JON BONSO AND CARLO ACEBEDO

AWS CERTIFIED

SECURITY SPECIALTY EXAM

Tutorials Dojo Study Guide

TABLE OF CONTENTS

INTRODUCTION

In the fast-paced IT industry today, there will always be a growing demand for certified IT Professionals that can design highly secure AWS cloud architectures. Companies are spending millions of dollars to optimize the performance of their applications and scale their infrastructure globally to serve customers around the world. They need a reliable and skillful IT staff to build highly available, fault-tolerant, and secure applications that are safe from common web exploits or even large-scale distributed denial-of-service (DDoS) attacks. Most companies have a dedicated IT Security team to improve the infrastructure security of their cloud environment, establish real-time security monitoring and encrypt their data both in transit and at rest.

This Study Guide and Cheat Sheets eBook for AWS Certified Security Specialty aims to equip you with the necessary knowledge and practical skill sets needed to pass the latest version of the AWS Certified Security Specialty exam. This eBook contains the essential concepts, exam domains, exam tips, sample questions, cheat sheets, and other relevant information about the AWS Certified Security Specialty exam. This study guide begins with the presentation of the exam structure, giving you an insight into the question types, exam domains, scoring scheme, and the list of benefits you'll receive once you pass the exam.

We used the official AWS exam guide to structure the contents of this guide, where each section discusses a particular exam domain. Various AWS concepts, related AWS services, and technical implementations are covered to give you an idea of what to expect on the actual exam.

Security Specialty Exam Notes:

Don't forget to read the boxed "**exam tips**" (like this one) scattered throughout the eBook, as these are the key concepts that you will likely encounter on your test. After covering the five domains, we have added a bonus section containing a curated list of AWS Cheat Sheets to fast-track your review. The last part of this guide includes a collection of articles that compares two or more similar AWS services to supplement your knowledge.

The AWS Certified Security Specialty certification exam is a difficult test to pass; therefore, anyone who wants to take it must allocate ample time for review. The exam registration cost is not cheap, which is why we spent considerable time and effort to ensure that this study guide provides you with the essential and relevant knowledge to increase your chances of passing the Security Specialty exam.

***Note: This eBook is meant to be just a supplementary resource when preparing for the exam. We highly recommend working on hands-on sessions and practice exams to further expand your knowledge and improve your test-taking skills.*

AWS CERTIFIED SECURITY SPECIALTY EXAM OVERVIEW

The AWS Certified Security Specialty exam is intended for IT Professionals who perform a security role in their respective organizations. This exam checks your ability to effectively demonstrate knowledge and your ability to secure your resources in AWS.

Exam Details

The AWS Certified Security Specialty certification is intended for individuals who perform a security role in their organization. This exam doesn't have any prerequisites, but it is recommended that you have at least two years of hands-on experience in implementing security controls to various AWS workloads. This validates your ability to demonstrate your understanding of specialized data classifications, data encryption methods, secure Internet protocols, security operations, and risk mitigation in AWS. It also checks your working knowledge of various AWS security services and features that you can use to implement a secure production environment.

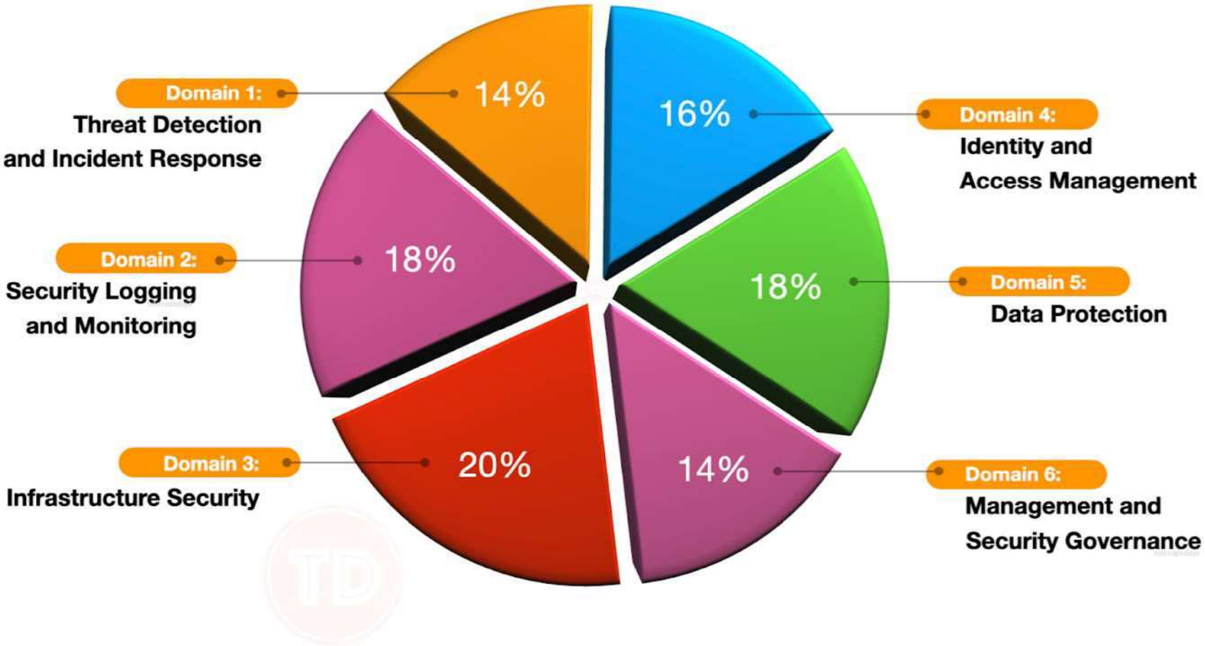
It is composed of scenario-based questions that can either be in multiple-choice or multiple-response formats. The first question type has one correct answer and three incorrect responses, while the latter has two or more correct responses out of five or more options. You can take the exam from a local testing center or online from the comfort of your home.

Exam Code:	SCS-C02
Release Date:	July 2023
Prerequisites:	None
No. of Questions:	65
Score Range:	100 - 1000
Cost:	300 USD
Passing Score:	750/1000
Time Limit:	3 hours (180 minutes)
Format:	Scenario-based. Multiple choice/multiple answers.
Delivery Method:	Testing center or online proctored exam.

Don't be confused if you see in your Pearson Vue booking that the duration is 190 minutes since they included an additional 10 minutes for reading the Non-Disclosure Agreement (NDA) at the start of the exam and the survey at the end of it.

Exam Domains

The AWS Certified Security Specialty (SCS-C02) exam has 6 different domains, each with corresponding weight and topic coverage. The exam domains are as follows: Threat Detection and Incident Response (14%), Security Logging and Monitoring (18%), Infrastructure Security (20%), Identity and Access Management (16%), Data Protection (18%) and Management and Security Governance (14%):



These are the six exam domains that you should prepare for if you are planning to take the AWS Certified Security Specialty (SCS-C02) test. The list of exam domains can be found in the official SCS-C02 Exam Guide.

Each exam domain has a corresponding weighting, so some sections can have more or fewer questions than others. One exam domain is comprised of several task statements. A task statement is a sub-category of the exam domain that contains the required cloud concepts, knowledge, and skills for you to accomplish a particular task or activity in AWS. Let's look at each of these domains one by one.

Domain 1: Threat Detection and Incident Response

1.1. Design and implement an incident response plan.
1.2. Detect security threats and anomalies by using AWS services.
1.3. Respond to compromised resources and workloads.

Domain 2: Security Logging and Monitoring

2.1. Design and implement monitoring and alerting to address security events.
2.2. Troubleshoot security monitoring and alerting.
2.3. Design and implement a logging solution.
2.4. Troubleshoot logging solutions.
2.5. Design a log analysis solution.

Domain 3: Infrastructure Security

3.1. Design and implement security controls for edge services.
3.2. Design and implement network security controls.
3.3. Design and implement security controls for compute workloads.
3.4. Troubleshoot network security.

Domain 4: Identity and Access Management

4.1. Design, implement, and troubleshoot authentication for AWS resources.
4.2. Design, implement, and troubleshoot authorization for AWS resources.

Domain 5: Data Protection

5.1. Design and implement controls that provide confidentiality and integrity for data in transit.
5.2. Design and implement controls that provide confidentiality and integrity for data at rest.
5.3. Design and implement controls to manage the lifecycle of data at rest.
5.4. Design and implement controls to protect credentials, secrets, and cryptographic key materials.

Domain 6: Management and Security Governance

6.1. Develop a strategy to centrally deploy and manage AWS accounts.
6.2. Implement a secure and consistent deployment strategy for cloud resources.
6.3. Evaluate the compliance of AWS resources.
6.4. Identify security gaps through architectural reviews and cost analysis.

Exam Scoring System

You can get a score from 100 to 1,000 with a minimum passing score of **750** when you take the Security Specialty exam. AWS uses a scaled scoring model to equate scores across multiple exam types that may have different difficulty levels. The complete score report will be sent to you by email after a few days.

Individuals who unfortunately do not pass the AWS exam must wait 14 days before they are allowed to retake the exam. Fortunately, there is no hard limit on exam attempts until you pass the exam. Take note that on each attempt, the full registration price of the AWS exam must be paid.

Within 5 business days of completing your exam, your AWS Certification Account will have a record of your complete exam results. The score report contains a table of your performance at each section/domain, which indicates whether you met the competency level required for these domains or not. AWS uses a compensatory scoring model, which means that you do not necessarily need to pass each and every individual section, only the overall examination. Each section has a specific score weighting that translates to the number of questions; hence, some sections have more questions than others. The Score Performance table highlights your strengths and weaknesses that you need to improve on.

Exam Benefits

If you successfully pass any AWS exam, you will be eligible for the following benefits:

- **Exam Discount -** You'll get a 50% discount voucher that you can apply for your recertification or any other exam you plan to pursue. To access your discount voucher code, go to the "Benefits" section of your AWS Certification Account, and apply the voucher when you register for your next exam.

- **AWS Certified Store -** All AWS-certified professionals would be given access to exclusive AWS Certified merchandise. You can get your store access from the "Benefits" section of your AWS Certification Account.

- **Certification Digital Badges** - You can showcase your achievements to your colleagues and employers with digital badges on your email signatures, Linkedin profile, or on your social media accounts. You can also show your Digital Badge to gain exclusive access to Certification Lounges at AWS re:Invent, regional Appreciation Receptions, and select AWS Summit events. To view your badges, simply go to the "Digital Badges" section of your AWS Certification Account.

- **Eligibility to join AWS IQ -** With the AWS IQ program, you can monetize your AWS skills online by providing hands-on assistance to customers around the globe. AWS IQ will help you stay sharp and well-versed in various AWS technologies. You can work in the comforts of your home and decide when or where you want to work.

You can visit the official AWS Certification FAQ page to view the frequently asked questions about getting AWS Certified and other information about the AWS Certification: https://aws.amazon.com/certification/faqs/**.**

AWS CERTIFIED SECURITY SPECIALTY EXAM - STUDY GUIDE AND TIPS

The AWS Specialty certification exams are intended for people who handle more specific responsibilities in AWS Cloud. Since these responsibilities demand a more advanced skill set with prior experience from a person, these AWS specialty exams are built so that they can reinforce and validate a person's eligibility for that role. There are no associate and professional levels in a specialty learning path, so the exams serve as the whole package already. And since they are made that way, expect no less from the specialty certification exams, as they will be as tough as the professional exams.

The name of the certificate immediately points out what to focus on — AWS Security. Although we mentioned earlier that specialty exams tackle more specific roles, security in AWS is quite broad and extensive. There are a lot of topics involved when we speak about AWS security, whether it be native AWS services or other third-party tools. If you need comprehensive review material for learning these topics, then this study guide is for you.

The AWS Certified Security – Specialty (SCS-C02) exam is meant for IT professionals who perform a security role such as, but not limited to, Security Engineers, DevSecOps, Solutions Architect and others. This Security-focused exam validates a person's ability to effectively demonstrate knowledge and skills about securing various types of AWS workloads.

The SCS-C02 exam also validates whether a candidate has the following:

- An understanding of specialized data classifications and AWS data protection mechanisms
- An understanding of data-encryption methods and AWS mechanisms to implement them
- An understanding of secure internet protocols and AWS mechanisms to implement them
- A working knowledge of AWS security services and features of services to provide a secure production environment
- Competency from 2 or more years of production deployment experience in using AWS security services and features
- The ability to make tradeoff decisions with regard to cost, security, and deployment complexity to meet a set of application requirements
- An understanding of security operations and risks.

Study Materials

Having prior knowledge and experience in handling (cloud) security will allow you to understand the concepts and strategies that appear in AWS reference materials. You will also find it easier to comprehend scenario-type questions in your exam. To know more about the AWS Security specialty exam, check out the official AWS Exam Blueprint here.

AWS documentation and whitepapers would be helpful for you to build your security knowledge in the AWS Cloud. Aside from our SCS-C02 AWS Certified Security Specialty Practice Exams, these literary pieces are your primary source of information. We recommend reading the following papers:

1. Introduction to AWS Security
2. AWS: Overview of Security Processes
3. AWS Well-Architected Framework
4. Security Pillar – AWS Well-Architected Framework
5. AWS Security Best Practices
6. AWS Key Management Service Best Practices
7. AWS Key Management Service Cryptographic Details
8. Encrypting File Data with Amazon Elastic File System
9. Secure Content Delivery with Amazon CloudFront
10. Use AWS WAF to Mitigate OWASP's Top 10 Web Application Vulnerabilities
11. Data Residency
12. AWS Best Practices for DDoS Resiliency
13. Application Logging in AWS
14. AWS Security Incident Response Guide
15. Best Practices for Security, Identity, & Compliance

Compliance whitepapers:

1. AWS Security by Design
2. AWS Risk & Compliance
3. Architecting for HIPAA Security and Compliance on AWS
4. Navigating GDPR Compliance on AWS
5. Architecting for PCI DSS Scoping and Segmentation on AWS
6. FedRAMP

AWS Services to Focus On

When we talk about security as a discipline, especially in the context of the cloud, we are tackling it as a combination of different domains. AWS enumerates its catalog of services and features under different domains based on their purposes. In this section, we will try to do the same and group AWS services according to their domains.

Identity and Access Control AWS IAM Identity Center

- AWS Identity and Access Management - You must learn every detail of AWS IAM since this is AWS' primary user management and access control service. Practice writing your own IAM policies.
- Resource-Based Policies - Although resource-based policies fall under AWS IAM, they tend to be ignored compared to user-based policies. Take note of which services support this type of policy and how they are different from user-based policies.
- S3 Presigned URLs - Know what is the purpose of S3 presigned URLs and how they differ from CloudFront signed URLs.
- CloudFront Signed URLs - Know what is the purpose of CloudFront signed URLs and how they differ from S3 presigned URLs or CloudFront signed cookies.
- Amazon Cognito - Read through the benefits of AWS Cognito and how to integrate it with web and mobile applications. Differentiate user pools from identity pools.
- AWS IAM Identity Center - Learn how you can use AWS IAM Identity Center together with other authentication protocols to securely authenticate users in your environment. AWS IAM Identity Center is commonly integrated with LDAP.
- AWS Security Token Service - Know the purpose and use cases of Amazon STS. Try building a program that utilizes temporary tokens as credentials.
- AWS Directory Service - Know the different options you have for AWS Directory Service. Each option solves a different requirement, and it is up to you to figure out how you can get your directory to gain access to your users and other information.
- AWS Organizations - AWS Organizations is a very helpful service when dealing with large-scale enterprises with multiple AWS accounts. Know the benefits of using this service (like consolidated billing feature) and how to build an organization hierarchy with Organization Units and Service Control Policies.
- AWS Resource Access Manager - AWS RAM allows you to securely share resources with other AWS accounts. Experiment with this service to know how to share your resources and what restrictions are involved.

Application and Infrastructure Security

- EC2 key pairs - This goes without saying, but EC2 key pairs play a very important role in protecting your EC2 instances.
- AWS Systems Manager - AWS SSM secures your applications through services like Patch Baselines, Run Command, Session Manager, and more. By utilizing automation and code, you run less risk in human error and unwanted/untracked changes to your application.
- AWS WAF - AWS WAF is essential in protecting your applications from common exploits like SQL injection or XSS attacks. Differentiate WAF from Shield and Firewall Manager.
- AWS Shield - AWS Shield complements AWS WAF since this service offers DDoS protection. Read what features are different between Shield Basic and Shield Advanced.
- AWS Firewall Manager - This service simplifies administration overhead when setting up AWS WAF, AWS Shield, and VPC security groups. Best to do hands-on service.

Data Security

- AWS KMS - Study the different types of KMS keys available and how you should manage them. Determine which AWS services support using AWS KMS for encryption.
- Amazon CloudHSM - Know when to use AWS KMS vs CloudHSM for your encryption needs.
- AWS SSM Parameter Store - It is important to know how AWS SSM Parameter Store can protect your referenceable information through *SecureString*.
- Amazon Secrets Manager - Secrets Manager is similar to Parameter Store, wherein you can store and retrieve sensitive strings in AWS securely.
- SSE-S3 Encryption - Read when it is better to use SSE-S3 keys or KMS keys for server-side encryption. Also, read how your encrypted buckets and objects are handled during operations such as replication, deletion, etc.
- S3 Glacier Vault Lock - Know the purpose of a Glacier Vault Lock and try implementing a policy yourself.
- Amazon Macie - Read how Macie automatically classifies and protects your data. This is one of those services that you will just understand better if you try it out.
- AWS Certificate Manager - Know which services integrate with your certificates stored in Certificate Manager. Try creating your own private CA and issue some custom certificates.

Network Security

- Amazon VPC - Know everything on VPCs since they are basic building blocks for a protected AWS environment. Differentiate security groups vs network ACLs. Study VPC endpoints, too.
- Amazon CloudFront - Study how CloudFront protects your endpoints from being publicly accessible. Read on setting up Origin Access Identity with S3 buckets. Know which services integrate with CloudFront, such as API Gateway and WAF. CloudFront has a feature that allows content access to only selected locations.
- AWS ELB - Study how ELB protects your web traffic and endpoints from malicious attacks. Understand how SSL certificates are being handled by ELB.

- Amazon API Gateway - Similar to ELB, API Gateway also protects your endpoints from being exposed to the public internet. Commonly used in serverless applications, study how APIs can secure Lambda functions. Also, know what services it integrates with, such as WAF.
- AWS VPN - Although AWS VPN is fairly new, you should have an overview of what this service is and how to set it up in your AWS environment.
- AWS Direct Connect - Read how a dedicated line from your network to AWS can protect your inbound and outbound traffic. A common way to secure your traffic in Direct Connect is by using an AWS Site-to-Site VPN.

Logging and Monitoring

- Amazon CloudWatch - Know everything about Cloudwatch (Logs, Alarms, Events, Metrics)
- Amazon CloudTrail - Know everything about CloudTrail, like how to store and encrypt your log files, how to monitor different regions and capture different types of data.
- Service Logs (VPC, ELB, API Gateway, S3, CloudFront) - Multiple AWS services support logging, which they forward to an S3 bucket. It would be good to have an idea of which services support logging. Logs are crucial when conducting incident response and analysis.
- Amazon Route 53 - Study how Route 53 can quickly handle network issues by performing DNS and endpoint health checks. Route 53 also helps in making your environment more resilient by performing automatic failovers.

Threat Detection, Prevention, Response and Remediation

- Amazon GuardDuty - Have an understanding of the use cases of Amazon GuardDuty.
- Amazon Inspector - Have an understanding of the use cases of Amazon Inspector.
- Amazon Detective - Know which services integrate with Amazon Detective. Also, have an understanding of the use cases of Amazon Detective.
- AWS Security Hub - Have an understanding of the use cases of AWS Security Hub.

Risk and Compliance Management

- AWS Artifact - Know the purpose of AWS Artifact and what kinds of reports it provides for you.
- AWS Config - AWS Config is an important compliance monitoring tool that you should learn about. Study the concepts and how they work. Practice writing a Config rule of your own to have a better understanding of the service.

Lastly, as we have repeatedly talked about, specialty exams are intended for experienced individuals. Therefore, you should go try out the services above in your own AWS account. Also, do not limit yourself to the Management Console. Some implementations can only be done via AWS CLI, AWS CDK or AWS SDK. Be comfortable with them all.

Common Exam Scenarios

Scenario	Solution
AWS Config	
A company requires a solution that will automatically detect and enable disabled VPC Flow Logs.	Create an AWS Config rule that will detect disabled VPC Flow Logs. Create a CloudWatch event based on that Config Rule to trigger a Lambda Function for enabling VPC Flow Logs.
Verify if EC2 instances are using approved AMI. Create a notification if non-compliant instances are detected.	Utilize the approved-amis-by-id managed rule in AWS Config to check if running instances are using an approved AMI. Use CloudWatch Alarms for notifications.
A Security Analyst needs to remediate the risks of having security groups that allow inbound traffic for the 0.0.0.0/0 CIDR range (Anywhere). The security group must only allow inbound traffic for the company's firewall IP address.	Create an AWS Config rule that will automatically detect security groups that allow inbound traffic from the 0.0.0.0/0 CIDR range. Associate a Lambda function in the Config rule to update the security group's inbound rule with the company's firewall IP address.
You need to build a solution that will allow the Security team to review the IAM policy assigned to an IAM user before and after a security incident has occurred.	Use AWS Config
Automatically detect and remediate an incident where API logging is disabled.	Create an AWS Config rule to detect disabled CloudTrail settings. Configure the rule to use an AWS Systems Manager Automation document to automatically re-enable CloudTrail logs.
Detect if someone is using the AWS account's root access to create new API keys without proper approval.	Set up an AWS Config rule to track the usage of the create-api-key command by the root IAM user.
AWS KMS	
A company requires a KMS key that automatically rotates every year.	Create a KMS key with AWS-generated key material.

A company needs to rotate a KMS key with imported key material.	Create a new KMS key with the new imported key material and point the existing alias to the new KMS key.
A company has to manage the access control for hundreds of KMS keys without having to edit key policies.	Use grants in AWS KMS.
A Security Specialist must use additional authenticated data (AAD) to prevent tampering against the ciphertext.	Add the kms:EncryptionContext condition when defining the key policy for the KMS key.
A company needs to migrate AWS resources encrypted with KMS into another region.	Use a new KMS key in the target region.
AWS WAF, AWS Shield	
An application hosted on an EC2 instance needs protection from common web exploits. Also, the outgoing traffic from the instance should be restricted only to trusted URLs.	Use AWS WAF for common web exploits protection and use a third-party solution to whitelist URLs for outbound traffic.
A Security Specialist needs to block high-volume requests from specific user-agent HTTP headers.	Use AWS WAF rate-based rule to limit the number of requests.
Which AWS Services has direct integration with AWS WAF?	Amazon CloudFront & Application Load Balancer
A company is serving static content using Amazon CloudFront, Amazon S3, and Amazon Route53. They must respond to DDoS attacks at L7, L4, and L3.	Use AWS Shield Advanced
AWS CloudTrail	
Protect CloudTrail Logs from tampering and unauthorized access	Enable the CloudTrail log file validation

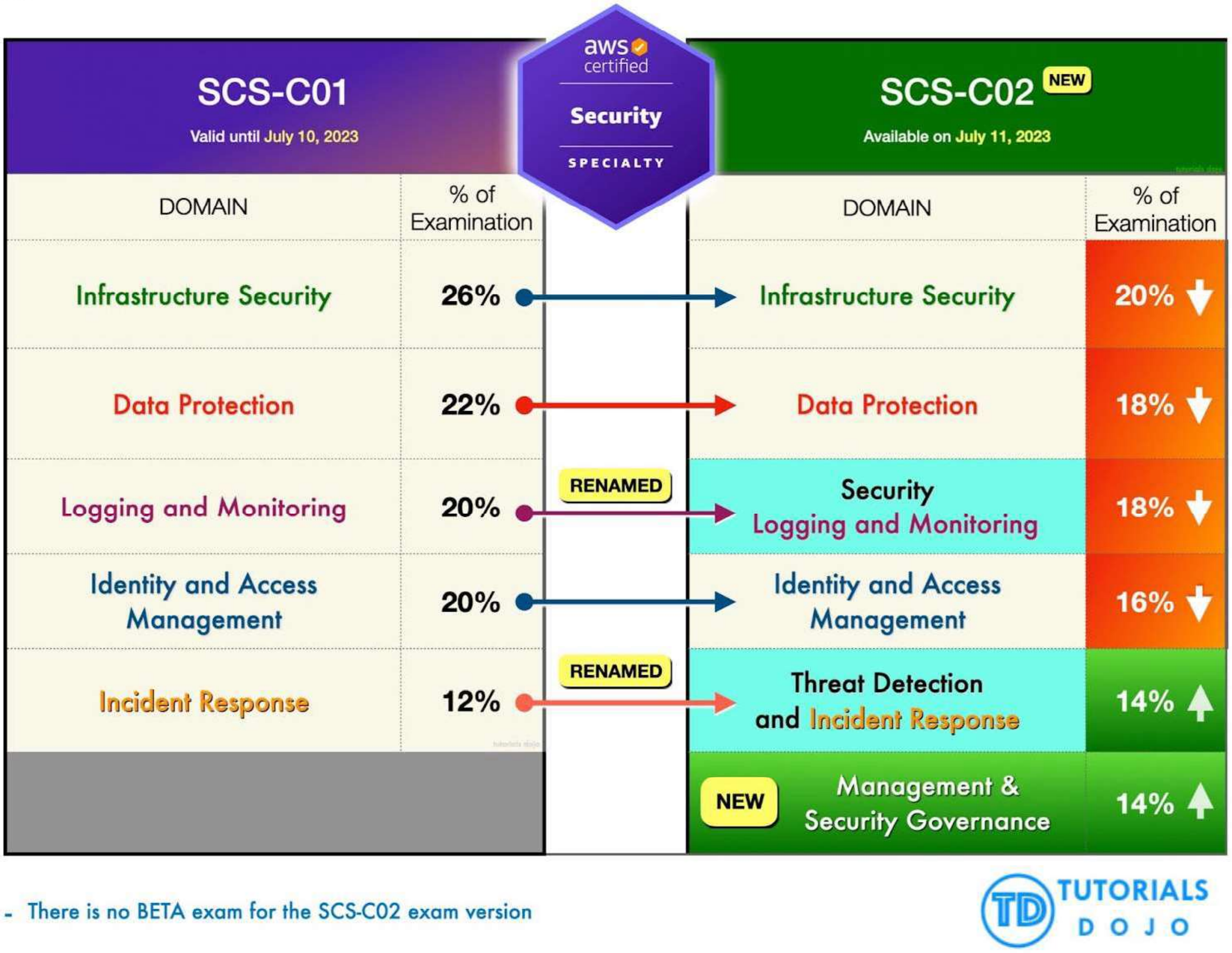
Some AWS accounts can't send CloudTrail logs in a centralized logging account. What are the steps to troubleshoot the issue?	1. Check if the AWS Account IDs are included within the Central account's S3 bucket policy. 2. Check if the AWS Accounts are using the correct S3 bucket name for centralized logging. 3. Check if all trails are active
A Security Specialist has updated the log file prefix for a trail but encountered a "There is a problem with the bucket policy." error.	First, update the new log file prefix in the S3 bucket policy, then specify the updated log file prefix in the CloudTrail Console.
A Security Engineer needs to review user activities from a specific access key within the past 3 months.	Review the user activities through the CloudTrail Console.
Amazon CloudWatch	
Some EC2 instances stop sending CloudWatch logs after a security incident. What are the steps to troubleshoot this issue?	1. Check if CloudWatch Logs agent is active and running in the EC2 instances. 2. Check if the EC2 instances have Internet access. 3. Check the validity of the OS Log rotation rules.
After an update to IAM policy, an application stops sending custom metrics to AWS CloudWatch.	Add the cloudwatch:putMetricData permission in the IAM policy.
A Security Engineer must build a near-real-time logging solution to collect logs from different AWS Accounts.	Use the Amazon CloudWatch cross-account log data sharing with subscriptions. Use Amazon Amazon Data Firehose to deliver the logs.
A company has set up a notification system using CloudWatch and CloudTrail that will alert a	Make sure that the value of the consecutive periods' alarm threshold is equal to or greater than 1.

Security Team when new access keys are created. The team is not receiving notifications.	
Amazon GuardDuty	
A company needs a threat detection system for monitoring malicious activities in an AWS Account.	Use Amazon GuardDuty
A company is using an Active Directory server to resolve DNS for EC2 instances in a VPC. A security engineer noticed that one of the instances is being used for command-and-control (C2C) operations, but GuardDuty has failed to recognize it.	GuardDuty does not recognize DNS requests coming from third-party DNS servers.
A company wants to perform a network port scan against EC2 instances in VPC but does not want to get alerts for specific instances.	Add the EIP of the specific instances to the trusted IP lists in Amazon GuardDuty.
Infrastructure Security	
A company has complex connectivity rules for Amazon EC2 instances. How should they manage these connection rules with no additional cost?	Implement the rules using the built-in host-based firewall such as iptables
A Security Engineer needs to inspect packet data.	1. Use a proxy software hosted on an EC2 instance. 2. Use a host-based agent on an EC2 instance. *Note that you can only perform packet data analysis with third-party solutions.*
A Security Engineer has a virtual security appliance. The Engineer is using a security group and NACL to comply with security requirements. How can he allow traffic through the virtual security appliance?	Disable the Source/Destination check of the Elastic Network Interface (ENI) associated with the virtual security appliance.

A Security Engineer needs to remediate the risk of users exploiting the instance metadata service to access AWS resources in other accounts.	Restrict the access to the instance metadata service using iptables.
The DevSecOps team needs help to securely create or connect the company's workforce identities and manage their access centrally across AWS accounts and applications. What is the is the recommended approach to use for workforce authentication and authorization on AWS?	Use IAM Identity Center
The AWS Security Hub service consumes, aggregates, organizes, and prioritizes findings from AWS security services and from the third-party product integrations. What is the standard findings format used by the Security Hub which eliminates the need for time-consuming data conversion efforts?	AWS Security Finding Format (ASFF)
A company has several AWS accounts that are connected using AWS Organizations. There's a requirement to centrally manage the security services and aggregating findings from all the accounts. What should the Security Engineer do?	Use delegated administration via AWS Config aggregators and AWS Security Hub.
A multinational corporation needs to continuously audit their AWS usage to simplify how they assess risk and compliance with regulations and industry standards. What service should be used to automate the process of evidence collection to make it easier to assess if the corporation's policies, procedures, and activities, are operating effectively?	AWS Audit Manager

The Old SCS-C01 vs the New SCS-C02 Exam Version

The latest AWS Certified Security Specialty SCS-C02 exam has some similarities with its previous version, but it also introduces a plethora of new knowledge areas, services, domains and features. One notable change is the brand new "Management & Security Governance" domain. This new addition checks your know-how in developing a strategy to centrally deploy and manage AWS accounts, implementing a secure and consistent deployment strategy for cloud resources, and evaluating the compliance of AWS resources, among others.



SCS-C01 Valid until July 10, 2023			SCS-C02 NEW Available on July 11, 2023	
DOMAIN	% of Examination		DOMAIN	% of Examination
Infrastructure Security	26%	→	Infrastructure Security	20% ↓
Data Protection	22%	→	Data Protection	18% ↓
Logging and Monitoring	20%	RENAMED →	Security Logging and Monitoring	18% ↓
Identity and Access Management	20%	→	Identity and Access Management	16% ↓
Incident Response	12%	RENAMED →	Threat Detection and Incident Response	14% ↑
			NEW Management & Security Governance	14% ↑

- There is no BETA exam for the SCS-C02 exam version

There are two existing exam domains that were renamed to properly reflect the task objectives for each domain. For instance, the "Logging and Monitoring" domain is now called "Security Logging and Monitoring" while the "Incident Response" is now called the "Threat Detection and Incident Response" exam domain

With the total number of domains now increased to six, the weighting distribution has been adjusted accordingly as well.

All of the existing exam domains have decreased their respective exam weighting, except for one, as shown below:

- "Infrastructure Security" domain went down from 26% to only 20%
- "Data Protection" domain decreased from 22% to 18%
- "Security Logging and Monitoring " domain was slightly cut down from 20% to 18%
- "Identity and Access Management" domain was decreased from 20% to 16%
- "Threat Detection and Incident Response" domain increased from 12 % to 14%

Validate Your Knowledge

We recommend that you try the Exam Readiness: AWS Certified Security - Specialty Course that you can get for free the AWS Skill Builder page. They provide sample questions that you can follow along and answer.

AWS also provides a sample exam on the AWS Certified Security Specialty page, which you can find here. Although this sample exam is not on the same level of difficulty one might expect on the real exam, it is still a helpful resource for your reviews.

Lastly, **Tutorials Dojo** also has a set of high-quality **SCS-C02 practice exams**, and this study guide eBook for the AWS Security Specialty certification. The practice exams and study guide eBook will help boost your preparedness for the real exam, and it will also help you determine which areas you are weak in, so you can focus your efforts on studying those areas.

Sample Practice Test Questions:

Question 1

An organization is implementing a security policy in which their cloud-based users must be contained in a separate authentication domain and prevented from accessing on-premises systems. Their IT Operations team is launching and maintaining a number of Amazon RDS for SQL Server databases and EC2 instances. The organization also has an on-premises Active Directory service that contains the administrator accounts that must have access to the databases and EC2 instances.

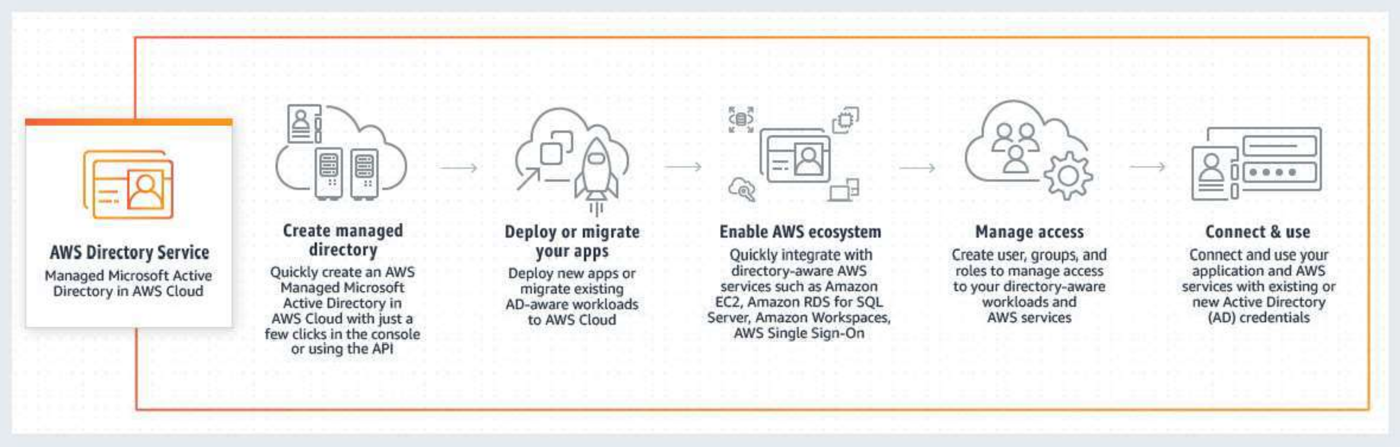
How would the Security Engineer manage the AWS resources of the organization in the MOST secure manner? (Select TWO.)

1. Using AWS Directory Service, set up an AWS Managed Microsoft AD to manage the RDS databases and EC2 instances.
2. Set up and configure AWS Service Catalog to manage the RDS databases and EC2 instances.
3. Set up a one-way incoming trust relationship from the existing Active Directory in the on-premises data center to the new Active Directory service in AWS.
4. Set up a one-way incoming trust relationship from the new Active Directory in AWS to the existing Active Directory service in the on-premises data center.
5. Set up a two-way trust relationship between the new Active Directory in AWS and the existing Active Directory service in the on-premises data center.

Correct Answer: 1,3

In **Active Directory**, trust relationships enable access to various resources that can be either one-way or two-way. A one-way trust is a unidirectional authentication path created between two domains. In a one-way trust between Domain A and Domain B, users in Domain A can access resources in Domain B. However, users in Domain B can't access resources in Domain A. Some one-way trusts can be either non-transitive or transitive, depending on the type of trust being created.

You can configure one and two-way external and forest trust relationships between your AWS Directory Service for Microsoft Active Directory and on-premises directories, as well as between multiple AWS Managed Microsoft AD directories in the AWS cloud. AWS Managed Microsoft AD supports all three trust relationship directions: Incoming, Outgoing, and Two-way (Bi-directional). When setting up trust relationships, you must ensure that your on-premises directory is and remains compatible with AWS Directory Services.


AWS Directory Service
Managed Microsoft Active Directory in AWS Cloud
Create managed directory
Quickly create an AWS Managed Microsoft Active Directory in AWS Cloud with just a few clicks in the console or using the API
Deploy or migrate your apps
Deploy new apps or migrate existing AD-aware workloads to AWS Cloud
Enable AWS ecosystem
Quickly integrate with directory-aware AWS services such as Amazon EC2, Amazon RDS for SQL Server, Amazon Workspaces, AWS Single Sign-On
Manage access
Create user, groups, and roles to manage access to your directory-aware workloads and AWS services
Connect & use
Connect and use your application and AWS services with existing or new Active Directory (AD) credentials

If you already have an AD infrastructure and want to use it when migrating AD-aware workloads to the AWS Cloud, AWS Managed Microsoft AD can help. You can use AD trusts to connect AWS Managed Microsoft AD to your existing AD. This means your users can access AD-aware and AWS applications with their on-premises AD credentials without needing you to synchronize users, groups, or passwords.

For example, your users can sign in to the AWS Management Console and Amazon WorkSpaces by using their existing AD user names and passwords. Also, when you use AD-aware applications such as SharePoint with AWS Managed Microsoft AD, your logged-in Windows users can access these applications without needing to enter credentials again.

There are three trust relationship directions:

1. **One-way:incoming -** Users in the specified realm will not be able to access any resources in this domain.
2. **One-way:outgoing -** Users in this domain will not be able to access any resources in the specified realm.
3. **Two-way (Bi-directional)** - Users in this domain and users in the specified realm will be able to access resources in *either* domain or realm.

Hence, the correct answers are:

- **Using AWS Directory Service, set up an AWS Managed Microsoft AD to manage the RDS databases and EC2 instances.**
- **Set up a one-way incoming trust relationship from the existing Active Directory in the on-premises data center to the new Active Directory service in AWS.**

The option that says: **Set up and configure AWS Service Catalog to manage the RDS databases and EC2 instances** is incorrect because AWS Service Catalog simply allows organizations to create and manage catalogs of IT services that are approved for use on AWS. You have to use AWS Directory Service instead.

The option that says: **Set up a one-way incoming trust relationship from the new Active Directory in AWS to the existing Active Directory service in the on-premises data center** is incorrect because this should be the other way around. Instead, you have to set up a one-way trust relationship from the existing Active Directory in the on-premises data center to the new Active Directory service in AWS.

The option that says: **Set up a two-way trust relationship between the new Active Directory in AWS and the existing Active Directory service in the on-premises data center** is incorrect because the scenario explicitly mentioned that the cloud-based users must be prevented from accessing on-premises systems. Hence, you have to use a one-way trust relationship only.

References:
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/usecase5.html
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust

Check out this AWS Directory Service Cheat Sheet:
https://tutorialsdojo.com/aws-directory-service/

Question 2

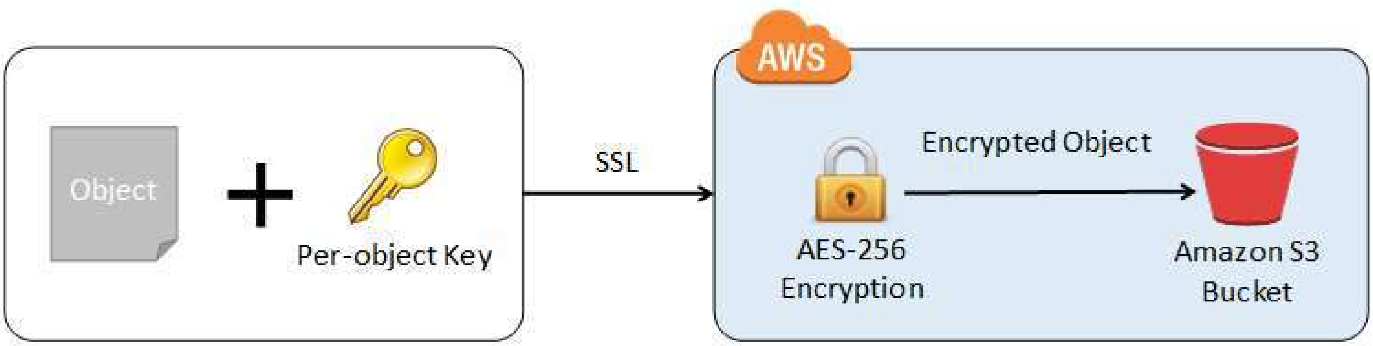
A company is planning to migrate its on-premises application to AWS. The application will be hosted in Elastic Beanstalk, which uses an external RDS database and an S3 bucket configured to use Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C). In this configuration, Amazon S3 does not store the encryption key you provide but instead stores a randomly salted hash-based message authentication code (HMAC) value of the encryption key in order to validate future requests. The Security Engineer was assigned to implement the required security measures for the application.

Which of the following is a valid consideration that the Engineer should keep in mind when implementing this architecture?

1. The salted HMAC value can be used to derive the value of the encryption key.
2. You will lose access to the S3 object if you lose the encryption key.
3. The salted HMAC value can be used to decrypt the contents of the encrypted object.
4. The salted HMAC value can be used to decrypt the S3 object in the event that you lose the encryption key.

Correct Answer: 2

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.



When you upload an object, Amazon S3 uses the encryption key you provide to apply AES-256 encryption to your data and removes the encryption key from memory. It is important to note that Amazon S3 does not store the encryption key you provide. Instead, it is stored in a randomly salted HMAC value of the encryption key in order to validate future requests. The salted HMAC value cannot be used to derive the value of the encryption key or to decrypt the contents of the encrypted object. That means if you lose the encryption key, you lose the object.

When you retrieve an object, you must provide the same encryption key as part of your request. Amazon S3 first verifies that the encryption key you provided matches and then decrypts the object before returning the object data to you.

Hence, the valid consideration that the developer should keep in mind when implementing this architecture is: **You will lose access to the S3 object if you lose the encryption key**.

The option that says: **The salted HMAC value can be used to derive the value of the encryption key** is incorrect because the salted HMAC is just used to validate future encryption requests. It cannot be used to derive the value of the encryption key or to decrypt the contents of the encrypted object.

The option that says: **The salted HMAC value can be used to decrypt the contents of the encrypted object** is incorrect because, just as mentioned above, the HMAC cannot be used to derive the value of the encryption key or to decrypt the contents of the encrypted object.

The option that says: **The salted HMAC value can be used to decrypt the S3 object in the event that you lose the encryption key** is incorrect because if you lose the encryption key, you will also lose access to that object. You cannot use the salted HMAC value to decrypt the object.

References:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html
https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html#RESTObjectPUT-responses-exam

ples
https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/

Check out these Amazon S3 and AWS KMS Cheat Sheets:
https://tutorialsdojo.com/amazon-s3/
https://tutorialsdojo.com/aws-key-management-service-aws-kms/

Click **here** for more **AWS Certified Security Specialty practice exam questions**.

Check out our other AWS practice test courses **here**:

TD TUTORIALS DOJO
REVIEWERS for aws CERTIFICATIONS
aws certified Cloud Practitioner FOUNDATIONAL
aws certified Solutions Architect ASSOCIATE
aws certified Developer ASSOCIATE
aws certified SysOps Administrator ASSOCIATE
aws certified Solutions Architect PROFESSIONAL
aws certified DevOps Engineer PROFESSIONAL
aws certified Advanced Networking SPECIALTY
aws certified Data Analytics SPECIALTY
aws certified Database SPECIALTY
aws certified Machine Learning SPECIALTY
aws certified Security SPECIALTY

With the growing number of security attacks each day, companies are now focusing their efforts in strengthening their digital security. This responsibility requires a team effort from both AWS engineers and industry professionals, which is why we have a shared responsibility model. Professionals will have to be equipped with the right tools and knowledge to protect what is valuable to them and to their company.

We hope that our guide has helped you achieve that goal, and we would love to hear back from you after your exam. Get some well-deserved rest, and we wish you the best of results.

Domain 1: Threat Detection and Incident Response

Overview

The first domain of the AWS Certified Security Specialty exam checks your preparedness on how well you are able to detect, automate, verify, evaluate, and remediate security incidents in your AWS infrastructure. Roughly 14% of questions in the actual Security Specialty exam revolve around this topic.

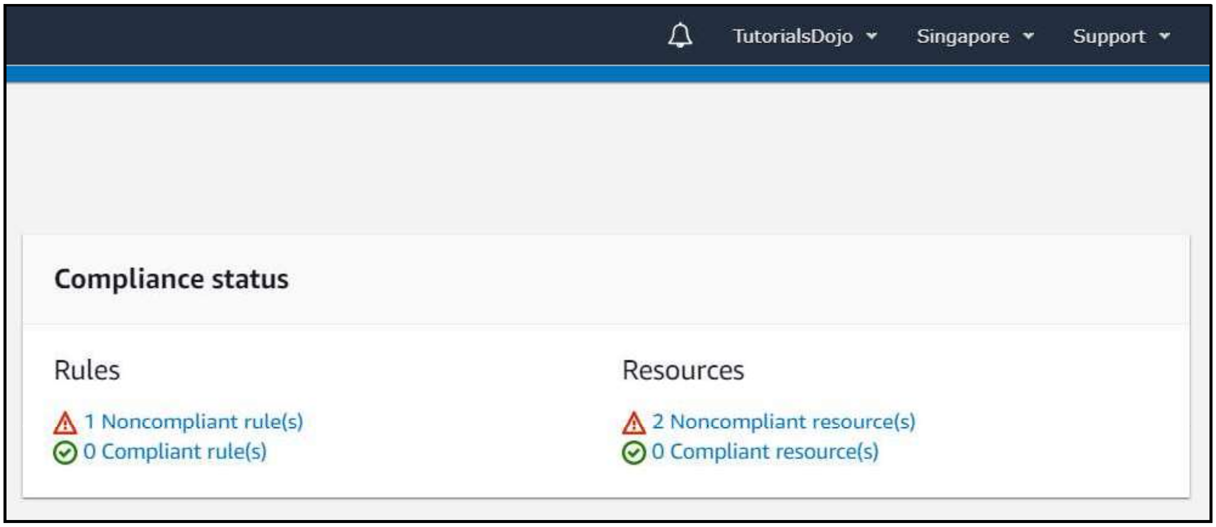
This domain will challenge your know-how in doing the following:

- Analyzing architectures to identify monitoring requirements and sources of data for security monitoring
- Analyzing environments and workloads to determine monitoring requirements
- Designing environment monitoring and workload monitoring based on business and security requirements
- Setting up automated tools and scripts to perform regular audits (for example, by creating custom insights in Security Hub)
- Defining the metrics and thresholds that generate alerts
- Analyzing the service functionality, permissions, and configuration of resources after an event that did not provide visibility or alerting
- Analyzing and remediating the configuration of a custom application that is not reporting its statistics
- Evaluating logging and monitoring services for alignment with security requirements
- Configuring logging for services and applications
- Identifying logging requirements and sources for log ingestion
- Implementing log storage and lifecycle management according to AWS best practices and organizational requirements
- Identifying misconfiguration and determining remediation steps for absent access permissions that are necessary for logging (for example, by managing read/write permissions, S3 bucket permissions, public access, and integrity)
- Determining the cause of missing logs and performing remediation steps
- Identifying patterns in logs to indicate anomalies and known threats
- Normalizing, parsing, and correlating logs

In this chapter, we will cover all of the related topics for Threat Detection and Incident Response Management in AWS that will likely show up in your Security Specialty exam. Take note that this domain has the least amount of weight in the exam (14%), which is similar to the new Domain 6: Management and Security Governance domain (14%), so make sure that you only spend ample time understanding the concepts in this section.

Using AWS Config Rules for Automated Checks and Remediation

AWS Config tracks and records configuration changes on your AWS resources. You can use this service to ensure your resources are properly configured and that they stay within the compliance requirements of your organization. AWS Config uses Config rules to evaluate whether a particular resource is compliant or not. You can view the compliance status of these evaluations on your AWS Config Dashboard.



Compliance status

Rules
1 Noncompliant rule(s)
0 Compliant rule(s)

Resources
2 Noncompliant resource(s)
0 Compliant resource(s)

AWS Config saves records of changes to an S3 bucket of your choosing or one that Config creates automatically. Optionally, you can set an SNS Topic to get alerts via email or SMS every time a change occurs.

There are two types of Config rules which you can check your compliance against:

- **AWS-Managed Rules** - These are rules that are defined and maintained by AWS. They require minimal to no configuration. You can use this to evaluate common security concerns such as:
  - *Do all of my security groups in use allow unrestricted incoming SSH traffic?*
  - *Is the account password policy for IAM users secure enough to meet the specified requirements?*
  - *Are all EBS volumes that are in an attached state encrypted?*

- **Custom Rules** - AWS-Managed rules are great, but it does not solve every problem as every business is built differently. If you want to check compliance against your company's internal security rules that are not readily defined in AWS, you can use Custom Rules. Custom rules are AWS Lambda functions that you create and maintain yourself. The Lambda function should contain the logic that will determine whether a resource is compliant or non-compliant.

AWS Config can take remediation actions against non-compliant resources using AWS Systems Manager Automation documents. You can use one of the prebuilt automation documents provided by AWS Config or write your own. An SSM automation document can be associated with a Config rule to take corrective actions automatically when a resource is evaluated as non-compliant. However, you may run the SSM automation document manually as well.

In other cases, it's also possible to create an EventBridge (CloudWatch Event) rule that triggers a Lambda function in response to a particular AWS Config event. Consider the following scenario:

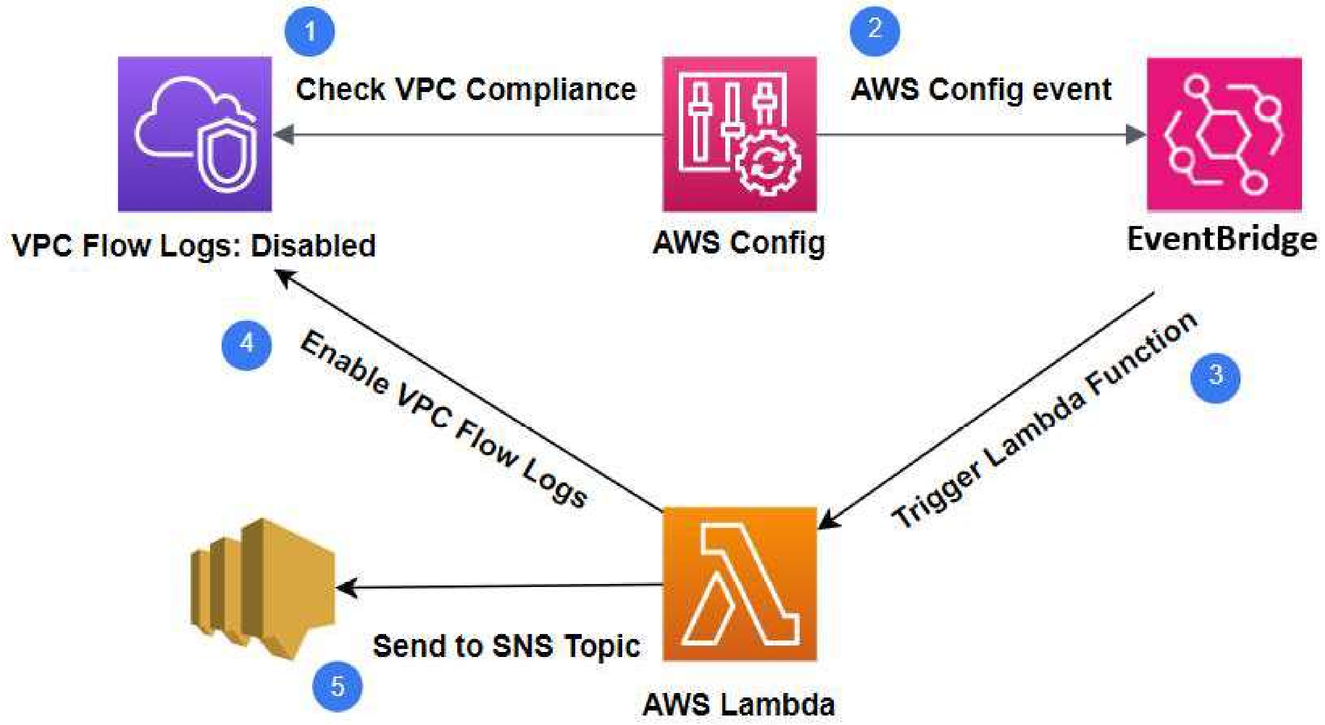
> *You are managing your development account where several teams are using it to test their applications. All VPCs created on the account should have VPC Flow Logs enabled, and the logs must be sent to a central S3 bucket for audit purposes. Since several teams created their own VPCs for testing, it is difficult for you to track all VPCs and manually enable VPC Flow Logs. The solution should easily detect non-compliant resources and automatically enable the VPC Flow Logs.*

The scenario addresses two problems: The first issue is about automatically tracking non-compliant VPCs (VPCs with disabled VPC Flow Logs). The second problem is about implementing the remedial action to take when Config detects a non-compliant VPC.

We can solve the problem by doing the following steps:

1. Create an AWS Config rule that will flag VPCs with disabled VPC Flow Logs.
2. Create a Lambda function that will enable the VPC Flow Logs on the non-compliant VPC.
3. Create an EventBridge(CloudWatch Event) event rule that triggers the Lambda function when AWS Config detects a non-compliant VPC.

You can optionally add an SNS topic to receive notifications for only that specific event. Below is the architecture diagram for the solution:

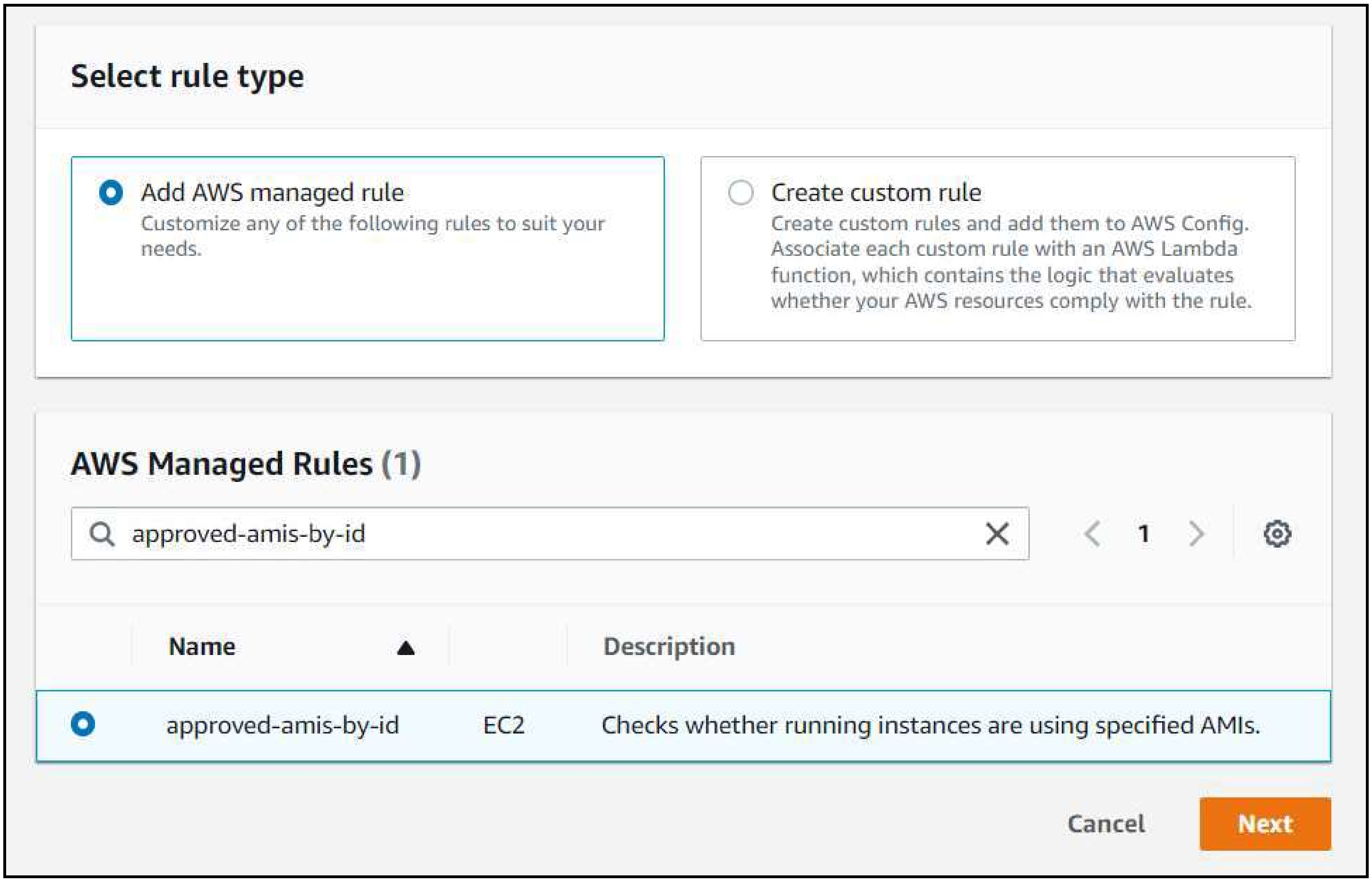


Using AWS Config to ensure that only approved AMIs are only launched

There are cases when you want to ensure that only the approved AMIs are used to launch EC2 instances for compliance and security reasons. Obviously, this could easily be done if you're involved in a small organization that manages two or more instances. You can just manually go through each of the instances and check their AMI IDs.

However, if you are managing hundreds of EC2 instances, that's a different situation. Let's say that you want to host a web application using a specific Linux distribution only. Manually inspecting individual instances would take you hours and is not very practical, especially now that we have access to modern tools that make our lives easier.

The better solution is to use the `approve-amis-by-id` managed rule in AWS Config. This is already pre-defined for you, so you don't have to create and maintain your own code to evaluate AMIs. This rule will detect any non-compliant AMIs, and you could automate the remediation action by following the same architecture that we previously discussed using Amazon EventBridge (Amazon CloudWatch Events).



Select rule type

● Add AWS managed rule
Customize any of the following rules to suit your needs.

○ Create custom rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

AWS Managed Rules (1)

approved-amis-by-id

	Name ▲		Description
●	approved-amis-by-id	EC2	Checks whether running instances are using specified AMIs.

Security Specialty Exam Notes:

You can use the AWS Config to monitor and assess non-compliant configurations in your resources. Send the event's status to Amazon EventBridge (Amazon CloudWatch Events) so it can trigger a Lambda Function that will fix the non-compliant configuration.

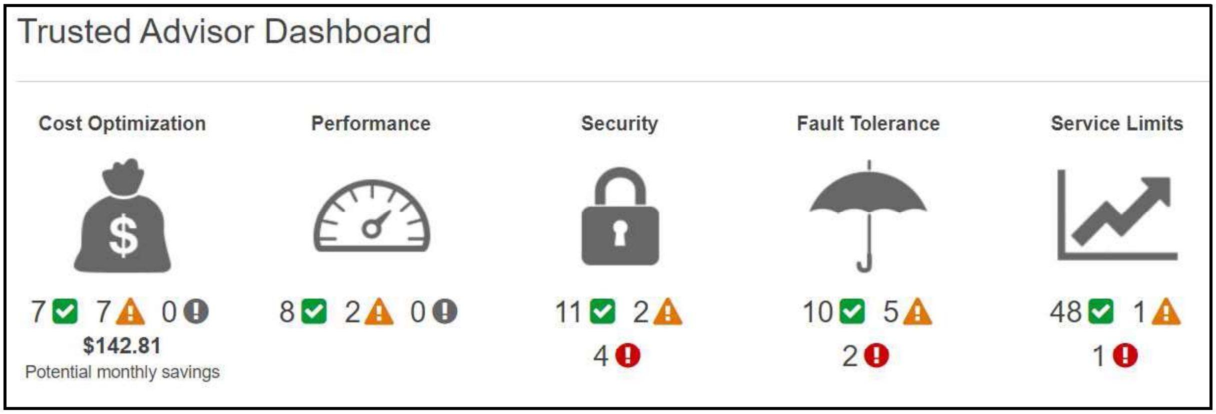
References:
https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html
https://docs.aws.amazon.com/config/latest/developerguide/monitor-config-with-cloudwatchevents.html
https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html

Incident Response Management using Trusted Advisor

Tracking a few AWS resources in your account is no sweat, but as your business grows, the number of resources you manage will eventually add up. This could pose a severe security problem for you as it'll be challenging to keep tabs on various resources in terms of how permissive and restrictive they are.

Here is where Trusted Advisor comes into play. Trusted Advisor is a service that will analyze your AWS environment and provide best practice recommendations for you in five categories:

- Cost Optimization
- Performance
- Security
- Fault Tolerance
- Service Limits



Trusted Advisor Dashboard

Cost Optimization	Performance	Security	Fault Tolerance	Service Limits
7 ✓ 7 ⚠ 0 ❗ $142.81 Potential monthly savings	8 ✓ 2 ⚠ 0 ❗	11 ✓ 2 ⚠ 4 ❗	10 ✓ 5 ⚠ 2 ❗	48 ✓ 1 ⚠ 1 ❗

Note: *Unlike AWS Config, Trusted Advisor does not allow users to specify resources to be assessed. AWS controls the resources and attributes to be inspected. You can think of it as a person who examines your AWS environment and gives you recommendations based on best practices.*

Since you're taking the AWS Certified Security Specialty Exam, our focus will be more on improving the security of your application on AWS. Below are some security best practices recommended to us by Trusted Advisor.

Multi-Factor Authentication on Root Account

AWS Trusted Advisor detects whether you have MFA enabled on your Root Account. It is advisable to use MFA when logging in as a root user for greater security. Note that an attacker will only need access to your account's email for him to reset your password. Without MFA, you're running the risk of only securing your account with your email credentials. MFA requires users to type a secret code in addition to their password before they can access their account.

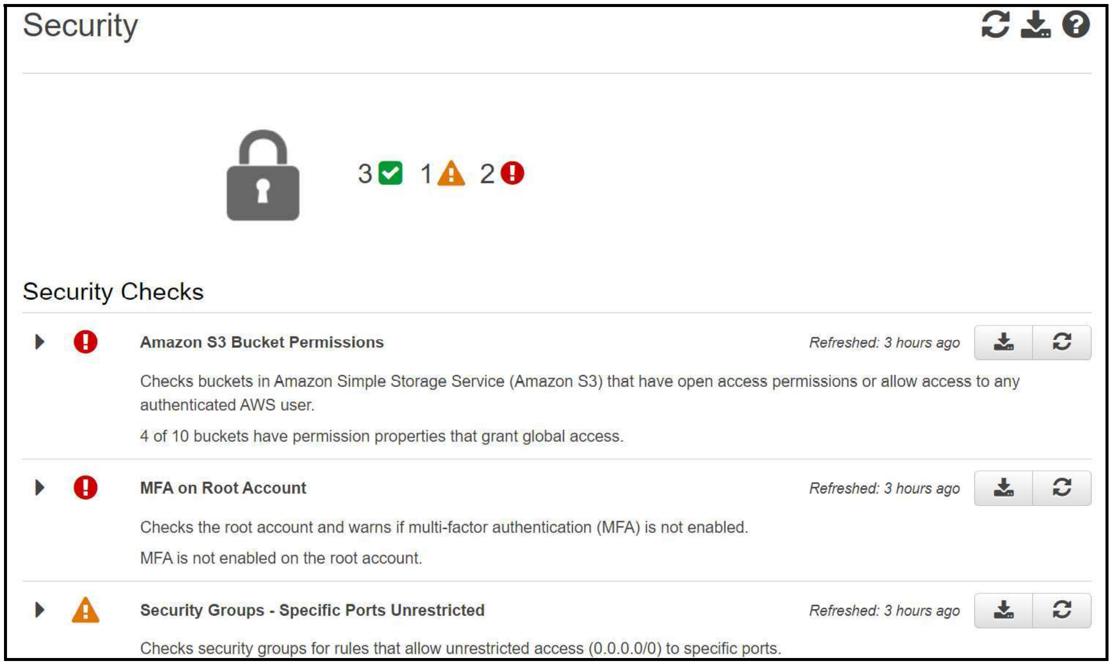
Amazon S3 Bucket Permissions

AWS Trusted Advisor checks if you have S3 buckets with open access permissions in your account. Confidential files stored on S3 buckets with open permissions can be exploited. Aside from storage, you also pay for requests against S3 buckets. Unauthorized users who spam S3 requests can lead to unexpected charges.

Security Groups - Unrestricted Access

AWS Trusted Advisor checks if you have security group rules that allow unrestricted access. Leaving your security groups open for other users increases your attack surface and is against the principle of least privilege access.

Here's how it looks on the Trusted Advisor Dashboard.



Security

3 ✓ 1 ⚠ 2 ❗

Security Checks

❗ **Amazon S3 Bucket Permissions** *Refreshed: 3 hours ago*

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions or allow access to any authenticated AWS user.

4 of 10 buckets have permission properties that grant global access.

❗ **MFA on Root Account** *Refreshed: 3 hours ago*

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

MFA is not enabled on the root account.

⚠ **Security Groups - Specific Ports Unrestricted** *Refreshed: 3 hours ago*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

As you can see, there are three alert criteria shown (denoted by green, yellow, and red). These criteria reflect the current incident severity levels of your resources.

✅ Green alert status means no problem is detected.

⚠ Yellow alert status indicates that an investigation should be done on the affected resources. You can think of this as an early warning for your resources that could create loopholes in your defense strategy.

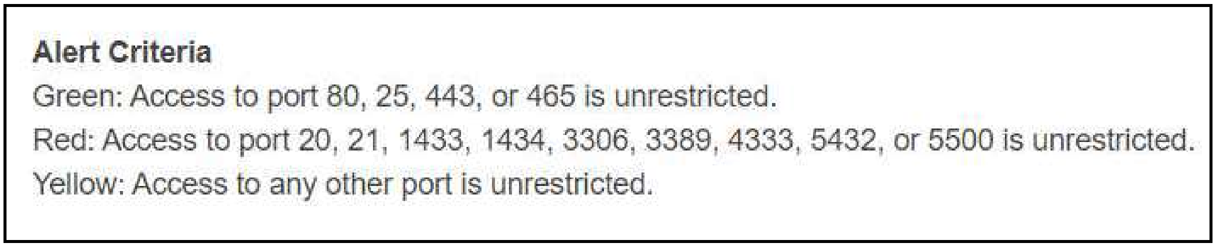
❗ Red alert status is the most critical alert criteria of the three. Resources tagged with red alerts have the most potential security vulnerabilities, which warrant an immediate solution.

Automated Monitoring of Trusted Advisor Security Checks

Like what we've discussed about AWS Config in the last section, we can also use Amazon EventBridge (Amazon CloudWatch Events) to detect the changes in the security check of Trusted Advisor based on an event rule. You can react to these changes by writing a function that will automatically take corrective action.

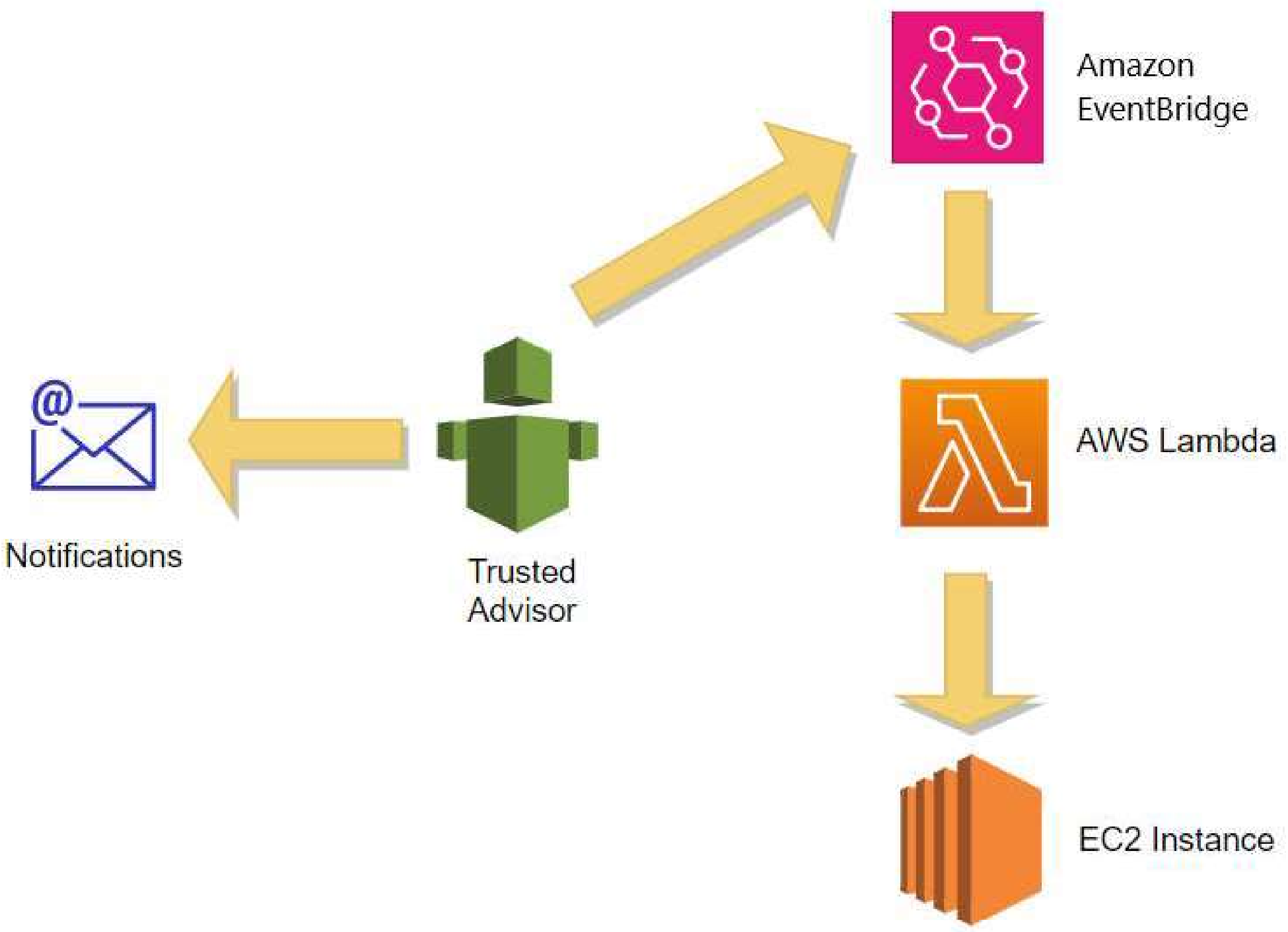
For example, let's say that you're managing an AWS account with different environments (Production, Development, UAT, etc.) with multiple EC2 instances. As part of your company's security policies, you need to restrict access to sensitive ports (e.g., port 22 for SSH, port 3306 for MySQL Database, etc.) by configuring the rules of security groups that are attached to active EC2 instances. It will be cumbersome to go through all the environments and check their security groups one by one. The Trusted Advisor can solve this dilemma.

By default, Trusted Advisor tags those security groups with access to sensitive ports as a red alert status, as you can see on the screenshot below:



Alert Criteria
Green: Access to port 80, 25, 443, or 465 is unrestricted.
Red: Access to port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432, or 5500 is unrestricted.
Yellow: Access to any other port is unrestricted.

We can create an event pattern in Amazon EventBridge (Amazon CloudWatch Events) that will trigger a Lambda Function every time the Trusted Advisor identifies a security group with red alert status. The Lambda Function contains the logic that will call the appropriate EC2 API command — updating the security group's rule to deny access to said vulnerable ports. Optionally, you can enable weekly email notifications from the Trusted Advisor to get information about your resources' status.



Security Specialty Exam Notes:

Trusted Advisor automatically checks your AWS environment against best practices. Similar to AWS Config, you can use **Amazon EventBridge (Amazon CloudWatch Events) + Lambda Function** for incident response.

References:
https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/
https://docs.aws.amazon.com/awssupport/latest/user/cloudwatch-events-ta.html