

# Exam Session - Knowledge Check: Management (SAA-C03) 1 of 2

 [cloudacademy.com/quiz/exam/3795216/results](https://cloudacademy.com/quiz/exam/3795216/results)

#1

Which Amazon CloudWatch feature allows CloudWatch to implement machine learning algorithms against your metric data to help detect any activity that sits outside of the normal baseline parameters?



alarms



anomaly detection



EventBridge



logs

Explanation

CloudWatch metrics also allow you to enable a feature known as anomaly detection. This allows CloudWatch to implement machine learning algorithms against your metric data to help detect any activity that sits outside of the normal baseline parameters that are generally expected.

 [/course/an-overview-of-amazon-cloudwatch-1222/what-is-amazon-cloudwatch/](#)

Covered in this lecture

What is Amazon CloudWatch?

Course:Management Fundamentals for AWS

11m



#2

What is the purpose of AWS Service Catalog?



✗

to allow you to meet, chat, and place business calls inside and outside your organization, all using a single application

✗

to provide a way to model a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their life cycles

✗

to provide secure, resizable compute capacity in the cloud

✓

to make provisioning and creating IT stacks easier for both the end user and IT admins

Explanation

AWS Service Catalog is an organizational tool developed with the purpose of making provisioning and creation of IT stacks easier for both the end user as well as your IT admins.

 [/course/provision-applications-with-service-catalog-1473/aws-service-catalog/](#)

#3

What is the primary function of AWS CloudTrail?

✓

To track and record API requests made in AWS

✗

To notify you regarding configuration changes to your AWS resources

✗

To monitor resource performance against specific service thresholds

✗

To provide feedback on your AWS cloud environment's configuration based on best practices

Explanation

CloudTrail is a service that has a primary function to record and track all AWS API requests made. These API calls can be programmatic requests initiated from a user using an SDK, the AWS Command Line Interface, from within the AWS management console, or even from a request made by another AWS service.

[/course/aws-management-fundamentals/aws-cloudtrail-1/](#)

Covered in this lecture

What is AWS CloudTrail?

Course:AWS CloudTrail: An Introduction

5m



#4



In AWS Service Catalog, a(n) \_\_\_\_\_ is a collection of products with configuration information that helps in determining who can use the products.



portfolio



tag



stack



array

Explanation

A portfolio is a collection of products with configuration information, which helps in determining who can use the products within.

[/course/provision-applications-with-service-catalog-1473/aws-service-catalog/](#)

#5

Amazon CloudWatch \_\_\_\_\_ allow you to implement automatic actions based on specific thresholds that you can configure related to each metric.



anomaly detections



rules



alarms



events

Explanation

Amazon CloudWatch alarms tightly integrate with the metrics that I just discussed and they allow you to implement automatic actions based on specific thresholds that you can configure related to each metric.

 </course/an-overview-of-amazon-cloudwatch-1222/what-is-amazon-cloudwatch/>

Covered in this lecture

What is Amazon CloudWatch?

Course:Management Fundamentals for AWS

11m



#6



Non-compliant resources identified through the use of AWS Config Rules are automatically removed from operational service.



True



False



It depends on the rule configuration



Only if it remains non-compliant for more than six hours

Explanation

Each time a change is made to one of your supported resources, AWS config will check its compliance against any Config Rules that you have in place. If there is a violation against these rules, then AWS Config will send a message to the Configuration Stream via SNS and the resource will be marked as 'noncompliant.'

It's important to note that this does not mean the resource will be taken out of service or it will stop working. It will continue to operate exactly as it is with its new configuration. AWS Config simply alerts you that there is a violation and it's up to you to take the appropriate action.

 [http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config\\_view-compliance.html](http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_view-compliance.html)

#7

\_\_\_\_\_ in AWS Control Tower help to keep all of your users' accounts and make sure everything is in compliance with basic security regulations.



Guardrails



Registries



Service control policies



Rule groups

Explanation

Guardrails is an appropriately named service that helps to keep all of your users' accounts and everything under AWS Control Tower and compliance with basic security regulations.

 </course/building-multi-account-aws-infrastructure-control-tower-1374/aws-control-tower/>

#8

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use \_\_\_\_\_.



trusted signers



optimistic locking



root credentialing



integrity validation

Explanation

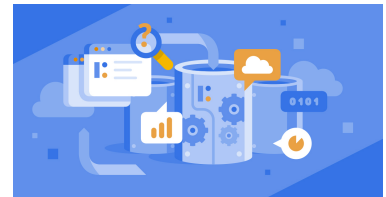
The AWS CloudTrail uses log file integrity validation to determine whether the log files were changed or modified since CloudTrail delivered them to an Amazon S3 bucket.

 <https://aws.amazon.com/cloudtrail/>

Covered in this lecture

CloudTrail Logging

Course:How to Implement & Enable Logging Across AWS Services (Part 1 of 2).



17m



#9

Which three AWS Config components use configuration items? (Choose 3 answers)



Configuration history



Configuration snapshots



Configuration streams




Configuration recorder

Explanation

Configuration items are used by other features and components of AWS Config, such as:

- Configuration History - Configuration items are used to look up all changes that have been made to a resource

- Configuration Streams - Configuration items are sent to an SNS Topic to enable analysis of the data
- Configuration Snapshots - Configuration items are used to create a point in time snapshot of all supported resources

 [/amazon-web-services/introduction-to-aws-config-course/key-components.html](https://aws.amazon.com/web-services/introduction-to-aws-config-course/key-components.html)

#10

What is a service control policy (SCP) within the AWS Organizations service?

✗

A hierarchical, visual representation of your company's entire AWS account structure

✗

A method of categorizing a company's multiple AWS accounts

✓

A method of controlling which AWS services are accessible for specific AWS accounts within your AWS account structure

✗

A container at the top of a company's AWS accounts structure

Explanation

An Organization is an element that serves to form a hierarchical structure of multiple AWS accounts. You could think of an organization as a family tree which provides a graphical view of your entire AWS account structure. At the very top of this Organization, there will be a Root container.

The Root object is simply a container that resides at the top of your Organization. All of your AWS accounts and Organizational units will then sit underneath this Root. Within any Organization, there will only be one single Root object.

Organizational Units (OUs) provide a means of categorizing your AWS Accounts. Again, like the Root, these are simply containers that allow you to group together specific AWS accounts. An organizational unit (or OU) can connect directly below the Root or even below another OU (which can be nested up to 5 times). This allows you to create a hierarchical structure as I mentioned previously.

Accounts. These are your AWS accounts that you use and create to be able to configure and provision AWS resources. Each of your AWS accounts has a 12 digit account number.

Service control policies, or SCPs, allow you to control what services and features are accessible from within an AWS account. These SCPs can either be associated with the Root, Organizational Units, or individual accounts. When an SCP is applied to any of these objects, its associated controls are fed down to all child objects. Think of it as a permission boundary that sets the maximum permission level for the objects that it is applied to.

[!\[\]\(d263118e0bfd47dc6bc704167d936b83\_img.jpg\) /course/securing-aws-organizations-with-service-control-policies-scps/aws-organizations/](#)

Covered in this lecture

Securing Your Organizations with Service Control Policies

Course:Securing AWS Organizations with Service Control Policies (SCPs)



13m



#11

Which of the following tasks can AWS Config help you accomplish?



Manage and maintain compliance



Track resource metrics



Automatically delete non-compliant resources



Log all API calls to your resources

Explanation


AWS Config can:

- Enforce rules that check the compliance of your resource against specific controls: Predefined and custom rules can be configured within AWS Config, allowing you to check resources compliance against these rules
- Act as a resource inventory:AWS Config can discover supported resources running within your environment allowing you to see data about that resource type

The other choices include services offered by Amazon CloudWatch and Amazon CloudTrail.



Store configuration history for individual resources: The service will record and hold all existing changes that have happened against the resource, providing a useful historical record of changes

 </amazon-web-services/introduction-to-aws-config-course/what-is-aws-config.html>

Covered in this lecture

Introduction

Course:How to Implement & Enable Logging Across AWS Services (Part 2 of 2)



4m



#12

In AWS Service Catalog, which type of constraint lets you configure where you want your products to launch?



tag update



template



launch



stack set

Explanation

Stack set constraint: This constraint gives you the option to configure where you want your products to launch.

 </course/provision-applications-with-service-catalog-1473/aws-service-catalog/>

#13

The \_\_\_\_\_ feature of AWS Systems Manager is a fully-managed capability that lets you connect to any managed instance using an interactive browser shell login for Linux, Windows, and MacOS instances.



Session Manager



Fleet Manager



Patch Manager



State Manager

Explanation

The Session Manager feature of Systems Manager is a fully-managed capability that lets you connect to any managed instance using an interactive browser shell login for Linux, Windows, and MacOS instances.

 [/course/aws-systems-manager-operational-insights-1699/aws-systems-manager-requirements-and-building-blocks/](#)

#14

In AWS Control Tower, a \_\_\_\_\_ is a multi-account architecture that follows the well-architected framework and is based around the ideas of security and compliance best practices.



drift



guardrail



landing zone



blueprint

Explanation

A landing zone is a multi-account architecture that follows the well-architected framework and is based around the ideas of security and compliance best practices.

[!\[\]\(cead67df4d82d6c83effe4f8699a7d8f\_img.jpg\) /course/building-multi-account-aws-infrastructure-control-tower-1374/aws-control-tower/](#)  
#15

In Amazon CloudWatch EventBridge, a(n) \_\_\_\_\_ acts as a filter for incoming streams of event traffic and then routes these events to the appropriate target.

✗

log

✗

event bus

✓

rule

✗

alarm

Explanation

A rule acts as a filter for incoming streams of event traffic and then routes these events to the appropriate target defined within the rule.

[!\[\]\(0d5ec72f61334709c3fc9450209b754f\_img.jpg\) /course/an-overview-of-amazon-cloudwatch-1222/what-is-amazon-cloudwatch/](#)

Covered in this lecture

What is Amazon CloudWatch?

Course:Management Fundamentals for AWS

11m



#16



AWS Control Tower is a service that offers a larger and more controlled method of \_\_\_\_\_.

✗

searching, visualizing, and analyzing up to petabytes of text and unstructured data

✓

creating, distributing, managing, and auditing multiple accounts




provisioning, managing, and deploying SSL/TLS certificates



centrally managing firewall rules

Explanation

AWS Control Tower is a service that offers a larger and more controlled method of creating, distributing, managing, and auditing multiple accounts.

 [/course/building-multi-account-aws-infrastructure-control-tower-1374/aws-control-tower/](#)  
#17

An IAM user is part of an IAM group that has read-only access to Amazon RDS databases within a company's production environment. This user is also part of an organizational unit (OU) which is granted full access to Amazon RDS databases in the company's production environment. If the IAM user attempts to modify the failover settings for a database in the company's production environment, what will happen?



The user's request will be **denied** because permissions can only be granted by AWS IAM, not AWS Organizations.



The user's request will be **granted** because permissions can be granted by either AWS IAM or AWS Organizations.



The user's request will be reviewed for approval by the owner of the related AWS account.



The user's request will be reviewed for approval by the master account of the related AWS Organization.

Explanation

Here is how AWS Organizations' SCPs and IAM policies work together:

Users and roles must still be granted permissions with appropriate IAM permission policies. A user without any IAM permission policies has no access, even if the applicable SCPs allow all services and all actions.

If a user or role has an IAM permission policy that grants access to an action that is also allowed by the applicable SCPs, the user or role can perform that action.

If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable SCPs, the user or role can't perform that action.

Here is how AWS Organizations' SCPs and IAM policies work together:

Users and roles must still be granted permissions with appropriate IAM permission policies. A user without any IAM permission policies has no access, even if the applicable SCPs allow all services and all actions.

If a user or role has an IAM permission policy that grants access to an action that is also allowed by the applicable SCPs, the user or role can perform that action.

If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable SCPs, the user or role can't perform that action.



[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html#scp-effects-on-permissions](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html#scp-effects-on-permissions)

Covered in this lecture

AWS Organizations

Course:Securing AWS Organizations with Service Control Policies (SCPs)



5m



#18

What is the primary function of Amazon CloudWatch?



To notify you regarding configuration changes to your AWS resources



To monitor your AWS resources' performance against specific metrics and thresholds



To track and record API requests made in AWS

✗

To provide feedback on your AWS cloud environment's configuration based on best practices

Explanation

The primary function of Amazon CloudWatch is to provide a means of monitoring the resources that you're running within AWS via a series of metrics, which are individual to each service that you are using. This allows you to quickly react to events, and diagnose, and dynamically adjust any availability or scalability issue that you might be experiencing.

 <https://aws.amazon.com/cloudwatch/>

Covered in this lecture

Summary

Course:Management Fundamentals for AWS

6m



#19



When creating metric filters in CloudWatch for your CloudTrail logs, you must create a \_\_\_\_\_ that determines what exactly you want CloudWatch to monitor and extract from your CloudTrail log files.

✓

filter pattern

✗

search pattern

✗

filter string

✗

search string

Explanation

When creating these metric filters, you must create a filter pattern which determines what exactly you want CloudWatch to monitor and extract from your files. These filter patterns are fully customizable strings, but as a result, a very specific pattern syntax is required. So if you

are creating these for the first time, you must understand the correct syntax



[https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.htm](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html)

1

Covered in this lecture

Summary

Course: AWS CloudTrail: An Introduction

3m



#20



An IAM user is part of an IAM group that is allowed permission to create Amazon EC2 instances. This user is also part of an organizational unit (OU) assigned a service control policy (SCP) that denies all access to Amazon EC2. If this user tries to create and launch an EC2 instance, what will happen?



The user will be denied access to Amazon EC2 because denies in SCPs assigned in AWS Organizations can overrule allows identity-based permissions granted through IAM.



The user will be granted access to Amazon EC2 because identity-based permissions allowed through IAM overrule denies in SCPs assigned through AWS Organizations.



The user's request will be reviewed for approval by the AWS Organizations master account.



The user's request will be reviewed for approval by both the owner of the related AWS account and the AWS Organizations master account.

Explanation

Here is how AWS Organizations' SCPs and IAM policies work together:

Users and roles must still be granted permissions with appropriate IAM permission policies. A user without any IAM permission policies has no access, even if the applicable SCPs allow all services and all actions.

If a user or role has an IAM permission policy that grants access to an action that is also allowed by the applicable SCPs, the user or role can perform that action.

If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable SCPs, the user or role can't perform that action.



[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html#scp-effects-on-permissions](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html#scp-effects-on-permissions)

Covered in this lecture

AWS Organizations

Course:Securing AWS Organizations with Service Control Policies (SCPs)



5m



#21

What is AWS Systems Manager?



a service that continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations



a service that monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost



a set of fully managed AWS services that enable automated configuration and ongoing management of systems at scale in a secure and reliable way across all your Linux and Windows instances running on Amazon EC2, your own data center, or other cloud platforms



a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account

Explanation



Systems Manager is a set of fully managed AWS services that enable automated configuration and ongoing management of systems at scale in a secure and reliable way across all your Linux and Windows instances running on Amazon EC2, your own data center, or other cloud platforms.

[!\[\]\(c8d96c8885d3000a912c2582004aed63\_img.jpg\) /course/aws-systems-manager-operational-insights-1699/introduction-to-aws-systems-manager/](#)

#22

Where does AWS Config record resource change information and relevant metadata related to the change?



In a Configuration Item



In an AWS Config rule



In a CloudTrail log



In a Conformance Pack

Explanation

AWS Config can capture resource changes. So any change to a resource supported by Config can be recorded, which will record what change along with other useful metadata all held within a file known as a configuration item, a CI.

It can act as a resource inventory. AWS Config can discover supported resources running within your environment, allowing you to see data about that resource type.

[!\[\]\(4f6bf54ae7e4144a72d78316053e412d\_img.jpg\) /course/aws-management-fundamentals/aws-config-2/](#)

Covered in this lecture

What is AWS Config?

Course: Audit, Monitor & Evaluate with AWS CloudTrail & AWS Config

6m



#23



What is the general workflow of AWS Systems Manager?



Group your AWS resources, examine your AWS resources' relevant operational data via dashboards, and take action to mitigate any issues reported.



View your resources via dashboards and take action to mitigate any issues reported.



Take action to mitigate any issues reported, group your AWS resources, and examine your AWS resources' relevant operational data via dashboards.



Examine your AWS resources' relevant operational data via dashboards, group your AWS resources, and take action to mitigate any issues reported.

Explanation

In general, using Systems Manager entails grouping your AWS resources, examining their relevant operational data via dashboards, and, finally, taking action to mitigate any issues reported.



[/course/aws-systems-manager-operational-insights-1699/systems-manager-requirements-and-building-blocks/](#)

#24

What is AWS Organizations?



a service that provides a means of centrally managing and categorizing multiple AWS accounts that you own, bringing them together into a single organization



a service that enables you to assess, audit, and evaluate the configurations of your AWS resources



a service that makes it easier to manage your software licenses from vendors such as Microsoft, SAP, Oracle, and IBM across AWS and on-premises environments



a service that enables you to launch and manage virtual private servers

Explanation

For those not familiar with AWS Organizations, it's a service that provides a means of centrally managing and categorizing multiple AWS accounts that you own, bringing them together into a single organization.



[/course/using-aws-firewall-manager-centrally-manage-firewall-rules-multiple-accounts-2258/aws-firewall-manager-and-prerequisites/](#)

#25

What allows you to add a level of customization to the type of API requests you want the corresponding trail to capture?



Event selectors



CloudTrail Logs



Events



CloudWatch Logs

Explanation

Event selectors allow you to add a level of customization to the type of API requests you want the corresponding trail to capture.



[/course/aws-cloudtrail-introduction/](#)

Covered in this lecture

How does AWS CloudTrail work?

Course:AWS CloudTrail: An Introduction

6m



