**QUESTION 68**

A company is migrating an application from on-premises servers to Amazon EC2 instances.

As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms.

The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time.

However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible.

The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

1. Create Amazon CloudWatch composite alarms where possible.

1. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
2. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
3. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

**Answer:** A

**QUESTION 175**

A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard.

The company's product manager needs to access this dashboard periodically.

The product manager does not have an AWS account.

A solution architect must provide access to the product manager by following the principle of least privilege.

Which solution will meet these requirements?

1. Share the dashboard from the CloudWatch console.

Enter the product manager's email address, and complete the sharing steps.

Provide a shareable link for the dashboard to the product manager.

1. Create an IAM user specifically for the product manager.

Attach the CloudWatch Read Only Access managed policy to the user.

Share the new login credential with the product manager.

Share the browser URL of the correct dashboard with the product manager.

1. Create an IAM user for the company's employees.

Attach the View Only Access AWS managed policy to the IAM user.

Share the new login credentials with the product manager.

Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.

1. Deploy a bastion server in a public subnet.

When the product manager requires access to the dashboard, start the server and share the RDP credentials.

On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

**Answer:** A