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

cloudacademy.com/quiz/exam/3792269/results

#1

Which of the following statements about IAM policy evaluation in AWS is false?

✓

An explicit allow will always take precedence over a deny.

✗

If a single deny exists within any policy associated with the same principle against the same resource, then that deny will overrule any previous allow that might exist for the same resource and action.

✗

By default, all access to a resource is denied.

✗

Access to a resource is only allowed if an allow has been specified within a policy associated with the principle.

Explanation

The rules for reviewing permissions across multiple policies in a single account are actually quite simple and can be summarized like this: by default, all access to a resource is denied. Access will only be allowed if an allow has been specified within a policy associated with the principle. If a single deny exists within any policy associated with the same principle against the same resource then that deny will overrule any previous allow that might exist for the same resource and action. So to reiterate, an explicit deny will always take precedence over an allow.

/course/using-iam-policies-define-manage-permissions-2256/policy-evaluation-logic/

#2

In AWS IAM, ______ allow(s) credentials external to AWS to be used as a means of authentication to your AWS resources.

✗

AWS Managed Policies

✗

Multi-Factor Authentication

✗

STS

✓

Federated Access

Explanation

Federated Access allows credentials external to AWS to be used as a means of authentication to your AWS resources.

/course/aws-iam-used-securely-manage-access-1843/iam-features/

#3

In cross-account access, _____ allow users and other AWS services and applications to adopt a set of temporary IAM permissions to access AWS resources.

✗

provisional access configurations

✓

IAM roles

✗

multi-factor authentications

✗

firewalls

Explanation

IAM roles allow users and other AWS services and applications to adopt a set of temporary IAM permissions to access AWS resources.

/course/implementing-cross-account-access-using-iam/implementing-cross-account-access-using-iam/

Covered in this lecture

Implementing Cross-Account Access Using IAM
Course:Implementing Cross-Account Access Using IAM

11m

#4

Which of the following lists correctly represents the order in which IAM policies are evaluated whenever someone tries to access a resource within AWS?

✕

IAM permission boundaries, Organizational Service Control, resource-based, identity-based

✕

resource-based, IAM permission boundaries, identity-based, Organizational Service Control

✓

Organizational Service Control, resource-based, IAM permission boundaries, identity-based

✕

identity-based, resource-based, Organizational Service Control, IAM permission boundaries

Explanation

There is an order in which policies are evaluated, and the following list of policies are shown in the order of evaluation. So firstly, we have any Organizational Service Control policies, then any resource-based policies, then IAM permission boundaries, and then, finally, identity-based policies.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

#5

In AWS, ______ allows you to create a customer-managed IAM policy by selecting options from a series of dropdown boxes.

✕

Policy Config

✓

Policy Generator

✕

Policy Maker

✕

Policy Studio

Explanation

We can use the Policy Generator, and this allows you to create a customer-managed policy by selecting options from a series of dropdown boxes.

🔗 /course/using-iam-policies-define-manage-permissions-2256/creating-an-aws-iam-policy/

#6

______ allows IAM users from one AWS account to access services within a different AWS account through the use of IAM roles.

✓

Cross-account access

✕

Multi-factor authentication

✕

Trusted account isolation

✕

Third-party authentication

Explanation

Let me quickly define what cross-account access is. Put simply, it allows IAM users from one AWS account to access services within a different AWS account through the use of IAM roles.

🔗 /course/implementing-cross-account-access-using-iam/implementing-cross-account-access-using-iam/

Covered in this lecture

Implementing Cross-Account Access Using IAM

Course:Implementing Cross-Account Access Using IAM

11m

#7

In AWS IAM, ______ are used for programmatic access to your AWS resources.

✗

auth certificates

✗

path structures

✗

MFAs

✓

access keys

Explanation

Access keys are used for programmatic access to your AWS resources, and they are comprised of two elements.

🔗 /course/managing-user-identities-long-term-credentials-aws-iam-1960/overview-of-the-user-dashboard/

#8

In AWS IAM, the ______ shows you which services a user can access, based on their current permissions, and also the last time that these services were accessed.

✗

Path Analyzer

✗

ARN

✓

Access Advisor

✗

RDS Policy

Explanation

We will go back up to the top to Access Advisor; I just wanted to show you this quickly. So what this does is that it will basically show you which services this user can access based on their current permissions, and also the last time that these services were accessed.

/course/managing-user-identities-long-term-credentials-aws-iam-1960/managing-iam-users/

#9

Why is it recommended to apply permissions to the group instead of individual users when configuring IAM?

✗

Group access is more secure than user access.

✗

Users who access resources programmatically are difficult to authenticate.

✓

Group access is less time-consuming to configure than user access.

✗

User access keys are sometimes faulty and must be reconfigured periodically.

Explanation

Group access is less time-consuming to configure than user access and for this reason, it is a recommended method for granting permission because multiple users can be granted permissions as part of a group. Group access is not more secure than user access, it is not difficult to authenticate users who access resources programmatically, and faulty user access keys that need to be reconfigured are not reasons for applying permissions to groups rather than users.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

#10

Which element of an AWS IAM policy can be set to either Allow or Deny?

✗

condition

✗
statement

✓
effect

✗
action

Explanation

Effect: This element can be set to either Allow or Deny, which either grants or restricts access to the actions defined in the statement.

🔗 /course/using-iam-policies-define-manage-permissions-2256/examining-the-json-policy-structure/
#11

______ used within AWS IAM are written as JSON documents and define what can and can’t be accessed.

✓
Policies

✗
Rules

✗
Roles

✗
User groups

Explanation

Policies used within IAM are written as JSON documents, and these define what can and can’t be accessed.

🔗 /course/aws-iam-used-securely-manage-access-1843/iam-features/
#12

In AWS IAM, a(n) ______ policy is one that is embedded within the user object itself.

✗
user

✗
role

✓
inline

✗
group

Explanation

At the top of the Permissions tab, we can add an inline policy for this user. So if we do that, then that will be a policy that is embedded within the user object itself.

/course/managing-user-identities-long-term-credentials-aws-iam-1960/managing-iam-users/
#13

What is the first step in the sequence of steps required to implement cross-account access using AWS IAM?

✗
Create a role from within the trusted account.

✗
Test the configuration by switching to the new role.

✓
Create a role from within the trusting account.

✗
Specify the permissions attached to the newly created role, which the users in the trusted account would assume to carry out their required actions and tasks.

Explanation

Let me break the process down. Firstly, you must create a role from within the trusting account, which, in our example, would be the production account. This is to establish a trust between the two accounts. This role will define the development account as a trusted entity.

Next, you must specify the permissions attached to this newly created role, which the users in the development account would assume to carry out their required actions and tasks. Next, you must switch to the trusted account--in this scenario the development account--to grant permissions to your developers to allow them to assume the newly created role in the trusted account. Finally, you can test the configuration by switching to the role.

/course/implementing-cross-account-access-using-iam/implementing-cross-account-access-using-iam/
Covered in this lecture
Implementing Cross-Account Access Using IAM
Course:Implementing Cross-Account Access Using IAM

11m

#14

What is the recommended last step in the sequence of steps to implement cross-account access using AWS IAM for a small company using two accounts?

✗

Create a role from within the trusted account.

✓

Test the configuration by switching to the new role.

✗

Use AWS SSO create access for new AWS users

✗

Specify the permissions attached to the newly created role.

Explanation

Let me break the process down. Firstly, you must create a role from within the trusting account, which would be the production account in our example. This is to establish a trust between the two accounts. This role will define the development account as a trusted entity. Next, you must specify the permissions attached to this newly created role, which the users in the development account would assume to carry out their required actions and tasks. Next, you must switch to the trusted account--in this scenario the development account--to grant permissions to your developers to allow them to assume the newly created role in the trusted account. Finally, you can test the configuration by switching to the role.

🔗 https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

Covered in this lecture

Introduction

Course:Implementing Cross-Account Access Using IAM

1m

#15

In AWS IAM, configuring ______ allows for an additional level of verification to be applied: namely, the user will have to enter a random six-digit number from a linked device after their usual password.

✗

AWS Managed Policies

✓

Multi-Factor Authentication

✗

STS

✗

Federated Access

Explanation

Configuring MFA allows for an additional level of verification to be applied. The user will have to enter a random six-digit number from a linked MFA device after their usual password.

🔗 /course/aws-iam-used-securely-manage-access-1843/iam-features/

#16

Which of the following describes IAM groups? (Choose 2 answers)

✓

IAM groups contain users

✓

IAM groups have IAM policies assigned to them

✗

IAM groups are used for authentication

✗

IAM groups are shared by an unlimited number of users by default

Explanation

IAM Groups containing IAM Users will have IAM policies associated with them that will allow or explicitly deny access to AWS resources. These policies are either AWS Managed policies that can be selected from within IAM, or customer-managed policies that are created by you, the customer.

IAM Groups are objects much like user objects, however, they are not used in any authentication process, but they are used to authorize access to AWS resources through the use of AWS Policies.

Groups are normally created that relate to a specific requirement or job role and can contain many users; however, the number and size of IAM resources in an AWS account are limited.

🔗 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

#17

AWS IAM can be defined by its ability to ______.

✗

provide hardware-based key storage for regulatory compliance

✗

provision, manage, and deploy SSL/TLS certificates

✓

manage, control, and govern authentication, authorization, and access control mechanisms of identities to your resources within your AWS account

✗

manage creation and control of encryption keys

Explanation

Essentially, IAM can be defined by its ability to manage, control, and govern authentication, authorization, and access control mechanisms of identities to your resources within your AWS account.

🔗 /course/aws-iam-used-securely-manage-access-1843/what-is-identity-and-access-management/