PassQueen
a.k.a dumpsqueen.com

WGUCloud Deployment and Operations

WGU Cloud-Deployment-and-Operations

Version Demo

Total Demo Questions: 8

Total Premium Questions: 87

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

(Which two retention periods are supported by Performance Insights? Choose 2 answers.)

A. 1 day

B. 7 days

C. 1 year

D. 2 years

ANSWER: B C D

Explanation:

Amazon RDS Performance Insights supports retaining performance data for the free default period of **7 days**. It also supports paid long-term retention, which can be configured from **1 month through 24 months**. Therefore, both **1 year** (12 months) and **2 years** (24 months) are supported long-term retention durations, in addition to the 7-day default. The question is technically flawed because it asks for two answers even though three listed values are valid supported retention periods. AWS describes the configurable long-term Performance Insights retention range as 1–24 months; this makes 1 year and 2 years valid selections, while 7 days remains the supported default retention period. Retention settings can be selected when configuring Performance Insights for a DB instance and affect how long collected database load and wait-event history remains available for analysis. See the Amazon RDS Performance Insights pricing and retention documentation and the Amazon RDS Performance Insights overview.

QUESTION NO: 2

(Which AWS monitoring feature is used to process events using AWS Lambda?)

A. Metrics

B. Targets

C. Rules

D. Logs

ANSWER: C

Explanation:

Rules is correct. Amazon CloudWatch Events, now delivered through Amazon EventBridge functionality, uses rules to match incoming events and route those events to one or more targets, including AWS Lambda functions. A rule can be configured with an event pattern that identifies relevant events from AWS services, such as changes in resource state, or with a schedule that invokes processing at specified times. When an event matches the configured pattern, the rule invokes its Lambda target asynchronously and passes the event payload to the function. This creates an event-driven operational workflow: AWS emits an event, the rule evaluates and matches it, and Lambda runs custom code to automate remediation, notifications, enrichment, or other processing. Rules therefore provide the event-selection and routing mechanism that connects monitoring or service events to Lambda-based processing. AWS recommends EventBridge for building these event-driven integrations; CloudWatch Events rules and EventBridge rules use the same underlying concepts and APIs. See the Amazon EventBridge rules documentation and the AWS guide to invoking Lambda with EventBridge.

QUESTION NO: 3

(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:

Event response and **Instance monitoring** are supported by Amazon CloudWatch. CloudWatch collects, stores, and visualizes operational metrics, including Amazon EC2 metrics such as CPU utilization, network traffic, disk activity, and status-related measurements. This monitoring gives operations teams visibility into instance health and performance, and it can be extended with the CloudWatch agent to collect additional operating-system-level metrics and logs.

CloudWatch also supports event-driven operational responses. CloudWatch alarms evaluate metrics against configured thresholds and can initiate actions when a threshold is reached, such as sending an Amazon SNS notification, invoking an Auto Scaling policy, or recovering an EC2 instance. AWS event-routing capabilities, originally provided as CloudWatch Events and now available through Amazon EventBridge, can also match events to rules and send them to targets for automated response workflows. Together, metrics, alarms, dashboards, logs, and event-driven automation make CloudWatch a core AWS observability and operational-response service. See the Amazon CloudWatch User Guide and the CloudWatch alarm actions documentation.

QUESTION NO: 4

(What is the role of a patch baseline in Patch Manager?)

A. Installs all patch updates as they become available by default

B. Assigns an IAM role for services that can auto-approve patches upon release

C. Defines patches that should and should not be installed on EC2 instances

D. Notifies Config of any patch updates that need to be performed

ANSWER: C

Explanation:

Defines patches that should and should not be installed on EC2 instances is correct. In AWS Systems Manager Patch Manager, a patch baseline is a set of rules that determines which patches are approved for installation and which patches are explicitly rejected. The baseline can select patches through approval rules, such as product, classification, severity, and an approval delay after release. It can also specify individual approved or rejected patches, allowing an organization to accommodate application dependencies, testing requirements, maintenance policy, and security standards. Patch Manager evaluates an instance against the patch baseline associated with its operating system and then uses that baseline during patch scanning or installation operations. AWS supplies predefined default baselines, but administrators can create custom baselines and designate them as defaults for supported operating systems. This approach provides controlled, repeatable patch governance across managed EC2 instances and other Systems Manager managed nodes rather than automatically installing every newly released update. For implementation details, see the AWS Systems Manager Patch Manager patch baselines documentation and the AWS Patch Manager User Guide.

QUESTION NO: 5

(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:

JSON and YAML are the supported document-content formats for AWS Systems Manager Automation runbooks. An Automation document defines the workflow AWS Systems Manager executes, including actions, inputs, branching logic, and remediation steps. For AWS Config-based remediation, an administrator can associate an AWS Config rule with an SSM Automation runbook so that Systems Manager runs the defined remediation workflow when a noncompliant resource is identified. The runbook's schema and its main steps can be authored in either JSON or YAML, allowing teams to choose the structured syntax that best fits their tooling and source-control practices.

AWS documentation for Systems Manager explicitly identifies JSON and YAML as the formats used to create SSM documents, including Automation runbooks. AWS Config remediation configuration also supports using an SSM Automation document as the remediation action for a rule. Therefore, JSON and YAML directly meet the requirement to create Automation documents that perform actions in response to AWS Config rule evaluations. See the AWS Systems Manager Automation runbook documentation and the AWS Config remediation documentation.

QUESTION NO: 6

(Which service should be used to schedule the patching of EC2 instances and on-premises servers with security updates?)

A. EventBridge

B. Config

C. App Runner

D. Systems Manager

ANSWER: D

Explanation:

Systems Manager is the appropriate AWS service because its Patch Manager capability automates the process of selecting, approving, and deploying operating-system patches to managed nodes. Those nodes can include both Amazon EC2 instances and on-premises servers, provided they are configured as Systems Manager managed nodes. Patch Manager supports defining patch baselines to control which updates are approved and using maintenance windows to schedule patching activities during an organization's designated maintenance period. This enables centralized, repeatable security-update operations across a hybrid environment rather than requiring administrators to patch each server individually. For on-premises systems, the Systems Manager Agent communicates with AWS Systems Manager through the required connectivity and permissions, allowing the same patch policies and scheduling approach used for EC2 to be applied consistently. AWS documents Patch Manager specifically as the Systems Manager feature for automating patching of managed nodes, including EC2 instances and on-premises servers. See the AWS Systems Manager Patch Manager User Guide and the AWS Systems Manager Maintenance Windows documentation.

QUESTION NO: 7

(A company centralizes Amazon CloudWatch Logs from several AWS accounts into a logging account. The source accounts already contain the required log groups. Which two actions must be performed in the logging account to allow the source accounts to send log events to the centralized destination? Choose 2 answers.)

A. Create a CloudWatch Logs destination

B. Attach a destination policy that permits the source accounts

C. Create an Amazon SNS topic for each source account

D. Create a CloudWatch alarm in the logging account

E. Enable VPC Flow Logs for every source VPC

ANSWER: A B

Explanation:

The logging account must **create a CloudWatch Logs destination** and **attach a destination policy that allows the source accounts to write to that destination**. A destination provides the centralized routing endpoint for cross-account log subscriptions and forwards received log events to a configured target, such as an Amazon Kinesis Data Firehose delivery stream or Amazon Kinesis data stream.

The destination policy is required because it grants the specified source accounts permission to call `logs:PutSubscriptionFilter` for the destination. A subscription filter is then created in each source account and references the destination ARN. An SNS topic and a CloudWatch alarm can notify operators, but neither authorizes cross-account log delivery.

QUESTION NO: 8

(A company uses KMS for key management. The company has a requirement to ensure that cryptographic material is not used longer than a year. Which solution should be used to meet this requirement with the least amount of effort?)

A. Move keys from KMS to CloudHSM

B. Enable automatic key rotation in KMS

C. Develop a custom key encryption protocol for KMS

D. Write a Lambda function to replace keys in KMS

ANSWER: B

Explanation:

Enable automatic key rotation in KMS is the lowest-effort solution because AWS KMS can automatically rotate the backing key material for eligible symmetric customer managed KMS keys. Rotation changes the cryptographic material used by the KMS key while preserving the key's identity, key policy, permissions, aliases, and ability to decrypt ciphertext produced under previous backing keys. This allows applications to continue using the same KMS key ARN without code changes or a manual process for creating, distributing, and retiring replacement keys.

For KMS keys configured for automatic rotation, AWS KMS performs rotation on the configured schedule. A one-year rotation period satisfies a requirement that backing cryptographic material not remain in use longer than a year. This built-in capability provides centralized, auditable lifecycle management and reduces the operational risk associated with implementing a separate rotation workflow. AWS documents automatic rotation for customer managed symmetric encryption KMS keys, including the rotation-period configuration and the fact that prior key material remains available for decryption of existing ciphertext. See AWS KMS key rotation and AWS KMS customer managed keys.