AWS Trust Advisor (TA)

* AWS Support plan affect the quantity of available TA check.
* provides recommendations that help you follow AWS best practices
* identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and **monitor service quota.**
* Basic support only can check for service quota
* [AWS Trusted Advisor Priority](https://aws.amazon.com/premiumsupport/technology/trusted-advisor-priority/) helps you focus on the most important recommendations to optimize your **cloud deployments, improve resilience, and address security gaps**. Available to [AWS Enterprise Support](https://aws.amazon.com/premiumsupport/plans/enterprise/) customers, Trusted Advisor Priority provides prioritized and context-driven recommendations that come from your AWS account team as well as machine-generated checks from AWS services.
* Check categories: Cost optimization, Performance, Security, Fault tolerance, Service limits

AWS RDS

* **Performance Insights** is an advanced performance monitoring feature that makes it easy to diagnose and solve performance problems on Amazon RDS. It displays the database load in an interactive graph, allowing you to analyze and troubleshoot the database workload. The load is categorized by SQL, waits, hosts, users, and other dimensions, providing detailed information about the sources of the load.

AWS Aurora

* Restoring a DB cluster to a point in time launches a new DB cluster and restores it from backup data or a DB cluster snapshot, which can take hours. **Backtracking** a DB cluster doesn't require a new DB cluster and rewinds the DB cluster in minutes.
* Backtracking is only available for DB clusters that were created with the Backtrack feature enabled. You can enable the Backtrack feature when you create a new DB cluster or restore a snapshot of a DB cluster. For DB clusters that were created with the Backtrack feature enabled, you can create a clone DB cluster with the Backtrack feature enabled. Currently, you can't perform backtracking on DB clusters that were created with the Backtrack feature disabled.
* The limit for a backtrack window is 72 hours.
* https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Backtrack.html

AWS CloudFormation

* OUTDATED = The CloudFormation template is trying to create a global resource that is not unique.
* InsufficientInstanceCapacity = AWS does not currently have enough available On-Demand capacity to fulfill your request. **Solution:** Modify the AWS CloudFormation template to not specify an Availability Zone for the EC2 instance $$ Modify the AWS CloudFormation template to use a different EC2 instance type.
* Private/Public IP/DNS name and AZ is Output for EC2:Instance

AWS NAT Gateway

* NAT gateway does not support IPv6

AWS Cloud Trail

* Save in S3 bucket.
* AWS CloudTrail Processing Library helps developers to read, process, and analyze AWS CloudTrail data
* Use AWS CLI to validate the integrity of CloudTrail log files.

AWS S3

* S3 buckets with S3 Object Lock can't be used as destination buckets for server access logs.
* Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects.
* s3 cp auto do multipart upload for big file (1TB?)

AWS Service Catalog

* When you share a portfolio using account-to-account sharing or AWS Organizations, you allow an AWS Service Catalog administrator of another AWS account to import your portfolio into his or her account and distribute the products to end users in that account.
* Import the shared portfolio to a local portfolio.

AWS Route53

* **Q: A company hosts a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses Amazon Route 53 to route traffic.  
  The company also has a static website that is configured in an Amazon S3 bucket.  
  A SysOps administrator must use the static website as a backup to the web application. The failover to the static website must be fully automated.  
  Which combination of actions will meet these requirements? (choose 2)**
* Create a primary failover routing policy record. Configure the value to be the ALB. Associate the record with a Route 53 health check.
* Create a secondary failover routing policy record. Configure the value to be the static website.
* **Reason: Secondary failover no need health check**
* Deploy a copy of the stack in the us-west-2 Region. Create an additional A record in Route 53 that includes the ELB in us-west-2 as an alias target. Configure the A records with a failover routing policy and health checks. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
* Application hosted in other ISP, and change from abc.com to edf.com, choose CNAME
* If route 53 to ALB, within AWS network. Use Alias.

AWS CloudWatch

* When you enable **anomaly detection** for a metric, CloudWatch applies statistical and machine learning algorithms. These algorithms continuously analyze metrics of systems and applications, determine normal baselines, and surface anomalies with minimal user intervention.

AWS Macie.

AWS EFS

* Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. You can enable encryption of data at rest when creating an Amazon EFS file system. You can enable encryption of data in transit when you mount the file system.

AWS ELB

* Create a public certificate in AWS Certificate Manager (ACM) and Attach Certificate to the ALB to secure traffic to the website over HTTPS connection.

AWS KMS

* To create new cryptographic material for your customer managed keys, you can create new KMS keys, and then change your applications or aliases to use the new KMS keys.

If you choose to import keys to AWS KMS or asymmetric keys or use a custom key store, you can manually rotate them by creating a new KMS key and **mapping an existing key alias** from the old KMS key to the new KMS key.

AWS EC2

* system status check = stop and restart
* instance status check = reboot
* InstanceLimitExceeded = use service quota to increase quota limit
* Standard Reserved Instances - Enables you to modify Availability Zone, scope, networking type, and instance size (within the same instance type) of your Reserved Instance.
* Convertible Reserved Instances - Enables you to exchange one or more Convertible Reserved Instances for another Convertible Reserved Instance with a different configuration, including instance family, operating system, and tenancy.

AWS VPC

* You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC.

AWS Config

* Detect security group with 0.0.0.0/0 and auto remediate noncompliant SG by restricting access to a specific CIDR block.

AWS Auto Scaling

* When a scale-in event occurs, a lifecycle hook pauses the instance before it is terminated and sends you a notification using Amazon EventBridge. While the instance is in the wait state, you can invoke an AWS Lambda function or connect to the instance to download logs or other data before the instance is fully terminated.

AWS CloudFront

* Already update file in S3 but the content is CloudFront still same. **Solution:** 1)Create a CloudFront invalidation and add the path of the updated files. 2)Update files by using the same name 3) Update by using a version identifier in the file name
* **Geoproximity** based on location of resources. **Geolocation** is used for based on location of users.