**WhizCards - AWS SysOps Administrator Associate**

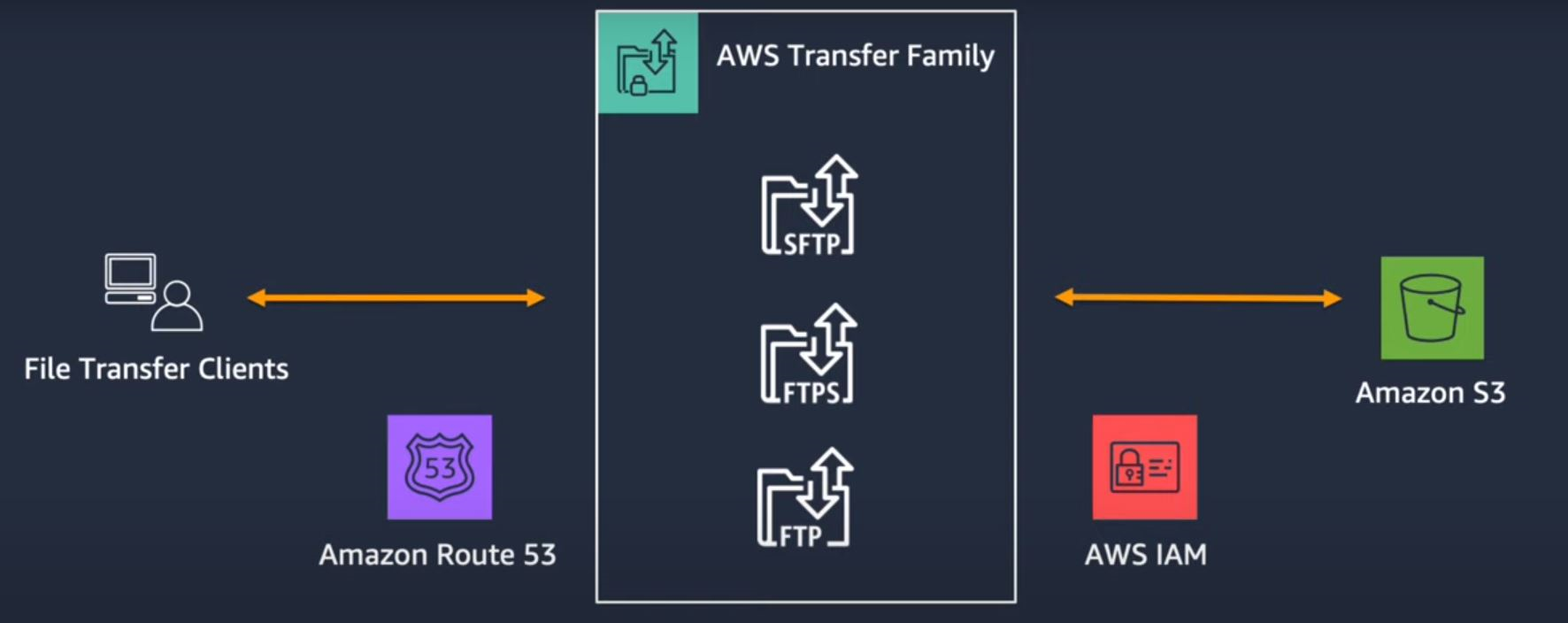
**AWS Transfer Family**

**What is AWS Transfer Family**?

* AWS Transfer Family is a fully managed & secure service that enables transfer of files using SFTP, FTPS & FTP.
* The destination storage services to which files are transferred are S3, EFS.
* It helps you to seamlessly migrate File Transfer workloads to AWS without having any impact on existing application integrations or configurations.

**Features:**

* AWS Transfer Family provides a fully managed endpoint for transferring files into and out of S3, EFS.
* The Secure File Transport Protocol (SFTP) is a file transfer provided over SSH.
* File Transfer Protocol over SSL (FTPS is a FTP over a TLS-encrypted channel.
* Plain File Transfer Protocol (FTP) that does not require a secure channel for transferring files.
* AWS Transfer Family exhibits Highly Availability across the globe.
* AWS Transfer Family provides compliance to regulations within your Region.
* Using a pay-as-you use model, the AWS Transfer Family service becomes cost effective and is simple to use.
* AWS Transfer Family has the ability to use custom Identity Providers using AWS API Gateway & Lambda

 *AWS Documentation*

**Best Practices:**

For improving Security posture while using AWS Transfer Family, the following best practices need to be adhered to.

* Use of a strong encryption mechanism for data in Transit - AWS Transfer Family provides a strong set of available ciphers for achieving this.
* Duplicate server’s Host Key - This will ensure that an imposter will not impersonate your AWS Transfer Family server.
* Provide additional security on your AWS Transfer Family server to increase security posture - Use of both a password & a Key will help protect your clients if any of them are compromised.
* While using custom Identity Providers with AWS Transfer Family, set the *authorizationType* property of your API Gateway method to AWS\_IAM - This will require the user to supply user credentials to be authenticated by the IdP.

**Use cases:**

* Use standard protocols (FTP) to get data into your application workflows like Data Lakes(S3) without having to rewrite applications using S3 API.
* Alleviate challenges of a traditional MFT for managing, securing, monitoring the MFT using AWS Transfer Family servers.
* MFT is found across industries
  + Regulated industries like Financial Services, Health Care where they use secure document exchanges(e.g. Financial claim) where data needs to be governed.
  + Supply chain where there is a trading partner relationship in its transactional data (eg purchase Orders).
  + Content distribution - Softwares, audio, video

A managed service like AWS File Transfer will be extremely useful in these scenarios.

**Exam Tip:**

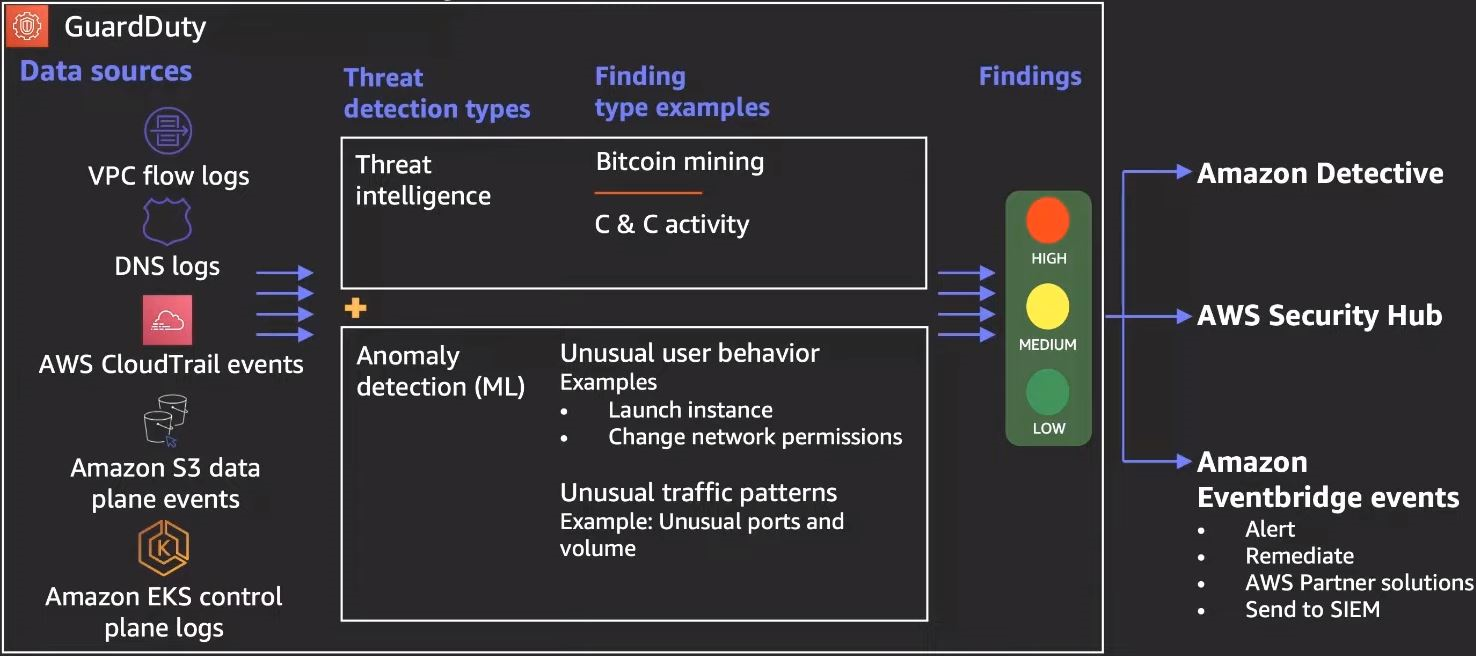
* IAM Roles are used to grant access to S3 buckets for file transfer clients in a secure way.
* Users can use Route 53 to migrate an existing File Transfer host name for use in AWS.
* SFTP & FTPS protocols can be set up to be accessible from the public internet while FTP is limited for access from inside a VPC using VPC endpoints.

**Amazon GuardDuty**

**What is Amazon GuardDuty**?

* Amazon GuardDuty is a threat detection service which uses Machine Learning, Anomaly detection, threat intelligence for identifying & prioritizing potential threats within your AWS Accounts & resources.
* It does it by monitoring different log sources like VPC flow logs, DNS logs, CloudTrail events, S3 data plane events, EKS control plane logs and analyzing them.

**Features:**

* Amazon GuardDuty performs threat detection in the following ways
  + Using a Threat Intelligence component by accessing a database of commonly known threats that is maintained by AWS.
  + Anomaly detection using ML for the unknown threats (eg Unusual behavior of a role trying to launch EC2 instances)
* Findings once detected by GuardDuty are assigned a severity of Low, Medium or High depending on the level of activity that is happening.
* GuardDuty findings are displayed in the GuardDuty console. They can also be sent to the following services for further analysis
  + AWS Detective.
  + AWS Security Hub.
  + As Amazon EventBridge events for exporting GuardDuty findings to applications like Splunk, Sumo Logic or sending event notifications(SNS).
* Multiple Accounts can be managed using GuardDuty through AWS Organizations integration.
* The threat detection activity performed by GuardDuty is scalable. Detection capacity is added only when required and reduces utilization when capacity is no longer required.
* GuardDuty provides comprehensive threat protection for containerized workloads. It helps detect malicious & suspicious activity for containerized workloads running on ECS with Fargate, provides container-level context with runtime monitoring, and identifies security coverage gaps in container workloads.
* Activating GuardDuty is simple with a one-step deployment through AWS Console or API call without the need for any additional software or infrastructure to deploy or manage.

*AWS Documentation*

**Best Practices:**

* Ensure that GuardDuty has complete visibility over Logs for complete Detection Coverage - Eg consider enabling VPC Flow logs for all Regions and required network interfaces that are being planned to monitor for threat detection.
* Ensure that CloudTrail S3 data events are enabled for monitoring by GuardDuty - Enable S3 protection in Amazon GuardDuty to enable it to start monitoring S3 data events.
* GuardDuty is Region specific and it is recommended to enable GuardDuty for all Regions for complete threat visibility.
* It is recommended to analyze GuardDuty monitoring activities with CloudTrail to ensure that users are not tampering with GuardDuty itself.
* It is recommended to integrate GuardDuty with EventBridge & Lambda for automating risk mitigation.

**Use cases:**

* Improve visibility of Security of your AWS environment operationally - Gain insights into compromised credentials, unusual data access of S3 storage, API calls from known malicious IP addresses using GuardDuty.
* Security analysts can be assisted to carry out investigations using the Security event findings from GuardDuty. It provides Context, Metadata, impacted resource details using which the root cause can be detected using GuardDuty console integration with Amazon Detective.
* GuardDuty can be used to identify files containing malware - EBS can be scanned for files containing malware that creates suspicious behavior on instance, container workloads running on EC2.

**Exam Tip:**

* When GuardDuty is enabled, the associated log sources that it accesses (VPC Flow logs, DNS Logs) need not be enabled separately. They are all enabled by default by GuardDuty and are provided access to GuardDuty.
* Amazon GuardDuty uses the following naming convention for listing threats that are detected.

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

* + ThreatPurpose - Primary purpose of the threat (eg CryptoCurrency mining).
  + ResourceTypeAffected - The AWS resource that is the target.
  + ThreatFamilyName - Description of the potential malicious activity (eg NetworkPortUnusual)
  + DetectionMechanism - Method that GuardDuty used for detecting the finding (TCP, UDP)
  + Artifact - Describes a resource that has been used in the malicious activity (eg DNS)

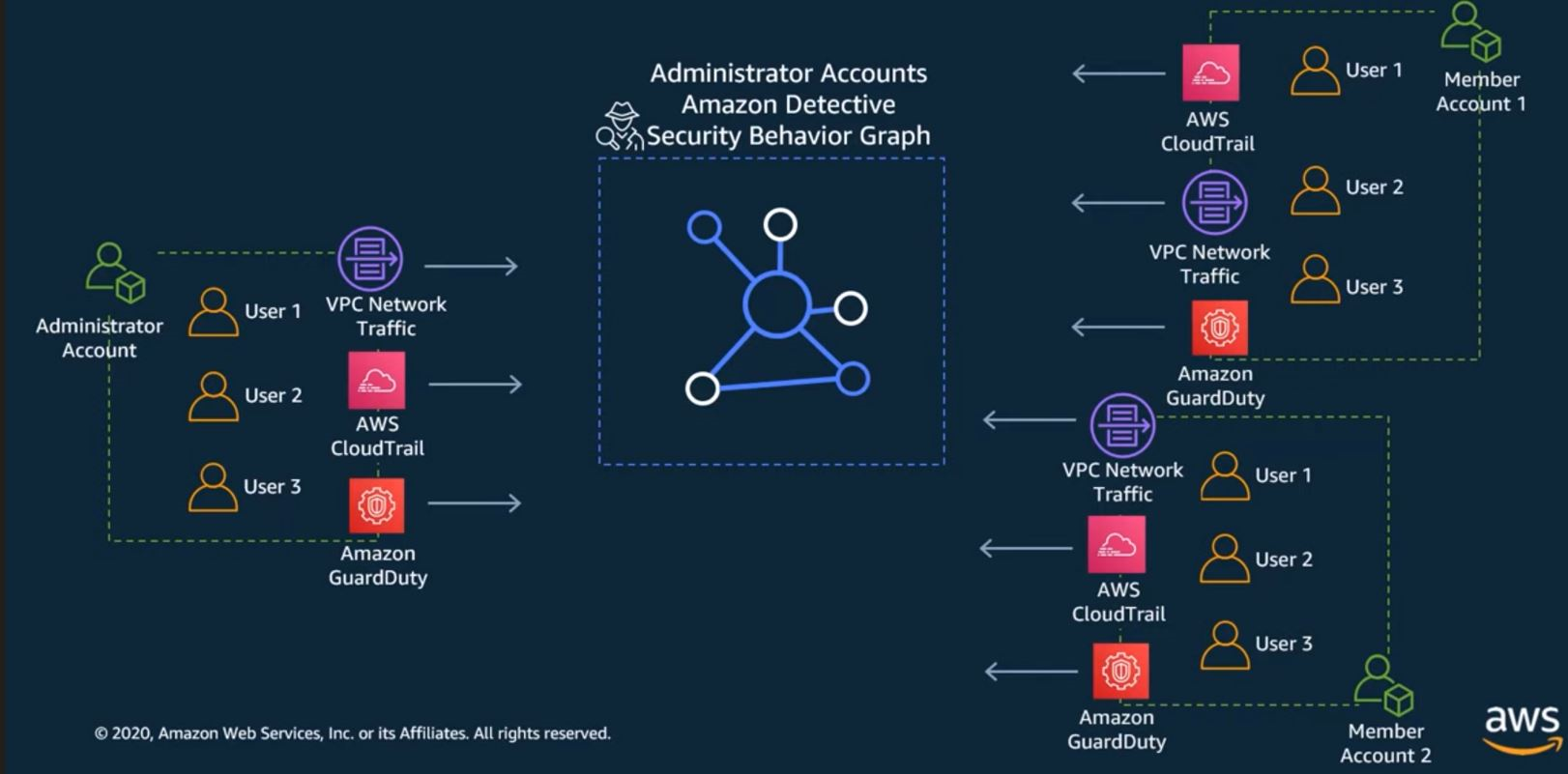
**Amazon Detective**

**What is Amazon Detective**?

* Amazon Detective is a service that makes it easy to analyze, investigate & quickly find out the root cause of security findings or suspicious activities within your AWS environment using ML, Statistical analysis, Graph theory.
* It does it by automatically collecting and processing events from VPC Flow logs, CloudTrail, Amazon GuardDuty to create an unified view.

**Features:**

* Amazon Detective is a multi-account service. Detective can be enabled in an AWS Organizations Management account.
* Amazon Detective creates a Security Behavior Graph for holding the log summaries & analytics of all member accounts in the Management account.
* The Management account invites member accounts. On accepting the invitations, CloudTrail management events, VPC network traffic, GuardDuty findings for all accounts flow into the Security Behaviour Graph in the Management account. The management account can then interact with the Security Behaviour Graph in the Detective console.
* The Security Behavioural Graph created by Detective consists of security-related relationships offering contextual & behavioral insights for quickly validating, comparing & correlating data for reaching conclusions.
* Amazon Detective provides interactive visualizations leading to effective investigations using Generative AI. This makes it easy to investigate issues faster with less effort.
* Amazon Detective integrates seamlessly with AWS Security services like Amazon GuardDuty, AWS Security Hub, Amazon Inspector. Aggregated findings from all these services help quickly investigate security issues identified in these services.
* Amazon Detective is simple to deploy by performing a few steps in the AWS Management Console.
* Amazon Detective is cost effective since there are no data sources that need to be enabled or configured for using Detective.



*AWS Documentation*

**Best Practices:**

* Prior to enabling Amazon Detective, ensure that Amazon GuardDuty is enabled for your Account.
* It is recommended to use an Administrator Account for Amazon Detective, GuardDuty & Security Hub for the following integration points to work seamlessly
  + Details of GuardDuty findings can be pivoted from the finding details to Amazon Detective’s finding profile.
  + While investigating a GuardDuty finding in Amazon Detective, an option to archive the finding can be chosen.
* In order to reduce the amount of time it takes for Detective to receive updates of GuardDuty findings, it is recommended to update the Amazon CloudWatch notification frequency to 15 minutes in GuardDuty rather than its default frequency of 6 hours.
* Best practices for Management account
  + When inviting member accounts for flowing findings data into Detective’s Security Behaviour Graph in the Management Account, only invite legitimate accounts.
  + Provide limited access to users for viewing the Security Behaviour Graph created by Detective.
* Best practices for Member accounts
  + Validate source of invitation by the Management account to a Security Behaviour Graph.
  + Verify that there is a legitimate reason for the inviting account for monitoring security data of the member account.

**Use cases:**

* Triage Security findings / alerts - Explore whether GaurdDuty findings need to be examined further. Amazon Detective helps users to see whether a finding is a concern.
* Incident investigation - Since Amazon Detective allows for viewing analysis & summaries going back upto an year, it can help answer questions like how long has the security issue been there, the resources affected because of that.
* Threat Hunting - Access indicators like IP addresses, user to see what interactions they would have had with the environment. Detective’s Security Behaviour Graph will help here.

**Exam Tip:**

* For Amazon Detective to be enabled, GuardDuty should be enabled for your Account for at least 48 hours.
* For Amazon Detective to be enabled, Volume of data flowing into Amazon Detective’s Security Behavior Graph for your account should be less than the maximum allowed by Detective.
* Amazon Detective is a Regional service and needs to be enabled for each Region.

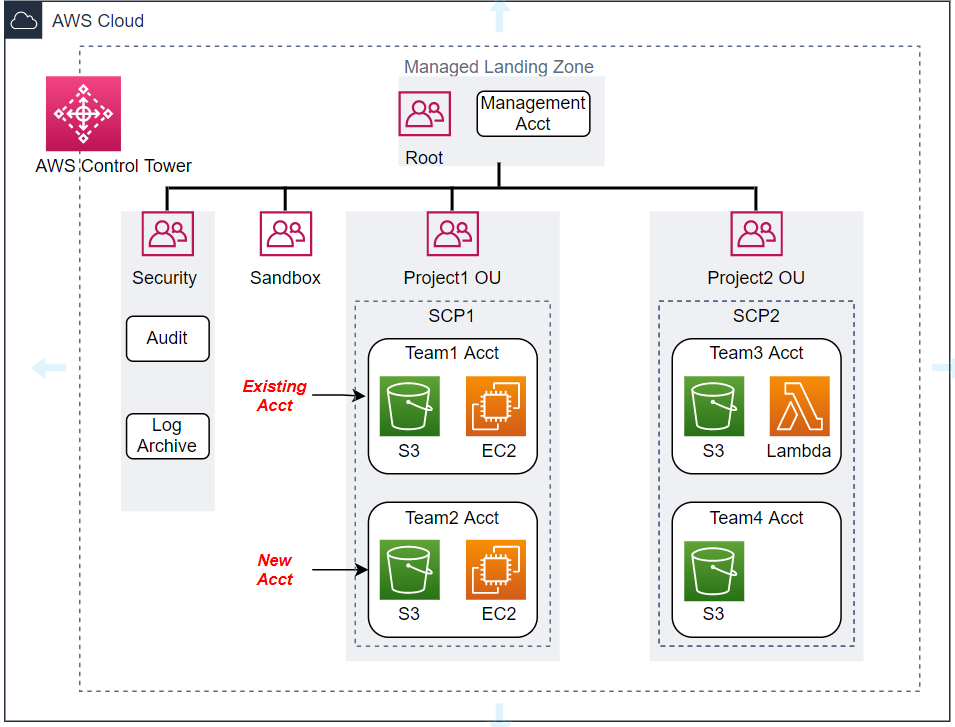
**Amazon Inspector**

**What is AWS Control Tower**?

* AWS Control Tower is an extension to AWS Organizations providing additional controls.
* AWS Control Tower helps create a *Landing Zone* which is a well architected Multi-Account baseline based on AWS best practices.
* An AWS Organization will be created if it does not already exist.

**Features:**

* As a part of the Landing Zone, Control Tower sets up a series of OU’s - Security OU, Sandbox OU, Production OU.
* Within the Security OU, Control Tower creates the Audit & Log Archive accounts.
* The Sandbox & Production OU’s does not contain any default accounts. Accounts related to Development & Production environments can be added in these OU’s.
* Control Tower integrates with AWS Identity Center. The directory sources for SSO can be AWS Identity Center directories(default), SAML IdPs, Microsoft AD.
* Control Tower creates a series of Guardrails that are used for Governance & Compliance.
* The Root user in the Management Account can perform actions that are disallowed by Guardrails similar to AWS Organizations where SCP’s cannot affect the Root user in the Management Account.
* Control Tower comes with a Dashboard providing oversights into the Landing Zone and central administrative views across all Accounts, OU’s, Guardrails & policies.
* Control Tower offers *Account Factory* which is a configurable Account Template for standardizing provisioning of new Accounts with Pre-approved Account configurations.



*AWS Documentation*

**Best Practices:**

* Since Control Tower provides high levels of customizations for creating a Multi-Account environment, it is important to understand and access your Organization's OU’s & workloads for correctly scoping & applying the right controls.
* AWS Control Tower uses compliance frameworks like PCI-DSS, CIS AWS Benchmark thus enabling controls for achieving specific compliance objectives for various Organizations. It's best for Organizations to align to these IT compliance frameworks which will offer a consistent & repeatable foundation for risk management and security configuration best practices in their AWS environment.
* It is advisable to test all Control Tower controls in non production OU’s for identifying & mitigating potential risks of misconfigurations early prior to actual production deployments.
* Use automation for detection & remediation of non-compliant controls by leveraging the synergy between AWS Control Tower controls and AWS Systems Manager.

**Use cases:**

* Management of multiple accounts for Private Sector Organizations having many teams or regional offices across the Globe - AWS Control Tower can enable managing multiple accounts easily on a single dashboard, enable Accounts & AWS Services to function as a single Entity by integrating them.
* Public Sector Organizations that are concerned with Governance, Security & Regulatory compliance will benefit from AWS Control Tower’s built-in Governance & best practices that provides visibility into compliance status quickly.
* Increased Agility for Governance - Both New & Existing Account configurations created by AWS Organizations can be Governed easily using AWS Control Tower which helps gain visibility into compliance status and enforce controls at scale.

**Exam Tip:**

* AWS Control Tower provides two configuration options
  + Launch AWS Control Tower in a new AWS Organization.
  + Launch AWS Control Tower in an existing AWS Organization.
* Guardrails created by AWS Control Tower for governance & compliance fall under the following categories
  + Preventive Guardrails - Are based on SCP’s that disallow certain API actions.
  + Detective Guardrails - Implemented using AWS Config & Lambda functions that monitor & govern compliance.

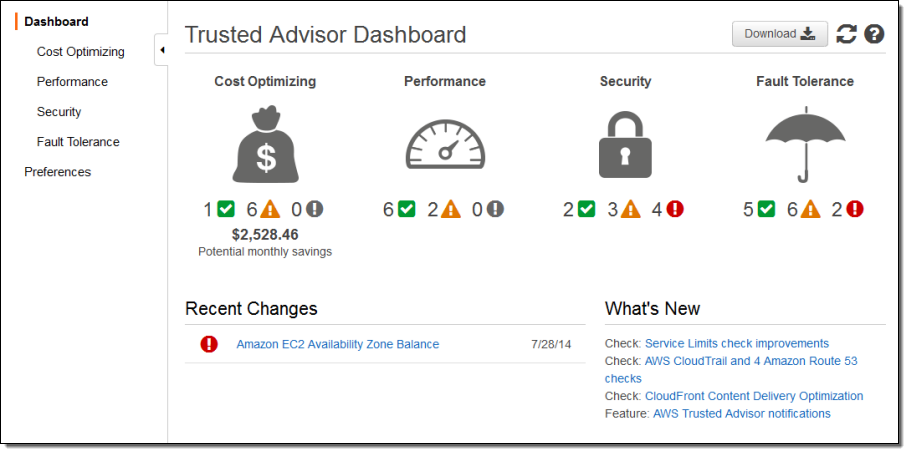
**AWS Trusted Advisor**

**What is AWS Trusted Advisor**?

* AWS Trusted Advisor is a service that provides real time guidance to Organizations using AWS Cloud to provision resources that follows AWS best practices.
* As a Global service, Trusted Advisor inspects your AWS infrastructure comparing it with AWS best practices and provides recommended actions for optimizing your infrastructure.

**Features:**

* Trusted Advisor inspects your AWS infrastructure in the following categories
  + Cost Optimization
  + Performance
  + Security
  + Fault Tolerance
  + Service Limits
* Trusted Advisor performs specific checks in each of the categories defined above. The checks are based on best practices identified by experts in each AWS service and learnings from serving customers.
* The Trusted Advisor Dashboard provides a category level summary of check results.
* For each category, the summary includes an aggregation of Check Status sorted by OK (Green), Warning (Yellow), Error (Red) across all Regions. Each category can be further drilled down or downloaded as an Excel sheet for viewing Alerts, recommended actions.
* Trusted Advisor adds new checks, new features, updates existing checks and expands to new Regions on an ongoing basis.
* Weekly email notifications can be set that will provide a summary of checks in each category, total monthly cost savings, and recent check status changes.
* Drill down results for specific resources, check statuses can be obtained by using a filter tag. Eg a specific Application, Business Unit.
* Trusted Advisor comes with the following types of plans
  + Basic & Developer plans.
  + Business & Enterprise support plans.



*AWS Documentation*

**Best Practices:**

Trusted Advisor itself provides checks based on Best Practices in the Cost Optimization, Security, Fault Tolerance, Performance improvement categories.

* Cost Optimization - Provides recommendations to Organizations for saving money on their AWS infrastructure by terminating unused & idle resources, using Reserved capacity for continuous usage.
* Security - Provides recommendations to Organizations for improving security of their applications by Restricting access using SG/ NACL, Checking permissions on S3 Buckets, enabling various security features.
* Fault Tolerance - increasing Availability, Redundancy of applications using Auto Scaling, Performing Health checks, configuring Multi-AZ environments, taking backups.
* Performance - Provides recommendations to Organizations for improving performance of applications by taking advantage of provisioned throughput, monitoring of over utilized instances
* Service Limits - Notifies Organizations when their resource usage is more than 80%.

**Use cases:**

* Optimization of cost & efficiency - Trusted Advisor helps identify resources that are not used to capacity or idle resources and provides recommendations to lower costs.
* Address Security Gaps - Trusted Advisor performs Security checks of your AWS environment based on security best practices. It flags off errors or warnings depending on the severity of the security threat e.g. Open SG/NACL ports for unrestricted external user’s access, open access permissions for S3 buckets in Accounts.
* Performance Improvement - Trusted Advisor checks for usage & configuration of your AWS resources and provides recommendations that can improve performance e.g. it can check for Provisioned IOPS EBS volumes on EC2 instances that are not EBS-optimized.

**Exam Tip:**

* The Basic & Developer support plans have Limited access to Trusted Advisor checks(7 checks) accessible through AWS Console only.
* The Business & Enterprise support plans have access to all Trusted Advisor checks through the console, access checks via API calls, setup of EventBridge to consume check results that can be sent as notifications to interested parties.