질문 45: 오답

The DevOps team at an e-commerce company wants to perform some maintenance work on a specific EC2 instance that is part of an Auto Scaling group using a step scaling policy. The team is facing a maintenance challenge - every time the team deploys a maintenance patch, the instance health check status shows as out of service for a few minutes. This causes the Auto Scaling group to provision another replacement instance immediately.

As a solutions architect, which are the MOST time/resource efficient steps that you would recommend so that the maintenance work can be completed at the earliest? (Select two)

설명
Correct options:

Put the instance into the Standby state and then update the instance by applying the maintenance patch. Once the instance is ready, you can exit the Standby state and then return the instance to service - You can put an instance that is in the InService state into the Standby state, update some software or troubleshoot the instance, and then return the instance to service. Instances that are on standby are still part of the Auto Scaling group, but they do not actively handle application traffic.

How Standby State Works: via - https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-enter-exit-standby.html

Suspend the ReplaceUnhealthy process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can manually set the instance's health status back to healthy and activate the ReplaceUnhealthy process type again - The ReplaceUnhealthy process terminates instances that are marked as unhealthy and then creates new instances to replace them. Amazon EC2 Auto Scaling stops replacing instances that are marked as unhealthy. Instances that fail EC2 or Elastic Load Balancing health checks are still marked as unhealthy. As soon as you resume the ReplaceUnhealthly process, Amazon EC2 Auto Scaling replaces instances that were marked unhealthy while this process was suspended.

Incorrect options:

Take a snapshot of the instance, create a new AMI and then launch a new instance using this AMI. Apply the maintenance patch to this new instance and then add it back to the Auto Scaling Group by using the manual scaling policy. Terminate the earlier instance that had the maintenance issue - Taking the snapshot of the existing instance to create a new AMI and then creating a new instance in order to apply the maintenance patch is not time/resource optimal, hence this option is ruled out.

Delete the Auto Scaling group and apply the maintenance fix to the given instance. Create a new Auto Scaling group and add all the instances again using the manual scaling policy - It's not recommended to delete the Auto Scaling group just to apply a maintenance patch on a specific instance.

Suspend the ScheduledActions process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can you can manually set the instance's health status back to healthy and activate the ScheduledActions process type again - Amazon EC2 Auto Scaling does not execute scaling actions that are scheduled to run during the suspension period. This option is not relevant to the given use-case.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-enter-exit-standby.html

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html

질문 17: 오답

An IT security consultancy is working on a solution to protect data stored in S3 from any malicious activity as well as check for any vulnerabilities on EC2 instances.

As a solutions architect, which of the following solutions would you suggest to help address the given requirement?

설명
Correct option:

Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances

Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon S3. GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

How GuardDuty works: via - https://aws.amazon.com/guardduty/

Amazon Inspector security assessments help you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

Incorrect options:

Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances

Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

These three options contradict the explanation provided above, so these options are incorrect.

References:

https://aws.amazon.com/guardduty/

https://aws.amazon.com/inspector/

질문 43: 오답

The IT department at a consulting firm is conducting a training workshop for new developers. As part of an evaluation exercise on Amazon S3, the new developers were asked to identify the invalid storage class lifecycle transitions for objects stored on S3.

Can you spot the INVALID lifecycle transitions from the options below? (Select two)

설명
Correct options:

As the question wants to know about the INVALID lifecycle transitions, the following options are the correct answers -

S3 Intelligent-Tiering => S3 Standard

S3 One Zone-IA => S3 Standard-IA

Following are the unsupported life cycle transitions for S3 storage classes - Any storage class to the S3 Standard storage class. Any storage class to the Reduced Redundancy storage class. The S3 Intelligent-Tiering storage class to the S3 Standard-IA storage class. The S3 One Zone-IA storage class to the S3 Standard-IA or S3 Intelligent-Tiering storage classes.

Incorrect options:

S3 Standard => S3 Intelligent-Tiering

S3 Standard-IA => S3 Intelligent-Tiering

S3 Standard-IA => S3 One Zone-IA

Here are the supported life cycle transitions for S3 storage classes - The S3 Standard storage class to any other storage class. Any storage class to the S3 Glacier or S3 Glacier Deep Archive storage classes. The S3 Standard-IA storage class to the S3 Intelligent-Tiering or S3 One Zone-IA storage classes. The S3 Intelligent-Tiering storage class to the S3 One Zone-IA storage class. The S3 Glacier storage class to the S3 Glacier Deep Archive storage class.

Amazon S3 supports a waterfall model for transitioning between storage classes, as shown in the diagram below. via - https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

질문 42: 정답

A gaming company is developing a mobile game that streams score updates to a backend processor and then publishes results on a leaderboard. The company has hired you as an AWS Certified Solutions Architect Associate to design a solution that can handle major traffic spikes, process the mobile game updates in the order of receipt, and store the processed updates in a highly available database. The company wants to minimize the management overhead required to maintain the solution.

Which of the following will you recommend to meet these requirements?

설명
Correct option:

Push score updates to Kinesis Data Streams which uses a Lambda function to process these updates and then store these processed updates in DynamoDB

To help ingest real-time data or streaming data at large scales, you can use Amazon Kinesis Data Streams (KDS). KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources. The data collected is available in milliseconds, enabling real-time analytics. KDS provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications.

Lambda integrates natively with Kinesis Data Streams. The polling, checkpointing, and error handling complexities are abstracted when you use this native integration. The processed data can then be configured to be saved in DynamoDB.

Incorrect options:

Push score updates to an SQS queue which uses a fleet of EC2 instances (with Auto Scaling) to process these updates in the SQS queue and then store these processed updates in an RDS MySQL database

Push score updates to Kinesis Data Streams which uses a fleet of EC2 instances (with Auto Scaling) to process the updates in Kinesis Data Streams and then store these processed updates in DynamoDB

Push score updates to an SNS topic, subscribe a Lambda function to this SNS topic to process the updates, and then store these processed updates in a SQL database running on Amazon EC2

These three options use EC2 instances as part of the solution architecture. The use-case seeks to minimize the management overhead required to maintain the solution. However, EC2 instances involve several maintenance activities such as managing the guest operating system and software deployed to the guest operating system, including updates and security patches, etc. Hence these options are incorrect.

Reference:

https://aws.amazon.com/blogs/big-data/best-practices-for-consuming-amazon-kinesis-data-streams-using-aws-lambda/

질문 3: 정답

An organization wants to delegate access to a set of users from the development environment so that they can access some resources in the production environment which is managed under another AWS account.

As a solutions architect, which of the following steps would you recommend?

설명
Correct option:

Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment

IAM roles allow you to delegate access to users or services that normally don't have access to your organization's AWS resources. IAM users or AWS services can assume a role to obtain temporary security credentials that can be used to make AWS API calls. Consequently, you don't have to share long-term credentials for access to a resource. Using IAM roles, it is possible to access cross-account resources.

Incorrect options:

Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment - There is no need to create new IAM user credentials for the production environment, as you can use IAM roles to access cross-account resources.

It is not possible to access cross-account resources - You can use IAM roles to access cross-account resources.

Both IAM roles and IAM users can be used interchangeably for cross-account access - IAM roles and IAM users are separate IAM entities and should not be mixed. Only IAM roles can be used to access cross-account resources.

Reference:

https://aws.amazon.com/iam/features/manage-roles/

질문 55: 오답

A research group needs a fleet of EC2 instances for a specialized task that must deliver high random I/O performance. Each instance in the fleet would have access to a dataset that is replicated across the instances. Because of the resilient application architecture, the specialized task would continue to be processed even if any instance goes down, as the underlying application architecture would ensure the replacement instance has access to the required dataset.

Which of the following options is the MOST cost-optimal and resource-efficient solution to build this fleet of EC2 instances?

설명
Correct option:

Use Instance Store based EC2 instances

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host instance. Instance store is ideal for the temporary storage of information that changes frequently such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance store volumes are included as part of the instance's usage cost.

As Instance Store based volumes provide high random I/O performance at low cost (as the storage is part of the instance's usage cost) and the resilient architecture can adjust for the loss of any instance, therefore you should use Instance Store based EC2 instances for this use-case.

EC2 Instance Store Overview: via -
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Incorrect options:

Use EBS based EC2 instances - EBS based volumes would need to use Provisioned IOPS (io1) as the storage type and that would incur additional costs. As we are looking for the most cost-optimal solution, this option is ruled out.

Use EC2 instances with EFS mount points - Using EFS implies that extra resources would have to be provisioned (compared to using instance store where the storage is located on disks that are physically attached to the host instance itself). As we are looking for the most resource-efficient solution, this option is also ruled out.

Use EC2 instances with access to S3 based storage - Using EC2 instances with access to S3 based storage does not deliver high random I/O performance, this option is just added as a distractor.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

질문 48: 오답

A software engineering intern at an e-commerce company is documenting the process flow to provision EC2 instances via the Amazon EC2 API. These instances are to be used for an internal application that processes HR payroll data. He wants to highlight those volume types that cannot be used as a boot volume.

Can you help the intern by identifying those storage volume types that CANNOT be used as boot volumes while creating the instances? (Select two)

설명
Correct options:

Throughput Optimized HDD (st1)

Cold HDD (sc1)

The EBS volume types fall into two categories:

SSD-backed volumes optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS.

HDD-backed volumes optimized for large streaming workloads where throughput (measured in MiB/s) is a better performance measure than IOPS.

Throughput Optimized HDD (st1) and Cold HDD (sc1) volume types CANNOT be used as a boot volume, so these two options are correct.

Please see this detailed overview of the volume types for EBS volumes. via -
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Incorrect options:

General Purpose SSD (gp2)

Provisioned IOPS SSD (io1)

Instance Store

General Purpose SSD (gp2), Provisioned IOPS SSD (io1), and Instance Store can be used as a boot volume.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html

질문 16: 오답

A US-based healthcare startup is building an interactive diagnostic tool for COVID-19 related assessments. The users would be required to capture their personal health records via this tool. As this is sensitive health information, the backup of the user data must be kept encrypted in S3. The startup does not want to provide its own encryption keys but still wants to maintain an audit trail of when an encryption key was used and by whom.

Which of the following is the BEST solution for this use-case?

설명
Correct option:

Use SSE-KMS to encrypt the user data on S3

AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer-managed CMK that you have already created. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Therefore SSE-KMS is the correct solution for this use-case.

Server Side Encryption in S3: via - https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

Incorrect options:

Use SSE-S3 to encrypt the user data on S3 - When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. However this option does not provide the ability to audit trail the usage of the encryption keys.

Use SSE-C to encrypt the user data on S3 - With Server-Side Encryption with Customer-Provided Keys (SSE-C), you manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption when you access your objects. However this option does not provide the ability to audit trail the usage of the encryption keys.

Use client-side encryption with client provided keys and then upload the encrypted user data to S3 - Using client-side encryption is ruled out as the startup does not want to provide the encryption keys.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

질문 58: 오답

The engineering team at an e-commerce company wants to establish a dedicated, encrypted, low latency, and high throughput connection between its data center and AWS Cloud. The engineering team has set aside sufficient time to account for the operational overhead of establishing this connection.

As a solutions architect, which of the following solutions would you recommend to the company?

설명
Correct option:

Use AWS Direct Connect plus VPN to establish a connection between the data center and AWS Cloud

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations.

With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection. Therefore, AWS Direct Connect plus VPN is the correct solution for this use-case.

AWS Direct Connect Plus VPN: via - https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html

Incorrect options:

Use site-to-site VPN to establish a connection between the data center and AWS Cloud - AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. However, Site-to-site VPN cannot provide low latency and high throughput connection, therefore this option is ruled out.

Use VPC transit gateway to establish a connection between the data center and AWS Cloud - A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks. A transit gateway by itself cannot establish a low latency and high throughput connection between a data center and AWS Cloud. Hence this option is incorrect.

Use AWS Direct Connect to establish a connection between the data center and AWS Cloud - AWS Direct Connect by itself cannot provide an encrypted connection between a data center and AWS Cloud, so this option is ruled out.

References:

https://aws.amazon.com/directconnect/

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html

질문 50: 정답

A company is in the process of migrating its on-premises SMB file shares to AWS so the company can get out of the business of managing multiple file servers across dozens of offices. The company has 200TB of data in its file servers. The existing on-premises applications and native Windows workloads should continue to have low latency access to this data without any disruptions after the migration. The company also wants any new applications deployed on AWS to have access to this migrated data.

Which of the following is the best solution to meet this requirement?

설명
Correct option:

Use Amazon FSx File Gateway to provide low-latency, on-premises access to fully managed file shares in Amazon FSx for Windows File Server. The applications deployed on AWS can access this data directly from Amazon FSx in AWS

For user or team file shares, and file-based application migrations, Amazon FSx File Gateway provides low-latency, on-premises access to fully managed file shares in Amazon FSx for Windows File Server. For applications deployed on AWS, you may access your file shares directly from Amazon FSx in AWS.

For your native Windows workloads and users, or your SMB clients, Amazon FSx for Windows File Server provides all of the benefits of a native Windows SMB environment that is fully managed and secured and scaled like any other AWS service. You get detailed reporting, replication, backup, failover, and support for native Windows tools like DFS and Active Directory.

Amazon FSx File Gateway: via - https://aws.amazon.com/storagegateway/file/

Incorrect options:

Use Amazon Storage Gateway's File Gateway to provide low-latency, on-premises access to fully managed file shares in Amazon FSx for Windows File Server. The applications deployed on AWS can access this data directly from Amazon FSx in AWS - When you need to access S3 using a file system protocol, you should use File Gateway. You get a local cache in the gateway that provides high throughput and low latency over SMB.

Amazon Storage Gateway's File Gateway does not support file shares for native Windows workloads, so this option is incorrect.

Amazon Storage Gateway's File Gateway:

Use Amazon Storage Gateway's File Gateway to provide low-latency, on-premises access to fully managed file shares in Amazon S3. The applications deployed on AWS can access this data directly from Amazon S3 - - When you need to access S3 using a file system protocol, you should use File Gateway. You get a local cache in the gateway that provides high throughput and low latency over SMB.

The given use case requires native Windows support for the applications. File Gateway can only be used to access S3 objects using a file system protocol, so this option is incorrect.

Use Amazon FSx File Gateway to provide low-latency, on-premises access to fully managed file shares in Amazon EFS. The applications deployed on AWS can access this data directly from Amazon EFS - Amazon FSx File Gateway provides access to fully managed file shares in Amazon FSx for Windows File Server and it does not support EFS. You should also note that EFS uses the Network File System version 4 (NFS v4) protocol and it does not support SMB protocol. Therefore this option is incorrect for the given use case.

References:

https://aws.amazon.com/storagegateway/file/fsx/

https://aws.amazon.com/storagegateway/faqs/

https://aws.amazon.com/blogs/storage/aws-reinvent-recap-choosing-storage-for-on-premises-file-based-workloads/

질문 30: 오답

A media agency stores its re-creatable assets on Amazon S3 buckets. The assets are accessed by a large number of users for the first few days and the frequency of access falls down drastically after a week. Although the assets would be accessed occasionally after the first week, but they must continue to be immediately accessible when required. The cost of maintaining all the assets on S3 storage is turning out to be very expensive and the agency is looking at reducing costs as much as possible.

As a Solutions Architect, can you suggest a way to lower the storage costs while fulfilling the business requirements?

설명
Correct option:

Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days - S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed and re-creatable data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. The minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA.

S3 One Zone-IA offers the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. S3 Storage Classes can be configured at the object level, and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Constraints for Lifecycle storage class transitions: via - https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

Supported S3 lifecycle transitions: via - https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

Incorrect options:

Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days

Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days

As mentioned earlier, the minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA or S3 Standard-IA, so both these options are added as distractors.

Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days - S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. But, it costs more than S3 One Zone-IA because of the redundant storage across availability zones. As the data is re-creatable, so you don't need to incur this additional cost.

References:

https://aws.amazon.com/s3/storage-classes/

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

질문 40: 오답

A financial services company uses Amazon GuardDuty for analyzing its AWS account metadata to meet the compliance guidelines. However, the company has now decided to stop using GuardDuty service. All the existing findings have to be deleted and cannot persist anywhere on AWS Cloud.

Which of the following techniques will help the company meet this requirement?

설명
Correct option:

Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon S3. GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

Disable the service in the general settings - Disabling the service will delete all remaining data, including your findings and configurations before relinquishing the service permissions and resetting the service. So, this is the correct option for our use case.

Incorrect options:

Suspend the service in the general settings - You can stop Amazon GuardDuty from analyzing your data sources at any time by choosing to suspend the service in the general settings. This will immediately stop the service from analyzing data, but does not delete your existing findings or configurations.

De-register the service under services tab - This is a made-up option, used only as a distractor.

Raise a service request with Amazon to completely delete the data from all their backups - There is no need to create a service request as you can delete the existing findings by disabling the service.

Reference:

https://aws.amazon.com/guardduty/faqs/

질문 65: 오답

An Electronic Design Automation (EDA) application produces massive volumes of data that can be divided into two categories. The 'hot data' needs to be both processed and stored quickly in a parallel and distributed fashion. The 'cold data' needs to be kept for reference with quick access for reads and updates at a low cost.

Which of the following AWS services is BEST suited to accelerate the aforementioned chip design process?

설명
Correct option:

Amazon FSx for Lustre

Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world’s most popular high-performance file system. It is used for workloads such as machine learning, high-performance computing (HPC), video processing, and financial modeling. The open-source Lustre file system is designed for applications that require fast storage – where you want your storage to keep up with your compute. FSx for Lustre integrates with Amazon S3, making it easy to process data sets with the Lustre file system. When linked to an S3 bucket, an FSx for Lustre file system transparently presents S3 objects as files and allows you to write changed data back to S3.

FSx for Lustre provides the ability to both process the 'hot data' in a parallel and distributed fashion as well as easily store the 'cold data' on Amazon S3. Therefore this option is the BEST fit for the given problem statement.

Incorrect options:

Amazon FSx for Windows File Server - Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. FSx for Windows does not allow you to present S3 objects as files and does not allow you to write changed data back to S3. Therefore you cannot reference the "cold data" with quick access for reads and updates at low cost. Hence this option is not correct.

Amazon EMR - Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR uses Hadoop, an open-source framework, to distribute your data and processing across a resizable cluster of Amazon EC2 instances. EMR does not offer the same storage and processing speed as FSx for Lustre. So it is not the right fit for the given high-performance workflow scenario.

AWS Glue - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing. AWS Glue does not offer the same storage and processing speed as FSx for Lustre. So it is not the right fit for the given high-performance workflow scenario.

질문 4: 오답

A news network uses Amazon S3 to aggregate the raw video footage from its reporting teams across the US. The news network has recently expanded into new geographies in Europe and Asia. The technical teams at the overseas branch offices have reported huge delays in uploading large video files to the destination S3 bucket.

Which of the following are the MOST cost-effective options to improve the file upload speed into S3? (Select two)

설명
Correct options:

Use Amazon S3 Transfer Acceleration to enable faster file uploads into the destination S3 bucket - Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

Use multipart uploads for faster file uploads into the destination S3 bucket - Multipart upload allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object's data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. Multipart upload provides improved throughput, therefore it facilitates faster file uploads.

Incorrect options:

Create multiple AWS direct connect connections between the AWS Cloud and branch offices in Europe and Asia. Use the direct connect connections for faster file uploads into S3 - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Direct connect takes significant time (several months) to be provisioned and is an overkill for the given use-case.

Create multiple site-to-site VPN connections between the AWS Cloud and branch offices in Europe and Asia. Use these VPN connections for faster file uploads into S3 - AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections are a good solution if you have low to modest bandwidth requirements and can tolerate the inherent variability in

Internet-based connectivity. Site-to-site VPN will not help in accelerating the file transfer speeds into S3 for the given use-case.

Use AWS Global Accelerator for faster file uploads into the destination S3 bucket - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. AWS Global Accelerator will not help in accelerating the file transfer speeds into S3 for the given use-case.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

질문 22: 오답

A leading carmaker would like to build a new car-as-a-sensor service by leveraging fully serverless components that are provisioned and managed automatically by AWS. The development team at the carmaker does not want an option that requires the capacity to be manually provisioned, as it does not want to respond manually to changing volumes of sensor data.

Given these constraints, which of the following solutions is the BEST fit to develop this car-as-a-sensor service?

설명
Correct option:

Ingest the sensor data in an Amazon SQS standard queue, which is polled by a Lambda function in batches and the data is written into an auto-scaled DynamoDB table for downstream processing

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

AWS manages all ongoing operations and underlying infrastructure needed to provide a highly available and scalable message queuing service. With SQS, there is no upfront cost, no need to acquire, install, and configure messaging software, and no time-consuming build-out and maintenance of supporting infrastructure. SQS queues are dynamically created and scale automatically so you can build and grow applications quickly and efficiently.

As there is no need to manually provision the capacity, so this is the correct option.

Incorrect options:

Ingest the sensor data in Kinesis Data Firehose, which directly writes the data into an auto-scaled DynamoDB table for downstream processing

Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon OpenSearch Service, Splunk, and any custom HTTP endpoint or HTTP endpoints owned by supported third-party service providers, including Datadog, Dynatrace, LogicMonitor, MongoDB, New Relic, and Sumo Logic.

Firehose cannot directly write into a DynamoDB table, so this option is incorrect.

Ingest the sensor data in an Amazon SQS standard queue, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing

Ingest the sensor data in a Kinesis Data Streams, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing

Using an application on an EC2 instance is ruled out as the carmaker wants to use fully serverless components. So both these options are incorrect.

References:

https://aws.amazon.com/sqs/

https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html

https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html

https://aws.amazon.com/kinesis/data-streams/faqs/

질문 28: 정답

A retail company uses Amazon EC2 instances, API Gateway, Amazon RDS, Elastic Load Balancer and CloudFront services. To improve the security of these services, the Risk Advisory group has suggested a feasibility check for using the Amazon GuardDuty service.

Which of the following would you identify as data sources supported by GuardDuty?

설명
Correct option:

VPC Flow Logs, DNS logs, CloudTrail events - Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.

GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail events, Amazon VPC Flow Logs, and DNS logs.

With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon EventBridge Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

How GuardDuty works: via - https://aws.amazon.com/guardduty/

Incorrect options:

VPC Flow Logs, API Gateway logs, S3 access logs

ELB logs, DNS logs, CloudTrail events

CloudFront logs, API Gateway logs, CloudTrail events

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

https://aws.amazon.com/guardduty/

질문 34: 정답

The sourcing team at the US headquarters of a global e-commerce company is preparing a spreadsheet of the new product catalog. The spreadsheet is saved on an EFS file system created in us-east-1 region. The sourcing team counterparts from other AWS regions such as Asia Pacific and Europe also want to collaborate on this spreadsheet.

As a solutions architect, what is your recommendation to enable this collaboration with the LEAST amount of operational overhead?

설명
Correct option:

The spreadsheet on the EFS file system can be accessed in other AWS regions by using an inter-region VPC peering connection

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

You can connect to Amazon EFS file systems from EC2 instances in other AWS regions using an inter-region VPC peering connection, and from on-premises servers using an AWS VPN connection. So this is the correct option.

Incorrect options:

The spreadsheet will have to be copied in Amazon S3 which can then be accessed from any AWS region

The spreadsheet data will have to be moved into an RDS MySQL database which can then be accessed from any AWS region

Copying the spreadsheet into S3 or RDS database is not the correct solution as it involves a lot of operational overhead. For RDS, one would need to write custom code to replicate the spreadsheet functionality running off of the database. S3 does not allow in-place edit of an object. Additionally, it's also not POSIX compliant. So one would need to develop a custom application to "simulate in-place edits" to support collabaration as per the use-case. So both these options are ruled out.

The spreadsheet will have to be copied into EFS file systems of other AWS regions as EFS is a regional service and it does not allow access from other AWS regions - Creating copies of the spreadsheet into EFS file systems of other AWS regions would mean no collaboration would be possible between the teams. In this case, each team would work on "its own file" instead of a single file accessed and updated by all teams. Hence this option is incorrect.

Reference:

https://aws.amazon.com/efs/

질문 43: 오답

Upon a security review of your AWS account, an AWS consultant has found that a few RDS databases are un-encrypted. As a Solutions Architect, what steps must be taken to encrypt the RDS databases?

설명 Correct option:

Take a snapshot of the database, copy it as an encrypted snapshot, and restore a database from the encrypted snapshot. Terminate the previous database

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

You can encrypt your Amazon RDS DB instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instances. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots.

You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created. However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. So this is the correct option.

Incorrect options:

Create a Read Replica of the database, and encrypt the read replica. Promote the read replica as a standalone database, and terminate the previous database - If the master is not encrypted, the read replicas cannot be encrypted. So this option is incorrect.

Enable Multi-AZ for the database, and make sure the standby instance is encrypted. Stop the main database to that the standby database kicks in, then disable Multi-AZ - Multi-AZ is to help with High Availability, not encryption. So this option is incorrect.

Enable encryption on the RDS database using the AWS Console - There is no direct option to encrypt an RDS database using the AWS Console.

Steps to encrypt an un-encrypted RDS database: Create a snapshot of the un-encrypted database Copy the snapshot and enable encryption for the snapshot Restore the database from the encrypted snapshot

Migrate applications to the new database, and delete the old database

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

질문 45: 오답

You have a team of developers in your company, and you would like to ensure they can quickly experiment with AWS Managed Policies by attaching them to their accounts, but you would like to prevent them from doing an escalation of privileges, by granting themselves the AdministratorAccess managed policy. How should you proceed?

설명 Correct option:

For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves

AWS supports permissions boundaries for IAM entities (users or roles). A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. Here we have to use an IAM permission boundary. They can only be applied to roles or users, not IAM groups.

Permissions boundaries for IAM entities: via - https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Incorrect options:

Create a Service Control Policy (SCP) on your AWS account that restricts developers from attaching themselves the AdministratorAccess policy - Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization’s access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren't available if your organization has enabled only the consolidated billing features. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. If you consider this option, since AWS Organizations is not mentioned in this question, so we can't apply an SCP.

Attach an IAM policy to your developers, that prevents them from attaching the AdministratorAccess policy - This option is incorrect as the developers can remove this policy from themselves and escalate their privileges.

Put the developers into an IAM group, and then define an IAM permission boundary on the group that will restrict the managed policies they can attach to themselves - IAM permission boundary can only be applied to roles or users, not IAM groups. Hence this option is incorrect.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

질문 57: 오답

A financial services company has developed its flagship application on AWS Cloud with data security requirements such that the encryption key must be stored in a custom application running on-premises. The company wants to offload the data storage as well as the encryption process to Amazon S3 but continue to use the existing encryption key.

Which of the following S3 encryption options allows the company to leverage Amazon S3 for storing data with given constraints?

설명 Correct option:

Server-Side Encryption with Customer-Provided Keys (SSE-C)

You have the following options for protecting data at rest in Amazon S3:

Server-Side Encryption – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.

Client-Side Encryption – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

For the given use-case, the company wants to manage the encryption keys via its custom application and let S3 manage the encryption, therefore you must use Server-Side Encryption with Customer-Provided Keys (SSE-C).

Please review these three options for Server Side Encryption on S3: via - https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

Incorrect options:

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) - When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. So this option is incorrect.

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) - Server-Side Encryption with Customer Master Keys (CMKs) stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer-managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region.

Client-Side Encryption with data encryption is done on the client-side before sending it to Amazon S3 - You can encrypt the data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

질문 5: 정답

A company is developing a healthcare application that cannot afford any downtime for database write operations. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution using Amazon Aurora.

Which of the following options would you recommend?

설명 Correct option:

Set up an Aurora multi-master DB cluster

In a multi-master cluster, all DB instances can perform write operations. There isn't any failover when a writer DB instance becomes unavailable, because another writer DB instance is immediately available to take over the work of the failed instance. AWS refers to this type of availability as continuous availability, to distinguish it from the high availability (with brief downtime during failover) offered by a single-master cluster. For applications where you can't afford even brief downtime for database write operations, a multi-master cluster can help to avoid an outage when a writer instance becomes unavailable. The multi-master cluster doesn't use the failover mechanism, because it doesn't need to promote another DB instance to have read/write capability.

via - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-multi-master.html#aurora-multi-master-workloads

Incorrect options:

Set up an Aurora serverless DB cluster

Set up an Aurora provisioned DB cluster

Set up an Aurora Global Database cluster

These three options represent Aurora single-master clusters. In a single-master cluster, a single DB instance performs all write operations and any other DB instances are read-only. If the writer DB instance becomes unavailable, a failover mechanism promotes one of the read-only instances to be the new writer. As there is a brief downtime during this failover, so these three options are incorrect for the given use case.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-multi-master.html#aurora-multi-master-workloads

질문 10: 정답

A company has many VPC in various accounts, that need to be connected in a star network with one another and connected with on-premises networks through Direct Connect.

What do you recommend?

설명 Correct option:

Transit Gateway

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. With AWS Transit Gateway, you only have to create and manage a single connection from the central gateway into each Amazon VPC, on-premises data center, or remote office across your network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. So, this is a perfect use-case for the Transit Gateway.

Without Transit Gateway via - https://aws.amazon.com/transit-gateway/

With Transit Gateway via - https://aws.amazon.com/transit-gateway/

Incorrect options:

VPC Peering - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection). VPC Peering helps connect two VPCs and is not transitive. It would require to create many peering connections between all the VPCs to have them connect. This alone wouldn't work, because we would need to also connect the on-premises data center through Direct Connect and Direct Connect Gateway, but that's not mentioned in this answer.

VPN Gateway - A virtual private gateway (also known as a VPN Gateway) is the endpoint on the VPC side of your VPN connection. You can create a virtual private gateway before creating the VPC itself. VPN Gateway is a distractor here because we haven't mentioned a VPN.

Private Link - AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. Private Link is utilized to create a private connection between an application that is fronted by an NLB in an account, and an Elastic Network Interface (ENI) in another account, without the need of VPC peering, and allowing the connections between the two to remain within the AWS network.

References:

https://aws.amazon.com/transit-gateway/

https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_CreateVpnGateway.html

질문 61: 정답

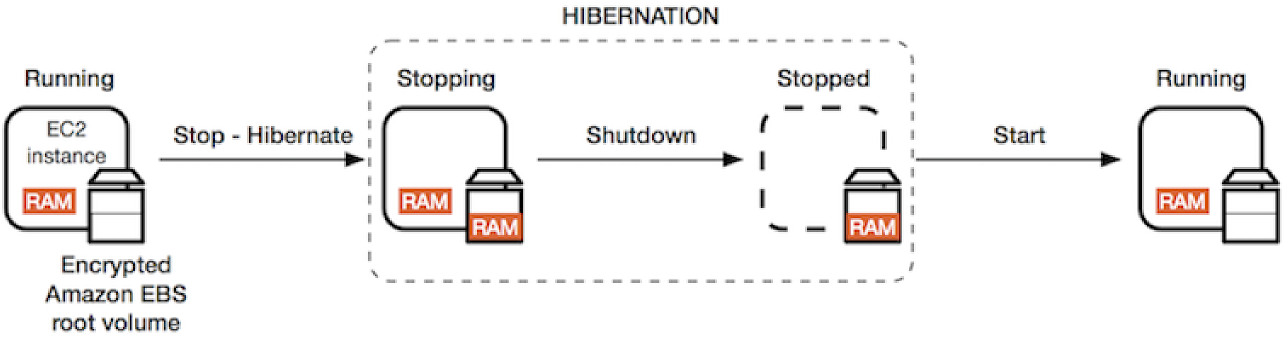
A Machine Learning research group uses a proprietary computer vision application hosted on an EC2 instance. Every time the instance needs to be stopped and started again, the application takes about 3 minutes to start as some auxiliary software programs need to be executed so that the application can function. The research group would like to minimize the application boostrap time whenever the system needs to be stopped and then started at a later point in time.

As a solutions architect, which of the following solutions would you recommend for this use-case?

설명 Correct option:

Use EC2 Instance Hibernate

When you hibernate an instance, AWS signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon EBS root volume. AWS then persists the instance's Amazon EBS root volume and any attached Amazon EBS data volumes.



When you start your instance:

The Amazon EBS root volume is restored to its previous state

The RAM contents are reloaded

The processes that were previously running on the instance are resumed

Previously attached data volumes are reattached and the instance retains its instance ID

Overview of EC2 hibernation: via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html

By using EC2 hibernate, we have the capability to resume it at any point of time, with the application already launched, thus helping us cut the 3 minutes start time.

Incorrect options:

Use EC2 User-Data - EC2 instance user data is the data that you specified in the form of a configuration script while launching your instance. Here, the problem is that the application takes 3 minutes to launch, no matter what. EC2 user data won't help us because it's just here to help us execute a list of commands, not speed them up.

Use EC2 Meta-Data - EC2 instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups. The EC2 meta-data is a distractor and can only help us determine some metadata attributes on our EC2 instances.

Create an AMI and launch your EC2 instances from that - An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.

Creating an AMI may help with all the system dependencies, but it won't help us with speeding up the application start time.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html