Answer Sheet

Q1) You need to install and configure software applications to an EC2 instance that you'll deploy using CloudFormation. You have to ensure that the applications are properly running before the stack creation proceeds.
Which of the following should you do to meet this requirement?

✅ Add a CreationPolicy attribute to the instance then send a success signal after the applications are installed and configured. Use the cfn-signal helper script to signal a resource.
Explanation:-You can associate the CreationPolicy attribute with a resource to prevent its status from reaching create complete until AWS CloudFormation receives a specified number of success signals or the timeout period is exceeded. To signal a resource, you can use the cfn-signal helper script or SignalResource API. AWS CloudFormation publishes valid signals to the stack events so that you track the number of signals sent. The creation policy is invoked only when AWS CloudFormation creates the associ

⚪ Use the UpdateReplacePolicy attribute and send a success signal after the applications are installed and configured using the cfn-signal helper script.
Explanation:-This option is incorrect because the UpdateReplacePolicy attribute is primarily used to retain or in some cases, backup the existing physical instance of a resource when it is replaced during a stack update operation.

⚪ Add a UpdatePolicy attribute to the instance then send a success signal after the applications are installed and configured. Use the cfn-signal helper script to signal a resource.
Explanation:-This option is incorrect because the UpdatePolicy attribute is primarily used for updating resources and for stack update rollback operations.

⚪ Use the DependsOn attribute and send a success signal after the applications are installed and configured using the cfn-init helper script.
Explanation:-This option is incorrect because the cfn-init helper script is not suitable to be used to signal another resource. You have to use cfn-signal instead. And although you can use the DependsOn attribute to ensure the creation of a specific resource follows another, it is still better to use the CreationPolicy attribute instead as it ensures that the applications are properly running before the stack creation proceeds.

Q2) You are working as a Systems Administrator for a leading software development company which provides various cloud-based solutions. A developer requested access to the AWS Management Console to view how your VPC is structured.
Which of the following options would you do to accomplish this?

⚪ Create an IAM user with both a console password and access keys.
Explanation:-This option is incorrect.

⚪ Create a new IAM user and generate access keys.
Explanation:-This option is incorrect.

✅ Create a new IAM user and generate a console password.
Explanation:-An IAM user is an entity that you create in AWS to represent the person or service that uses it to interact with AWS. A user in AWS consists of a name and credentials. You can grant access to AWS in different ways depending on the user credentials:
-Console password: A password that the user can type to sign in to interactive sessions such as the AWS Management Console.
-Access keys: A combination of an access key ID and a secret access key. You can assign two to a user at a time. Thes

⚪ Provide root AWS Account credentials to the developer.
Explanation:-This option is incorrect.

Q3) You are the Technical Lead of the SysOps team of your company where you are developing a NodeJS application that will be hosted on AWS. The application needs to send messages across various sub-components which are hosted in an Auto Scaling group of EC2 instances in which the order of the messages should be preserved.
Which of the following options would you provision for this requirement?

⚪ Kinesis stream
Explanation:-This option is incorrect as Kinesis Stream is used for data analytics and for real-time data processing over large, distributed data streams.

⚪ Standard SQS queue
Explanation:-This option is incorrect because the Standard SQS queue does not preserve the order of messages, unlike the FIFO queue.

⚪ SNS Topic
Explanation:-This option is incorrect as SNS is a notification service.

✅ SQS FIFO queue
Explanation:-FIFO queues have all the capabilities of the standard queue and improves upon and complements the standard queue. The most important features of this queue type are FIFO (First-In-First-Out) delivery and exactly-once processing:
-The order in which messages are sent and received is strictly preserved and a message is delivered once and remains available until a consumer processes and deletes it.
-Duplicates aren't introduced into the queue.
In addition, FIFO queues support messag

Q4) You are working as a SysOps Administrator for a commercial bank which recently started using AWS. You are designing a CloudFormation template that will launch a large On-Demand EC2 Instance and install the 3rd-party application package. Once the instance has been launched and the application installed successfully, it should signal AWS CloudFormation that the process is complete. Conversely, it should also signal AWS CloudFormation if the installation fails.
Which of the following options will you use to achieve this requirement?

⚪ Use the cfn-hup and cfn-init helper scripts.
Explanation:-This option is incorrect because the cfn-hup helper script is basically a daemon that detects changes in resource metadata and runs user-specified actions when a change is detected.

⚪ Use the cfn-get-metadata and cfn-init helper scripts.
Explanation:-This option is incorrect because the cfn-get-metadata helper script is mainly used to fetch a metadata block from AWS CloudFormation and print it to standard out.

⚪ Use the cfn-init helper script to install the third-party package and send notification back to AWS CloudFormation.
Explanation:-This option is incorrect because the cfn-init helper script is mainly used to read template metadata from the AWS::CloudFormation::Init key. Although this can be used to install software packages in the EC2 instance, you still need to use the cfn-signal helper script to indicate whether the Amazon EC2 instance and the 3rd party package have been successfully created.

✅ Use the cfn-signal and cfn-init helper scripts.

Explanation:-The cfn-signal helper script signals AWS CloudFormation to indicate whether Amazon EC2 instances have been successfully created or updated. If you install and configure software applications on instances, you can signal AWS CloudFormation when those software applications are ready.
You use the cfn-signal script in conjunction with a CreationPolicy or an Auto Scaling group with a WaitOnResourceSignals update policy. When AWS CloudFormation creates or updates resources with those policies, it

---

Q5)

A robotics firm is building a serverless RESTful API using API Gateway, Lambda, and DynamoDB in AWS. An AWS Lambda function was created to fetch data from a DynamoDB table.

Which of the following options would you do to ensure that the Lambda function can access the DynamoDB table successfully?

✅ Ensure the IAM role attached to the function has DynamoDB access.
Explanation:-You can use Lambda functions as triggers for your Amazon DynamoDB table. Triggers are custom actions you take in response to updates made to the DynamoDB table. To create a trigger, first you enable Amazon DynamoDB Streams for your table. Then, you write a Lambda function to process the updates published to the stream.
Regardless of what invokes a Lambda function, AWS Lambda always executes a Lambda function on your behalf. If your Lambda function needs to access any AWS resources, you need
⚪ Use the AWS Serverless Application Model (AWS SAM) to allow the Lambda function to access the DynamoDB table.
Explanation:-This option is incorrect because the AWS Serverless Application Model (AWS SAM) is just a model to define serverless applications for AWS Lambda. It does not have the ability to grant permissions or an IAM role to access DynamoDB.
⚪ Modify the Security Group of the Lambda function to allow access to the DynamoDB table.
Explanation:-This option is incorrect because Security Groups are usually used for EC2 instances and not for Lambda functions.
⚪ Modify the associated Network ACL of the Lambda function to allow access to the DynamoDB table.
Explanation:-This option is incorrect because a Network ACL is unnecessary in this scenario since both the DynamoDB table and the Lambda function exist in the same VPC. You only need to provision an IAM role in this particular scenario.

Q6) A technology company is planning to use an Auto Scaling group of On-Demand EC2 Instances that would be used to host a suite of web-based applications written in ReactJS and NodeJS. These applications would be running 24/7 throughout the year and as the Systems Administrator, you are responsible in ensuring that the architecture is both elastic and cost-effective. The instance type would need to be upgraded during the year depending on the usage of the application.
Which of the following is the most suitable instance purchasing option to use?

⚪ On-Demand Instances
Explanation:-This option is incorrect.
⚪ Spot Instances
Explanation:-This option is incorrect.
⚪ Standard Reserved Instances
Explanation:-This option is incorrect.
✅ Convertible Reserved Instances
Explanation:-When you purchase a Reserved Instance, you can choose between a Standard or Convertible offering class. The Reserved Instance applies to a single instance family, platform, scope, and tenancy over a term. If your computing needs change, you may be able to modify or exchange your Reserved Instance, depending on the offering class. You can choose between: Standard Reserved Instance or a Convertible Reserved Instance.
In this scenario, the keyword is "instance type". You can upgrade or downgra

---

Q7) A multinational investment bank is planning to deploy their high-volume transaction processing system on a fleet of On-Demand EC2 Instances, which should be able to automatically scale and handle up to a million requests per second. You have to design the architecture to distribute the incoming traffic to the EC2 Instances across multiple Availability Zones.
Which of the following would you implement for this requirement?

⚪ An SQS queue
Explanation:-This option is incorrect because there is no mention on the need for decoupling or distribution of messages between components of the application.
⚪ A Classic Load Balancer
Explanation:-This option is incorrect because a Classic ELB cannot scale to handle millions of requests per second.
✅ A Network Load Balancer
Explanation:-A Network Load Balancer can scale to millions of requests per second. From the AWS Documentation, using a Network Load Balancer has the following benefits:
-Ability to handle volatile workloads and scale to millions of requests per second.
-Support for static IP addresses for the load balancer. You can also assign Elastic IP address per subnet enabled for the load balancer.
-Support for registering targets by IP address, including targets outside the VPC for the load balancer.
⚪ An Application Load Balancer
Explanation:-This option is incorrect because an Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. It cannot scale to handle millions of requests per second.

Q8) You have been tasked to migrate your company's data analytics applications to their new service center. The service center managers will also need to learn how to manage the infrastructure. Since the industry requires standards compliance, Chef recipes must be used to build and configure the stack.
What is the best way to perform this in a simple and straighforward manner using AWS?

⚪ Use CodeDeploy to deploy applications and application content into the servers.
Explanation:-This option is incorrect.
⚪ Use CloudFormation to create a template for your infrastructure.
Explanation:-This option is incorrect.
⚪ Use Elastic Beanstalk to provision and connect resources for you.
Explanation:-This option is incorrect.

✅ Use OpsWorks to create a stack, then add layers and configure lifecycle events.

Explanation:-OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises

---

Q9) A web development company is using a fleet of On-Demand EC2 instances. You are working as their IT Consultant when a critical security vulnerability was discovered on the OS that the company is using. You are instructed to ensure that all EC2 instances are updated with the latest security patches as soon as possible.
Which of the following AWS services can you use to fulfill this task?

⚪ AWS Trusted Advisor

Explanation:-This option is incorrect because AWS Trusted Advisor can only provide recommendations but it could not apply the required patches in the EC2 instances.

⚪ AWS Config

Explanation:-This option is incorrect as AWS Config is mainly used as a configuration service.

⚪ AWS Inspector

Explanation:-This option is incorrect because AWS Inspector is more suitable in checking system vulnerabilities and not on patching the underlying OS of the EC2 instances.

✅ AWS System Manager

Explanation:-AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Amazon Linux, and Amazon Linux 2. You can sca

---

Q10) An IAM user in your VPC has created a new public subnet that will replace an existing subnet which has two running EC2 instances. You have launched a couple of instances on the new subnet and you are about to delete the old public subnet.
What will happen in this scenario?

⚪ The subnet will not be deleted while its associated routes are still present in the main route table.

⚪ The subnet will be deleted including the remaining EC2 instances.

✅ The subnet will not be deleted until the instances are terminated.

Explanation:-If you no longer need your subnet, you can delete it. You must terminate any instances in the subnet first. You will be prompted with an error message in the AWS Console when you try to delete a subnet with instances.
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

⚪ The subnet will be deleted and will automatically move its EC2 instances to the default subnet of the VPC.

Q11) A DevOps Engineer reported a problem accessing his EC2 instance with a private IP address of 172.31.8.11 from his corporate laptop. The EC2 instance is hosting a web application which works well but he is still experiencing an issue establishing a connection to manage the instance.
As the SysOps Administrator, which of the following options is the most suitable solution in this scenario based on the VPC flow log entries below?
2 123456789010 eni-abc123de 110.217.100.70 172.31.8.11 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK

✅ Allow incoming RDP traffic in the security group of the EC2 instance including the inbound and outbound rules in the Network ACL.

Explanation:-Based on the VPC flow log record provided, the RDP traffic (destination port 3389, TCP protocol) to network interface eni-abc123de in the AWS account 123456789010 was rejected. The RDP connection request came from the DevOps engineer's laptop (with an IP address of 110.217.100.70) and it is trying to access the EC2 instance with a private IP address of 172.31.8.11.
Although the scenario did not explicitly say what type of remote connection protocol the DevOps engineer used, it is quite clea

⚪ Based on the log, the DevOps Engineer's IP address is 110.217.100.70 which is not whitelisted to access the instance. Add an inbound rule in the security group to allow SSH traffic to the instance coming from this specific IP address.

Explanation:-This option is incorrect because although the DevOps Engineer's IP address is indeed 110.217.100.70, you should allow the RDP traffic instead of SSH traffic. Based on the logs, the DevOps engineer is connecting to the instance using RDP and not via SSH.

⚪ Attach an Elastic IP address to the EC2 instance.

Explanation:-This option is incorrect because even though you attached an Elastic IP address to your EC2 instance, the issue will persist since the RDP traffic is still not allowed in your security group or network ACL.

⚪ Based on the log, the DevOps Engineer's IP address is actually 172.31.8.11 and not 110.217.100.70 which is what the user reported. Tell the user to connect to the 110.217.100.70 IP address instead.

Explanation:-This option is incorrect because based on the flow log record, the DevOps Engineer's IP address is indeed 110.217.100.70 and not 172.31.8.11. The primary issue here is that the RDP traffic is not properly allowed in the security group and network ACL of the EC2 instance.

Q12) You are working as a SysOps administrator for a consultancy company where you are instructed to deploy their multi-tier web application to AWS. The front end application servers will be using NGINX and for the database-tier, they will be using a MariaDB cluster which will be hosted on three large Reserved EC2 Instances. For security purposes, you also need to ensure that the database servers are not accessible over the Internet to avoid any data security breach.
Which of the following options would you implement to satisfy the above requirement? (Choose 2)

⚪ Launch an Internet-facing load balancer for the database servers.

Explanation:-This option is incorrect as it is the complete opposite.

✅ Launch an internal load balancer for the database server.

Explanation:-If your application has multiple tiers, for example web servers that must be connected to the Internet and database servers that are only connected to the web servers, you can design an architecture that uses both internal and Internet-facing load balancers.
Create an Internet-facing load balancer and register the web servers with it. Create an internal load balancer and register the database servers with it. The web servers receive requests from the Internet-facing load balancer and send r

⚪ Launch a NAT Gateway on a private subnet to ensure that the database server could initiate outbound IPv4 traffic to the Internet but prevent the instances from receiving inbound traffic initiated by someone on the Internet.

Explanation:-This option is incorrect because neither a NAT instance nor a NAT Gateway is needed on this scenario. There is no requirement that says the database server could initiate outbound IPv4 traffic to the Internet but prevent it from receiving inbound traffic from the Internet. In addition,

a NAT Instance or NAT Gateway should be deployed on a public subnet and not on a private one.

- Launch a NAT Instance to ensure that the database server could not initiate outbound IPv4 traffic to the Internet.

Explanation:-This option is incorrect because neither a NAT instance nor a NAT Gateway is needed on this scenario. There is no requirement that says the database server could initiate outbound IPv4 traffic to the Internet but prevent it from receiving inbound traffic from the Internet. In addition, a NAT Instance or NAT Gateway should be deployed on a public subnet and not on a private one.

- ✅ Launch an Internet-facing application load balancer for the web servers.

Explanation:-If your application has multiple tiers, for example web servers that must be connected to the Internet and database servers that are only connected to the web servers, you can design an architecture that uses both internal and Internet-facing load balancers.
Create an Internet-facing load balancer and register the web servers with it. Create an internal load balancer and register the database servers with it. The web servers receive requests from the Internet-facing load balancer and send r

- Launch an internal load balancer for the web servers.

Q13) One of the Systems Administrators in your team has created a VPC with a CIDR block of 20.0.0.0/16 using the VPC wizard. There is a requirement to implement a hybrid cloud architecture in which you have to connect the client's data center to its VPC in AWS. You created a public subnet with a CIDR block of (20.0.0.0/24) and a VPN-only subnet with a CIDR block of (20.0.1.0/24) along with the VPN gateway (vgw-51898) to connect to the data center, which has a CIDR block of 172.12.0.0/12. To allow traffic to the internet from the VPN subnet, you also made an additional setup for a NAT instance (i-918273).
Which of the following options is not a valid entry for the main route table in this scenario?

- Destination: 172.12.0.0/12 and Target: vgw-51898
- Destination: 0.0.0.0/0 and Target: i-918273
- ✅ Destination: 20.0.1.0/24 and Target: i-918273

Explanation:-The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel. This is a recommended scenario if you want to extend your network into the cloud and also directly access the Internet from your VPC.
This scenario enables you to run a multi-tiered application with a scalable web front end in a public subnet, and to house your data in a pri

- Destination: 20.0.0.0/16 and Target: local

Q14) You send a ping command from your home computer, with an IP address of 110.237.99.166, to your EC2 instance which has a private IP address of 172.31.17.140. However, the response ping is dropped and does not reach your home computer. To troubleshoot the issue, you checked the flow logs of your VPC and you saw the following entries as shown below.
Which is the most likely root cause of this issue?

2 123456789010 eni-1235b8ca 110.237.99.166 172.31.17.140 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.17.140 110.237.99.166 0 0 1 4 336 1432917094 1432917142 REJECT OK

- Your network ACL does not permit inbound ICMP traffic.

Explanation:-In this scenario, the ping command from your home computer to your EC2 instance failed and there are two VPC Flow logs provided in the scenario. The logs basically mean that the first one is the record of the traffic flow that goes from your home computer to your EC2 instance and the latter is the record of the traffic flow that goes back from the EC2 instance back to your home computer.
Apparently, the first one is an ACCEPT record and the second one is a REJECT record, which means that t

- Your security group's inbound rules do not allow ICMP traffic.

Explanation:-In this scenario, the ping command from your home computer to your EC2 instance failed and there are two VPC Flow logs provided in the scenario. The logs basically mean that the first one is the record of the traffic flow that goes from your home computer to your EC2 instance and the latter is the record of the traffic flow that goes back from the EC2 instance back to your home computer.
Apparently, the first one is an ACCEPT record and the second one is a REJECT record, which means that t

- ✅ Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic.

Explanation:-In this scenario, the ping command from your home computer to your EC2 instance failed and there are two VPC Flow logs provided in the scenario. The logs basically mean that the first one is the record of the traffic flow that goes from your home computer to your EC2 instance and the latter is the record of the traffic flow that goes back from the EC2 instance back to your home computer.
Apparently, the first one is an ACCEPT record and the second one is a REJECT record, which means that t

- Your security group has an inbound rule that allow ICMP traffic but does not have an outbound rule to explicitly allow outgoing ICMP traffic.

Explanation:-In this scenario, the ping command from your home computer to your EC2 instance failed and there are two VPC Flow logs provided in the scenario. The logs basically mean that the first one is the record of the traffic flow that goes from your home computer to your EC2 instance and the latter is the record of the traffic flow that goes back from the EC2 instance back to your home computer.
Apparently, the first one is an ACCEPT record and the second one is a REJECT record, which means that t

---

Q15) A financial start-up has recently adopted a hybrid cloud infrastructure with AWS Cloud. They are planning to migrate their online payments system that supports an IPv6 address and uses an Oracle database in a RAC configuration. As the AWS Consultant, you have to make sure that the application can initiate outgoing traffic to the Internet but blocks any incoming connection from the Internet.
Which of the following options would you do to properly migrate the application to AWS?

- ✅ Migrate the Oracle database to an EC2 instance. Launch the application on a separate EC2 instance and then set up an egress-only Internet gateway.

Explanation:-An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with your instances. An instance in your public subnet can connect to the Internet through the Internet gateway if it has a public IPv4 address or an IPv6 address. Similarly, resources on the Internet can initiate a connection to your instan

- Migrate the Oracle database to RDS. Launch the application on a separate EC2 instance and then set up a NAT Instance.

Explanation:-This options is incorrect because a NAT instance does not support IPv6 address. You have to use an egress-only Internet gateway instead. In addition, RDS does not support Oracle RAC which is why, you have to launch the database in an EC2 instance.

- Migrate the Oracle database to an EC2 instance. Launch an EC2 instance to host the application and then set up a NAT Instance.

Explanation:-This options is incorrect because a NAT instance does not support IPv6 address. You have to use an egress-only Internet gateway instead. In addition, RDS does not support Oracle RAC which is why, you have to launch the database in an EC2 instance.

- Migrate the Oracle database to RDS. Launch an EC2 instance to host the application and then set up a NAT gateway instead of a NAT instance for better availability and higher bandwidth.

Explanation:-This option is incorrect as RDS does not support Oracle RAC. Although it is true that NAT Gateway provides better availability and higher bandwidth than NAT instance, it still does not support IPv6 address unlike an egress-only Internet gateway.

Q16) You are migrating a suite of web applications hosted in your on-premises data center to your AWS Cloud in which you have to deploy a total of 30 EC2 instances. A new VPC should be created and should be configured with AWS Client VPN to securely access your AWS resources and the resources in your on-premises network.
Which of the following IPv4 CIDR block should you use to satisfy this requirement?

✅ 10.0.0.0/26
Explanation:-To calculate the total number of IP addresses of a given CIDR Block, you simply need to follow the 3 easy steps below. Let's say you have a CIDR block /26:
1. Subtract 32 with the mask number : (32 - 26) = 6
2. Raise the number 2 to the power of the answer in Step #1 :
2^ 6 = (2 * 2 * 2 * 2 * 2 * 2) = 64
3. Subtract the answer to Step #2 to 5 to get the number of usable IP addresses.
The answer in Step #2 is the total number of IP addresses available in the given CIDR

⚪ 10.0.0.0/27
Explanation:-This option is incorrect because a /27 netmask can only provide you with 27 usable IP addresses. This is insufficient since you need a total of 30 usable IP addresses.

⚪ 10.0.0.0/28
Explanation:-This option is incorrect because a /28 netmask can only provide you with 11 usable IP addresses. This is insufficient since you need a total of 30 usable IP addresses.

⚪ 10.0.0.0/29
Explanation:-This option is incorrect because the only allowed block size is between a /28 netmask and /16 netmask. Hence, a /29 netmask is invalid.

Q17) You used Route 53 to register the domain name of an online timesheet application named: "www.tutorialsdojo-timesheet.com" and deployed the application on ECS. After a few months, a new version of the timesheet application is ready to be deployed which contains bug fixes and new features. The DevOps team launched a separate ECS instance for the new version and they instructed you to direct the initial set of traffic to the new version so they can do their production verification tests. Once verified that the new version is working, you can now totally route all traffic coming from the www.tutorialsdojo-timesheet.com domain to the new ECS instance.
Which of the following would you do to smoothly deploy the new application version?

✅ Launch 2 resource records based on the Weighted Routing policy
Explanation:-To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group.
For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resou

⚪ Launch 2 resource records based on the Failover Routing policy
Explanation:-This option is incorrect because this type is only used when you want to route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy.

⚪ Launch a resource record based on the Latency routing policy
Explanation:-This option is incorrect as this is used when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.

⚪ Launch a resource record based on the Geoproximity routing policy
Explanation:-This option is incorrect as this is only used when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.

Q18) You are working as a Systems Administrator for a medical device manufacturer which has recently adopted a hybrid cloud infrastructure. They need to establish a dedicated connection between their on-premises network and their AWS VPC. In the next couple of weeks, they will migrate their applications and move their data from their on-premises network to AWS, which is why they need a more consistent network experience than Internet-based connections.
Which of the following options would you implement for this scenario?

⚪ Set up an AWS VPN CloudHub
Explanation:-This option incorrect because a VPN is an Internet-based connection, unlike Direct Connect which provide a dedicated connection. An Internet-based connection means that the traffic from the VPC and to the on-premises network traverse the public Internet, which is why it is slow. You should use Direct Connect instead.

⚪ Set up a VPC peering
Explanation:-This option is incorrect because VPC Peering is mainly used to connect two or more VPCs.

✅ Set up a Direct Connect connection
Explanation:-AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. Hence, this option is correct for this scenario.

⚪ Set up a VPN Connection
Explanation:-This option incorrect because a VPN is an Internet-based connection, unlike Direct Connect which provide a dedicated connection. An Internet-based connection means that the traffic from the VPC and to the on-premises network traverse the public Internet, which is why it is slow. You should use Direct Connect instead.

Q19) You are working as a Systems Administrator for a leading fast moving consumer goods company. You are required to add a new subnet in your VPC, which will allow you to host 20 EC2 instances.
Which of the following IPv4 CIDR block should you use for this requirement?

✅ 172.0.0.0/27
Explanation:-To calculate the total number of IP addresses of a given CIDR Block, you simply need to follow the 2 easy steps below. Let's say you have a CIDR block /27:
1. Subtract 32 with the mask number : (32 - 27) = 5
2. Raise the number 2 to the power of the answer in Step #1 : 2^ 5 = (2 * 2 * 2 * 2 * 2) = 32
The answer in Step #2 is the total number of IP addresses available in the given CIDR netmask. Don't forget that in AWS, the first 4 IP addresses and the last IP address in each subn

172.0.0.0/28

Explanation:-This option is incorrect as a netmask of /28 only supports 16 IP Addresses.

172.0.0.0/30

Explanation:-This option incorrect as the only allowed block size is between a /28 netmask and /16 netmask.
To add a CIDR block to your VPC, the following rules apply:
The allowed block size is between a /28 netmask and /16 netmask.
The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
You cannot increase or decrease the size of an existing CIDR block.
You have a limit on the number of CIDR blocks you can associate with a VPC and the number of

172.0.0.0/29

Explanation:-This option incorrect as the only allowed block size is between a /28 netmask and /16 netmask.
To add a CIDR block to your VPC, the following rules apply:
The allowed block size is between a /28 netmask and /16 netmask.
The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
You cannot increase or decrease the size of an existing CIDR block.
You have a limit on the number of CIDR blocks you can associate with a VPC and the number of

---

Q20) A company wants to set up a hybrid cloud architecture to connect their on-premises infrastructure and their AWS VPC. As their SysOps Administrator, you need to ensure that the company can reliably and securely transfer large data sets from their on-premises data center to AWS.
Which of the following will you implement for this requirement?

AWS Placement Groups

Explanation:-AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
This Option is incorrect since this is used for improved netw

AWS VPC Peering

Explanation:-AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
This Option is incorrect since this is used to connect multip

AWS Direct Connect

Explanation:-AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

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

AWS VPN

Explanation:-AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
This Option is incorrect. A VPN allows you to securely transf

---

Q21) A technology company is planning to improve its online services by migrating their applications hosted on their on-premises data center to AWS. They have a total of 200 TB of data that need to be transferred to S3 as soon as possible.
Which of the following options is the fastest way to transfer the data in AWS?

Use AWS Snowball.

Explanation:-AWS Snowball is a service that accelerates transferring large amounts of data into and out of AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at faster-than internet speeds. This transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping containers, complete with E Ink shipping labels. With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-prem

Use AWS Snowmobile.

Explanation:-This option is incorrect because Snowmobile is more suitable in migrating large datasets of 10PB or more in a single location. For datasets less than 10PB or distributed in multiple locations, you should use Snowball.

Set up an AWS Direct Connect connection between the on-premises data center and your VPC.

Explanation:-This option is incorrect because an AWS Direct Connect connection is more suitable in setting up a hybrid cloud architecture and not for data migration.

Set up an AWS Managed VPN Connection between the on-premises data center and your VPC.

Explanation:-This option is incorrect because a VPN Connection traverses the public Internet. Hence, it would take a significant amount of time to completely transfer all 200 TB of data to AWS.

Q22) You are the IT Lead of a mobile game application startup. Since they have no storage capacity that would sufficiently cater to the expected 500,000 users each month, you decided to use AWS. They want to store the objects and metadata separately. What are the possible options to ensure that their data is secure, costs are optimized, and storage capacity is both scalable and durable?

Use EFS for object and metadata storage, and DynamoDB for the database.

Explanation:-This option is incorrect because EFS is more suited for file systems.

Use S3 for object and metadata storage, and DynamoDB for the database.

Explanation:-S3 is designed to have 99.999999999% durability and 99.99% availability over a given year and is used primarily for object storage. Meanwhile, DynamoDB also provides high availability and durability since it replicates data across AWS regions. It is also fast, flexible and easily scalable, which is perfect for mobile backend.

Use EBS for object and metadata storage, and DynamoDB for the database.

Explanation:-This option is incorrect because EBS provides block level storage for use with EC2 instances, and is not a standalone storage option like S3.

- Use S3-RRS for object and metadata storage, and use RDS for the database.

Explanation:-This option is incorrect because RDS is not as flexible as its NoSQL counterpart and I/O throughput is more important in this scenario. S3-RRS is often used for storing non-critical, reproducible data, which might not be optimal for a gaming app.

Q23) A stock brokerage company is setting up a PostgreSQL database on a large Reserved EC2 Instance for its online stock trading platform. Since the database is hosting critical financial data, you are instructed to ensure that the database-tier is fault tolerant.
Which of the following options would you implement to satisfy this requirement?

- Set up a RAID 0 configuration with multiple EFS volumes together.

Explanation:-This option is incorrect.

- Set up a RAID 5 configuration with multiple EFS volumes together.

Explanation:-This option is incorrect.

- ✅ Set up a RAID 1 configuration with multiple EBS volumes together.

Explanation:-With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level.
For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together which can also offers

- Set up a RAID 6 configuration with multiple EBS volumes together.

Explanation:-This option is incorrect.

Q24) An online stock trading application is extensively using an S3 bucket to store client data. To comply with the financial regulatory requirements, you need to generate a report on the replication and encryption status of all of the objects stored in your bucket. The report should show which type of server-side encryption is being used by each object.
As the Systems Administrator of the company, how can you meet the above requirement with the least amount of effort?

- ✅ Use S3 Inventory to generate the required report.

Explanation:-Amazon S3 inventory is one of the tools Amazon S3 provides to help manage your storage. You can use it to audit and report on the replication and encryption status of your objects for business, compliance, and regulatory needs. You can also simplify and speed up business workflows and big data jobs using Amazon S3 inventory, which provides a scheduled alternative to the Amazon S3 synchronous List API operation. Hence, this option is correct.
Amazon S3 inventory provides comma-separated valu

- Use S3 Select to generate the required report which retrieves specific data, such as replication and encryption status of your object, using simple SQL expressions without having to retrieve the entire object.

Explanation:-This option is incorrect because S3 Select is only used to retrieve specific data from the contents of an object using simple SQL expressions without having to retrieve the entire object. It does not generate a detailed report, unlike S3 Inventory.

- Use S3 Analytics to generate the report and Amazon Athena to query the data.

Explanation:-This option is incorrect because S3 Analytics is primarily used to analyze storage access patterns to help you decide when to transition the right data to the right storage class. It does not provide a report containing the replication and encryption status of your objects.

- Create a custom script which uses the GET and List bucket inventory REST APIs to generate the required report.

Explanation:-This is incorrect because although this is a valid answer, this solution entails a lot of effort in creating a custom script or program to fetch data and generate a report. You can use S3 Inventory instead to generate the report in the least amount of effort.

Q25) You are working as an AWS Technical Specialist for a renewable energy company. They currently have an application that uses an Oracle database deployed in a large EC2 instance, which houses data that are infrequently accessed.
What storage type for the EC2 instance is the most cost-effective solution that can host the database?

- EBS General Purpose SSD

Explanation:-This option is incorrect because a General purpose SSD volume costs more and it is mainly used for a wide variety of workloads. It is recommended to be used as system boot volumes, virtual desktops, low-latency interactive apps, and many more.

- Throughput Optimized HDD

Explanation:-This option is incorrect because Throughput Optimized HDD is primarily used for frequently accessed, throughput-intensive workloads. In this scenario, Cold HDD perfectly fits the requirement as it is used for their infrequently accessed data and provides the lowest cost, unlike Throughput Optimized HDD.

- ✅ Cold HDD

Explanation:-Cold HDD volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than Throughput Optimized HDD, this is a good fit ideal for large, sequential cold-data workloads. If you require infrequent access to your data and are looking to save costs, Cold HDD provides inexpensive block storage. Take note that bootable Cold HDD volumes are not supported. Cold HDD provides the lowest cost HDD volume and is designed for less fr

- Provisioned IOPS SSD

Explanation:-This options is incorrect because Provisioned IOPS HDD costs more than the Cold HDD and thus, not cost-effective for this scenario. It provides the highest performance SSD volume for mission-critical low-latency or high-throughput workloads, which is not needed in the scenario.

Q26) You are working as a Systems Administrator for a large audit firm where you have an assignment to tightly manage the flow of data between your Amazon Redshift cluster and your other AWS resources. The IT Security team of your company instructed you to use VPC flow logs to monitor all the COPY and UNLOAD traffic of your Redshift cluster.
How can you implement this solution in AWS?

- Create a new flow log that tracks the traffic of your Amazon Redshift cluster.

Explanation:-This option is incorrect because, by default, you cannot create a flow log for your Amazon Redshift cluster. You have to enable Enhanced VPC Routing and set up the required VPC configuration.

- Use the Amazon Redshift Spectrum feature.

Explanation:-This option is incorrect because the Redshift Spectrum is primarily used to run queries against exabytes of unstructured data in Amazon S3, with no loading or ETL required.

- ✅ Enable Enhanced VPC routing on your Amazon Redshift cluster.

Explanation:-When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster

and your data repositories through your Amazon VPC. By using Enhanced VPC Routing, you can use standard VPC features, such as VPC security groups, network access control lists (ACLs), VPC endpoints, VPC endpoint policies, internet gateways, and Domain Name System (DNS) servers. Hence, this option is the correct answer.
You use these features to tightly manage the flow o

- Enable Audit Logging in your Amazon Redshift cluster.

Explanation:-This option is incorrect because the Audit Logging feature is primarily used to get the information about the connection, queries, and user activities in your Redshift cluster.

Q27) A government organization has implemented a file gateway to keep copies of the home drives of their employees in a separate S3 bucket. As the SysOps Administrator, you noticed that most files are rarely accessed after 60 days but it is required that the files should still be available immediately in the event of a surprise audit.
In this scenario, what can you do to reduce the storage costs while continuing to provide access to the files for the employees?

- Set up an S3 bucket policy to limit user access to only newer files that are created in less than 60 days.

Explanation:-This option is incorrect.

- Create a lifecycle policy to moves files older than 60 days to Glacier storage class.

Explanation:-This option is incorrect.

- Enable versioning on the S3 bucket.

Explanation:-This option is incorrect.

- ✅ Set up a lifecycle policy that move the employee files older than 60 days to Infrequent Access storage class.

Explanation:-You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example: When you know objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. You might want to archive objects that you don't need to access in real time to the GLACIER storage class.

Q28) An enterprise supply chain application uses Glacier in archiving its data. You have to deploy and enforce compliance controls for individual Glacier vaults by specifying controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits for regulatory compliance. This is to ensure that once the Glacier vault is locked, the policy can no longer be changed.
Which is the most suitable approach to satisfy the given requirement?

- Use a combination of IAM policies to secure your Glacier vaults and Amazon S3 Glacier Select.

Explanation:-This option is incorrect because although you can deploy a variety of compliance controls in a vault lock policy using an AWS Identity and Access Management (IAM) policy, you still have to set up Amazon Glacier Vault Lock to secure and prevent any future changes to your vaults.

- Set up an Amazon S3 Glacier Data Retrieval Policy.

Explanation:-This option is incorrect because a Glacier Data Retrieval Policy is primarily used to easily set data retrieval limits and manage the data retrieval activities across your AWS account in each region.

- ✅ Use Amazon S3 Glacier Vault Lock.

Explanation:-Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual Glacier vaults with a vault lock policy. You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed. Hence, this option is correct.
Glacier enforces the controls set in the vault lock policy to help achieve your compliance objectives, for example, for data retention. You can deploy a v

- Set up an Amazon S3 Glacier vault access policy.

Explanation:-This option is incorrect because a vault lock policy is different than a vault access policy. Both policies govern access controls to your vault, however, a vault lock policy can be locked to prevent future changes, providing strong enforcement for your compliance controls compared to a regular vault access policy.

Q29) An aerospace engineering company is planning to migrate a large amount of data from their on-premises data center to Amazon S3. You are planning on transferring an initial amount of around 200 TB of data to S3 before moving the rest of their data.
Which of the following would be the ideal way to transfer this amount of data?

- ✅ Use the AWS Snowball Service.

Explanation:-AWS Snowball is a service that accelerates transferring large amounts of data in and out AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at a faster-than-internet speeds. Their transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping container, complete with E-Ink shipping labels. With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premise

- Set up VPC Peering from your on-premises network to AWS.

Explanation:-AWS Snowball is a service that accelerates transferring large amounts of data in and out AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at a faster-than-internet speeds. Their transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping container, complete with E-Ink shipping labels. With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premise

- Set up an AWS Direct Connect Connection.

Explanation:-AWS Snowball is a service that accelerates transferring large amounts of data in and out AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at a faster-than-internet speeds. Their transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping container, complete with E-Ink shipping labels. With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premise

- Set up an AWS Managed VPN Connection.

Explanation:-AWS Snowball is a service that accelerates transferring large amounts of data in and out AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at a faster-than-internet speeds. Their transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping container, complete with E-Ink shipping labels. With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premise

---

Q30) A startup company is planning to build their cloud-based enterprise resource planning application in AWS. You are working as their SysOps Administrator and one of the founders asked you to design and build a cost-effective cloud architecture. After deploying and configuring the resources, you have to ensure that it complies with the AWS best practices.
Which of the following services would you use to help you reduce cost, increase performance, and improve the security of your AWS resources?

AWS CloudFront
Explanation:-This options is incorrect because CloudFront is used as a Content Distribution Service.
AWS WAF
Explanation:-This option is incorrect because AWS WAF is used as a Web Application firewall in AWS and only provides security to your VPC.
AWS Inspector
Explanation:-This is incorrect because AWS Inspector is used to check for vulnerabilities in resources such as EC2 Instances. It does not provide a report on how you can further improve your architecture, unlike with Trusted Advisor.
AWS Trusted Advisor
Explanation:-Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. It also provides real time guidance to help you provision your resources in compliance with the AWS best practices.

Q31) You have multiple On-Demand EC2 instances that are deployed in the private subnet which are used to host a corporate portal. To protect any unauthorized access to your servers, your manager instructed you to set up a secure cloud architecture to allow access to your instances from the on-premises data center.
Which of the following options could you use to accomplish this?

Add a bastion host in a public subnet.
Explanation:-This Option is the correct answer. In an Amazon Web Services (AWS) context, a bastion host is defined as "a server whose purpose is to provide access to a private network from an external network, such as the Internet". Because of its limited exposure to potential attack, a bastion host can minimize the chances of penetration. Here's a VPC diagram on where bastions hosts should be placed.
Reference:
https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html
Add a bastion host in a private subnet.
Explanation:-In an Amazon Web Services (AWS) context, a bastion host is defined as "a server whose purpose is to provide access to a private network from an external network, such as the Internet". Because of its limited exposure to potential attack, a bastion host can minimize the chances of penetration. Here's a VPC diagram on where bastions hosts should be placed.
This Option is incorrect since the bastion host needs to be in a public subnet for it to be accessible from outside AWS.
Reference: <
Modify the Route tables for the subnet to add the NAT gateway.
Explanation:-In an Amazon Web Services (AWS) context, a bastion host is defined as "a server whose purpose is to provide access to a private network from an external network, such as the Internet". Because of its limited exposure to potential attack, a bastion host can minimize the chances of penetration. Here's a VPC diagram on where bastions hosts should be placed.
This Option is incorrect since the NAT gateway is used for outgoing communication from the EC2 Instances only. You need to allow incoming
Modify the Route tables for the subnet to add the Internet gateway.
Explanation:-In an Amazon Web Services (AWS) context, a bastion host is defined as "a server whose purpose is to provide access to a private network from an external network, such as the Internet". Because of its limited exposure to potential attack, a bastion host can minimize the chances of penetration. Here's a VPC diagram on where bastions hosts should be placed.
This Option is incorrect since this would expose the servers to the Internet.
Reference:
https://docs.aws.amazon.com/quickstart/

Q32) You are working as a SysOps Administrator for an IT Consulting company which has a VPC in the us-east-1 (N. Virginia) region for their business operations. Last month, the entire us-east-1 AWS region went down which totally rendered all of your cloud systems unavailable and eventually resulted in a financial loss. To prevent this from happening again, you are instructed by the CTO to set up a notification system which provides alerts via their Slack messaging channel when AWS is experiencing events that may impact their cloud resources.
Which of the following can you implement to meet this requirement?

Use AWS Health Events with CloudWatch Events and a Lambda function to send a notification to a Slack channel when an event occurs.
Explanation:-You can use Amazon CloudWatch Events to detect and react to changes in the status of AWS Personal Health Dashboard (AWS Health) events. Then, based on the rules that you create, CloudWatch Events invokes one or more target actions when an event matches the values that you specify in a rule.
Depending on the type of event, you can send notifications, capture event information, take corrective action, initiate events, or take other actions. You can select the following types of targets when u
Use a combination of CloudWatch Alarms, Lambda functions, and SES to send a notification to a Slack channel when an event occurs.
Explanation:-You can use Amazon CloudWatch Events to detect and react to changes in the status of AWS Personal Health Dashboard (AWS Health) events. Then, based on the rules that you create, CloudWatch Events invokes one or more target actions when an event matches the values that you specify in a rule.
Depending on the type of event, you can send notifications, capture event information, take corrective action, initiate events, or take other actions. You can select the following types of targets when u
Use a combination of CloudWatch Alarms and SNS to send a notification to a Slack channel when an event occurs.
Explanation:-You can use Amazon CloudWatch Events to detect and react to changes in the status of AWS Personal Health Dashboard (AWS Health) events. Then, based on the rules that you create, CloudWatch Events invokes one or more target actions when an event matches the values that you specify in a rule.
Depending on the type of event, you can send notifications, capture event information, take corrective action, initiate events, or take other actions. You can select the following types of targets when u
Set up an alert using AWS Trusted Advisor to send a notification to a Slack channel when an event occurs.
Explanation:-You can use Amazon CloudWatch Events to detect and react to changes in the status of AWS Personal Health Dashboard (AWS Health) events. Then, based on the rules that you create, CloudWatch Events invokes one or more target actions when an event matches the values that you specify in a rule.
Depending on the type of event, you can send notifications, capture event information, take corrective action, initiate events, or take other actions. You can select the following types of targets when u

---

Q33) A financial firm is hosting their mission critical system in AWS. As their Lead Systems Administrator, you are responsible for properly monitoring the status of their cloud resources and setting up an alert system so that you and the Operations team are notified for any technical issues. Since the system is critical to the day-to-day operations of the business, you also need to be notified of any issues that occur in the underlying hardware that hosts the AWS resources.
Which of the following is the best way to achieve this?

Set up a custom monitoring tool using CloudTrail that will send API requests to check the health of your AWS resources.

Explanation:-AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan

Set up a Service Health Dashboard that will automatically send alerts for any system issues.

Explanation:-AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan

Use the Personal Health Dashboard which provides information about AWS Health events that can affect your account.

Explanation:-AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan

Simply use a CloudWatch Dashboard to automatically check the status of underlying hardware that hosts your AWS resources and send alerts for any outages.

Explanation:-AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan

---

Q34)

You are setting up a CloudWatch Dashboard which should track the memory and swap usage of all Linux EC2 Instances in your VPC. There would be an upcoming IT audit and this should be done as soon as possible.

Which of the following do you need to do to achieve this?

Enable basic monitoring on the instance.

Explanation:-You can use the AWS CloudWatch Monitoring Scripts for Amazon Elastic Compute Cloud (Amazon EC2) Linux-based instances to produce and consume Amazon CloudWatch custom metrics. These sample Perl scripts comprise a fully functional example that reports memory, swap, and disk space utilization metrics for a Linux instance.

This option is incorrect because these monitoring options will not give you memory and swap statistics for your instances. You need to use custom metrics for these values.

• Enable detailed monitoring on the instance.

Explanation:-You can use the AWS CloudWatch Monitoring Scripts for Amazon Elastic Compute Cloud (Amazon EC2) Linux-based instances to produce and consume Amazon CloudWatch custom metrics. These sample Perl scripts comprise a fully functional example that reports memory, swap, and disk space utilization metrics for a Linux instance.

This option is incorrect because these monitoring options will not give you memory and swap statistics for your instances. You need to use custom metrics for these values.