QUESTION 1
A company has a website hosted on AWS The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.
What should a solutions architect do to meet this requirement?

A. Update the ALB's network ACL to accept only HTTPS traffic
B. Create a rule that replaces the HTTP in the URL with HTTPS.
C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Answer: C
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/

QUESTION 2
A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.
Which solution will meet these requirements with the LEAST operational overhead?

A. Store the database credentials in the instance metadata.
Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.
B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket.
Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time.
Use S3 Versioning to ensure the ability to fall back to previous values.
C. Store the database credentials as a secret in AWS Secrets Manager.
Turn on automatic rotation for the secret.
Attach the required permission to the EC2 role to grant access to the secret.
D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store.
Turn on automatic rotation for the encrypted parameters.

Attach the required permission to the EC2 role to grant access to the encrypted parameters.

Answer: C

QUESTION 3
A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB).
The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA).
The certificate must be rotated each year before the certificate expires.
What should a solutions architect do to meet these requirements?

A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate.
Apply the certificate to the ALB.
Use the managed renewal feature to automatically rotate the certificate.
B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate.
Import the key material from the certificate. Apply the certificate to the ALB.
Use the managed renewal feature to automatically rotate the certificate.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA.
Apply the certificate to the ALB.
Use the managed renewal feature to automatically rotate the certificate.
D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate.
Apply the certificate to the ALB.
Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration.
Rotate the certificate manually.

Answer: D

QUESTION 4
A company runs its Infrastructure on AWS and has a registered base of 700.000 users for res document management application. The company intends to create a product that converts large pdf files to jpg Imago files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over lime.
Which solution meets these requirements MOST cost-effectively?

A. Save the pdf files to Amazon S3.
Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to jpg format and store them back in Amazon S3.
B. Save the pdf files to Amazon DynamoDB.
Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to jpg format and store them hack in DynamoDB.
C. Upload the pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances.
Amazon Elastic Block Store (Amazon EBS) storage and an Auto Scaling group.
Use a program In the EC2 instances to convert the files to jpg format Save the .pdf files and the .jpg files In the EBS store.
D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EPS) storage, and an Auto Scaling group.
Use a program in the EC2 instances to convert the file to jpg format Save the pdf files and the jpg files in the EBS store.

Answer: D

QUESTION 5
A company has more than 5 TB of file data on Windows file servers that run on premises Users and applications

interact with the data each day
The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS.
What should a solutions architect do to meet these requirements?

A. Deploy and configure Amazon FSx for Windows File Server on AWS.
Move the on-premises file data to FSx for Windows File Server.
Reconfigure the workloads to use FSx for Windows File Server on AWS.
B. Deploy and configure an Amazon S3 File Gateway on premises.
Move the on-premises file data to the S3 File Gateway.
Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway
C. Deploy and configure an Amazon S3 File Gateway on premises.
Move the on-premises file data to Amazon S3.
Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.
D. Deploy and configure Amazon FSx for Windows File Server on AWS.
Deploy and configure an Amazon FSx File Gateway on premises.
Move the on-premises file data to the FSx File Gateway.
Configure the cloud workloads to use FSx for Windows File Server on AWS.
Configure the on-premises workloads to use the FSx File Gateway.

Answer: A

QUESTION 6
A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports. Which solution will meet these requirements with the LEAST operational overhead?

A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
B. Use Amazon Textract to extract the text from the reports.
Use Amazon SageMaker to identify the PHI from the extracted text.
C. Use Amazon Textract to extract the text from the reports.
Use Amazon Comprehend Medical to identify the PHI from the extracted text.
D. Use Amazon Rekognition to extract the text from the reports.
Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Answer: C

QUESTION 7
A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days
Which storage solution is MOST cost-effective?

A. Create an S3 bucket lifecycle policy to move Mm from S3 Standard to S3 Glacier 30 days from object creation.
Delete the Tiles 4 years after object creation
B. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone-infrequent Access (S3 One Zone-IA) 30 days from object creation.
Delete the fees 4 years after object creation
C. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard -IA) 30 from object creation.

Delete the ties 4 years after object creation

D. Create an S3 bucket Lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation.
Move the files to S3 Glacier 4 years after object carton.

Answer: C

QUESTION 8
A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.
What should a solutions architect do to ensure messages are being processed once only?

A. Use the CreateQueue API call to create a new queue
B. Use the Add Permission API call to add appropriate permissions
C. Use the ReceiveMessage API call to set an appropriate wail time
D. Use the ChangeMessageVisibility APi call to increase the visibility timeout

Answer: D
Explanation:
The visibility timeout begins when Amazon SQS returns a message. During this time, the consumer processes and deletes the message. However, if the consumer fails before deleting the message and your system doesn't call the DeleteMessage action for that message before the visibility timeout expires, the message becomes visible to other consumers and the message is received again. If a message must be received only once, your consumer should delete it within the duration of the visibility timeout.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html
Keyword: SQS queue writes to an Amazon RDS From this, Option D best suite & other Options ruled out [Option A -You can't intruduce one more Queue in the existing one; Option B - only Permission & Option C -Only Retrieves Messages] FIF O queues are designed to never introduce duplicate messages. However, your message producer might introduce duplicates in certain scenarios: for example, if the producer sends a message, does not receive a response, and then resends the same message. Amazon SQS APIs provide deduplication functionality that prevents your message producer from sending duplicates. Any duplicates introduced by the message producer are removed within a 5-minute deduplication interval. For standard queues, you might occasionally receive a duplicate copy of a message (at-least-once delivery). If you use a standard queue, you must design your applications to be idempotent (that is, they must not be affected adversely when processing the same message more than once).

QUESTION 9
A solutions architect is designing a new hybrid architecture to extend a company s on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.
What should the solutions architect do to meet these requirements?

A. Provision an AWS Direct Connect connection to a Region.
Provision a VPN connection as a backup if the primary Direct Connect connection fails.
B. Provision a VPN tunnel connection to a Region for private connectivity.
Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
C. Provision an AWS Direct Connect connection to a Region.
Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
D. Provision an AWS Direct Connect connection to a Region.
Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Answer: A
Explanation:
"In some cases, this connection alone is not enough. It is always better to guarantee a fallback connection as the

backup of DX. There are several options, but implementing it with an AWS Site-To-Site VPN is a real cost-effective solution that can be exploited to reduce costs or, in the meantime, wait for the setup of a second DX."
https://www.proud2becloud.com/hybrid-cloud-networking-backup-aws-direct-connect-network-connection-with-aws-site-to-site-vpn/

QUESTION 10
A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.
Which solution will meet these requirements with the LEAST operational effort?

A. Place the EC2 instances in different AWS Regions.
Use Amazon Route 53 health checks to redirect traffic.
Use Aurora PostgreSQL Cross-Region Replication.
B. Configure the Auto Scaling group to use multiple Availability Zones.
Configure the database as
Multi-AZ. Configure an Amazon RDS Proxy instance for the database.
C. Configure the Auto Scaling group to use one Availability Zone.
Generate hourly snapshots of the database.
Recover the database from the snapshots in the event of a failure.
D. Configure the Auto Scaling group to use multiple AWS Regions.
Write the data from the application to Amazon S3.
Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Answer: B

QUESTION 11
A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.
The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.
What should a solutions architect do to meet these requirements?

A. Enable HTTP health checks on the NLB. supplying the URL of the company's application.
B. Add a cron job to the EC2 instances to check the local application's logs once each minute.
If HTTP errors are detected, the application will restart.
C. Replace the NLB with an Application Load Balancer.
Enable HTTP health checks by supplying the URL of the company's application.
Configure an Auto Scaling action to replace unhealthy instances.
D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB.
Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Answer: C

QUESTION 12
A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour.
What should the solutions architect recommend to meet these requirements?

A. Configure DynamoDB global tables.
For RPO recovery, point the application to a different AWS Region.

B. Configure DynamoDB point-in-time recovery.
For RPO recovery, restore to the desired point in time.
C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis.
For RPO recovery, import the data from S3 Glacier to DynamoDB.
D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes.
For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Answer: B

QUESTION 13
A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.
How can the solutions architect meet this requirement?

A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through It.
B. Deploy a NAT gateway into a public subnet and attach an end point policy that allows access to the S3 buckets.
C. Deploy the application Into a public subnet and allow it to route through an internet gateway to access the S3 Buckets
D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Answer: D

QUESTION 14
A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection to the bastion host and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO)

A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances
B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company
C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company
D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host
E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host

Answer: CD
Explanation:
https://digitalcloud.training/ssh-into-ec2-in-private-subnet/

QUESTION 15
A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet Security is a high priority for the company.
How should security groups be configured in this situation? (Select TWO)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.

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

Answer: AC
Explanation:
"Security groups create an outbound rule for every inbound rule." Not completely right. Statefull does NOT mean that if you create an inbound (or outbound) rule, it will create an outbound (or inbound) rule. What it does mean is: suppose you create an inbound rule on port 443 for the X ip. When a request enters on port 443 from X ip, it will allow traffic out for that request in the port 443. However, if you look at the outbound rules, there will not be any outbound rule on port 443 unless explicitly create it. In ACLs, which are stateless, you would have to create an inbound rule to allow incoming requests and an outbound rule to allow your application responds to those incoming requests.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#SecurityGroupRules

QUESTION 16
A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.
Which solution meets these requirements and is the MOST operationally efficient?

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer.
Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services. Most Voted
B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures.
Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group.
Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group.
Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Answer: A
Explanation:
https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-4/

QUESTION 17
A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-lime analytics.
A secure transfer is important because the data is considered sensitive.
Which solution offers the MOST reliable data transfer?

A. AWS DataSync over public internet
B. AWS DataSync over AWS Direct Connect
C. AWS Database Migration Service (AWS DMS) over public internet

D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Answer: B
Explanation:
These are some of the main use cases for AWS DataSync:
- Data migration
- Move active datasets rapidly over the network into Amazon S3, Amazon EFS, or FSx for Windows File Server.
DataSync includes automatic encryption and data integrity validation to help make sure that your data arrives securely, intact, and ready to use.
DataSync includes encryption and integrity validation to help make sure your data arrives securely, intact, and ready to use.
https://aws.amazon.com/datasync/faqs/

QUESTION 18
A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.
Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream.
Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source.
Use AWS Lambda functions to transform the data.
Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue.
Stop source/destination checking on the EC2 instance.
Use AWS Glue to transform the data and to send the data to Amazon S3.
C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream.
Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source.
Use AWS Lambda functions to transform the data.
Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
D. Configure an Amazon API Gateway API to send data to AWS Glue.
Use AWS Lambda functions to transform the data.
Use AWS Glue to send the data to Amazon S3.

Answer: C

QUESTION 19
A company needs to keep user transaction data in an Amazon DynamoDB table.
The company must retain the data for 7 years.
What is the MOST operationally efficient solution that meets these requirements?

A. Use DynamoDB point-in-time recovery to back up the table continuously.
B. Use AWS Backup to create backup schedules and retention policies for the table.
C. Create an on-demand backup of the table by using the DynamoDB console.
Store the backup in an Amazon S3 bucket.
Set an S3 Lifecycle configuration for the S3 bucket.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function.
Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket.
Set an S3 Lifecycle configuration for the S3 bucket.

Answer: C

QUESTION 20

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.
What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.
B. Create a DynamoDB table with a global secondary index.
C. Create a DynamoDB table with provisioned capacity and auto scaling.
D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Answer: A