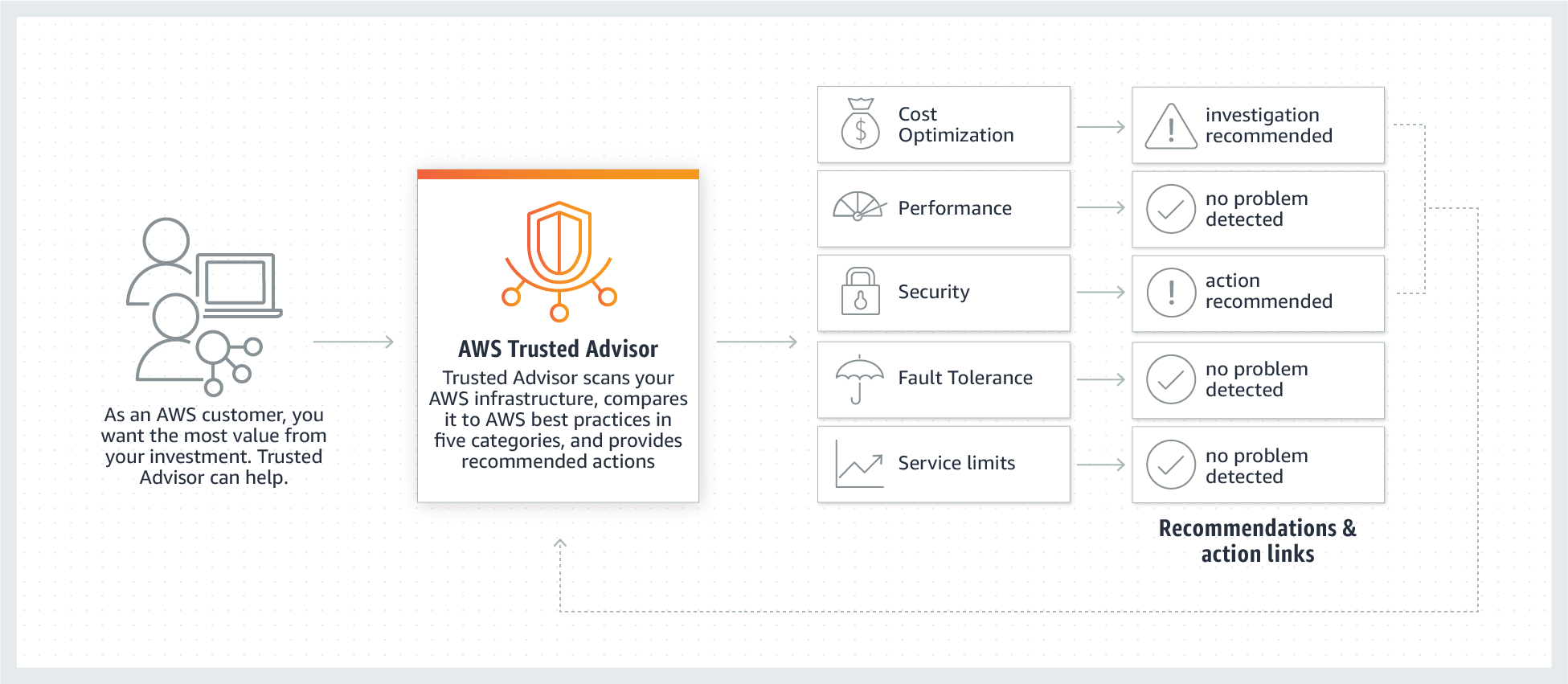
**AWS Trusted Advisor**

## **What is AWS Trusted Advisor**

AWS Trusted Advisor is an AWS tool that provides you **with real-time assistance to help** you provision your resources following AWS best practices. It checks to help optimize your AWS infrastructure, provide better security and performance, reduce your overall costs, and also monitor service limits. Whether you want to develop applications, or as part of ongoing improvement, Always take advantage of the recommendations provided by Trusted Advisor it helps keep your

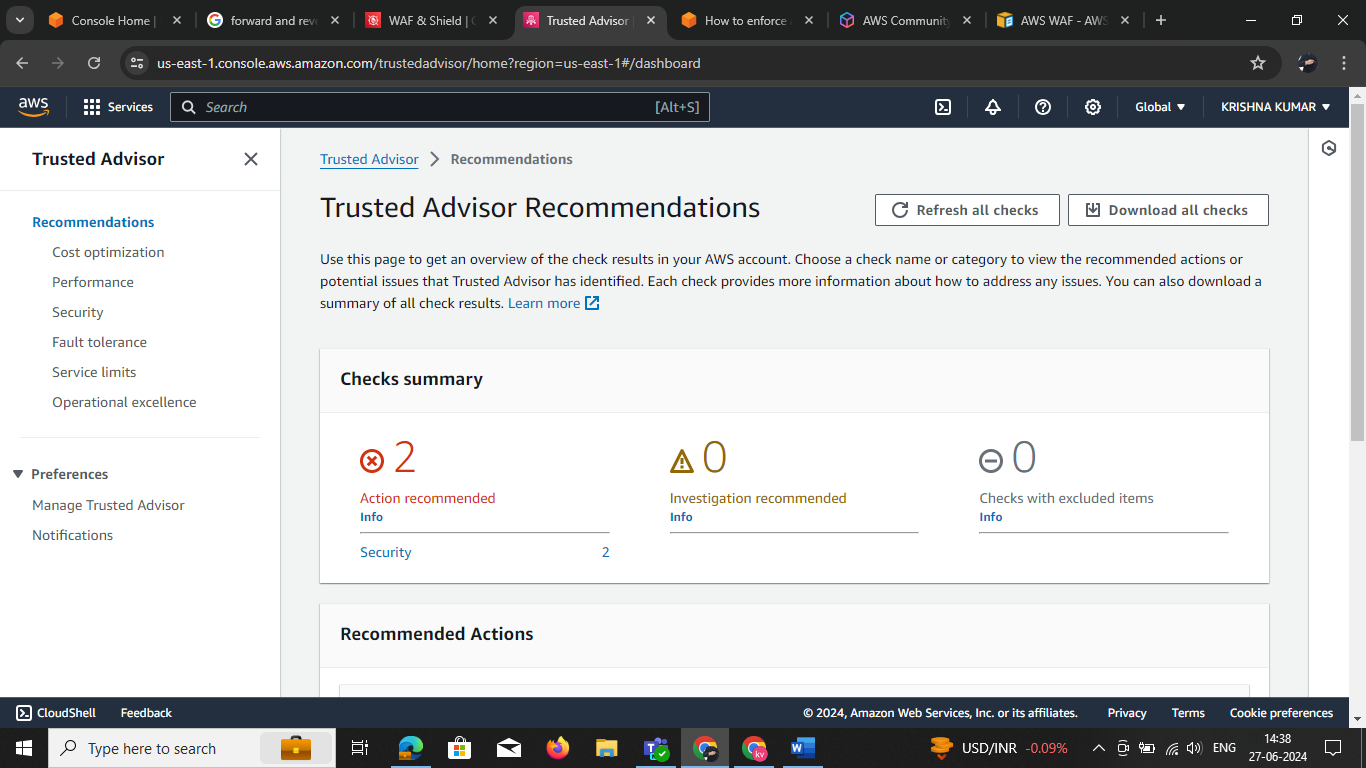
**AWS Trusted Advisor Check a**large section of services which can be grouped into four categories:

1. **Cost Optimization**—recommendations provided by Trusted Advisor can reduce expenses by highlighting idle resources or by committing reserved resources.
2. **Security**—With the help of AWS Trusted Advisor users can harden their AWS services against intruders by enabling various security features.
3. **Fault Tolerance**—suggestions that enhance the resilience of your applications by highlighting health issues, missing backups, and redundancy shortfalls.
4. **Performance**—recommendations that can increase the overall performance of your applications and cloud infrastructure by checking your service limits and monitoring instances.

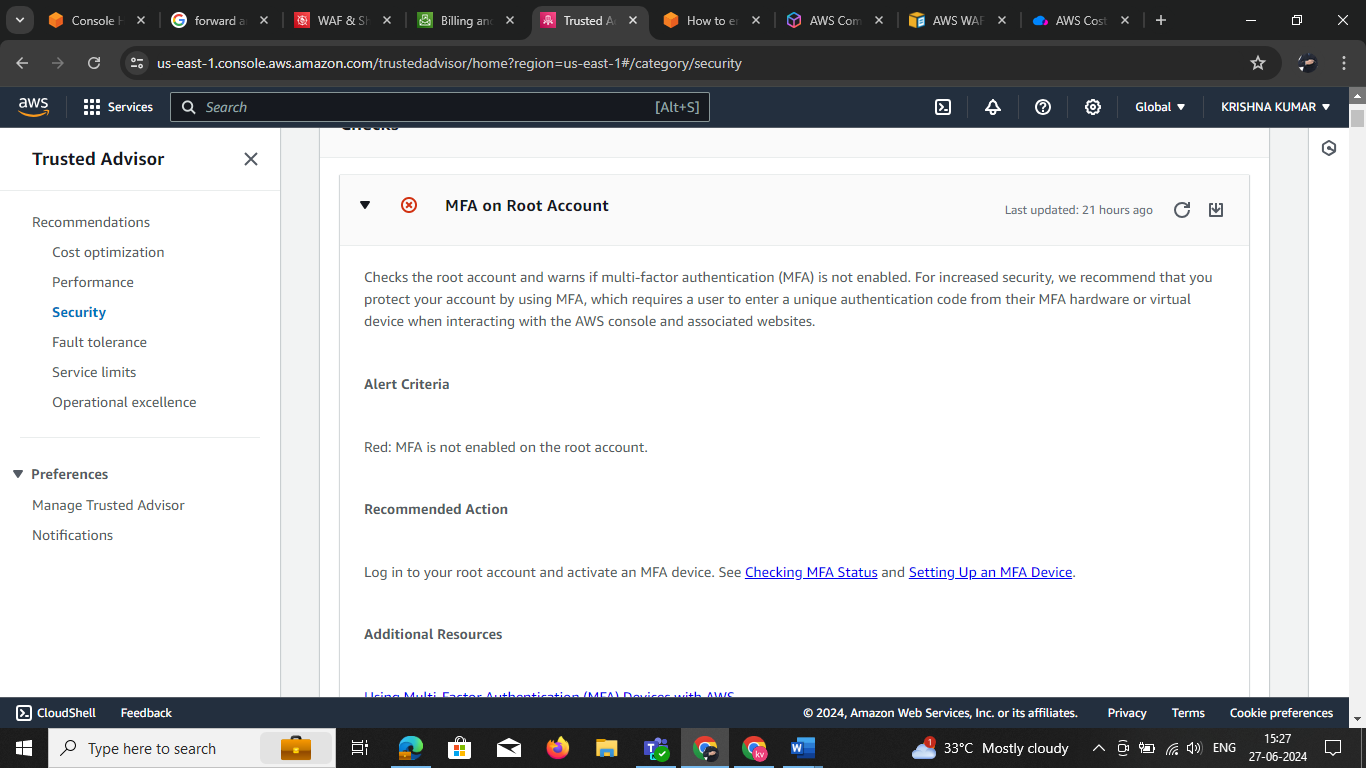
**  
Best Practices Of AWS Trusted Advisor At No Charge**

The following Trusted Advisor checks are now available to all AWS users:

* **Service Limits Check** – This check inspects your usage 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

**Step 1:** Go to 🡪Trusted Advisor 🡪 Recommendations

**step2:** Hear in above see check sum Go🡪 security check the it and recommendation



**Step:3**  it can shows the recommendation

