

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

 [cloudacademy.com/quiz/exam/3795230/results](https://cloudacademy.com/quiz/exam/3795230/results)

#1

Which of the following actions is not a best practice for AWS resource tagging?



Audit and maintain your tags.



Maximize the number of different tags you adopt.



Automate tag management.



Set up policies to forbid launching untagged resources.

Explanation

Let's look at some tagging best practices. Limit the number of tags you adopt. Automate tag management. Set up policies to forbid launching untagged resources. And, finally, audit and maintain your tags.



</course/aws-cost-management-tagging-1696/tagging-best-practices/>

#2

An AWS CloudFormation \_\_\_\_\_ allows you to create, update, or delete your stacks across a number of AWS accounts in different regions with a single template.



StackSet



stack instance



stack policy



stack trigger

Explanation

StackSets allow you to create, update, or delete your stacks across a number of AWS accounts in different regions with a single template.



[/course/aws-cloudformation-introduction-infrastructure-code/components-of-cloudformation/](#)

[Covered in this lecture](#)

[Components of AWS CloudFormation](#)

[Course:AWS CloudFormation: Introduction to Infrastructure as Code](#)



4m



#3

How does AWS CloudFormation make it easier for others to review and verify your code?



The entire infrastructure is deployed via scripted code, which allows it to be reviewed easily.



Code reviews and comments are managed automatically in AWS CloudFormation using SNS messages.



Code reviews and comments are managed automatically in AWS CloudFormation using AWS Lambda functions.



It allows you to deploy the same level of infrastructure and resources across multiple regions.

Explanation

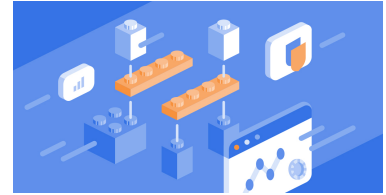
Simply Code: As the entire infrastructure is deployed via scripted code, it may make it easy for other members of your team or people outside of the team to review and verify your code to ensure that it's correct before deployment.

[/course/aws-cloudformation-introduction-infrastructure-code/what-aws-cloudformation/](#)

Covered in this lecture

Summary

Course:AWS CloudFormation: Introduction to Infrastructure as Code



3m



#4

Which of the following services lets you easily visualize and analyze your data, create detailed and precise visualizations, and then publish your dashboards and analyses?



Amazon QuickSight



Amazon Athena



AWS Glue



Amazon Rekognition

Explanation

Amazon QuickSight lets you easily visualize and analyze your data. Similar to Athena, you can put datasets from AWS and outside sources into the service and let it process the data for you for easier exploration and deeper analysis. What's more, you can create outstandingly detailed and precise visualizations. Moreover, the service lets you publish and share your dashboards and analyses with anyone, regardless of the receiver's AWS knowledge.

[/course/aws-cost-management-visualizing-costs-1772/amazon-quicksight/](#)

#5

AWS \_\_\_\_\_ reports include items for each unique combination of product, usage type, and operation that is used in your AWS environment.



cost and usage



financial



KPI



efficiency and resource

Explanation

With the help of AWS cost and usage reports, you can track the monthly AWS costs and usage associated with your AWS account. The report includes items for each unique combination of product, usage type, and operation that is used in your AWS environment.



</course/aws-cost-management-tagging-1696/tagging/>

#6

The AWS \_\_\_\_\_ is a complex CSV file that stores all details about your cost and usage data for all AWS resources.



Financial Report (FR)



Recurrent Charges Report (RCR)



Billing Report (BR)



Cost and Usage Reports (CUR)

Explanation

The CUR is a pretty complex CSV file that stores all details about your cost and usage data for all AWS resources. Enabling the CUR is super important because it's the most granular and detailed mechanism with which to collect data for AWS costs and usage. It offers historical by-the-hour data that can offer clarity on trends and lead to a more accurate data-driven insight.

[!\[\]\(f4912148590488019602cab6e009e597\_img.jpg\) /course/aws-cost-management-tools-1299/cost-and-usage-reports/](#)

#7

The \_\_\_\_\_ contains details of all the logs delivered within the last hour along with a hash for each of them.



Digest file



Hash File



Log File



Data File

Explanation

CloudTrail creates a new file every hour, called a digest file, which is used to help verify your log files have not changed. The digest file contains details of all the logs delivered within the last hour along with a hash for each of them.

[!\[\]\(0fb13ad0bfa3d86868cdd3883e5665b3\_img.jpg\) /course/how-implement-enable-logging-across-aws-services-part-1-2/cloudtrail-](#)

[logging/](#)

[Covered in this lecture](#)

[CloudTrail Logging](#)

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

17m

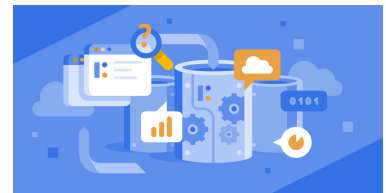


#8

What is an AWS CloudFormation stack?



a JSON or YAML file that describes your environment and resources to build within your account



✗

a tool that allows you to replicate existing infrastructure that wasn't deployed using CloudFormation

✓

a set of AWS resources that you can provision, update, or delete all at once

✗

a tool that allows you to visually create your environment through a drag-and-drop interface, which allows CloudFormation to automatically create a template based off of your design

Explanation

A CloudFormation stack is a set of AWS resources that you can provision, update, or delete all at once.



[/course/aws-cloudformation-introduction-infrastructure-code/components-of-cloudformation/](#)

Covered in this lecture

Summary

Course:AWS CloudFormation: Introduction to Infrastructure as Code



3m



#9

In AWS, \_\_\_\_\_ allow the user to receive notifications when costs or usage exceed a certain predefined amount.

✓

budgets

✗

quotas

✗

thresholds

✗

alarms

## Explanation

Budgets allow the user to get notified when costs or usage exceed a certain predefined amount.

 [/course/aws-cost-management-tools-1299/budgets/](#)

#10

AWS Artifact reports are known as \_\_\_\_\_.



compliance agreements



SOC artifacts




audit artifacts



identity-based policies

## Explanation

AWS Artifact reports consist of AWS auditor-issued reports and include everything from ISO certifications to PCI and SOC reports. These reports, known as audit artifacts, may be shared with auditors and regulators by creating IAM users with an associated identity-based policy that grants access only to the necessary reports.

 [/course/how-find-compliance-data-using-aws-artifact-2529/finding-compliance-data-with-aws-artifact/](#)

#11

To enable logging for your CloudFront distribution, the user account activating that feature need to have access to which of the policies? (Choose 2 answers)



S3 GetBucketAcl



S3 PutBucketAcl

✗

S3 GetObjectAcl

✗

S3 PutObjectAcl

Explanation

To enable logging for your distribution, the user account activating that feature must have full control on the ACL for the S3 bucket, along with the S3 GetBucketAcl and S3 PutBucketAcl.

[/course/how-implement-enable-logging-across-aws-services-part-2-2/cloudfront-access-logs/](#)

[Covered in this lecture](#)

[Course Summary](#)

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



5m



#12

Which of the following actions is not a best practice for AWS resource tagging?

✗

Keep the number of different tags as low as necessary, but the information value of each tag as high as possible.

✓

Tag maintenance should involve at most one or two people from the team.

✗

Make it a habit to review tags from time to time and verify their purpose.

✗

Make use of tools like the AWS tag editor to automate your tagging.

Explanation



Let's look at some tagging best practices. Obviously, the more tags you have, the more tags you have to deal with. Keep the number as low as necessary, but the information value as high as possible. Make use of tools like the AWS Tag Editor to automate your tagging. Make it a habit to review tags from time to time and verify their purpose. Tag maintenance is essential and should involve everyone on the team.

 </course/aws-cost-management-tagging-1696/tagging-best-practices/>

#13

\_\_\_\_\_ allows you to capture IP traffic information that travels between the network interfaces of your resources within your VPC.



VPC Flow Logs



Data Logs



IP Logs



CloudFront access logs

Explanation

VPC Flow Logs allows you to capture IP traffic information that flows between your network interfaces of your resources within your VPC.

 </course/how-implement-enable-logging-across-aws-services-part-2-2/vpc-flow-logs/>

Covered in this lecture

Course Summary

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

5m



#14

\_\_\_\_\_ tags are special tags that are used by Cost Explorer and other services for allocation and visualization.





Simple Resource Name



Cost allocation



Environment



Cost visualization

Explanation

Cost allocation tags are special tags that are used by Cost Explorer and other services for allocation and visualization.



</course/aws-cost-management-tagging-1696/aws-generated-cost-allocation-tags/>

#15

Which of the following actions is not a best practice for AWS resource tagging?



Use a consistent tag naming convention.



Tag as few resources as possible.



Think of a certain use case before adding a tag.



Find redundancies and overlapping tags and simplify them.

Explanation

Let's look at some tagging best practices. Tag everything. Tag as many resources as possible so that no resource is left untagged. Make this a rule. Next, find a purpose for each tag. Think of a certain use case before adding a tag. Find redundancies and overlapping tags and simplify them. Next, consistency is key. Use a consistent naming convention.

</course/aws-cost-management-tagging-1696/tagging-best-practices/>

#16

Which AWS Glue component can scan data in all kinds of repositories, classify it, extract schema information from it, and store the metadata automatically?



AWS Glue Crawlers



AWS Glue Data Catalog



AWS Glue ETL Operations



AWS Glue Jobs system

Explanation

AWS Glue also lets user set up crawlers that can scan data in all kinds of repositories, classify it, extract schema information from it, and store the metadata automatically in the AWS Glue Data Catalog. The AWS Glue Data Catalog can then be used to guide ETL operations.

</course/developing-serverless-etl-aws-glue/overview-aws-glue/>

Covered in this lecture

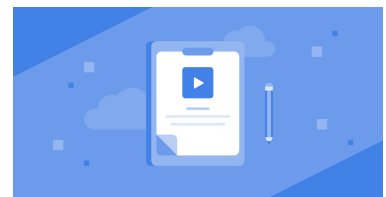
Summary

Course:Developing Serverless ETL with AWS Glue

3m



#17



Which of the following are use cases for AWS Glue? (Choose 3 answers)



Queries against an Amazon S3 data lake



Unified view of data across multiple data stores




Analyze log data in data warehouse



Generate the schema for structured data

Explanation

We can use the AWS Glue Data Catalog to quickly discover and search across multiple AWS data sets without moving the data. Once the data is cataloged, it is immediately available for search and query using Amazon Athena, Amazon EMR, and Amazon Redshift Spectrum. AWS Glue generates the schema for User semi-structured data, creates ETL code to transform, flatten, and enrich User data, and loads User data warehouse on a recurring basis.

 </course/developing-serverless-etl-aws-glue/glue-introduction/>

Covered in this lecture

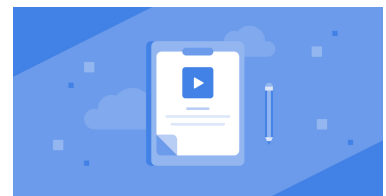
An overview of AWS Glue

Course: Developing Serverless ETL with AWS Glue

9m



#18



In AWS Cost Explorer, \_\_\_\_\_ costs represent your usage costs on the day that they are charged to you, or, in finance terms, they represent your costs on a cash basis of accounting.



standard



recurrent



unblended



amortized

Explanation

The unblended costs represent your usage costs on the day that they are charged to you, or, in finance terms, they represent your costs on a cash basis of accounting.

 </course/aws-cost-management-tools-1299/cost-explorer/>

#19

Arrange the following steps in the correct order for creating an AWS Glue Crawler. A. Create a new name for Crawler. B. Create the schedule for this crawler and configure the crawler's output. C. Choose a data store for the crawler and include a path to the data store.

✗

A - B - C

✗

B - C - A

✓


A - C - B

✗

B - A - C

Explanation

Firstly, name crawler. User must then choose a data store and include a path to it and here User might include aced glued patterns. Optionally, add another data store, select the IAM row or create a new one. Create the schedule for this crawler, configure the crawler's output and in this step, User must add or select an existing database which contains tables created by the crawler User are creating and finally there are other configuration options as per the requirments.

 </course/developing-serverless-etl-aws-glue/overview-aws-glue/>

Covered in this lecture

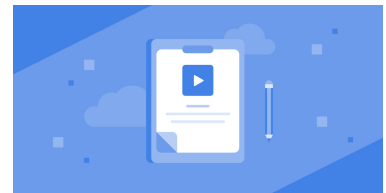
An overview of AWS Glue

Course:Developing Serverless ETL with AWS Glue

9m



#20



What is the purpose of AWS CloudFormation?



to provision infrastructure resources via a simple template in a YAML or JSON format



to connect to, configure, and provision an RDS or DynamoDB database



to create a Virtual Private Cloud with both private and public subnets with Network Access Control Lists for security



to introduce autoscaling and elastic load balancers for higher variability

Explanation

Now, by using AWS CloudFormation you can provision all of your infrastructure resources that you require via a simple template in a YAML or JSON format.

 [/course/aws-cloudformation-introduction-infrastructure-code/what-aws-cloudformation/](#)

[Covered in this lecture](#)

[Summary](#)

[Course:AWS CloudFormation: Introduction to Infrastructure as Code](#)

[3m](#)



#21



When a log file is delivered to an S3 bucket, CloudTrail creates a \_\_\_\_\_ which is a set of unique characters created from a data source.



Hash File



Log File



Data File



Action File

Explanation

When a log file is delivered to an S3 bucket a hash is created for it by CloudTrail. A hash file is a set of characters that are unique that are created from a data source.

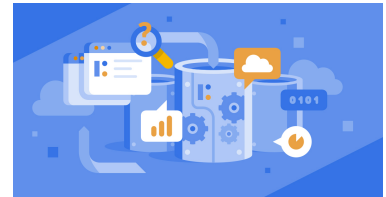


[/course/how-implement-enable-logging-across-aws-services-part-1-2/cloudtrail-logging/](#)

[Covered in this lecture](#)

[CloudTrail Logging](#)

[Course:How to Implement & Enable Logging Across AWS Services \(Part 1 of 2\)](#)



17m



#22

With \_\_\_\_\_, AWS introduced a sort of reward system for particularly active users and developers.



billing



credits



vouchers



rewards

Explanation

With credits, AWS introduced a sort of reward system for particularly active users and developers. You can use them instead of spending money on certain services.



[/course/aws-cost-management-tools-1299/credits/](#)

#23

In AWS Cost Explorer, \_\_\_\_\_ costs are a powerful tool if you seek to gain insight into the effective daily costs associated with your reservation portfolio, or when you are looking for an easy way to normalize costs and usage information when operating at scale.



standard



recurrent



unblended



amortized

Explanation

Amortized costs are a powerful tool if you seek to gain insight into the effective daily costs associated with your reservation portfolio, or when you are looking for an easy way to normalize costs and usage information when operating at scale.

 </course/aws-cost-management-tools-1299/cost-explorer/>

#24

To install the CloudWatch Logs agent on EC2 instances to send data back to CloudWatch, you need to correctly configure an IAM role and attach it to your instance. When attaching permissions policies, what option(s) should you select?



Only CloudWatch Agent Server Policy



Only Amazon EC2 Role for SSM



CloudWatch Agent Server Policy and with Amazon EC2 Role for SSM



Only Amazon Cloudwatch service role for SSM

Explanation



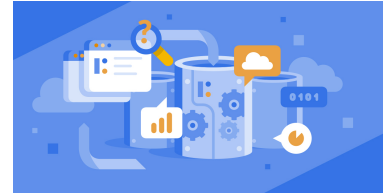
The role that is simply used to install the agent and send data back to CloudWatch needs the following configuration, the 'select type of trusted identity' needs to be 'AWS service'. The option 'choose the service that will use this role' needs to be 'EC2 Allows EC2 instances to call AWS services on your behalf'. And finally under the 'Attach Permissions Policies' it needs to be 'CloudWatch Agent Server Policy' and 'Amazon EC2 Role for SSM'.

[!\[\]\(c8d96c8885d3000a912c2582004aed63\_img.jpg\) /course/how-implement-enable-logging-across-aws-services-part-1-2/cloudwatch-logging-agent/](#)

Covered in this lecture

CloudWatch Logging Agent

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



16m



#25

Which of the following statements about audit artifacts in AWS Artifact is false?



They can and should inform the security controls you choose to implement as part of your own cloud architecture and solution design.



The compliance reports provided within AWS Artifact certify the security/compliance of your company, organization, or application.



They allow you to provide evidence of AWS security controls to ensure compliance with any applicable governance, regulations, or frameworks when architecting solutions in the AWS cloud.




They may be shared with auditors and regulators by creating IAM users with an associated identity-based policy that grants access only to the necessary reports.

Explanation

These reports, known as audit artifacts, may be shared with auditors and regulators by creating IAM users with an associated identity-based policy that grants access only to the necessary reports. And these audit artifacts allow you to provide evidence of AWS security controls to ensure compliance with any applicable governance, regulations, or frameworks

when architecting solutions in the AWS cloud. Now, of course, this is always done in accordance with the AWS Shared Responsibility Model, where AWS is responsible for the underlying security OF the cloud, but you remain responsible for your own systems' and applications' security IN the cloud. However, these audit artifacts can and should inform the security controls you choose to implement as part of your own cloud architecture and solution design.

 [/course/how-find-compliance-data-using-aws-artifact-2529/finding-compliance-data-with-aws-artifact/](#)