

# Exam Session - Knowledge Check: Overview of AWS Identity and Access Management (IAM)

 [cloudacademy.com/quiz/exam/3758622/results](https://cloudacademy.com/quiz/exam/3758622/results)

#1

For IAM user, a virtual Multi-Factor Authentication (MFA) device uses an application that generates \_\_\_\_\_-digit authentication codes that are compatible with the time-based one-time password (TOTP) standard.



six



two



four



five

## Explanation

A virtual MFA device uses an application that generates six-digit authentication codes that are compatible with the time-based one-time password (TOTP) standard.

Therefore, any application that you wish to use in order to make your smart phone your virtual MFA device needs to conform with the standard.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_enable\\_virtual.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html)

Covered in this lecture

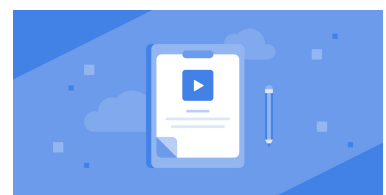
Multi-Factor Authentication (MFA)

Course: Security & Compliance (SOA-Co2)

6m



#2



As you begin developing your new mobile app, you start reviewing options for identity federation and choose Amazon as your identity provider. When using a web identity provider to enable federated AWS access, what security consideration should you keep in mind?



Provide a “root” role to all users to ensure they can use the entire AWS platform.



Ask the user when they login for their desired permissions and pass this to your app.



Secure roles to ensure users have limited access to only the resources required by the app.



Ensure that the web identity provider defines the roles you expect to use in AWS.

#### Explanation

We strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

#3

A system admin has created the policy given below and applied it to an S3 object named aws.jpg. The aws.jpg is inside a bucket named cloudacademy. What does this policy define?

```
"Statement": [{  "Sid": "Stmt1388811069831",  "Effect": "Allow",  "Principal": { "AWS": "*" },  "Action": ["s3:GetObject"],  "Resource": [ "arn:aws:s3:::cloudacademy/aws.jpg" ] }]
```



The policy converts all the objects bucket cloudacademy to public and allows access to all objects in the bucket.



The policy makes the object 'aws.jpg' in bucket 'cloudacademy' readable to all AWS accounts.



The policy converts the bucket 'cloudacademy' to public.

✗

It allows access to the 'cloudacademy' bucket and returns the aws.jpg object.

Explanation

The access policy has some basic elements used in the bucket policies and in the user policies. The elements are: Resources, Actions, Effect, and Principal. This policy statement allows access to the bucket called cloud academy. An object named aws.jpg is stored in the bucket. Because this is a bucket policy, it includes the Principal element, which specifies who gets the permission.

 <http://docs.aws.amazon.com/AmazonS3/latest/dev/access-policy-language-overview.html>

Covered in this lecture

Summary

Course:Increasing Your Security Posture when Using Amazon S3

7m



#4



IAM's policy evaluation logic follows several basic rules. Which statement regarding these rules is incorrect?

✓

An explicit deny never overrides any allows.

✗

By default, all requests receive a default deny, except for requests that use the AWS account's root security credentials.

✗

An explicit allow overrides any default denies.

✗

The order in which the policies are evaluated is not important.

Explanation

The IAM's Policy Evaluation Logic follows several basic rules to determine if certain request is to be allowed or denied. The evaluation algorithm follows the next steps:

1. By default, all requests are denied, except for those that use the AWS account's root security credentials.
2. Every "allow" policy overrides any default "denies."
3. An explicit "deny" overrides any existing "allows."
4. The order in which the policies are evaluated is not important.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage\\_EvaluationLogic.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html)

#5

What is a benefit of using identity federation?



It minimizes the amount of administration required within IAM.



You do not need to configure any IAM policies to control access.



You can use the same user to authenticate multiple users externally to your account.



It allows you to authenticate other users from other AWS accounts.

Explanation


Identity federation allows you to access and manage AWS resources even if you don't have a user account within IAM.

Identity federation allows users from identity providers (IdP) which are external to AWS to access AWS resources securely without having to supply AWS user credentials from a valid IAM user account. An example of an identity provider can be your own corporate Microsoft Active Directory; federated access would then allow the users within it to access AWS. Other forms of identity providers can be any OpenID Connect (OIDC) web provider. Common examples of these are FaceBook, Google & Amazon.

As a result, if you need users to access AWS resources that already have identities that could be used as an identity provider, then you could allow access to your environment using these existing accounts instead of setting each of them up a new identity within AWS IAM. The benefits of this are two-fold:

1. It minimizes the amount of administration required within IAM.

2. It allows for a Single Sign-On (SSO) solution.

 <https://aws.amazon.com/iam/details/manage-federation/>

#6

If a request does not meet all the conditions included in an IAM policy, what will be the result?



A deny



An allow



An explicit allow



None of these

Explanation

If a request does not meet all the conditions included in an IAM policy, the result will be a deny.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage\\_ElementDescriptions.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html)

#7

What is web identity federation?



Use of an identity provider like Google or Facebook to exchange for temporary AWS security credentials.



Use of AWS IAM User tokens to log in as a Google or Facebook user.



Use of an identity provider like Google or Facebook to become an AWS IAM User.

## Explanation

... users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account.

 [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

#8

If a user requires programmatic access to your AWS resources, what is required to authenticate?



Access Keys



MFA activated on the user account



Key pair



A role association

## Explanation

Access keys are comprised of 2 elements:

1. Access Key ID
2. Secret Access Key ID

The Access Key ID is made up of 20 random uppercase alphanumeric characters such as:

**AKJAI15DV7JP24WTLAJA**

The Secret Access Key ID is made up of 40 random upper and lowercase alphanumeric and non-alphanumeric characters such as:

**RvPO/n6NoAw9FFyjANkWBukXds6UI8am5D/BaXGh**

These access keys must be applied and associated with the application that you are using that requires the relevant access. For example, if you were using the AWS CLI to access AWS resources, you would first have to instruct the AWS CLI to use these Access Keys to

authenticate and provide authorization. The method of performing this association varies based on the application and system that you are using. However, once this association has taken place, it ensures that all API request made to AWS are signed with this digital signature.

 <http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys>  
#9

Which type of IAM role is pre-defined, and can only be edited in a limited number of cases?



AWS Service Roles



AWS Service-Linked Roles



Cross-Account Access Roles




Identity Provider Access Roles

Explanation

The method that you use to edit a service-linked role depends on the service. Some services might allow you to edit the permissions for a service-linked role from the service console, API, or CLI. However, after you create a service-linked role, you cannot change the name of the role because various entities might reference the role. You can edit the description of any role from the IAM console, API, or CLI.

For information about which services support using service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column. To learn whether the service supports editing the service-linked role, choose the Yes link to view the service-linked role documentation for that service.

 [https://docs.amazonaws.cn/en\\_us/IAM/latest/UserGuide/using-service-linked-roles.html#edit-service-linked-role](https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/using-service-linked-roles.html#edit-service-linked-role)  
#10

When writing a policy to control access to your Amazon RDS resources, you can use \_\_\_\_\_ in the resource field, to refer to all your resources, or as the last character of a string.



\*



\$



@



#

### Explanation

When writing a policy to control access to your Amazon RDS resources, you can use \* (wildcard) in the resource field, to refer to all your resources, or as the last character of a string, e.g test\* to refer to all the resources whose name starts with 'test'.



<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAM.html>

#11

In AWS Identity and Access Management, roles can be used by an external user authenticated by an external identity provider (IdP) service that is compatible with \_\_\_\_\_ or \_\_\_\_\_. (Choose 2 answers)



Secure Markup Language (SML)



Security Assertion Markup Language 2.0 (SAML 2.0)



ColdFusion Markup Language (CFML)



OpenID Connect (OIDC)

### Explanation

In AWS Identity and Access Management, roles can be used by an external user authenticated by an external identity provider (IdP) service that is compatible with SAML 2.0 (Security Assertion Markup Language 2.0) or OIDC.



 [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_terms-and-concepts.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html)

#12

There are a number of ways to create a customer managed policy, except which of the following choices?



Edit a copy of an existing AWS managed policy



Use the policy generator



Write a policy from scratch



Copy a policy from the AWS marketplace

Explanation

There are a number of ways to create a customer managed policy:

- Copy any AWS managed policy: It is possible to copy an existing AWS managed policy and then edited to create a new customer managed policy
- Policy generator allows you to create a customer managed policy by selecting options from a series of dropdown boxes
- Create Your Own Policy: If you are proficient in JSON and the syntax of IAM policy writing then you can write your own policies from scratch, or paste in a JSON policy from another source

 <https://awspolicygen.s3.amazonaws.com/policygen.html>

Covered in this lecture

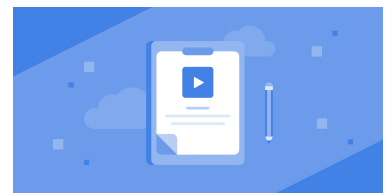
IAM Policies

Course:Security & Compliance (SOA-Co2)

17m



#13



Within an IAM policy, in the \_\_\_\_\_ element, you build expressions in which you use boolean condition operators (equal, less than, etc.) to match the condition in the policy against values in the request.



Condition



Resource



Action



Vendor

Explanation

In the Condition element, you build expressions in which you use boolean condition operators (equal, less than, etc.) to match the condition in the policy against values in the request.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage\\_ElementDescriptions.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html)

#14

Which AWS security component allows Amazon S3 buckets to trigger AWS Lambda functions?



Using an S3 Bucket access control list (ACL)



Using an AWS Organizations service control policy



Using an identity-based policy rule



Using a resource policy rule

## Explanation

When you configure an Amazon S3 bucket to send messages to an AWS Lambda function, a resource policy rule will be created that grants access.

 <http://aws.amazon.com/lambda/faqs/>

#15

A user is included in multiple IAM group policies. One allows read-only access to Amazon EC2 with no actions denied. The other allows full access to Amazon EC2. What happens when this user tries to launch an instance?

✗

The group with least privilege takes precedent. The EC2 instance launch will fail because one IAM group policy has read-only access.

✗

Amazon EC2 will not allow the user to access the service because of the conflict between their two IAM group policies.

✓

Multiple IAM group policies are aggregated. Amazon EC2 will allow the user to launch the instance.

✗

It depends. Only one IAM group policy can apply at a time, depending on how the IAM user has logged into AWS.

## Explanation

The IAM group policy is always aggregated. In this case, if the user does not have permission for one group, but has permission for another group, they will have full access to EC2. Unless there is specific deny policy, the user will be able to access EC2.

 <http://docs.aws.amazon.com/IAM/latest/UserGuide/PoliciesOverview.html>

#16

You can create a cross-account access role between \_\_\_\_\_, and also between \_\_\_\_\_. (Choose 2 answers)

✓

two of your own AWS accounts



your AWS account and an AWS account owned by another party




your account and a web identity provider



a third party account and a web identity provider

Explanation

Roles for Cross-Account Access offers two options. Providing access between AWS accounts that you own, and providing access between an account that you own and an AWS account owned by another party.

 [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_terms-and-concepts.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html)

Covered in this lecture

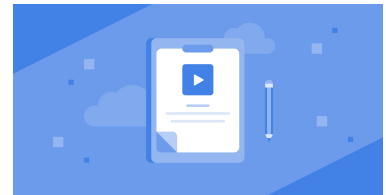
Users, Groups & Roles

Course:Security & Compliance (SOA-Co2)

24m



#17



By default, a brand new IAM user created using the AWS CLI or AWS API \_\_\_\_\_.



has no credentials of any kind.



has a default preset password and credentials, but no permission to access AWS resources or services.



cannot be created without a password.



has a default preset password and a limited, default set of AWS permissions.

Explanation

A brand new IAM user has no password and no access key (neither an access key ID nor a secret access key), and no credentials of any kind. A brand new IAM user has no permissions to do anything. By default, the user is not authorized to perform any AWS actions or to access any AWS resources.

 [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

#18

A(n) \_\_\_\_\_ is a document that provides a formal statement of one or more permissions.



policy



datasource




grant token



artifact

Explanation

A policy is a document that provides a formal statement of one or more permissions.

 [http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

#19

An IAM group is a:



collection of resources that a user can use.



collection of IAM users.



collection of AWS accounts.



group of EC2 machines that gain the permissions specified in the group.

### Explanation

Within the IAM service, a group is regarded as a collection of users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/Using\\_WorkingWithGroupsAndUsers.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html)

Covered in this lecture

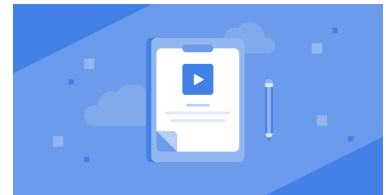
Users, Groups & Roles

Course: Security & Compliance (SOA-Co2)

24m



#20



Which statement about the Sid element of an IAM policy is true?



It is an optional identifier you provide for a policy statement.



It can be used to retrieve a particular statement within an IAM policy.



It specifies whether a statement will result in an allow or an explicit deny.



It is the main element for a policy.

### Explanation

Among the elements that can be added to an IAM policy statement, there is an optional element, namely the Sid that can be included to provide an identifier for a statement inside of a policy. This Sid can't however be used to retrieve a particular statement of a policy and is currently not exposed through the IAM API.



[http://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_elements.html#Sid](http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html#Sid)

Covered in this lecture

Introduction to CISM - Part One

Course:CISM Foundations: Introduction

9m

