**Cloudtrail interview Questions:**

**Question1: What is Cloudtrail?**

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.

**Question 2: Explain the functions of AWS CloudTrail.**

AWS CloudTrail is a service offered by AWS. This AWS service enables AWS users to implement governance, compliance, operational auditing, and risk auditing of their AWS accounts. Users can set up CloudTrail to log and continuously monitor the account activities.

AWS CloudTrail can retain the account activities across the AWS infrastructure of an organization. CloudTrail provides event history AWS account activities. It can do that for actions taken through the AWS Management Console, AWS SDKs (Software Development Kits), command-line tools, and other AWS services. CloudTrail can log and track API calls too.

You can use this event history for security analysis and tracking changes. These event histories also help with troubleshooting.

Question 3 : Which tasks can you perform using AWS CloudTrail?

CloudTrail records two types of events: **Management events capturing control plane actions on resources such as creating or deleting Amazon Simple Storage Service (Amazon S3) buckets**, and data events capturing data plane actions within a resource, such as reading or writing an Amazon S3 object.

Question 4: What does CloudTrail not record?

CloudTrail delivers log files to your S3 bucket approximately every 5 minutes. CloudTrail does not deliver **log files if no API calls are made on your account**.

Question 5: What is AWS CloudTrail logging?

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. ... For an ongoing record of activity and events in your AWS account, create a trail.

Question 6: What are the two types of events that can be logged in CloudTrail?

There are three types of events that can be logged in CloudTrail: **management events, data events, and CloudTrail Insights events**. By default, trails log management events, but not data or Insights events. All event types use a CloudTrail JSON log format. CloudTrail does not log all AWS services and all events.

Question 7: What are the benefits of CloudTrail?

CloudTrail **helps you prove compliance, improve security posture, and consolidate activity records across regions and accounts**. CloudTrail provides visibility into user activity by recording actions taken on your account.

Question 8: How many trails can she create in an AWS Region?

You can create up to **5 trails** per region (a trail that applies to all regions exists in each region and counted as 1 trail per region).

Question 9: Can you edit CloudTrail?

Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/ . In the navigation pane, choose Trails, and then choose a trail name. In General details, choose Edit to change the following settings. You cannot change the name of a trail.

Question 10: Can CloudTrail events be deleted?

Open the Trails page of the CloudTrail console. Choose the trail name. At the **top of the trail details page**, choose Delete. When you are prompted to confirm, choose Delete to delete the trail permanently.

Question 11: Is CloudTrail a SIEM?

A comprehensive SIEM to monitor your AWS cloud environment  
  
USM Anywhere unifies essential cloud security management in a single platform. With its AWS-native sensor, this cloud monitoring solution offers full AWS SIEM capabilities, including: CloudTrail monitoring and alerting. Event correlation.