1. An Internet-facing multi-tier web application must be highly available. An ELB Classic Load Balancer is deployed in front of the web tier. Amazon EC2 instances at the web application tier are deployed evenly across two Availability Zones. The database is deployed using RDS Multi-AZ. A NAT instance is launched for Amazon  
EC2 instances and database resources to access the Internet. These instances are not assigned with public IP addresses.  
Which component poses a potential single point of failure in this architecture?

A. Amazon EC2

B. NAT instance

C. ELB Classic Load Balancer

D. Amazon RDS

Answer : B

Explanation

일반적으로 보면 ELB가 장애가 나면 그 밑에 티어들에 대해 접근이 불가하다. 그러나 문제에서는 Multi-AZ에 구성이 되어있다. Multi-AZ에서 작동하는 ELB가 보기에는 하나로 보이지만, 각 ZONE마다 하나의 ELB들이 논리적으로 구성되어있는 형태를 띈다. 그래서 ELB를 single point of failure라고 언급하지 않는다.(추가 : 알아서 장애 해결일 경우는 위에 해당하지 않는다.)

Reference

[stackoverflow.com/questions/46698011/are-amazon-elastic-load-balancer-elb-failure-proof](https://stackoverflow.com/questions/46698011/are-amazon-elastic-load-balancer-elb-failure-proof)

2. A call center application consists of a three-tier application using Auto Scaling groups to automatically scale resources as needed. Users report that every morning at 9:00 AM the system becomes very slow for about 15 minutes. A Solution Architect determines that a large percentage of the call center staff starts work at 9:00  
AM, so Auto Scaling does not have enough time to scale out to meet demand.  
How can the Architect fix the problem?

A. Change the Auto Scaling group’s scale out event to scale based on network utilization.

B. Create an Auto Scaling scheduled action to scale out the necessary resources at 8:30AM every morning.

C. Use Reserved Instance to ensure the system has reserved the right amount of capacity for the scale-up events.

D. Permanently keep a steady state of instances that is needed at 9:00AM to guarantee available resources, but leverage Spot Instance

Answer : B

Explanation

대부분의 콜센터 직원이 9:00시에 일을 시작하면서 시스템이 매우 느려진다고 한다. 이 경우 Auto Scaling을 통해 문제를 해결 할 수 있다. 이 점에서 답이 A와 B가 될 수 있지만, 현재 이 문제에서는 Network Traffic으로 인해 발생되는 문제인지 알 수 없다. 그러므로 보다 정확한 B가 적절하다.

3. An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled the week after the product is launched.  
Which is the MOST efficient way for management to ensure that capacity requirements are met?

A. Add a Step Scaling policy.

B. Add a Dynamic Scaling policy.

C. Add a Scheduled action.

D. Add Amazon Ec2 Spot Instance.

Answer : B

Explanation

Traffic이 급증하여 제품을 출시하고 그 다음주 까지 용량을 2배로 늘리겠다고 Management가 결정했다. “그 다음주”라는 키워드 때문에 C라고 생각 할 수도 있지만, Dynamic Scaling Policy를 통해 최소 용량을 선택 할 수 있기 때문에 2배로 늘리는 것도 만족 할 수 있고 2배의 용량을 뛰어넘는 traffic상황에서도 대처할 수 있기 때문에 B가 적절하다.

Reference : docs.aws.amazon.com/ko\_kr/autoscaling/ec2/userguide/as-scale-based-on-demand.html

4. A customer owns a simple API for their website that receives about 1,000 requests each day and has an average response time of 50 ms. It is currently hosted on one c4.large instance.  
Which changes to the architecture will provide high availability at the LOWEST cost?

A. Create an Auto Scaling group with a minimum of one instane and a maximum of two instances, then use an Application Load Balancer to balance the traffic.

B. Recreate API using Amazon API Gateway and use AWS Lambda as the service backend.

C. Create an Auto Scaling group ith a maximum of two instances,then use an Application Load Balancer to balance the traffic

D. Recreate the API using Amaozn API Gateway and integrate the new with the existing backend service.

Answer : B

Explanation

위 질문 리스트 중 고가용성을 보장하는 것은 serverless 한 lambda와 api를 통해 요청을 처리하는 것이다.

Reference : docs.aws.amazon.com/ko\_kr/lambda/latest/dg/welcome.html

5. A Solution Architect is designing an application that uses Amazon EBS volumes. The volumes must be backed up to a different region.  
How should the Architect meet this requirement?

A. Create EBS snapshots directly from one region to another.

B. Move the data to an Amazon Se bucket and enable cross-region replication.

C. Create EBS snapshots and then copy them to the desired region.

D. Use a script to copy data from the current Amazon EBS volume to the destination Amazon EBS volume.

Answer : B

Explanation

스냅샷을 다른 region에서 쓰게 하기 위해서는 해당 instance에서 스냅샷을 생성한 다음, 그 스냅샷을 다른 region으로 복사하여야 한다. S3는 단순 AMI(Amazon Machine Image)를 저장 할 수 있고, instance의 상태까지 복사 할 수 있는 snapshot는 지원하지 않는다. 그러므로 위 문제에서 요구한 Volume이 backup되어야하는 부분을 만족하는 것은 C이다.

Reference

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html

6. A company is using an Amazon S3 bucket located in us-west-2 to serve videos to their customers. Their customers are located all around the world and the videos are requested a lot during peak hours. Customers in Europe complain about experiencing slow downloaded speeds, and during peak hours, customers in all locations report experiencing HTTP 500 errors.  
What can a Solutions Architect do to address these issues?

A. Place an elastic load balancer in front of the Amazon S3 bucket to distribute the load during peak hours

B. Cache the web content with Amazon CloudFront and use all Edge locations for content delivery.

C. Replicate the bucket in EU-west-1 and sue an Amazon Route 53 failover routing policy to determine which bucket it should serve the request to.

D. Use an Amazon Route 53 weighted routing policy for the CloudFront domain name to distribute the GET request between CloudFront and the Amazon S3 bucket directly.

Answer : B

Explanation

전 세계의 사용자가 비디오를 us-west-2에 위치한 S3 bucket에서 다운받고있다. 한 자원을 다양한 region의 사람들이 접근하므로 그만큼 부하가 걸릴 수 밖에 없다. 이를 CloudFront를 사용하여 캐싱서버를 구현하게 되면, 각 사용자들의 가까운 Edge-Location에서 요청을 처리 할 수 있기 때문에 위의 error 상황을 해결 할 수 있다.

Reference : docs.aws.amazon.com/ko\_kr/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

7. A Solutions Architect is designing a solution that includes a managed VPN connection.  
To monitor whether the VPN connection is up or down, the Architect should use:

A. an external service to ping the VPN end point from outside the VPC

B. AWS CloudTrail to monitor the endpoint

C. the CloudWatch TunnelState Metric.

D. an AWS Lambda function that parses the VPN connection logs.

Answer : C

Explanation

A같은 경우, VPN은 public과 단절이기 때문에 ping을 보내든 안보내든 무응답이다. Cloudtrail는 api 호출 관련 이벤트를 처리하는 서비스이고, lambda는 지원하지 않는다.

Reference : docs.aws.amazon.com/ko\_kr/vpn/latest/clientvpn-admin/monitoring-overview.html

8. A social networking portal experiences latency and throughput issues due to an increased number of users. Application servers use very large datasets from an  
Amazon RDS database, which creates a performance bottleneck on the database.  
Which AWS service should be used to improve performance?

A. Auto Scaling

B. Amazon SQS

C. Amaozn ElastiCache

D. ELB Application Load Balancer

Answer : C

Explanation

Auto Scaling은 퍼포먼스 이슈보다는 고가용성을 해결하는 솔루션이다. SQS는 요청의 내구성과 안정성을 보장하는 서비스이며, ELB도 고가용성을 위한 솔루션이다. ElastiCache를 이용하여 In-memory cache환경을 구축하여 자주 사용하는 요청에 대해 캐시응답을 제공함으로써 퍼포먼스를 향상 시킬 수 있다.

Reference : docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/elasticache-use-cases.html

9. A Solutions Architect is designing network architecture for an application that has compliance requirements. The application will be hosted on Amazon EC2 instances in a private subnet and will be using Amazon S3 for storing data. The compliance requirements mandate that the data cannot traverse the public Internet.  
What is the MOST secure way to satisfy this requirement?

A. Use a NAT Instance

B. Use a NAT Gateway

C. Use a VPC endpoint

D. Use a Virtual Private Gateway.

Answer : C

Explanation

통상적으로 내부 자원을 보호하기 위해서 모두 퍼블릭으로 처리하는 것이 아니라 VPC를 구성하여 보호해야 할 자원들은 private subnet을 구성하여 보안을 향상시킨다. 이 private subnet과 안전하게 외부 자원에 대해 통신을 할 때 vpc endpoint를 이용하면 고가용성과 secure connection을 보장한다.

Reference : aws.amazon.com/ko/blogs/aws/new-vpc-endpoint-for-amazon-s3/

10. A Solutions Architect is designing a photo application on AWS. Every time a user uploads a photo to Amazon S3, the Architect must insert a new item to a DynamoDB table.  
Which AWS-managed service is the BEST fit to insert the item?

A. Lambda@Edge

B. AWS Lambda

C. Amazon API Gateway

D. Amazon Ec2 instance.

Answer : A

Explanation

Lambda@Edge는 lambda를 확장하여 lambda요청을 각 cloudfront상으로 처리 할 수 있게 해주는 서비스이다. Lambda와 기능적으로는 차이가 없지만, cloudfront를 이용하여 빠른 처리를 제공하는데 있어서 더 유리하다.

Reference

aws.amazon.com/ko/lambda/features/

docs.aws.amazon.com/ko\_kr/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html

11. An application relies on messages being sent and received in order. The volume will never exceed more than 300 transactions each second.  
Which service should be used?

A. Amazon SQS

B. Amazon SNS

C. Amazon ECS

D. Amazon STS

Answer : A

Explanation

Amazon SQS서비스를 통하여 안정성을 보장한 transaction을 수행할 수 있다. SQS 대기열 방식은 크게 2가지가 있다.

Standard Queue(표준 대기열) : 처리량이 중요한 application에 최적화

* 거의 무제한에 가까운 TPS를 제공
* 메시지가 최소 1번 전달되며, 가금 2개 이상의 메시지 복사본이 전달되는 경우가 있음.
* 메시지 순서와 다르게 전달 될 수 있음.

FIFO Queue : 이벤트 순서가 중요한 application에 최적화

* 일괄 처리를 통해 초당 최대 3000개의 메시지 지원
* 메시지가 한번 전달되고 consumer가 한번 처리할 때 까지 유지된다. 중복항목은 없음.
* 메시지가 전송되고 수신되는 순서가 엄격함.

“Being sent and received in order”의 문구를 참조하면 FIFO Queue를 사용하면 가장 적절할 것이다.

12. A Solutions Architect is designing an application on AWS that uses persistent block storage. Data must be encrypted at rest.  
Which solution meets the requirement?

A. Enable SSL on Amazon EC2 instances.

B. Encrypt Amazon EBS volumes on Amazon EC2 instances.

C. Enable server-side encryption on Amazon S3.

D. Encrypt Amazon EC2 Instance Storage.

Answer : B

Explanation

암호화 되어서 저장되어야 하고 persistent block storage임을 모두 만족하는 것은 B가 유일하다. D의 경우, 휘발성이기 때문에 persistent하지 못하다. SSL과 server-side encryption만으로 데이터가 유휴 상태일 때 암호화 할 수 없다.

Reference : docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/EBSEncryption.html

13. A company is launching a static website using the zone apex (mycompany.com). The company wants to use Amazon Route 53 for DNS.  
Which steps should the company perform to implement a scalable and cost-effective solution? (Choose two.)

A. Host the website on an Amazon EC2 instance with ELB and Auto Scaling, and map a Route 53 alias record to the ELB endpoint.

B. Host the website using AWS Elastic Beanstalk, and map a Route 53 alias record to the Beanstalk stack.

C. Host the website on an Amazon EC2 instance, and map a Route 53 alias record to the public IP endpoint.

D. Serve the website from an Amazon S3 bucket, and map a Route 53 alias record to the website endpoint.

E. Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers.

Answer : D, E

Explanation

문제에서 static website를 launching한다고 되어있기 때문에, EC2상에 직접 호스팅 하는 것은 비효율 적이다. S3상에다가 static file들을 업로드 하게 되면 그에 맞는 url이 생성되는데, 이를 Route 53을 통해 record와 website endpoint를 alias시켜주면 된다.

S3를 사용하기 때문에 거의 무한정으로 scalable하고, EC2보다 상대적으로 cost-effective하다.

Reference

docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingHostedZone.html

docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

14. A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analyzed in the future as needed.  
What is the SIMPLEST method to store this streaming data at scale?

A. Create an Amazon Kinesis Firehouse delivery stream to store the data in Amazon S3.

B. Create an Auto Scaling group of Amazon EC2 servers behind ELBs to write the data into Amazon RDS.

C. Create an Amazon SQS queue, and have the machines write to the queue.

D. Create an Amazon EC2 server farm behind an ELB to store the data in Amazon EBS Clod HDD Volumes.

Answer : A

Explanation : 기계에서 나오는 실시간 데이터는 정형화 되지 않았기 때문에 RDS의 경우 변환작업을 거쳐야 한다. 그러나 Amazon Kinesis Firehouse같은 경우 데이터를 바로 저장 할 수 있어 RDS보다 상대적으로 작업량이 적어 B보다는 A에 정답이 가깝다.

Reference : docs.aws.amazon.com/ko\_kr/firehose/latest/dev/what-is-this-service.html

15. A bank is writing new software that is heavily dependent upon the database transactions for write consistency. The application will also occasionally generate reports on data in the database, and will do joins across multiple tables. The database must automatically scale as the amount of data grows.  
Which AWS service should be used to run the database?

A. Amazon S3

B. Amazon Aurora

C. Amazon DynamoDB

D. Amazon Redshift

Answer : B

Explanation

위 제품들 중 “automatically scale as the amount of data grows”를 만족하는 것은 Aurora와 DynamoDB,, redshift밖에 없다. S3는 테이블이 존재하지 않기 때문에 제외한다. 문제의 2번째 조건을 보면 “join across multiple tables”가 등장한다. Nosql기반인 DynamoDB와 Redshift는 join처리 능력에서 RDS보다 떨어진다. 그러므로 유일한 RDS인 Aurora가 정답.

16. A Solutions Architect is designing a new application that needs to access data in a different AWS account located within the same region. The data must not be accessed over the Internet.  
Which solution will meet these requirements with the LOWEST cost?

A. Add rules to the security groups in each account.

B. Establish a VPC Peering connection between accounts

C. Configure Direct Connect in each account

D. Add a NAT Gateway to the data account.

Answer : B

Explanation

보통 app은 여러 티어로 구성되어 있기 때문에 VPC로 구성하는게 일반적이다. VPC는 기본적으로 private이기 때문에 다른 외부와 통신이 되지 않는다. 이를 VPC Peering을 통해 가능케 한다.

Reference : docs.aws.amazon.com/ko\_kr/vpc/latest/peering/what-is-vpc-peering.html

17. A Solutions Architect is designing a mobile application that will capture receipt images to track expenses. The Architect wants to store the images on Amazon S3. However, uploading images through the web server will create too much traffic.  
What is the MOST efficient method to store images from a mobile application on Amazon S3?

A. Upload directly to S3 using pre-signed URL.

B. Upload to a second bucket, and have a Lambda event copy the image to the primary bucket.

C. Upload to a separate Auto Scaling group of servers behind an ELB Classic Load Balancer, and have them write to the Amazon S3 bucket.

D. Expand the web server fleet with Spot instance to provide the resources to handle the images.

Answer : A

Explanation

C와 D는 서버 리소스를 사용하는 방식이고, B는 버킷을 불필요하게 하나 더 만드는 작업이다. A는 instance를 사용하지 않고 바로 S3에 올리기 때문에 보다 빠른 속도를 제공한다.

18. A company requires that the source, destination, and protocol of all IP packets be recorded when traversing a private subnet.  
What is the MOST secure and reliable method of accomplishing this goal.

A. Create VPC flow logs on the subnet.

B. Enable source destination check on private Amazon EC2 instances.

C. Enable AWS CloudTrail logging and specify an Amazon S3 bucket for storing log files.

D. Create an Amazon CloudWatch log to capture packet information

Answer : A

Explanation

말이 필요없다 Reference를 참곻자.

Reference

docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

19. A Solutions Architect has a multi-layer application running in Amazon VPC. The application has an ELB Classic Load Balancer as the front end in a public subnet, and an Amazon EC2-based reverse proxy that performs content-based routing to two backend Amazon EC2 instances hosted in a private subnet. The Architect sees tremendous traffic growth and is concerned that the reverse proxy and current backend set up will be insufficient.  
Which actions should the Architect take to achieve a cost-effective solution that ensures the application automatically scales to meet traffic demand? (Select two.)

A. Replace the Amazon EC2 reverse proxy with an ELB internal Classic Load Balancer.

B. Add Auto Scaling to the Amazon EC2 backend fleet.

C. Add Auto Scaling to the Amazon EC2 reverse proxy layer.

D. Use t2 burstable instance types for the backend fleet.

E. Replace both the front-end and reverse proxy layers with an ELB Application Load Balancer.

Answer : B, E

Explanation

Content-based Routing을 제공하는 ELB는 Application Load Balancer밖에 없다. 현재 reverse proxy는 content-based routing을 제공하고 있는데, 이를 auto-scaling하는 방법도 좋지만, 이를 Application Load Balancer로 교체하는 것이 훨씬 더 비용적인 측면에서 좋다. Backend의 성능을 높이기 위해서 Auto-Scaling을 통해 해결한다.

Reference

aws.amazon.com/ko/blogs/korea/new-advanced-request-routing-for-aws-application-load-balancers/

aws.amazon.com/ko/elasticloadbalancing/features/#compare

20. A company is launching a marketing campaign on their website tomorrow and expects a significant increase in traffic. The website is designed as a multi-tiered web architecture, and the increase in traffic could potentially overwhelm the current design.  
What should a Solutions Architect do to minimize the effects from a potential failure in one or more of the tiers?

A. Migrate the database to Amazon RDS.

B. Set up DNS failover to a statistic website.

C. Use Auto Scaling to keep up with demand.

D. Use both a SQL and a NoSQL database in the region.

Answer : C

Explanation

Auso-scaling 을 통해 자동으로 traffic에 따라 용량을 조절 할 수 있다. 말이 필요없음.

21. A web application experiences high compute costs due to serving a high amount of static web content.  
How should the web server architecture be designed to be the MOST cost-efficient?

A. create an Auto Scaling group to scale out based on average CPU usage.

B. Create an Amazon CloudFront distribution to pull static content from an Amazon S3 bucket

C. Leverage Reserved Instances to add additional capacity at a significantly lower price.

D. Create a multi-region deployment using an Amazon Route 53 geolocation routing policy.

Answer : B

Explanation

S3와 CloudFront를 이용하면 빠르면서도 비용적으로 효율적인 웹컨텐츠를 제공 할 수 있다. Auto Scaling과 RI를 이용하면 그만큼의 인스턴스 비용이 나가고, multi-region역시 그러하다.

Reference

docs.aws.amazon.com/ko\_kr/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

aws.amazon.com/ko/premiumsupport/knowledge-center/cloudfront-https-requests-s3/

22. A Solutions Architect plans to migrate NAT instances to NAT gateway. The Architect has NAT instances with scripts to manage high availability.  
What is the MOST efficient method to achieve similar high availability with NAT gateway?

A. Remove source/destination chech on NAT instances.

B. Launch a NAT gateway in each Avilability Zone.

C. Use a mix of NAT instances and NAT gateway.

D. Add an ELB Application Load Balancer in front of NAT gateway.

Answer : B

Explanation

NAT gateway는 각 AZ에다가 하나씩 생성하는 것이 일반적임.

Reference

docs.aws.amazon.com/ko\_kr/vpc/latest/userguide/vpc-nat-comparison.html

23. A Solutions Architect is designing a solution to store a large quantity of event data in Amazon S3. The Architect anticipates that the workload will consistently exceed 100 requests each second.  
What should the Architect do in Amazon S3 to optimize performance?

A. Randomize a key name prefix.

B. Store the event data in separate buckets.

C. Randomize the key name suffix.

D. Use Amazon S3 Transfer Acceleration.

Answer : A

Explanation

레퍼런스에 따르면 key name prefix에 따라서 저장되는 파티션이 달라진다고한다. 즉, key name prefix를 randomize하게 되면 그만큼 데이터들의 파티션이 분산되어서 저장되는 효과가 있고, 접근 시 한 파티션에 집중 되는 것을 피할 수 있다.

그러나 현재는 그럴 필요가 없어졌다고 공식 doc에 설명되어 있다.

Reference

aws.amazon.com/ko/blogs/aws/amazon-s3-performance-tips-tricks-seattle-hiring-event/ (2012)

docs.aws.amazon.com/ko\_kr/AmazonS3/latest/dev/optimizing-performance.html (latest)

24. A news organization plans to migrate their 20 TB video archive to AWS. The files are rarely accessed, but when they are, a request is made in advance and a 3 to 5-hour retrieval time frame is acceptable. However, when there is a breaking news story, the editors require access to archived footage within minutes.  
Which storage solution meets the needs of this organization while providing the LOWEST cost of storage?

A. Store the archive in Amazon S3 Reduced Redundancy Store.

B. Store the archive in Amazon Glacier and use standard retrieval for all content.

C. Store the archive in Amazon Glacier and pay the additional charge for expedited retrieval when needed

D. Store the archive in Amazon S3 with lifecycle policy to move this to S3 Infrequent Access after 30 days.

Answer : C

Explanation

Editor가 수분 이내로 접근이 가능하도록 요구하였으며, 20TB에 달하는 용량을 AWS에 archiving하려한다. 20TB의 용량은 S3보다는 Glacier에 적합하며, Glacier중 수분 내로 접근이 가능하게 하는 것은 expedited옵션이다. 그러므로 C가 가장 적절하다.

Reference

docs.aws.amazon.com/ko\_kr/AmazonS3/latest/dev/storage-class-intro.html

docs.aws.amazon.com/ko\_kr/AmazonS3/latest/dev/restoring-objects.html

25. A Solutions Architect is building a multi-tier website. The web servers will be in a public subnet, and the database servers will be in a private subnet. Only the web servers can be accessed from the Internet. The database servers must have Internet access for software updates.  
Which solution meets the requirements?

A. Assign Elastic IP addresses to the database instances.

B. Allow Internet on the private subnet through the network ACL.

C. Use a NAT Gateway

D. Use an egress-only Internet Gateway

Answer : C

Explanation

NAT instance 또는 Gateway를 통해 private subnet이 외부 인터넷과 통신 할 수 있다.

Reference

docs.aws.amazon.com/ko\_kr/vpc/latest/userguide/vpc-nat.html

26. A Solutions Architect is designing a Lambda function that calls an API to list all running Amazon RDS instances.  
How should the request be authorized?

A. Create an IAM access and secret key and store in the Lambda function

B. Create an IAM role to the Lambda function with permissions to list all Amazon RDS instances.

C. Create an IAM role to Amazon RDS with permissions to list all Amazon RDS instances.

D. Create an IAM access and secret key and store it in an encrypted RDS database.

Answer : B

Explanation

Lambda로 접근하려고 하면 Lambda에다가 IAM권한을 주어서 처리하는게 바람직하다.

Reference

docs.aws.amazon.com/ko\_kr/lambda/latest/dg/vpc-rds.html

27. A Solutions Architect is building an application on AWS that will require 20,000 IOPS on a particular volume to support a media event. Once the event ends, the IOPS need is no longer required. The marketing team asks the Architect to build the platform to optimize storage without incurring downtime.  
How should the Architect design the platform to meet these requirements?

A. Change the Amazon EC2 instant types.

B. Change the EBS volume type to Provisioned IOPS.

C. Stop the Amazon EC2 instance and provision IOPS for the EBS volume.

D. Enable an API Gateway to change the endpoints for the Amazon EC2 instance.

Answer : B

Explanation

20,000 IOPS를 지원하는 EBS Storage는 Privisioned IOPS SSD이다. 이에 맞는 답은 B와 C이며, C의 경우 instance를 stop시키기 때문에 B보다 비효율적이다.

Reference

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

28. A Solutions Architect is building a new feature using a Lambda to create metadata when a user uploads a picture to Amazon S3. All metadata must be indexed.  
Which AWS service should the Architect use to store this metadata?

A. Amazon S3

B. Amazon DynamoDB

C. Amazon Kinesis

D. Amazon EFC

Answer : B

Explanation

문제에서 메타데이터를 Lambda로 취급하고, 모든 메타데이터는 indexed 되여아한다는 조건을 모두 만족하는 것은 DynamoDB이다.

Reference

aws.amazon.com/ko/blogs/big-data/building-and-maintaining-an-amazon-s3-metadata-index-without-servers/

29. An interactive, dynamic website runs on Amazon EC2 instances in a single subnet behind an ELB Classic Load Balancer.  
Which design changes will make the site more highly available?

A. move some Amazon EC2 instances to a subnet in a different Zone(원래는 way인데 오타).

B. Move the website to Amazon S3.

C. Change the ELB to an Application Load Balancer.

D. Move some Amazon EC2 instances to a subnet in the same Availability Zone.

Answer : A

Explanation

고가용성을 보장하기 위해서는 EC2를 다른 존에다가 옮기면 하나의 Zone이 죽어도 다른 Zone이 작동하기 때문에 고가용성을 보장 할 수 있다.

Reference

기초내용임. 백서 참조.

30. A Solutions Architect is designing a web application that is running on an Amazon EC2 instance. The application stores data in DynamoDB. The Architect needs to secure access to the DynamoDB table.  
What combination of steps does AWS recommend to achieve secure authorization? (Select two.)

A. Store an Access key on the Amazon EC2 instance with rights to the DynamoDB table.

B. Attach an IAM user to the Amazon EC2 instance.

C. Create an IAM role with permissions to write to the DynamoDB table.

D. Attach an IAM role to the Amazon EC2 instance.

E. Attach an IAM policy to the Amazon EC2 instance.

Answer : C, D

Explanation

Access key를 직접 EC2안에 저장하는 것은 보안상 매우 좋지 않다. DynamoDB의 데이터를 app이 꺼내쓰는 구조인데, 이를 제어하기 위해선 DynamoDB접근을 허용하는 IAM 역할을 생성한 뒤 그 역할을 필요한 곳에다 부여하는 된다. 이를 만족하는 절차는 C -> D 이다.

Reference

31. A Solutions Architect is about to deploy an API on multiple EC2 instances in an Auto Scaling group behind an ELB. The support team has the following operational requirements:  
 1 They get an alert when the requests per second go over 50,000  
 2 They get an alert when latency goes over 5 seconds  
 3 They can validate how many times a day users call the API requesting highly-sensitive data  
Which combination of steps does the Architect need to take to satisfy these operational requirements? (Select two.)

A. Ensure that CloudTrail is enabled.

B. Create a custom CloudWatch metric to monitor the API for data access.

C. Configure CloudWatch alarms for any metrics the support team requires.

D. Ensure that detailed monitoring for the EC2 instances is enabled.

E. Create an application to export and save CloudWatch metircs for longer term trending analysis.

Answer : A,C

Explanation

설명 보충 필요. 직감으로는 A,C인데 잘모르겠음

Reference

32. A media company asked a Solutions Architect to design a highly available storage solution to serve as a centralized document store for their Amazon EC2 instances. The storage solution needs to be POSIX-compliant, scale dynamically, and be able to serve up to 100 concurrent EC2 instances.  
Which solution meets these requirements?

A. Create an Amazon S3 bucket and store all of the documents in this bucket.

B. Create an Amazon EBS volume and allow multiple users to mount that volume to their EC2 instances.

C. Use Amazon Glacier to store all of the documents.

D. Create an Amazon Elastic File System (Amazon EFS) to store and share the documents.

Asnwer : D

Explanation

위 문제의 가장 큰 조건은 POSIX(이식가능한)와 centralized document store for their Amazon EC2 instances 이다. 즉, 이식 가능하며 중앙 문서관리가 되어야 하므로 위 선택지 중 EFS가 가장 적당하다.

Reference

docs.aws.amazon.com/ko\_kr/efs/latest/ug/whatisefs.html

33. A Solution Architect has a two-tier application with a single Amazon EC2 instance web server and Amazon RDS MySQL Multi-AZ DB instances. The Architect is re-architecting the application for high availability by adding instances in a second Availability Zone.  
Which additional services will improve the availability of the application? (Choose two.)

A. Auto Scaling group

B. AWS CloudTrail

C. ELB Classic Load Balancer

D. Amazon DynamoDB

E. Amazon ElastiCache

Answer : A, C

Explanation

CloudTrail는 API호출의 tracing을 제공하고, DyanamoDB와 ElastiCache는 HA와 거리가 멀다.

Reference

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/ec2-increase-availability.html

34. A company is migrating its data center to AWS. As part of this migration, there is a three-tier web application that has strict data-at-rest encryption requirements. The customer deploys this application on Amazon EC2 using Amazon EBS, and now must provide encryption at-rest.  
How can this requirement be met without changing the application?

A. Use AWS Key Management Service and move the encrypted data to Amazon S3.

B. Use an application-specific encryption API with AWS server-side encryption.

C. Use encrypted EBS storage volumes with AWS-managed keys.

D. Use Third-party tools to encrypt the EBS data volumes with Key Management Service Bring Your Own Keys.

Answer : C

Explanation

AWS에서는 KMS를 통해 EBS volume의 encryption을 제공한다. 자세한 내용은 reference참조.

Reference

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/EBSEncryption.html

35. A Solutions Architect is developing software on AWS that requires access to multiple AWS services, including an Amazon EC2 instance. This is a security sensitive application, and AWS credentials such as Access Key ID and Secret Access Key need to be protected and cannot be exposed anywhere in the system.  
What security measure would satisfy these requirements?

A. Store the AWS Access Key ID/Secret Access Key combination in software comments.

B. Assign an IAM user to the Amazon EC2 instance.

C. Assign an IAM role to the Amazon EC2 instance.

D. Enable multi-factor authentication for the AWS root account.

Answer : C

Explanation

EC2 instance에서 민감한 app이 돌아가고있다. 이 앱에 대한 인증 정보가 노출되어서는 안된다. 즉, EC2 instance에 함부로 접근 못하게 막으면 된다. 그럴 때는 EC2접근에 IAM을 부여하면 되는데, user단위로 하는 거 보다 role단위로 하는 것이 훨씬 효율적이다.

Reference

36. An AWS workload in a VPC is running a legacy database on an Amazon EC2 instance. Data is stored on a 200GB Amazon EBS (gp2) volume. At peak load times, logs show excessive wait time.  
What solution should be implemented to improve database performance using persistent storage?

A. Migrate the data on the Amazon EBS volume to an SSD-backed volume.

B. Change the EC2 instance type to one with EC2 instance store volumes.

C. Migrate the data on the EBS volume to provisioned IOPS SSD (io1).

D. Change the EC2 instance type to one with burstable performance.

Answer : C

Explanation

데이터베이스 퍼포먼스를 높이는데 다양한 방법이 있다. 그 중에서도 CPU의 성능을 높이거나 스토리지 엑세스 속도가 빠르거나 다양한 방법이 존대한다. D가 답이 될 수도 있겠지만, D를 적용시키기 위해서는 인스턴스를 정지시키고 작업을 해야한다. 이 방법은 문제에서 요구한 persistent storage조건에 위배되기 때문에 정답은 C가 된다.

Reference

www.eversql.com/5-easy-ways-to-improve-your-database-performance/ -> about performance

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/ec2-instance-resize.html

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

37. A company’s website receives 50,000 requests each second, and the company wants to use multiple applications to analyze the navigation patterns of the users on their website so that the experience can be personalized.  
What can a Solutions Architect use to collect page clicks for the website and process them sequentially for each user?

A. Amazon Kinesis Stream

B. Amazon SQS standard queue

C. Amazon SQS FIFO queue

D. AWS CloudTrail

Answer : A

Explanation

SQS는 단순 큐 형태로 데이터의 처리 순서만 보장해주는 보안 호스팅 대기열만을 제공하는 서비스이고, CloudTrail은 API호출을 모니터링 하는 서비스이다. Kinesis는 위와 같은 빅데이터나 실시간 데이터 스트림 처리에 특화된 서비스이다.

Reference

aws.amazon.com/ko/blogs/aws/amazon-kinesis-real-time-processing-of-streamed-data/

docs.aws.amazon.com/ko\_kr/streams/latest/dev/introduction.html

38. A company wants to migrate a highly transactional database to AWS. Requirements state that the database has more than 6 TB of data and will grow exponentially.  
Which solution should a Solutions Architect recommend?

A. Amazon Aurora

B. Amazon Redshift

C. Amazon DynamoDB

D. Amazon RDS MySQL

Answer : A

Explanation

Aurora는 DB유형 중 OLTP(OnLine Transactional Processing)이고, RedShift는 OLAP(OnLine Analytic Processing)에 속한다. 둘다 될 수 있겠지만. 문제에서 요구한 것은 tramsactonal database를 요구 하였으므로 Aurora가 답에 가깝다.

Reference

blog.treasuredata.com/blog/2016/02/10/whats-the-difference-between-aws-redshift-aurora/

39. A company hosts a two-tier application that consists of a publicly accessible web server that communicates with a private database. Only HTTPS port 443 traffic to the web server must be allowed from the Internet.  
Which of the following options will achieve these requirements? (Choose two.)

A. Security group rule that allows inbound internet traffic for port 443.

B. Security group rule that denies all inbound internet traffic except port 443.

C. Network ACL rule that allows port 443 inbound and all ports outbound for internet traffic.

D. Security group rule that allows internet traffic for port 443 in both inbound and outbound.

E. Network ACL rule that allows port 443 for both inbound and outbound for all internet traffic.

Answer : A, E

Explanation

먼저 Security group과 NCAL의 inbound는 deny를 할 수 있는 rule이 없다. 기본으로 all deny가 설정되어있기 때문에 B는 답이 아니다. 443(HTTPS)로 통신을 하기 위해서는 outbound, inbound에 443포트가 모두 등록이 되어 있어야 한다. 이제 하나씩 살펴보자.

Security Group (basic rule : all deny inbound, all accept outbound)

443 inbound open vs 443 inbound, outbound open

전자가 적절하다. 외부와는 443포트로만 통신이 가능하기 때문에 inbound 443은 필수로 열어 두어야 하고, outbound의 경우는 모두 열어두어야 내부의 다른 서브넷과 통신이 가능하기 때문에 열어 놓는 것이 좋다. 그러므로 Security group의 경우의 답은 A가 적절하다.

Network ACL

443 inbound open & all outbound open vs 443 inbound and outbound open

후자가 적절하다. 문제 조건에서 오직 443포트만 웹서버(외부인터넷)과 통신이 가능하므로 443만 열고 나머지는 통신이 안되도록 차단하여야 한다.

Reference

40. A Solutions Architect is designing an Amazon VPC. Applications in the VPC must have private connectivity to Amazon DynamoDB in the same AWS Region.  
The design should route DynamoDB traffic through:

A. VPC peering connection

B. NAT gateway

C. VPC endpoint

D. AWS Direct Connect

Answer : C

Explanation

VPC endpoint를 통해 외부와 통신이 되지 않는 VPC내부 instance와 AWS service를 안전하게 연결 할 수 있다.

Reference

docs.aws.amazon.com/ko\_kr/vpc/latest/userguide/vpc-endpoints.html

41. A Solutions Architect is architecting a workload that requires a performant object-based storage system that must be shared with multiple Amazon EC2 instances.  
Which AWS service meets this requirement?

A. Amazon EFS

B. Amazon S3

C. Amaozn EBS

D. Amazon ElastiCache

Answer : B

Explanation

문제의 키워드는 “must be shared with multiple Amazon EC2”와 “object-based storage”이다. 이를 만족하는 서비스는 S3밖에 없다,

Reference

aws.amazon.com/ko/efs/when-to-choose-efs/

42. A Solutions Architect is developing a solution for sharing files in an organization. The solution must allow multiple users to access the storage service at once from different virtual machines and scale automatically. It must also support file-level locking.  
Which storage service meets the requirements of this use case?

A. Amazon S3

B. Amazon EFS

C. Amazon EBS

D. Cached Volumes

Answer : B

Explanation

여러명의 유저들이 여러 가상머신의 스토리지 서비스를 사용 할 수 있게 하여야 하며, 자동으로 용량을 조절한다. 그리고 무엇보다도 가장 중요한 “file-level locking”을 지원하여야 한다. S3도 locking을 지원하지만, file-level이 아닌 object-level이기 때문에 EFS가 적절하다.

Reference

docs.aws.amazon.com/ko\_kr/efs/latest/ug/whatisefs.html

43. A company runs a legacy application with a single-tier architecture on an Amazon EC2 instance. Disk I/O is low, with occasional small spikes during business hours. The company requires the instance to be stopped from 8 PM to 8 AM daily.  
Which storage option is MOST appropriate for this workload?

A. Amazon EC2 instance storage

B. Amazon EBS General Purpose SSD (gp2) storage

C. Amazon S3

D. Amazon EBS Provision IOPS SSD (io1) storage

Answer : B

Explanation

문제 조건 중 8PM~8AM까지는 instance가 stop되어야 하는 것으로 보아 휘발성 storage인 instance storage는 답이 아니다. D를 쓰자니 비싼 가격으로 인해 비 효율적이다. S3는 disk i/o가 이루어 지는 걸로 보아서 DB가 있는 것으로 보이는데 S3와 현재 상황과는 어울리지 않는다. 그러므로 답은 B. 가격이 S3가 쌀지는 몰라도 i/o특성으로 인해 EBS가 적절하다.

44. As part of securing an API layer built on Amazon API gateway, a Solutions Architect has to authorize users who are currently authenticated by an existing identity provider. The users must be denied access for a period of one hour after three unsuccessful attempts.  
How can the Solutions Architect meet these requirements?

A. Use AWS IAM authorization and add least-privileged permissions to each respective IAM role.

B. Use an API Gateway custom authorizer to invoke an AWS Lambda function to validate each user’s identity.

C. Use Amazon Cognito user pools to provide built-in user management.

D. Use Amazon Cognito user pools to integrate with external identity providers.

Answer : D

Explanation : ?????

Reference

es.slideshare.net/AmazonWebServices/security-best-practices-for-serverless-applications-july-2017-aws-online-tech-talks

serverless-stack.com/chapters/cognito-user-pool-vs-identity-pool.html

aws.amazon.com/ko/cognito/faqs/?nc1=h\_ls

45. An organization runs an online media site, hosted on-premises. An employee posted a product review that contained videos and pictures. The review went viral and the organization needs to handle the resulting spike in website traffic.  
What action would provide an immediate solution?

A. Redesign the website to use Amazon API Gateway, and use AWS Lambda to deliver content.

B. Add server instances using Amazon EC2 and use Amazon Route 53 with a failover routing policy.

C. Serve the images and videos via an Amazon CloudFront distribution create using the news site as the origin.

D. Use Amazon ElastiCache for REdis for caching and reducing the load requests from the origin.

Answer : C

Explanation

On-premise에 있는 media contents로 인한 spike를 다루기 위해서는 역시 CloudFront가 제일이다. 캐싱을 통해 빠른 응답속도를 구현 할 수 있고, 원본에 접근 하지 않아도 되기 때문이다.

Reference

docs.aws.amazon.com/ko\_kr/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

46. A client notices that their engineers often make mistakes when creating Amazon SQS queues for their backend system.  
Which action should a Solutions Architect recommend to improve this process?

A. Use the AWS CLI to create queues using AWS IAM Access Keys.

B. Write a script to create the Amazon SQS queue using AWS Lambda.

C. Use AWS Elastic Breanstalk to automatically create the Amazon SQS queues.

D. Use AWS CloudFormation Templates to manage the Amazon SQS queue creation.

Answer : B, D

Explanation

밑 링크를 참조 바람.

Reference

docs.aws.amazon.com/ko\_kr/lambda/latest/dg/with-sqs.html

docs.aws.amazon.com/ko\_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-create-queue.html#create-queue-cloudformation

47. A development team is building an application with front-end and backend application tiers. Each tier consists of Amazon EC2 instances behind an ELB Classic Load Balancer. The instances run in Auto Scaling groups across multiple Availability Zones. The network team has allocated the 10.0.0.0/24 address space for this application. Only the front-end load balancer should be exposed to the Internet. There are concerns about the limited size of the address space and the ability of each tier to scale.  
What should the VPC subnet design be in each Availability Zone?

A. One public subnet for the load balancer tier one public subnet for the front-end-tier, and one private subnet for the backend tier.

B. One shared public subnet for all tiers of the application.

C. One public subnet for the load balancer tier and one shared private subnet for the application.

D. One shared private subnet for all tiers of the application.

Answer : C

Explanation

Classic load balancer의 경우 default로 public DNS가 주어진다. 그렇기 때문에 ELB-private subnet-private subnet으로 구성하지 못하고 ELB-public subnet-private subnet으로 구성되어야 한다.

Reference

docs.aws.amazon.com/ko\_kr/elasticloadbalancing/latest/classic/elb-internet-facing-load-balancers.html

48. A Solutions Architect must select the storage type for a big data application that requires very high sequential I/O. The data must persist if the instance is stopped.  
Which of the following storage types will provide the best fit at the LOWEST cost for the application?

A. Amazon EC2 instance store local SSD volume.

B. Amazon EBS provisioned IOPS SSD volume.

C. Amazon EBS throughput optimized HDD volume.

D. Amazon EBS general purpose SSD volume.

Answer : C

Explanation

HDD는 빅데이터와 높은 I/O에 특화되어 있다. 가격적인 측면에서도 SSD보다 쌈.

Reference

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

49. Two Auto Scaling applications, Application A and Application B, currently run within a shared set of subnets. A Solutions Architect wants to make sure that Application A can make requests to Application B, but Application B should be denied from making requests to Application A.  
Which is the SIMPLEST solution to achieve this policy?

A. Using security groups that the security groups of the other application

B. Using security groups that the application server’s IP address.

C. Using Network Access Control Lists to allow/deny traffic based on application IP address.

D. Migration the applications to separate subnets from each other.

Answer : A

Explanation

Subnet 안에 2개의 application(instance)가 있다. 이들을 컨트롤 할 수 있는 것은 Network Access Control List가 아닌 Security group이다. 각 application의 역할이 다르므로 Security group를 다르게 가져가 accept/deny를 설정 해 줄 수 있다.

Reference

50. Legacy applications currently send messages through a single Amazon EC2 instance, which then routes the messages to the appropriate destinations. The Amazon EC2 instance is a bottleneck and single point of failure, so the company would like to address these issues.  
Which services could address this architectural use case? (Choose two.)

A. Amazon SNS

B. AWS STS

C. Amazon SQS

D. Amazon Route 53

E. Amazon Glue

Answer : A, C

Explanation

A를 통해 장애에 대한 알림을 받아 신속대응을 할 수 있다. 또한 SQS를 통해 대기하고 있는 메시지를 보호해줄 수 있다.

STS는 Security Token Service이기 때문에 병목 현상과 관계가 없으며, Route 53을 이용해 처리 하려고 해도 single EC2에서 legacy application이 돌아가고 있기 때문에 관계가 없다. Glue는 데이터의 분류, 정리에 사용되는 서비스이다

51. A Solutions Architect needs to design an architecture for a new, mission-critical batch processing billing application. The application is required to run Monday, Wednesday, and Friday from 5 AM to 11 AM.  
Which is the MOST cost-effective Amazon EC2 pricing model?

A. Amazon EC2 Spot instances

B. On-Demand Amazon EC2 instances

C. Scheduled Reserved Instances

D. Dedicated Amazon EC2 Instances

Answer : C

Explanation

중요한 배치작업이라고 했기 때문에 갑자기 종료될 위험성이 있는 spot instance는 적합하지 않다. 또한 장기간 이용시 on-demand보다는 reserved instance가 더 싸고, dedicated EC2는 자신의 하드웨어 자원을 쓰는 것이기 때문에 비용이 많이 든다.

Reference

docs.aws.amazon.com/ko\_kr/AWSEC2/latest/UserGuide/instance-purchasing-options.html

52. A workload consists of downloading an image from an Amazon S3 bucket, processing the image, and moving it to another Amazon S3 bucket. An Amazon EC2 instance runs a scheduled task every hour to perform the operation.  
How should a Solutions Architect redesign the process so that it is highly available?

A. Change the Amazon EC2 instance to compute optimized

B. Launch a second Amazon EC2 instance to monitor the health of the first.

C. Trigger a Lambda function when a new object is uploaded

D. Initially copy the images to an attached Amazon EBS volume.

Answer : C

Explanation

S3 bucket에 올리는 작업의 고가용성을 보장하는 방법에 대해서 질문하고 있다. A는 성능에 치우친 항목이고, B는 단순 모니터링이라 관계가 없다. D는 initial image만 뜬다고 해서 작업에 대해 HA가 보장되는 것이 아니다. C의 lambda를 이용하여 작업 후 작업이 제대로 이루어졌는지 체크 후 제대로 되었으면 ok, 안되었으면 다시 작업하게 하는 Lambda 함수를 작성하면 HA를 보장할 수 있다.

Reference

aws.amazon.com/ko/lambda/

53. An application is running on an Amazon EC2 instance in a private subnet. The application needs to read and write data onto Amazon Kinesis Data Streams, and corporate policy requires that this traffic should not go to the internet.  
How can these requirements be met?

A. Configure a NAT gateway in a public subnet and route all traffic to Amazon Kinesis through the NAT gateway

B. Configure a gateway VPC endpoint for Kinesis and route all traffic to Kinesos through the gateway VPC endpoint

C. Configure an interface VPC endpoint for Kinesis and route all traffic to Kinesis through the gateway VPC endpoint

D. Configure an AWS Direct Connect private virtual interface for Kinesis and route all traffic to Kinesis through the virtual interface.

Answer : C

Explanation

VPC상에서 AWS의 다른 서비스와 안전하게 통신하는데는 VPC endpoint를 이용하면 좋다. VPC endpoint에는 2종류가 있다.

Gateway VPC endpoint : dynamoDB, S3

Interface VPC endpoint : 그 외 다수. Reference 참고.

이에 해당하는 조건은 C이다.

Reference

docs.aws.amazon.com/ko\_kr/vpc/latest/userguide/vpc-endpoints.html

54. A Solutions Architect is building an application that stores object data. Compliance requirements state that the data stored is immutable.  
Which service meets these requirements?

A. Amazon S3

B. Amazon Glacier

C. Amazon EFS

D. AWS Storage Gateway

Answer : B

Explanation

순간적으로 A를 떠올릴 수도 있지만, S3는 object의 CRUD가 가능하다. 그래서 문제의 조건인 immutable를 만족시키지 못한다. Immutable를 만족 시키는 storage는 B이다.

Reference

aws.amazon.com/ko/glacier/features/

55. A Solutions Architect is defining a shared Amazon S3 bucket where corporate applications will save objects.  
How can the Architect ensure that when an application uploads an object to the Amazon S3 bucket, the object is encrypted?

A. Set a CORS configuration

B. Set a bucket policy to encrypt all Amazon S3 objects

C. Enable default encryption on the bucket

D. Set permission for users.

Answer :

Explanation

Reference