OBJECTIVE : MANAGEMENT TOOLS

Attempt	1	**Completed on**	Monday , 28 January 2019 , 07:10 PM
Marks Obtained	0 / 10	**Time Taken**	00 H 00 M 25 S
Your score is	0.0%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	10	0	1	9

10 Questions	**0** Correct	**1** Incorrect	**9** Unattempted	Show Answers	All ⌄

QUESTION 1   INCORRECT

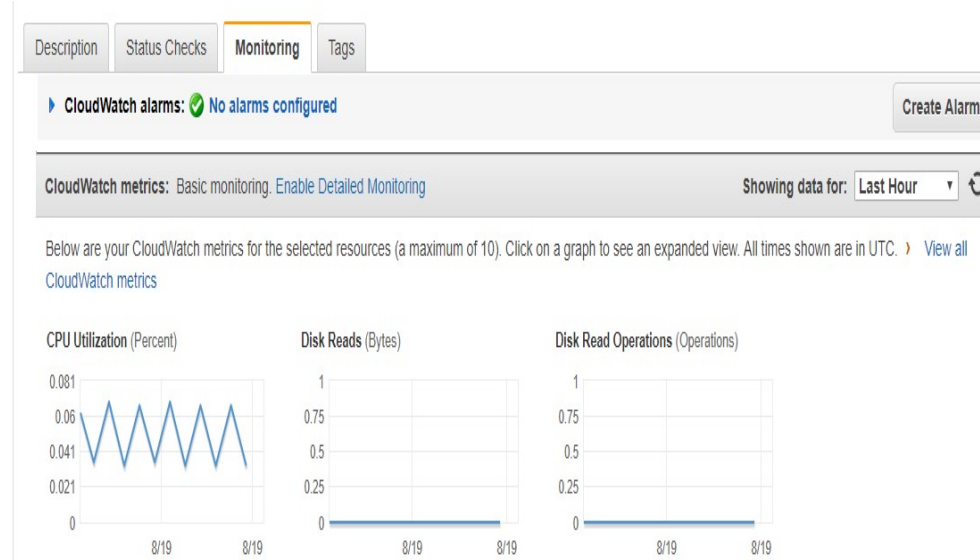Topic - Designing highly available, cost-efficient, fault-tolerant, scalable systems

Which of the following statements about Cloudwatch is true. Choose 3 answers from the options given below

☑ **A.** You can monitor custom metrics using cloudwatch ✔

☑ **B.** You can create alarms based on thresholds using cloudwatch ✔

☐ **C.** You can save money by monitoring resources in your AWS account ✔

☑ **D.** You need to pay for the basic monitoring package provided for EC2 Instances ✖

Explanation :

Answer - A, B and C
The Basic monitoring package for EC2 Instances comes free. When you launch your EC2 instances , you can actually view these metrics under the monitoring tab

| Description | Status Checks | **Monitoring** | Tags |

▶ **CloudWatch alarms:** ✅ **No alarms configured**   Create Alarm

CloudWatch metrics: Basic monitoring. Enable Detailed Monitoring   Showing data for: Last Hour ▼ ↻

Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC. › View all CloudWatch metrics

CPU Utilization (Percent)   Disk Reads (Bytes)   Disk Read Operations (Operations)

For more information on Cloudwatch , please refer to the below URL:

• http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html)

Ask our Experts   👍 👎

QUESTION 2   UNATTEMPTED

Topic – Implementation and Deployment

You have a number of resources created in your AWS Account. You want your monitoring team to have a consolidated view of the monitoring of critical resources. How can this be achieved?

○ **A. Create a Cloudwatch dashboard for these resources** ✔

○ **B. Create a Cloudwatch logs for these resources**

○ **C. Use Cloudtrail to monitor the critical resources**

○ **D. Use SNS to notify on important events of the critical resources**

Explanation :

Answer - A

The AWS documentation mentions

Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, even those resources that are spread across different regions. You can use CloudWatch dashboards to create customized views of the metrics and alarms for your AWS resources.

For more information on Cloudwatch dashboards, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html)

Ask our Experts

QUESTION 3   UNATTEMPTED

Topic – Implementation and Deployment

You have a number of resources created in your AWS Account. You want your monitoring team to be notified whenever a threshold is reached for critical resources. How can this be achieved? Choose 3 answers from the options give below

- ☐ **A.** Define the critical AWS resources that need to be monitored ✔
- ☐ **B.** Create a Cloudwatch alarms for these resources based on defined thresholds ✔
- ☐ **C.** Create Cloudwatch logs for each of the critical resources
- ☐ **D.** Use SNS to notify the monitoring team once an alarm is triggered. ✔

Explanation :

Answer - A,B and D
The AWS documentation mentions
You can create a CloudWatch alarm that watches a single metric. The alarm performs one or more actions based on the value of the metric relative to a threshold over a number of time periods. The action can be an Amazon EC2 action, an Auto Scaling action, or a notification sent to an Amazon SNS topic
For more information on Cloudwatch alarms, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html)

Ask our Experts

QUESTION 4   UNATTEMPTED

Topic - Designing highly available, cost-efficient, fault-tolerant, scalable systems

You have a number of resources created in your AWS Account. Your supervisor is worried about the charges that would be incurred by hosting these resources and wants to be notified beforehand before the charges go beyond a certain value. How can you achieve this in the best possible way?

○ **A.** Monitor the Billing dashboard everyday to see if you are going beyond that certain threshold

○ **B.** Create a utility to see the utilization of the resources and calculate the cost accordingly.

○ **C.** Create billing alarms with the thresholds defined accordingly. ✔

○ **D.** Define cloudwatch logs to log all the utilization and then calculate the cost accordingly.

Explanation :

Answer - C

Amazon CloudWatch alarm can be used to monitor your estimated charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

The Billing and Cost Management service provides a feature which you can use to estimate and plan your AWS costs, receive alerts if your costs exceed a threshold than your set, it assess your biggest investments in AWS resources, and, if you work with multiple AWS accounts, simplify your accounting. You can use Amazon CloudWatch to create billing alerts when your AWS costs exceed specified thresholds.

Reference Link: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html (http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html)
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/monitor-charges.html (http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/monitor-charges.html)
For more information on monitoring with Cloudwatch, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/gs_monitor_estimated_charges_with_cloudwa (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/gs_monitor_estimated_charges_with_cloudwatc

Ask our Experts   👍 👎

QUESTION 5   UNATTEMPTED

Topic – Implementation and Deployment

You have an EC2 Instance hosted in your AWS environment. You have been requested to advise the IT Monitoring team on monitoring a specific functionality of an application hosted on this EC2 Instance. How can you achieve this in the best possible way?

○ **A.** Run scripts to send data from the EC2 Instance to Cloudwatch Logs. Stream the logs to EMR and perform the required analysis.

○ **B.** Run scripts to send data from the EC2 Instance to S3. Stream the logs to EMR and perform the required analysis.

○ **C.** Publish custom metrics about the application onto Cloudwatch. Publish a widget on a Cloudwatch dashboard. ✔

○ **D.** Publish custom metrics about the application onto Cloudtrail

Explanation :

Answer - C

The best way is to publish custom metrics about the application. Since only metrics is required and no analysis is required , this is the best way.

The AWS Documentation specifies

You can publish your own metrics to CloudWatch using the AWS CLI or an API. You can view statistical graphs of your published metrics with the AWS Management Console.

For more information on monitoring with Cloudwatch custom metrics, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html)

Ask our Experts

Topic – Implementation and Deployment

To which of the following destinations can CloudTrail deliver events to?

Choose 2 answers from the options given below.

- ☐ **A.** Cloudwatch Logs ✔
- ☐ **B.** SNS
- ☐ **C.** SQS
- ☐ **D.** S3 ✔

Explanation :

Answer - A and D

The AWS documentation mentions

A trail is a configuration that enables delivery of CloudTrail events to an Amazon S3 bucket, CloudWatch Logs, and CloudWatch Events. You can use a trail to filter the CloudTrail events you want delivered, encrypt your CloudTrail event log files with an AWS KMS key, and set up Amazon SNS notifications for log file delivery.

For more information on Cloudtrail, please refer to the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html)

Ask our Experts

Topic – Implementation and Deployment

When you apply a Cloudtrail that applies to all regions , which of the following statement is false with regards to this configuration

○ **A.** An S3 bucket is created for each region to create the trail in ✔

○ **B.** It becomes easier to manage the trail for all regions

○ **C.** The configuration settings for the trail apply consistently across all regions

○ **D.** If a new region launches , you will automatically get events for the new region

---

Explanation :

Answer - A
The AWS Documentation specifies
A trail that applies to all regions has the following advantages:

- The configuration settings for the trail apply consistently across all regions.

- You receive CloudTrail events from all regions in a single S3 bucket and optionally in a CloudWatch Logs log group.

- You manage trail configuration for all regions from one location.

- You immediately receive events from a new region. When a new region launches, CloudTrail automatically creates a trail for you in the new region with the same settings as your original trail.

- You can create trails in regions that you don't use often to monitor for unusual activity

For more information on Cloudtrail, please refer to the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html)

Ask our Experts   👍 👎

Topic - Data Security

 Your supervisor wants to use the CLoudtrail service to monitor the API calls in the company's AWS account. But there is a concern on the security aspects on the data stored via Cloudtrail. As an architect , how can you explain the security features in terms of the way Cloudtrail stores the data. Choose 2 answers from the options given below

☐ **A.** Cloudtrail stores the data in plain text format , but encryption can be enabled using AES 256 bit encryption.

☐ **B.** By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon SSE-S3 ✔

☐ **C.** You can also opt to encrypt files using AWS KMS–managed keys (SSE-KMS) ✔

☐ **D.** By default, the log files delivered by CloudTrail to your bucket are encrypted by AWS KMS–managed keys (SSE-KMS)

Explanation :

Answer - B and C

The AWS documentation mentions

By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3). To provide a security layer that is directly manageable, you can instead use server-side encryption with AWS KMS–managed keys (SSE-KMS) for your CloudTrail log files.

For more information on Cloudtrail encryption, please refer to the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html)

Ask our Experts 👍 👎

QUESTION 9   UNATTEMPTED

Topic – Implementation and Deployment

You have configuring Cloudtrail to send the trails to an S3 bucket. What must be ensured that the trail logs can be delivered to the S3 bucket successfully.

○ **A.** Ensure the S3 bucket is created in the same region as CloudTrail

○ **B.** Ensure versioning is enabled on the S3 bucket

○ **C.** Ensure CloudTrail has access to the S3 bucket ✔

○ **D.** Ensure logging is enabled on the S3 bucket.

Explanation :

Answer - C

The AWS Documentation mentions

By default, S3 buckets and objects are private. Only the resource owner (the AWS account that created the bucket) can access the bucket and objects it contains. The resource owner can grant access permissions to other resources and users by writing an access policy.

To deliver log files to an S3 bucket, CloudTrail must have the required permissions.

For more information on CloudTrail and S3, please refer to the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html)

Ask our Experts 👍 👎

Topic - Data Security

Which of the following services provides risk auditing of your AWS Account?

○   **A.** Cloudwatch

○   **B.** Cloudwatch logs

○   **C.** Cloudtrail ✔

○   **D.** Trusted Advisor

Explanation :

Answer – C
The AWS Documentation mentions
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
For more information on Cloudtrail , please refer to the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14574)

Certification

⊘ Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)

⊘ Java Certification (https://www.whizlabs.com/oracle-java-certifications/)

⊘ PM Certification (https://www.whizlabs.com/project-management-certifications/)

⊘ Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Company

⊘ Support (https://help.whizlabs.com/hc/en-us)

⊘ Discussions (http://ask.whizlabs.com/)

⊘ Blog (https://www.whizlabs.com/blog/)

Mobile App

📱 Android ^{Coming Soon}

 iOS ^{Coming Soon}

Follow us

f

(https://www.facebook.com/whizlabs.software/)

in

(https://in.linkedin.com/company/whizlabs-software)

🐦

(https://twitter.com/whizlabs?lang=en)

G+

(https://plus.google.com/+WhizlabsSoftware)