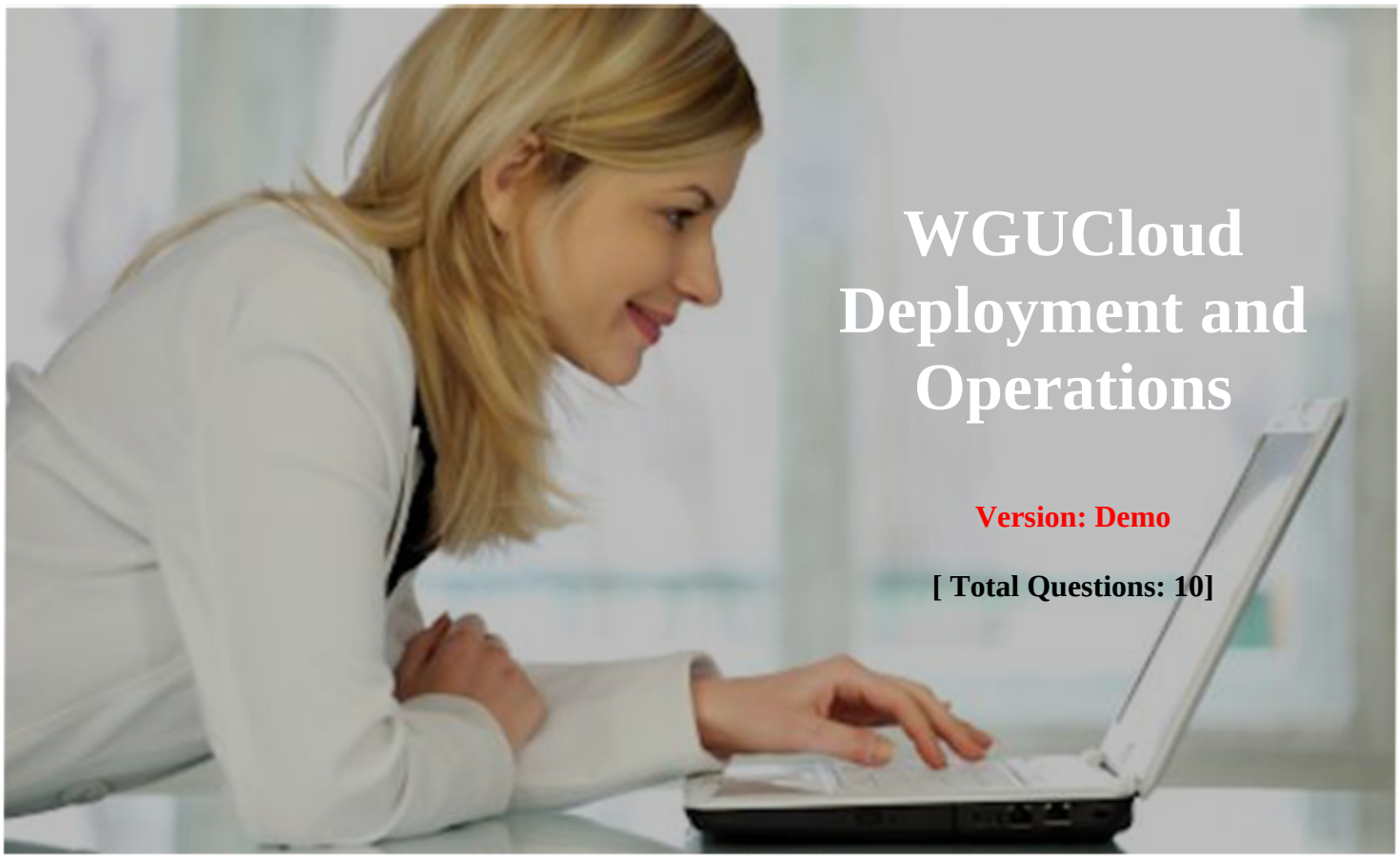
DumpsCafe

WGU

Cloud-Deployment-and-Operations



Web: www.dumpscafe.com

Email: support@dumpscafe.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpscafe.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@dumpscafe.com and our technical experts will provide support within 24 hours.

Copyright

Category Breakdown

Category	Number of Questions
Automates Cloud Provisioning	3
Remediates AWS Issues	2
Configures Network Connectivity	2
Implements AWS Protection Services	2
Determines Optimal Cost and Performance Baseline	1
TOTAL	10

Question #:1 - [Automates Cloud Provisioning]

(An administrator needs to create Systems Manager Automation documents to take action based on AWS Config rules. Which two file formats should be used? Choose 2 answers.)

A. JSON

B. YAML

C. XML

D. CSV

Answer: A B

Explanation

Systems Manager Automation documents can be created using JSON or YAML file formats to define workflows and actions based on AWS Config rules. These formats allow administrators to specify the steps and parameters for automation tasks, such as remediation actions triggered by Config rule evaluations. The WGU Cloud Deployment and Operations Study Guide (Section 5.1, Systems Manager Automation) states that both JSON and YAML are supported formats for writing Automation documents, providing flexibility in scripting automation logic. XML and CSV are not supported formats for this purpose.

Question #:2 - [Remediates AWS Issues]

(Which two solutions are supported by CloudWatch? Choose 2 answers.)

A. Load balancing

B. Threat detection

C. Event response

D. Instance monitoring

Answer: C D

Explanation

Amazon CloudWatch supports several monitoring and management solutions, including event response and instance monitoring. Event response is facilitated through CloudWatch Events, which can trigger actions based on predefined rules, such as invoking AWS Lambda functions. Instance monitoring involves collecting and tracking metrics from Amazon EC2 instances, providing visibility into performance and health. The WGU Cloud Deployment and Operations Study Guide (Section 4.1, CloudWatch Overview) highlights that CloudWatch is designed for instance monitoring and event-driven responses, while load balancing and threat detection are handled by services like Elastic Load Balancing and GuardDuty, respectively.

Question #:3 - [Automates Cloud Provisioning]

(What is a patch baseline attached to if it is not defined in Patch Manager?)

A. Baseline data set

B. Default patch group

C. Patch process

D. Accelerate patch baseline

Answer: B

Explanation

If a patch baseline is not explicitly defined in Patch Manager, it is attached to the default patch group. This default group applies a preconfigured baseline with AWS-recommended patches, ensuring basic compliance for instances without custom baselines. The WGU Cloud Deployment and Operations Study Guide (Section 5.2, Patch Manager) states, "If no custom patch baseline is defined, instances are associated with the default patch group, which uses AWS-provided baseline settings for automatic patch approval." Options A, C, and D are not valid attachments for patch baselines.

Question #:4 - [Automates Cloud Provisioning]

(An organization uses CloudFormation to deploy AWS infrastructure. The templates are built in JSON and deploy EC2 instances across multiple regions. Which solution should be used to set values in the template based on region-specific AMI IDs?)

A. Outputs

B. WaitCondition

C. Mappings

D. Resources

Answer: C

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

The Mappings section in a CloudFormation template should be used to set values based on region-specific AMI IDs. Mappings allow the template to define a lookup table that associates regions with corresponding AMI IDs, enabling dynamic selection during stack creation across multiple regions. The WGU Cloud Deployment and Operations Study Guide (Section 5.3, CloudFormation Mappings) states, "The Mappings section enables region-specific configurations, such as mapping AMI IDs to regions (e.g., 'us-east-1': 'ami-123456'), ensuring the correct AMI is used based on the deployment region." Outputs, WaitCondition, and Resources do not provide this mapping functionality.

Question #:5 - [Configures Network Connectivity]

(An administrator deploys an EC2 instance with the public IP address 54.18.127.233 into a newly created VPC in us-west-2. The EC2 instance must be accessible via ec2-public-54.18.127.233.us-west-2.compute.amazonaws.com from the internet. Which solution should be used?)

A. Assign a resource tag to the EC2 instance

B. Set the VPC attribute enableDnsHostnames to true

C. Set the VPC attribute enableDnsSupport to false

D. Assign a resource-based name to the EC2 instance

Answer: B

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

To make the EC2 instance accessible via a public DNS hostname like ec2-public-54.18.127.233.us-west-2.compute.amazonaws.com, the administrator must set the VPC attribute enableDnsHostnames to true. This enables the automatic assignment of public DNS hostnames to instances with public IP addresses in the VPC. The WGU Cloud Deployment and Operations Study Guide (Section 3.2, VPC Configuration) states, "Setting enableDnsHostnames to true in the VPC configuration ensures that EC2 instances with public IPs receive a public DNS hostname (e.g., ec2-public-<ip>.<region>.compute.amazonaws.com), facilitating internet accessibility." Resource tags, disabling DNS support, and resource-based names do not enable this functionality.</region></ip>

Question #:6 - [Remediates AWS Issues]

(An administrator successfully accesses an EC2 instance via SSH from a local computer then stops it and starts it. Following the restart, the EC2 instance is no longer accessible. Which solution should be used to resolve the issue?)

A. Add a rule to the security group associated with the NIC of the EC2 instance

B. Change the port used to connect to EC2 instance

C. Add a route to the route table associated with the EC2 instance subnet

D. Change the IP address used to connect to the EC2 instance

Answer: A

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

After stopping and starting an EC2 instance, the public IP address may change (unless an Elastic IP is attached), but the security group rules remain intact. If the instance is no longer accessible via SSH, it's likely due to an inbound rule (e.g., for port 22) not being correctly configured or applied. Adding or verifying a rule in the security group associated with the network interface (NIC) to allow SSH (port 22) from the administrator's IP resolves this. The WGU Cloud Deployment and Operations Study Guide (Section 3.2, Security Groups) states, "Stopping and starting an EC2 instance may require verifying or adding an inbound SSH rule (port 22) in the security group if connectivity is lost due to IP or rule misconfiguration." Route table or IP changes are not the primary issue here.

Question #:7 - [Implements AWS Protection Services]

(Which solution should be used to host content to be processed for Amazon Made?)

A. DocumentDB

B. DynamoDB

C. S3

D. EC2

Answer: C

Explanation

Amazon S3 (Simple Storage Service) should be used to host content to be processed for Amazon Made, as it provides scalable object storage ideal for storing and retrieving large amounts of data, such as media files or documents, for processing workflows. The WGU Cloud Deployment and Operations Study Guide (Section 2.1, Amazon S3) states, "S3 is the preferred solution for hosting content to be processed by services like Amazon Made, offering durable and highly available storage with support for lifecycle policies and integration with other AWS services." DocumentDB, DynamoDB, and EC2 are not designed for this content hosting purpose.

Question #:8 - [Configures Network Connectivity]

(A company that uses five Elastic IP addresses does not want to request more from AWS. Which solution should be used to route requests to a healthy endpoint?)

A. Adjust the TTL of the IP packets

B. Edit the route table for the VPC

C. Use Systems Manager to update endpoints

D. Register a DNS name to an auto-assigned public IP address

Answer: D

Explanation

To route requests to a healthy endpoint without requesting additional Elastic IP addresses, the company should register a DNS name to an auto-assigned public IP address using a service like Route 53. This leverages dynamic DNS to distribute traffic, reducing reliance on fixed EIPs. The WGU Cloud Deployment and Operations Study Guide (Section 3.1, Route 53) states, "Registering a DNS name with an auto-assigned public IP in Route 53 allows traffic routing to healthy instances, avoiding the need for additional Elastic IP addresses." TTL adjustment, route table edits, and Systems Manager are not relevant solutions.

Question #:9 - [Determines Optimal Cost and Performance Baseline]

(Which Performance Insights view provides information on the hardware resource that may be causing a bottleneck?)

A. Wait event

B. Users

C. Hosts

D. Statement

Answer: A

Explanation

The Wait event view in Amazon RDS Performance Insights provides information on hardware resources (e.g., CPU, I/O, memory) that may be causing bottlenecks by showing wait times for database operations. The WGU Cloud Deployment and Operations Study Guide (Section 7.2, Performance Insights) states, "The Wait event view in Performance Insights identifies resource bottlenecks (e.g., I/O wait times) by analyzing wait states, helping optimize database performance on hardware resources." Users, Hosts, and Statement views focus on different aspects and do not directly address hardware bottlenecks.

Question #:10 - [Implements AWS Protection Services]

(What can AWS Config directly invoke to cause remediation of findings?)

A. Lambda function

B. Control Tower guardrail

C. CloudWatch alarm

D. Systems Manager document

Answer: A

Explanation

AWS Config can directly invoke an AWS Lambda function to cause remediation of findings by triggering automated responses to configuration changes or non-compliant resources. This integration enables real-time corrective actions. The WGU Cloud Deployment and Operations Study Guide (Section 6.1, AWS Config) states, "AWS Config can invoke a Lambda function as a remediation action, allowing automated fixes for non-compliant resources (e.g., terminating unauthorized instances)." Control Tower guardrails, CloudWatch alarms, and Systems Manager documents are not directly invoked by Config for this purpose.

About dumpscafe.com

dumpscafe.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@dumpscafe.com
- Feedback: feedback@dumpscafe.com
- Support: support@dumpscafe.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.