AWS Solution Architect Associate Certification Training – Module 25

25. Trusted advisor

AWS Trusted Advisor acts like your customized cloud expert, and it helps you provision your resources by following best practices. Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps. Since 2013, customers have viewed over 2.6 million best-practice recommendations and realized over $350 million in estimated cost reductions.

Features and Benefits

AWS Trusted Advisor provides best practices in four categories: cost optimization, security, fault tolerance, and performance improvement. You can use Trusted Advisor checks to monitor and improve the deployment of Amazon EC2, Elastic Load Balancing, Amazon EBS, Amazon S3, Auto Scaling, AWS Identity and Access Management, and other services. You can view the overall status of your AWS resources and savings estimations on the Trusted Advisor dashboard.

Four Best practices at no charge

Service Limit Check - This check inspects your position with regard to the most important service limits for each AWS product. It alerts you when you are using more than 80% of your allocation resources such as EC2 instances and EBS volumes.

Security Groups – Specific Ports Unrestricted Check – This check will look for and notify you of overly permissive access to your EC2 instances and help you to avoid malicious activities such as hacking, denial-of-service attacks, and loss of data.

IAM Use Check – This check alerts you if you are using account-level credentials to control access to your AWS resources instead of following security best practices by creating users, groups, and roles to control access to the resources.

MFA on Root Account Check – This check recommends the use of multi-factor authentication (MFA), to improve security by requiring additional authentication data from a secondary device.

Cost Optimization example

Checks the Amazon EC2 instances that were running at any time during the last 14 days and alerts you If the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Security Example

- Checks the root account and warns if MFA (multi-factor authentication) is not enabled.

- Recommends not to use root credentials
- Checks the permission settings for your Amazon Elastic Block Store (Amazon EBS) volume snapshots and alerts you if any snapshots are marked as public.

Fault tolerance example

- Checks the availability of resources associated with launch configurations and your auto-scaling groups
- Checks for S3 buckets that do not have versioning enabled or have versioning suspended
- Checks the automated backups of Amazon RDS DB instances