Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy.
D. Set up web, application, and Amazon RDS for MySQL instances in each Region. Set up the application so that reads are local and writes are partitioned based on the user. Set up a Multi-AZ failover for the web, application, and database servers. Set up cross-Region replication for the database layer.
E. Set up active-active web and application servers in each Region. Deploy an Amazon Aurora global database with clusters in each Region. Set up the application to use the in-Region Aurora database endpoints. Create snapshots of the web application servers and store them in an Amazon S3 bucket in both Regions.

答案:BD
解析:

539. AWS has introduced T2 instances with credit for CPU consumption. A business has a need that an instance be operational for 24 hours. However, the group is most active between the hours of 11 a.m. and 12 p.m. The firm intends to accomplish this goal by using a T2 tiny instance.

If the company has been operating numerous instances since January 2012, which of the following choices should it use when creating a T2 instance?
A. The organization must migrate to the EC2-VPC platform first before launching a T2 instance.
B. While launching a T2 instance the organization must create a new AWS account as this account does not have the EC2-VPC platform.
C. Create a VPC and launch a T2 instance as part of one of the subnets of that VPC .
D. While launching a T2 instance the organization must select EC2-VPC as the platform.

答案:C
解析: Correct Answer: C
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC . The
AWS account provides two platforms:
EC2-CLASSIC and EC2-VPC , depending on when the user has created his AWS account and which regions he is using. If the user has created the AWS account after 2013-12-04, it supports only EC2-VPC . In this scenario, since the account is before the required date the supported platform will be EC2-CLASSIC. It is required that the organization creates a VPC as the T2 instances can be launched only as a part of VPC .
Reference:
http://docs.AWS .amazon.com/AWS EC2/latest/UserGuide/VPC -migrate.html
Question #70

540. You're working on a new mobile application and contemplating using AWS to store user preferences. 2w This would give a more consistent cross-device experience for consumers who access the application through numerous mobile devices. Each user's preference data is projected to be 50KB in size. Additionally, the program is planned to be used on a daily basis by 5 million subscribers.

How would you build a system that is cost-effective, highly available, scalable, and secure?
A. 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
B. 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.
C. 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.
D. 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’ 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.

答案:B
解析: Correct Answer: B
Here are some of the things that you can build using fine-grained access control:
A mobile app that displays information for nearby airports, based on the user’s location. The app can access and display attributes such airline names, arrival times, and flight numbers. However, it cannot access or display pilot names or passenger counts.
A mobile game which stores high scores for all users in a single table. Each user can update their own scores, but has no access to the other ones.
Reference:
https://AWS .amazon.com/blogs/AWS /fine-grained-access-control-for-amazon-dynamodb/

541. A business maintains many AWS accounts for the purpose of hosting IT applications. On every Amazon EC2 instances, an Amazon CloudWatch Logs agent is deployed. The organization want to concentrate all security incidents in a dedicated AWS account for log storage.
Security administrators must collect and correlate events across numerous AWS accounts in near-real time.

Which solution meets these criteria?
A. Create a Log Audit IAM role in each application AWS account with permissions to view CloudWatch Logs, configure an AWS Lambda function to assume the Log Audit role, and perform an hourly export of CloudWatch Logs data to an Amazon S3 bucket in the logging AWS account.
B. Configure CloudWatch Logs streams in each application AWS account to forward events to CloudWatch Logs in the logging AWS account. In the logging AWS account, subscribe an Amazon Kinesis Data Firehose stream to Amazon CloudWatch Events, and use the stream to persist log data in Amazon S3.
C. Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to CloudWatch Logs streams in each application AWS account, configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams as its source, and persist the log data in an Amazon S3 bucket inside the logging AWS account.
D. Configure CloudWatch Logs agents to publish data to an Amazon Kinesis Data Firehose stream in the logging AWS account, use an AWS Lambda function to read messages from the stream and push messages to Data Firehose, and persist the data in Amazon S3.

答案:C
解析: Correct Answer: C
Reference:
https://noise.getoto.net/2018/03/03/central-logging-in-multi-account-environments/

542. What is the indication that an object has been successfully stored in Amazon S3?
A. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
B. Amazon S3 is engineered for 99.999999999% durability. Therefore there is no need to confirm that data was inserted.
C. A success code is inserted into the S3 object metadata.
D. Each S3 account has a special bucket named _s3_logs. Success codes are written to this bucket with a timestamp and checksum.

答案:A
解析:

543. A significant financial institution is utilizing AWS CloudFormation to deliver apps to the AWS Cloud using Amazon EC2 and Amazon RDS instances.
CloudFormation's stack policy is as follows:

```
{
      "Statement" : [
         {
            "Effect" : "Allow",
            "Action" : ["Update:*"],
            "Principal": "*",
            "Resource" : "*"
         }
      ]
}
```

The organization aims to guarantee that developers do not lose data while changing the CloudFormation stack by mistakenly deleting or replacing RDS instances.
Additionally, developers must be allowed to alter or delete EC2 instances as required.

What changes should be made to the company's stack policy to comply with these requirements?
A. Modify the statement to specify ƛ €Effectƛ €: ƛ €Denyƛ €, ƛ €Actionƛ €:[ƛ €Update:*ƛ €] for all logical RDS resources.
B. Modify the statement to specify ƛ €Effectƛ €: ƛ €Denyƛ €, ƛ €Actionƛ €:[ƛ €Update:Deleteƛ €] for all logical RDS resources.
C. Add a second statement that specifies ƛ €Effectƛ €: ƛ €Denyƛ €, ƛ €Actionƛ €:[ƛ €Update:Deleteƛ €, ƛ € Update:Replaceƛ €] for all logical RDS resources.
D. Add a second statement that specifies ƛ €Effectƛ €: ƛ €Denyƛ €, ƛ €Actionƛ €:[ƛ €Update:*ƛ €] for all logical RDS resources.

答案:C
解析:

544. AWS is used by an enterprise to run a scalable online application. To scale the application, the business has implemented ELB and Auto Scaling.

Which of the following assertions is not necessary when an application intends to run a web application on VPC ?
A. The ELB and all the instances should be in the same subnet.
B. Configure the security group rules and network ACLs to allow traffic to be routed between the subnets in the VPC .
C. The internet facing ELB should have a route table associated with the internet gateway.
D. The internet facing ELB should be only in a public subnet.

答案:A
解析: Correct Answer: A
Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services
(AWS) cloud. The user has complete control over the virtual networking environment. Within this virtual private

cloud, the user can launch AWS resources, such as an ELB, and EC2 instances. There are two ELBs available with VPC : internet facing and internal (private) ELB. For the internet facing ELB it is required that the
ELB should be in a public subnet. After the user creates the public subnet, he should ensure to associate the route table of the public subnet with the internet gateway to enable the load balancer in the subnet to connect with the internet. The ELB and instances can be in a separate subnet. However, to allow communication between the instance and the ELB the user must configure the security group rules and network ACLs to allow traffic to be routed between the subnets in his VPC .
Reference:
http://docs.AWS .amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/CreateVPC ForELB.html

545. A business employed Amazon EC2 instances to deploy a web fleet for the purpose of hosting a blog. The EC2 instances are configured in an Auto Scaling group and are behind an Application Load Balancer (ALB). All blog material is stored on an Amazon EFS disk by the web application.
The firm recently implemented a tool that allows bloggers to include video in their postings, which resulted in a tenfold increase in user traffic. Users report experiencing buffering and timeout difficulties when trying to access the site or view videos at busiest periods of the day.

Which deployment option is the most cost-effective and scalable in terms of resolving customer issues?
A. Reconfigure Amazon EFS to enable maximum I/O.
B. Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.
C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
D. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.

答案:C
解析:

546. What is the maximum length of a role name in Amazon IAM?
A. 128 characters
B. 512 characters
C. 64 characters
D. 256 characters

答案:C
解析: Correct Answer: C
In Amazon IAM, the maximum length for a role name is 64 characters.
Reference:
http://docs.AWS .amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

547. MapMySite is configuring an AWS virtual private cloud (VPC) for a web application. The firm has chosen to utilize an AWS RDS instance rather than its own database instance to meet its high availability and disaster recovery needs.
Additionally, the business wishes to safeguard RDS access.

How should an RDS-enabled web application be configured?

A. 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.
B. Setup a public and two private subnets in different AZs within a VPC and create a subnet group. Launch RDS with that subnet group.
C. Create a network interface and attach two subnets to it. Attach that network interface with RDS while launching a DB instance.
D. Create two separate VPC s and launch a Web app in one VPC and RDS in a separate VPC and connect them with VPC peering.
答案:B
解析: Correct Answer: B
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources, such as RDS into a virtual network that the user has defined. Subnets are segments of a VPC 's IP address range that the user can designate to a group of VPC resources based on the security and operational needs.
A DB subnet group is a collection of subnets (generally private) that a user can create in a VPC and assign to the RDS DB instances. A DB subnet group allows the user to specify a particular VPC when creating the DB instances. Each DB subnet group should have subnets in at least two Availability Zones in a given region.
Reference:
http://docs.AWS .amazon.com/AmazonRDS/latest/UserGuide/USER_VPC .html

548. A firm is using Elastic Beanstalk to create a highly scalable application. The firm utilizes ELB and RDS in conjunction with VPC . Within the cloud, the company has both public and private subnets.

Which of the setups listed below will not work in this scenario?
A. To setup RDS in a private subnet and ELB in a public subnet.
B. The configuration must have public and private subnets in the same AZ.
C. The configuration must have two private subnets in separate AZs.
D. The EC2 instance should have a public IP assigned to it.

答案:D
解析: Correct Answer: D
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web
Services (AWS) cloud. The user has complete control over the virtual networking environment. If the organization is planning to implement a scalable secure application using RDS, VPC and ELB the organization should follow below mentioned configurations:
Setup RDS in a private subnet Setup ELB in a public subnet
Since RDS needs a subnet group, the organization should have two private subnets in the same zone
The ELB needs private and public subnet to be part of same AZs It is not required that instances should have a public IP assigned to them. The instances can be a part of a private subnet and the organization can setup a corresponding routing mechanism.
Reference:
http://docs.AWS .amazon.com/elasticbeanstalk/latest/dg/VPC -rds.html

549. On AWS , a business is now operating a production workload that is very I/O heavy. Its workload is distributed over a single tier and is comprised of ten c4.8xlarge instances, each with a 2 TB gp2 volume. Recently, both the quantity of processing tasks and latency have grown. The crew is aware that they are limited by the IOPS. They need

to boost the IOPS by 3,000 for each instance in order for the application to run effectively.

Which of the following designs will most effectively achieve the performance objective?
A. Change the type of Amazon EBS volume from gp2 to io1 and set provisioned IOPS to 9,000.
B. Increase the size of the gp2 volumes in each instance to 3 TB.
C. Create a new Amazon EFS file system and move all the data to this new file system. Mount this file system to all 10 instances.
D. Create a new Amazon S3 bucket and move all the data to this new bucket. Allow each instance to access this S3 bucket and use it for storage.

答案:B
解析:

550. A security audit is being conducted on a company. The auditor is requesting access to the AWS VPC settings, since the business has hosted all apps on AWS . The auditor is located in a faraway location and requires access to AWS in order to see all VPC information.

How can the firm satisfy the auditor's requirements without jeopardizing the security of its AWS infrastructure?
A. The organization should not accept the request as sharing the credentials means compromising on security.
B. Create an IAM role which will have read only access to all EC2 services including VPC and assign that role to the auditor.
C. Create an IAM user who will have read only access to the AWS VPC and share those credentials with the auditor.
D. 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.

答案:c
解析: Correct Answer: C
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC . The
VPC also works with IAM and the organization can create IAM users who have access to various VPC services. If an auditor wants to have access to the AWS
VPC to verify the rules, the organization should be careful before sharing any data which can allow making updates to the AWS infrastructure. In this scenario it is recommended that the organization creates an IAM user who will have read only access to the VPC . Share the above mentioned credentials with the auditor as it cannot harm the organization. The sample policy is given below:
{
"Effect":"Allow", "Action": ["ec2:DescribeVPC s", "ec2:DescribeSubnets",
"ec2: DescribeInternetGateways", "ec2:DescribeCustomerGateways", "ec2:DescribeVpnGateways",
"ec2:DescribeVpnConnections", "ec2:DescribeRouteTables",
"ec2:DescribeAddresses", "ec2:DescribeSecurityGroups", "ec2:DescribeNetworkAcls", "ec2:DescribeDhcpOptions",
"ec2:DescribeTags", "ec2:DescribeInstances"
],
"Resource":"*"
}
Reference:
http://docs.AWS .amazon.com/AmazonVPC /latest/UserGuide/VPC _IAM.html

551. An AWS IAM policy's Statement element comprises an array of individual statements. Eacheach statement is encased in braces （ as a（n）

Block
A. XML
B. JavaScript
C. JSON
D. AJAX

答案:C
解析: Correct Answer: C
The Statement element, of an IAM policy, contains an array of individual statements. Each individual statement is a JSON block enclosed in braces { }.
Reference:
http://docs.AWS .amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

552. A business already has an on-premises three-tier web application. Because the material is updated multiple times a day from numerous sources, the Linux web servers provide it through a centralized file share on a NAS server. The current infrastructure is inefficient, and the organization want to migrate to AWS in order to have the capacity to dynamically scale resources in response to demand. AWS Direct Link is used to connect on-premises and AWS resources.

How can the organization transition its online infrastructure to AWS without causing a delay in the process of content refreshment?
A. Create a cluster of web server Amazon EC2 instances behind a Classic Load Balancer on AWS . Share an Amazon EBS volume among all instances for the content. Schedule a periodic synchronization of this volume and the NAS server.
B. Create an on-premises file gateway using AWS Storage Gateway to replace the NAS server and replicate content to AWS . On the AWS side, mount the same Storage Gateway bucket to each web server Amazon EC2 instance to serve the content.
C. Expose an Amazon EFS share to on-premises users to serve as the NAS serve. Mount the same EFS share to the web server Amazon EC2 instances to serve the content.
D. Create web server Amazon EC2 instances on AWS in an Auto Scaling group. Configure a nightly process where the web server instances are updated from the NAS server.
答案:B
解析:

553. A firm uses Amazon API Gateway, Amazon DynamoDB, and AWS Lambda to run a blog post application on AWS . At the moment, the application does not utilize API keys to authorize queries. The following is the API model:
To get detailed information on a post, use the GET/posts/[postid] method.
GET/users[userid] to get user information
To get detailed information about a remark, use the GET/comments/[commentid] method.
The organization has observed that customers are actively debating themes in the comments area and want to improve user engagement by highlighting remarks as they come in real time.

Which design should be adopted to enhance user experience and decrease comment latency?
A. Use edge-optimized API with Amazon CloudFront to cache API responses.
B. Modify the blog application code to request GET comment[commented] every 10 seconds.
C. Use AWS AppSync and leverage WebSockets to deliver comments.
D. Change the concurrency limit of the Lambda functions to lower the API response time.

答案:D

解析:

554. For Amazon EC2 difficulties, you must check the cloud-init and cfn logs when troubleshooting AWS CloudFormation.

Determine a directory in which these logs will be stored.
A. /var/opt/log/ec2
B. /var/log/lastlog
C. /var/log/
D. /var/log/ec2

答案:C
解析: Correct Answer: C
When you use AWS CloudFormation, you might encounter issues when you create, update, or delete AWS CloudFormation stacks.
For Amazon EC2 issues, view the cloud-init and cfn logs. These logs are published on the Amazon EC2 instance in the /var/log/ directory. These logs capture processes and command outputs while AWS CloudFormation is setting up your instance. For Windows, view the EC2Configure service and cfn logs in %
ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.
You can also configure your AWS CloudFormation template so that the logs are published to Amazon CloudWatch, which displays logs in the AWS Management
Console so you don't have to connect to your Amazon EC2 instance.
Reference:
http://docs.AWS .amazon.com/AWS CloudFormation/latest/UserGuide/troubleshooting.html

555. Polling an Amazon SQS queue and updating entries in an Amazon DynamoDB database is accomplished using a fleet of Amazon ECS instances. The table is not being updated, and the SQS queue is rapidly growing. When trying to update the table, Amazon CloudWatch Logs consistently display 400 failures. The supplied write capacity units are set adequately, and there is no throttling.

Which of the following is the MOST LIKELY cause of the failure?
A. The ECS service was deleted.
B. The ECS configuration does not contain an Auto Scaling group.
C. The ECS instance task execution IAM role was modified.
D. The ECS task role was modified.

答案:C
解析:

556. Due to authorization difficulties on an Amazon S3 bucket, a corporation faced a compromise of very private personal information. To further limit access, the Information Security team has tightened the bucket policy. Additionally, the following needs must be satisfied in order to be better prepared for future attacks:
- Determine which external IP addresses are attempting to access the bucket objects.
- Receive notifications when the bucket's security policy is modified.
- Automatically rectify policy changes.

Which tactics should be used by the Solutions Architect?
A. Use Amazon CloudWatch Logs with CloudWatch filters to identify remote IP addresses. Use CloudWatch Events rules with AWS Lambda to automatically remediate S3 bucket policy changes. Use Amazon SES with CloudWatch

Events rules for alerts.
B. Use Amazon Athena with S3 access logs to identify remote IP addresses. Use AWS Config rules with AWS Systems Manager Automation to automatically remediate S3 bucket policy changes. Use Amazon SNS with AWS Config rules for alerts.
C. Use S3 access logs with Amazon Elasticsearch Service and Kibana to identify remote IP addresses. Use an Amazon Inspector assessment template to automatically remediate S3 bucket policy changes. Use Amazon SNS for alerts.
D. Use Amazon Macie with an S3 bucket to identify access patterns and remote IP addresses. Use AWS Lambda with Macie to automatically remediate S3 bucket policy changes. Use Macie automatic alerting capabilities for alerts.

答案:B
解析:

557. If you use and the request originates from an Amazon EC2 instance when applying the policy keys in AWS Direct Connect, the instance's public IP address is checked to determine if access is permitted.
A. AWS :SecureTransport
B. AWS :EpochIP
C. AWS :SourceIp
D. AWS :CurrentTime

答案:C
解析: Correct Answer: C
While implementing the policy keys in Amazon RDS, if you use AWS : SourceIp and the request comes from an Amazon EC2 instance, the instance's public IP address is evaluated to determine if access is allowed.
Reference:
http://docs.AWS .amazon.com/directconnect/latest/UserGuide/using_iam.html

558. Which of the following procedures is not available using the DynamoDB console?
A. Updating an item
B. Copying an item
C. Blocking an item
D. Deleting an item

答案:C
解析: Correct Answer: C
By using the console to manage DynamoDB, you can perform the following: adding an item, deleting an item, updating an item, and copying an item.
Reference:
http://docs.AWS .amazon.com/amazondynamodb/latest/developerguide/AddUpdateDeleteItems.html

559.A user is attempting to construct a vault in Amazon Web Services Glacier. The user desires notification enablement.

Which of the following settings allows the user to activate AWS console notifications?
A. Glacier does not support the AWS console
B. Archival Upload Complete
C. Vault Upload Job Complete
D. Vault Inventory Retrieval Job Complete

答案:D

解析: Correct Answer: D
From AWS console the user can configure to have notifications sent to Amazon Simple Notifications Service (SNS). The user can select specific jobs that, on completion, will trigger the notifications such as Vault Inventory Retrieval Job Complete and Archive Retrieval Job Complete.
Reference:
http://docs.AWS .amazon.com/amazonglacier/latest/dev/configuring-notifications-console.html

560. Using the VPC wizard, a user constructed a VPC using the CIDR 20.0.0.0/16. To connect to the user's data center, the user has built public and VPN-only subnets, as well as hardware VPN access. The user has not yet started any instances or edited or removed any configurations. He wants to erase this virtual private cloud from the console.

Is it possible for the user to erase the VPC from the console?
A. Yes, the user can detach the virtual private gateway and then use the VPC console to delete the VPC .
B. No, since the NAT instance is running, the user cannot delete the VPC .
C. Yes, the user can use the CLI to delete the VPC that will detach the virtual private gateway automatically.
D. No, the VPC console needs to be accessed using an administrator account to delete the VPC .

答案:A
解析: Correct Answer: A
You can delete your VPC at any time (for example, if you decide it's too small). However, you must terminate all instances in the VPC first. When you delete a
VPC using the VPC console, Amazon deletes all its components, such as subnets, security groups, network ACLs, route tables, Internet gateways, VPC peering connections, and DHCP options. If you have a VPN connection, you don't have to delete it or the other components related to the VPN (such as the customer gateway and virtual private gateway).
Reference:
http://docs.AWS .amazon.com/AmazonVPC /latest/UserGuide/VPC _Subnets.html#VPC _Deleting

561. Every day, a photo-sharing and publishing firm gets between 10,000 and 150,000 photographs. The firm obtains the photographs from a variety of providers and registered users. The organization is migrating to AWS and want to augment current information via the use of Amazon Rekognition.
As an illustration of the extra data, consider the following:

```
list celebrities [name of the personality] wearing [color] looking
[happy, sad] near [location example Eiffel Tower in Paris]
```

The organization moved existing picture data to Amazon S3 as part of the cloud migration initiative and instructed consumers to contribute photographs directly to Amazon S3.

What actions should the Solutions Architect take to ensure that these criteria are met?
A. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon DynamoDB to store the metadata and Amazon ES to create an index. Use a web front-end to provide search capabilities backed by Amazon ES.
B. Use Amazon Kinesis to stream data based on an S3 event. Use an application running in Amazon EC2 to extract metadata from the images. Then store the data on Amazon DynamoDB and Amazon CloudSearch and create an index. Use a web front-end with search capabilities backed by CloudSearch.
C. Start an Amazon SQS queue based on S3 event notifications. Then have Amazon SQS send the metadata information to Amazon DynamoDB. An application running on Amazon EC2 extracts data from Amazon Rekognition using the API and adds data to DynamoDB and Amazon ES. Use a web front-end to provide search capabilities backed by Amazon ES.

D. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon RDS MySQL Multi-AZ to store the metadata information and use Lambda to create an index. Use a web front-end with search capabilities backed by Lambda.

答案:D
解析:

562. Personal identifiable information is logged by a financial services organization in its application logs, which are saved in Amazon S3. The log files must be encrypted at rest to comply with regulatory compliance standards. The security team has specified that the CMK content be generated using the company's on-premises hardware security modules (HSMs).

What procedures should the solutions architect take to ensure compliance with these requirements?
A. Create an AWS CloudHSM cluster. Create a new CMK in AWS KMS using AWS _CloudHSM as the source for the key material and an origin of AWS _CLouDHSM. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket that disallows uploads of unencrypted data and requires that the encryption source be AWS KMS.
B. Provision an AWS Direct Connect connection, ensuring there is no overlap of the RFC 1918 address space between on-premises hardware and the VPC s. Configure an AWS bucket policy on the logging bucket that requires all objects to be encrypted. Configure the logging application to query the on-premises HSMs from the AWS environment for the encryption key material, and create a unique CMK for each logging event.
C. Create a CMK in AWS KMS with no key material and an origin of EXTERNAL. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AWS . Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.
D. Create a new CMK in AWS KMS with AWS -provided key material and an origin of AWS _KMS. Disable this CMK, and overwrite the key material with the key material from the on-premises HSM using the public key and import token provided by AWS . Re-enable the CMK. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.

答案:D
解析:

563. When does an AWS Data Pipeline end the computing resources maintained by the AWS Data Pipeline?
A. AWS Data Pipeline terminates AWS Data Pipeline-managed compute resources every 2 hours.
B. When the final activity that uses the resources is running
C. AWS Data Pipeline terminates AWS Data Pipeline-managed compute resources every 12 hours.
D. When the final activity that uses the resources has completed successfully or failed

答案:D
解析: Correct Answer: D
Compute resources will be provisioned by AWS Data Pipeline when the first activity for a scheduled time that uses those resources is ready to run, and those instances will be terminated when the final activity that uses the resources has completed successfully or failed.
Reference:
https://AWS .amazon.com/datapipeline/faqs/

564. A business wishes to transition its on-premises data analytics infrastructure to AWS . Two simple Node.js apps

comprise the environment. One of the apps gathers and stores sensor data in a MySQL database. The other program generates reports from the data. When the aggregation tasks are executed, some of the load jobs fail to execute properly.
The company's data loading problem must be resolved. Additionally, the firm requires that the move take place without causing any disruptions or modifications to the company's clients.

What actions should a solutions architect take to ensure that these criteria are met?
A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer (NLB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the NLB.
B. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Move the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS .
C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS .
D. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as an Amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream.

答案:B
解析:

565.A company is using AWS Organizations to manage multiple AWS accounts For security purposes, the company requires the creation of an Amazon Simple Notification Service（Amazon SNS） topic that enables integration with a third-party alerting system in all the Organizations member accounts
A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.
What should the solutions architect do to deploy the CloudFormation Stack Sets in all AWS accounts?
A. Create a stack set in the Organizations member accounts. Use service-managed permissions Set deployment options to deploy to an organization Use CloudFormation stack Sets drift detection
B. Create stacks in the Organizations member accounts Use self-service permissions Set deployment options to deploy to an organization. Enable the CloudFormation Stack Sets automatic deployment
C. Create a stack set in the Organizations management account. Use service-managed permissions Set deployment options to deploy to the organization. Enable CloudFormation Stack Sets automatic deployment
D. Create stacks in the Organizations managemet account. Use service-managed permissions Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection

答案:C
解析:

566.a software company is using three AWS accounts for each of its 10 development teams. The company has developed an AWs Cloud Formation standard VPC template that includes three nat gateways. The template is added to each account for each team. The company is concerned that network costs will increase each time a new development team is added. a solutions architect must maintain the reliability of the company' s solutions and minimize operational complexity
What should the solutions architect do to reduce the network costs while meeting these requirements?
A.Create a single VPC with three naT gateways in a shared services account. Configure each account VPC with a default route through a transit gateway to the nat gateway in the shared services account VPC. Remove all nat gateways from the standard VPC template
B. Create a single VPC with three NAT gateways in a shared services account. Configure each account VPC with a default route through a VPC peering connection to the NAt gateway in the shared services account VPC. Remove all NAT gateways from the standard VPC template
C. Remove two NAT gateways from the standard VPC template Rely on the NAT gateway SLA to cover reliability for the remaining NAT gateway
D.Create a single VPC with three NAT gateways in a shared services account. Configure a Site-to-Site VPN connection from each account to the shared services account. Remove all NAT gateways from the standard VPC template

答案:A
解析:

567. A retail company is hosting an ecommerce website on AWS across multiple AWS Regions. The company wants the website to be operational at all times for online purchases. The website stores data in an Amazon RDs for MySQL DB instance
Which solution will provide the HIGHEST availability for the database?
A.Configure automated backups on Amazon RDS. In the case of disruption, promote an automated backup to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source
B. Configure global tables and read replicas on Amazon RDS. Activate the cross-Region scope. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region
C.Configure global tables and automated backups on Amazon RDS. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region
D.Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source
答案:C
解析:

568.A company has more than 10,000 sensors that send data to an on-premises apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol. The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon s3 bucket.

Recently, the Kafka server crashed. The company lost sensor data while the server was being restored. A solutions architect must create a new design on AwS that is highly available and scalable to prevent a similar occurrence
Which solution will meet these requirements?
A.Launch two Amazon EC2 instances to host the Kafka server in an active/standby configuration across two Availability Zones. Create a domain name in Amazon Route 53. Create a Route 53 failover policy. Route the sensors to send the data to the domain name
B.Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka（Amazon MSK）。 Create a Network Load Balancer（NLB）that points to the Amazon MSK broker Enable NLB health checks. Route the sensors to send the data to the nlB
C.Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream. Use an AWS Lambda function to handle data transformation Route the sensors to send the data to AWS IOT Core
D. Deploy AWS IoT Core, and launch an Amazon EC2 instance to host the Kafka server. Configure AWS IoT Core to send the data to the EC2 instance. Route the sensors to send the data to AWS IoT Core
答案:C
解析:

569.a company is running a log processing application on an Amazon Elastic Container Service（Amazon ECS）cluster on Amazon EC2 instances. The instances use a 40 GB General Purpose SSD（gp3 ）Amazon Elastic Block Store （Amazon EBS）root volume. The app plication do ds data from an Amazon s3 bucket in the form of zip files, which can vary in size by up to 5 GB. The application then extracts the data from the zip files, runs log analysis routines, and uploads the results to another S3bucket
The application initially works as expected. However, in 1-2 hours, log processing output slows after a scale out to the cluster's max capacity of 60 instances. All instances are still performing log processing tasks. Initial analysis shows neither a sudden increase in CPU utilization nor a memory-related issue. The application itself is not producing error messages
What should a solutions architect recommend to resolve this issue with the LEast amount of code change?
A.Increase the size of the EC2 instances Use compute optimized instances
B.Increase the IOPS of the root volume to fulfill the requirements of the log processing application
C.Create a 100 GB Provisioned IOPS SSD (io2) EBS volume with 3， 000 Provisioned IOPS Reconfigure the application to use the new volume as a log processing temporary area
D.Change the ECS cluster so that it uses AWS Fargate
答案:C
解析:

570.A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWs and use at least two Availability Zones in each tier.
Company policy requires it to durably store nightly backups of all its data in at least two locations:production and disaster recovery the locations must be in different geographic regions the company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location. All backup processes must be fully automated
What is the MOsT cost-effective backup solution that will meet all requirements
A.Back up all the data to a large Amazon EBS volume attached to the backup media server in the production region. Run automated scripts to snapshot these volumes nightly, and copy these snapshots to the disaster recovery region
B.Back up all the data to Amazon S3 in the disaster recovery region. Use a lifecycle policy to move this data to Amazon Glacier in the production region immediately. Only the data is replicated； remove the data from the S3 bucket in the disaster recovery region

C.Back up all the data to Amazon Glacier in the production region. Set up cross-region replication of this data to Amazon Glacier in the disaster recovery region. Set up a lifecycle policy to delete any data older than 60 days
D.Back up all the data to Amazon S3 in the production region. Set up cross-region replication of this s3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier
答案:D
解析:

571.A company is developing a messaging application that is based on a microservices architecture. a separate team develops each microservice by using Amazon Elastic Container Service（Amazon ECS）。 The teams deploy the microservices multiple times daily by using AWS Cloud Formation and AWS Code Pipeline
The application recently grew in size and complexity. Each service operates correctly on its own during development, but each service produces error messages when it has to interact with other services in production. A solutions architect must improve the application's availability
Which solution will meet these requirements with the LEAST amount of operational overhead?
A.Add an extra stage to CodePipeline for each service. Use the extra stage to deploy each service to a test environment Test each service after deployment to make sure that no error messages occur
B.Add an AWS:Code Deploy Blue Green Transform section and Hook section to the template to enable blue/green deployments by using AWS Code Deploy in CloudFormation. Configure the template to perform ECS blue/green deployments in proauction
C.Add an extra stage to CodePipeline for each service. Use the extra stage to deploy each service to a test environment. Write integration tests for each service. Run the tests automatically after deployment
D.Use an ECS Deployment Configuration parameter in the template to configure AWS CodeDeploy to perform a rolling update of the service. Use a CircuitBreaker property to roll back the deployment if any error occurs during deployment
答案:B
解析:

572.A company wants to allow its marketing team to perform sQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The team manager must have the ability to manage users and groups but no team members should have access to services or resources not required for the SQL queries. Additionally, administrators need to audit the queries made and receive notifications when a query violates rules defined by the security team
AWS Organizations has been used to create a new account and an AWs IAM user with administrator permissions for the team manager
Which design meets these requirements?
A.Apply a service control policy（SCP） that allows access to IAM, Amazon RDs, and AWS CloudTrail Load customer records in Amazon RDs My SQL and train users to run queries using the AWS CLI, Stream the query logs to Amazon CloudWatch Logs from the RDs database instance. Use a subscription filter with AWs Lambda functions to audit and alarm on queries against personal data
B.Apply a service control policy （SCP）that denies access to all services except IAM, Amazon Athena, Amazon S3, and AWS CloudTrail Store customer record files in Amazon S3 and train users to run queries using the CLI via Athena. Analyze CloudTrail events to audit and alarm on queries against personal data
C.Apply a service control policy（SCP）that denies access to all services except IAM, Amazon DynamoDB, and AWS Cloud Trail. Store customer records in DynamoDB and train users to run queries using the AWS CLI. Enable DynamoDB streams to track the queries that are issued and use an AWS Lambda function for real-time monitoring and alerting

D.Apply a service control policy (SCP) that allows access to IAM, Amazon Athena, Amazon S3, and AWS Cloud Trail. Store customer records as files in Amazon S3 and train users to leverage the Amazon S3 Select feature and run queries using the AWS CLI, Enable S3 object-level logging and analyze Cloud Trail events to audit and alarm on queries against personal data
答案:B
解析:

573.A financial services company in North America plans to release a new online web application to its customers on AWS. The company will launch the application in the us-east- 1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover
Which solution will meet these requirements?
A.Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering. In the us-east- 1 VPC, create an Application Load Balancer（ALB）that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group
B. Create a VPC in us-east-1 and a VPC in us-west-1 In the us-east-1 VPC, create an Application Load Balancer （ALB）that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC Create an Amazon Route 53 hosted zone. Create separate records for each ALB. Enable health checks to ensure high availability between Regions
C.Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer（ALB）that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east- 1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC Create an Amazon Route 53 hosted zone, Create separate records for each ALB. Enable health checks and configure a failover routing policy for each record
D.Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer（ALB）that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB. Create an Amazon Route 53 hosted zone. Create a record for the ALB
答案:B
解析:

574.A company is hosting a three-tier web application in an on-premises environment. due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to Aws The application is written in NET and has a dependency on a MySQL database. a solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users
Which steps should the solutions architect take to design an appropriate solution?
A.Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer（NLB）in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NIB
B.Use AWS Cloud Formation to launch a stack containing an Application Load Balancer（ALB） in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora My SQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company 's domain to the ALB
C.Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer （ALB）in each Region. Create a Multi-AZ deployment of an Amazon

Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions
D.Use AWS CloudFormation to launch a stack containing an Application Load Balancer（ALB）in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB
答案:B
解析:

575.A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift. Major updates to the sales data occur on the final calendar day of the month For the remainder of the month, the data warehouse only receives minor daily updates and is primarily used for reading and reporting. Because of this the migration process must start on the first day of the month and must be complete before the next set of updates occur This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse. Because the migration cannot impact normal business network operations the bandwidth allocated to the migration for moving data over the internet is 50 Mbps. The company wants to keep data migration costs low
Which steps will allow the solutions architect to perform the migration within the specified timeline?
A.Install Oracle database software on an Amazon EC2 instance. Configure VPN connectivity between AWs and the company's data center. Configure the Oracle database running on Amazon EC2 to join the Oracle Real Application Clusters（RAC）。 When the Oracle database on Amazon EC2 finishes synchronizing, create an AWS DMS ongoing replication task to migrate the data from the Oracle database on Amazon EC2 to Amazon Redshift. Verify the data migration is complete and perform the cut over to Amazon Redshift
B.Create an AWS Snowball import job. Export a backup of the Oracle data warehouse. Copy the exported data to the Snowball device. Return the Snowball device to AWS. Create an Amazon RDS for Oracle database and restore the backup file to that RDs instance. Create an AWS DMS task to migrate the data from the Rds for Oracle database to Amazon Redshift. Copy daily incremental backups from Oracle in the data center to the rds for Oracle database over the internet. Verify the data migration is complete and perform the cut over to Amazon Redshift
C.Install Oracle database software on an Amazon EC2 instance To minimize the migration time, configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection. Configure the Oracle database running on Amazon EC2 to be a read replica of the data center Oracle database. Start the synchronization process between the company 's on-premises data center and the Oracle database on Amazon EC2. When the oracle database on Amazon EC2 is synchronized with the on-premises database, create an AWS DMS ongoing replication task to migrate the data from the Oracle database read replica that is running on Amazon EC2 to Amazon Redshift. Verify the data migration is complete and perform the cut over to Amazon Redshift
D. Create an AWS Snowball import job. Configure a server in the companys data center with an extraction agent Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema. Create a new project in AWS SCT using the registered data extraction agent. Create a local task and an AWs DMs task in AWS SCT with replication of ongoing changes. Copy data to the snowball device and return the snowball device to AWS Allow AWs DMS to copy data from Amazon S3 to Amazon Redshift. Verify that the data migration is complete and perform the cut over to Amazon Redshift
答案:D
解析:

576.An electric automobile company uses AWs to provide services to drivers around the world. The company has thousands of customers worldwide. The company designed a web-based solution and built the solution as a cloud-native application The company deploys the architecture in a single AWS Region, eu-west-1. The company

uses Elastic Load Balancing and Amazon Elastic Container Service（Amazon ECs）to process the requests and implement business logic. All the application data is stored in Amazon DynamoDB
The application does not currently use encryption. A, solutions architect must ensure that the application encrypts data at rest and in transit
Which solution meets these requirements MOST cost-effectively?
A.Encrypt the data at rest by using an AWS Key Management Service（AWS KMS）CMK Provision certificates for encryption in transit with AWS Certificate Manager （ACM）。 Modify any existing IAM policies to ensure that the existing roles can use the CMK and follow least privilege principles
B.Encrypt the data at rest by using AWs CloudHSM with an Aws Key Management Service（AWS KMS）CMK Provision certificates for encryption in transit with AWS Certificate Manager（ACM）。 Modify any existing IAM policies to ensure that the existing roles can use the CMK and follow least privilege principles
C. Modify any existing IAM policies to ensure that the existing roles follow least privilege principles
D.Encrypt the data at rest and in transit by using an AWS Key Management Service（AWs KMS）CMK. Modify any existing IAM policies to ensure that the existing roles can use the CMK and follow least privilege principles
答案:B
解析:

577.A company has many Aws accounts and uses Aws Organizations to manage all of them. a solutions architect must implement a solution that the company can use to share a common network across multiple accounts The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to. manage the network. Individual accounts cannot have the ability to manage their own networks. However individual accounts must be able to create aws resources within subnets
Which combination of actions should the solutions architect perform to meet these requirements? （Select Two）
A.Create a transit gateway in the infrastructure account
B.Enable resource sharing from the AWs Organizations management account
C.Create VPCs in each AWS account within the organization in AWS Organizations. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account. Peer the VPCs in each individual account with the VPC in the infrastructure account
D.Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each subnet to associate with the resource share
E.Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWs Organizations OU that will use the shared network. Select each prefix list to associate with the resource share
答案:BE
解析:

578.A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging Management requires cost center numbers and project id numbers for all existing and future DynamoDB tables and RDS instances Which strategy should the solutions architect provide to meet these requirements?
A.Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources
B.Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role

C.Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project iD Use SCPs to restrict resource creation that do not have the cost center and project id on the resource
D.Create cost allocation tags to define the cost center and project id and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project id on the resource
答案:B
解析:

579.A company uses AWs Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted
The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config ules to meet the company's policies
Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?
A.Remove the organization's root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard Aws Config rules and deploy them throughout the organization, including the new account
B.Create a temporary oU named Onboarding for the new account. Apply an SCP to the Onboarding oU to allow AWS Config actions. Move the new account to the Production OU when adjustments to AWs Config are complete
C.Convert the organization s root SCPs from deny list sCPs to allow list SCPs to allow the required services only. Temporarily apply an SCP to the organization ' s root that allows Aws Config actions for principals only in the new account
D.Create a temporary OU named Onboarding for the new account. Apply an SCp to the Onboarding oU to allow AWS Config actions. Move the organization s root sCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete
答案:B
解析:

580.A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MysQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWs services with an Rto of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2, and has configured Amazon Route 53 health checks and dNS failover to us-west-2
Which additional step should the solutions architect take?
A.Migrate the database to an Amazon RDS for My SQL instance with a cross-Region read replica in us-west-2
B.Migrate the database to an Amazon Aurora global database with the primary in us-east- 1 and the secondary in us-west-2
C.Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment
D.Create a My SQL standby database on an Amazon EC2 instance in us-west-2
答案:B
解析:

581.A large company in Europe plans to migrate its applications to the Aws Cloud. The company uses multiple AWS accounts for various business groups. a data privacy law requires the company to restrict developer's access to AWS European Regions
What should the solutions archit st do to meet this requirement with the LEaST amount of management overhead?
A.Create IAM users and IAM groups in each account. Create IAM policies to limit access to non-European Regions Attach the IAM policies to the IAM groups
B. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions Create SCPs to limit access to non-European Regions and attach the policies to the OUs
C. Set up AWS Single Sign-On and attach AWS accounts. Create permission sets with policies to restrict access to non-European Regions Create IAM users and IAM groups in each account
D.Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions Create permission sets with policies to restrict access to non-European Regions Create IAM users and IAM groups in the primary account
答案:B
解析:

582.A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. All domains and target URLs are defined in a JsoN document All DNS records are managed by Amazon Route 53
A solutions architect must implement a redirect service that accepts Http and Https requests
Which combination of steps should the solutions architect take to meet these requirements with the LEaST amount of operational effort? （Select THREE
A.Create a dynamic webpage that runs on an Amazon EC2 instance. Configure the webpage to use the JSoN document in combination with the event message to look up and respond with a redirect URL
B.Create an aPplication Load Balancer that includes Http and HttpS listeners
C.Create an AWS Lambda function that uses the JsoN document in combination with the event message to look up and respond with a redirect URL.
D.Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function
E.Create an Amazon CloudFront distribution Deploy a Lambda（ @Edge function
F.Create an SSL certificate by using AWS Certificate Manager（ACM） Include the domains as Subject Alternative Names
答案:ABE
解析:

583.A company has a legacy monolithic application that is critical to the company's business. The company hosts the application on an Amazon EC2 instance that runs Amazon Linux 2. The company's application team receives a directive from the legal department to back up the data from the instance's encrypted Amazon Elastic Block Store （Amazon EBS）volume to an Amazon s3 bucket. The application team does not have the administrative ssH key pair for the instance. The application must continue to serve the users
Which solution will meet these requirements?
A.Attach a role to the instance with permission to write to Amazon S3. Use the AWS Systems Manager Session Manager option to gain access to the instance and run commands to copy data into Amazon S3
B.Create an image of the instance with the reboot option turned on. Launch a new EC2 instance from the image Attach a role to the new instance with permission to write to Amazon s3. Run a command to copy data into Amazon S3
C.Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager（Amazon DLM).Copy the data to Amazon S3

D.Create an image of the instance. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3
答案:c
解析:

584.A retail company is running an application that stores invoice files in an Amazon S3 bucket and metadata about the files in an Amazon DynamoDB table The application software runs in both us-east-1 and eu-west-1 The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region
Which optio on meets these requirements?
A.Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Enable versioning on the S3 bucket
B.Create an AWS Lambda function triggered by Amazon CloudWatch Events to make regular backups of the DynamoDB table, Set up S3 cross-region replication from us-east- 1 to eu-west-1. Set up MFA delete on the S3 bucket in us-east-1
C.Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable versioning on the S3 bucket Implement strict ACLs on the S3 bucket
D.Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east- 1. Set up S3 cross-region replication from us-east- 1 to eu-west-1
答案:D
解析:

585.a company has multiple AWS accounts as part of an organization created with AWS Organizations. Each account has a VPc in the us-east-2 Region and is used for either production or development workloads. Amazon EC2 instances across production accounts need to communicate with each other, and EC2 instances across development accounts need to communicate with each other, but production and development instances should not be able to communicate with each other
To facilitate connectivity the company created a common network account. The company used AWS Transit Gateway to create a transit gateway in the us-east-2 Region in the network account and shared the transit gateway with the entire organization by using AWS Resource Access Manager Network administrators then attached VPCs in each account to the transit gateway, after which the EC2 instances were able to communicate across accounts. However, production and development accounts were also able to communicate with one another
Which set of steps should a solutions architect take to ensure production traffic and development traffic are completely isolated?
A.Modify the security groups assigned to development EC2 instances to block traffic from production EC2 instances. Modify the security groups assigned to production EC2 instances to block traffic from development EC2 instances
B.Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached. Using the Network Manager feature of Aws Transit Gateway, create policies that restrict traffic between VPCs based on the value of this tag
C.Create separate route tables for production and development traffic. Delete each account's association and route propagation to the default Aws Transit Gateway route table. Attach development VPCs to the development Aws Transit Gateway route table and production VPCs to the production role, and enable automatic route propagation on each attachment.
D.Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached. Modify the AWS Transit Gateway routing table to route production tagged attachments to one another and development tagged attachments to one another
答案:C

解析:

586.A company is managing all of its AWs accounts by using an organization in AWS Organizations. a recent audit revealed that some of the company 's documents were stored in Amazon s3 buckets outside the company's compliant AwS Regions

After the audit, the company moved all the noncompliant s3 buckets to a compliant Region in the United States （Us）.The company needs an SCP that prevents the creation of S3 buckets outside the Us

Which SCP should the company use to meet these requirements with the LEAST amount of operational overhead?

A.

```
{
    "Version":"2012-10-17",
    "Statement":[
      {
        "NotAction":[
          "s3:*"
        ],
        "Resource":"*",
        "Effect":"Deny",
        "Condition":{
          "StringNotEquals":{
            "aws:RequestedRegion":[
              "af-south-1",
              "ap-east-1",
              "ap-south-1",
              "ap-northeast-1",
              "ap-northeast-2",
              "ap-northeast-3",
              "ap-southeast-1",
              "ap-southeast-2",
              "ap-southeast-3",
              "ca-central-1",
              "eu-central-1",
              "eu-west-1",
              "eu-west-2",
              "eu-west-3",
              "eu-south-1",
              "eu-north-1",
              "me-south-1",
              "sa-east-1"
            ]
          }
```

B.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "NotAction":[
            "s3:*"
         ],
         "Resource":"*",
         "Effect":"Deny",
         "Condition":{
            "StringEquals":{
               "aws:RequestedRegion":[
                  "us-east-1",
                  "us-east-2",
                  "us-west-1",
                  "us-west-2"
               ]
            }
         }
```

C.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "NotAction":[
            "s3:*"
         ],
         "Resource":"*",
         "Effect":"Deny",
         "Condition":{
            "StringNotEquals":{
               "aws:RequestedRegion":[
                  "us-east-1",
                  "us-east-2",
                  "us-west-1",
                  "us-west-2"
               ]
            }
         }
```

D.

```
) {
    "Version":"2012-10-17",
    "Statement":[
      {
        "Action":[
          "s3:*"
        ],
        "Resource":"*",
        "Effect":"Deny",
        "Condition":{
          "StringEquals":{
            "aws:RequestedRegion":[
              "af-south-1",
              "ap-east-1",
              "ap-south-1",
              "ap-northeast-1",
              "ap-northeast-2",
              "ap-northeast-3",
              "ap-southeast-1",
      "ap-southeast-2",
      "ap-southeast-3",
      "ca-central-1",
      "eu-central-1",
      "eu-west-1",
      "eu-west-2",
      "eu-west-3",
      "eu-south-1",
      "eu-north-1",
      "me-south-1",
      "sa-east-1"
    ]
  }
```

答案:D
解析: