CS 519 Cloud Computing Overview

**VL09: Optimizing with Trusted Advisor**

School of Technology and Computing

## **Instructions**

## For this activity you will be study this case:

## <https://aws.amazon.com/solutions/case-studies/hungama/>

Below you are given a table of service and corresponding limits. Based on the case study, identify which services were checked against with Trusted Advisor.

## Service limits

Checks for service usage that is more than 80% of the service limit. Values are based on a snapshot, so your current usage might differ. Limit and usage data can take up to 24 hours to reflect any changes.

The following table shows the limits that Trusted Advisor checks.  
Source: <https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

|  |  |
| --- | --- |
| **Service** | **Limits** |
| Amazon DynamoDB (DynamoDB) – No | Read capacity Write capacity |
| Amazon Elastic Block Store (Amazon EBS) - Yes, it has been audited. As an AWS Support, Enterprise-level tier customer, Hungama has access to AWS Trusted Advisor, which customers can use to audit their AWS usage against known best practices. AWS Trusted Advisor identifies opportunities to save money, improve system performance, and security. Hungama used AWS Trusted Advisor to run Cost Optimizing checks, which audited Amazon Elastic Block Store (Amazon EBS) volumes in Hungama’s environment. | Active volumes Active snapshots General Purpose (SSD) volume storage (GiB) Provisioned IOPS Provisioned IOPS (SSD) volume storage (GiB) Magnetic volume storage (GiB) |
| Amazon Elastic Compute Cloud (Amazon EC2) - Yes, it has been audited. As an AWS Support, Enterprise-level tier customer, Hungama has access to AWS Trusted Advisor, which customers can use to audit their AWS usage against known best practices. AWS Trusted Advisor identifies opportunities to save money, improve system performance, and security. Hungama used AWS Trusted Advisor to run Cost Optimizing checks, which audited Amazon EC2 instances volumes in Hungama’s environment. | Elastic IP addresses (EIPs) Reserved Instances - purchase limit (monthly) On-Demand instances |
| Amazon Kinesis Streams – No | Shards |
| Amazon Relational Database Service (Amazon RDS) - Yes, it has been audited. Hungama uses [Amazon Elastic Compute Cloud](https://aws.amazon.com/ec2/) (Amazon EC2) and [Amazon Relational Database Service](https://aws.amazon.com/rds/) (Amazon RDS) | Clusters Cluster parameter groups Cluster roles DB instances DB parameter groups DB security groups DB snapshots per user Event subscriptions Max auths per security group Option groups Read replicas per master Reserved Instances Storage quota (GiB) Subnet groups Subnets per subnet group |
| Amazon Route 53 (Route 53) – No | Hosted zones per account Max health checks per account Reusable delegation sets per account Traffic policies per account Traffic policy instances per account |
| Amazon Simple Email Service (Amazon SES) – No | Daily sending quota |
| Amazon Virtual Private Cloud (Amazon VPC) – No | Elastic IP addresses (EIPs) Internet gateways VPCs |
| Auto Scaling – No | Auto Scaling groups Launch configurations |
| AWS CloudFormation – No | Stacks |
| Elastic Load Balancing (ELB) – No | Application Load Balancer Network Load Balancer Classic Load Balancer |
| Identity and Access Management (IAM) – No | Groups Instance profiles Policies Roles Server certificates Users |

**Write a 150-word summary to explain your understandings and findings from this lab assignment.**

Cloud Audit is a specification for the presentation of information about how a cloud computing service provider addresses control frameworks. The goal of Cloud Audit is to provide cloud service providers with a way to make their performance and security data readily available for potential customers. AWS Audit Manager helps continuously audit AWS usage to simplify how assess risk and compliance with regulations and industry standards. With Audit Manager, it is easy to assess if your policies, procedures, and activities – also known as controls – are operating effectively.

* Be thorough. Look at all aspects of your security configuration, including those you might not use regularly.
* Don't assume. If you are unfamiliar with some aspect of your security configuration (for example, the reasoning behind a particular policy or the existence of a role), investigate the business need until you are satisfied.
* Keep things simple. To make auditing (and management) easier, use IAM groups, consistent naming schemes, and straightforward policies.