OBJECTIVE : SECURE TOKEN SERVICE

Attempt	1
Marks Obtained	6 / 8
Your score is	75%
Completed on	Tuesday , 20 November 2018 , 11:29 AM
Time Taken	00 H 05 M 56 S
Result	Pass

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	8	6	2	0

8 Questions	**6** Correct	**2** Incorrect	**0** Unattempted

Show Answers

All

QUESTION 1 CORRECT

Topic : Implementation and Deployment

You have an on-premise infrastructure which consists of Active Directory. You want you users who have accounts in the Active Directory AD to connect to resources in a federated fashion to AWS. Which of the following roles would suit this purpose

- A. AssumeRoleWithSAML ✔
- B. AssumeRole
- C. AssumeRoleWithWebIdentity
- D. AssumeRoleWithAD

Explanation :

Answer - A
The AssumeRoleWithSAML Returns a set of temporary security credentials for users who have been authenticated via a SAML authentication response. This operation provides a mechanism for tying an enterprise identity store or directory to role-based AWS access without user-specific credentials or configuration.
Option B is invalid because this is the general AssumeRole available
Option C is invalid because this is used for web applications
Option D is invalid because there is no case of AssumeRoleWithAD
For more information on STS with SAML please refer to the below URL:

- http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html (http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html)

Ask our Experts

QUESTION 2 CORRECT

Topic : Implementation and Deployment

What is the default validity of a session token received when using STS with SAML Federation

- A. 1 hour ✔
- B. 12 hours
- C. 24 hours
- D. 5 days

Explanation :

Answer – A
The temporary security credentials are valid for the duration that you specified when calling AssumeRole, or until the time specified in the SAML authentication response's SessionNotOnOrAfter value, whichever is shorter. The duration can be from 900 seconds (15 minutes) to **a maximum of 12 Hours**. The default is 1 hour.
For more information on STS with SAML please refer to the below URL:

- http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html (http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html)

Ask our Experts

QUESTION 3 CORRECT

Topic : Implementation and Deployment

You currently have multiple AWS accounts in your infrastructure. You have a separate account for developers and a separate account for production users. The development users need temporary access to the resources in the production account. Which of the following actions would you take.

- A. Configure Cross Account access ✔
- B. Configure SAML federation
- C. Configure Web Identity Federation
- D. Configure AWS federation

Explanation :

Answer – A
Option B is invalid because this is used for federated access if you have an on-premise identity store.
Option C is invalid because this is if you need access from a web application
Option D is invalid because there is no such case as AWS Federation
The Cross Account Delegation is useful for allowing existing IAM users to access AWS resources that they don't already have access to, such as resources in another AWS account. It is also useful for existing IAM users as a means to temporarily gain privileged access—for example, to provide multi-factor authentication (MFA). You must call this API using existing IAM user credentials
For more information on Cross Account Delegation please refer to the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html)

Ask our Experts

QUESTION 4 CORRECT

Topic : Data Security

You are the architect for an application which will be used to get temporary security credentials from the STS service. You want to ensure that the right permissions are set whenever a request for the credentials are made using STS. Which of the following design principles would you adopt in this case

- **A.** Ensure the right session timeout is placed in the request for the credentials
- **B.** Ensure a policy is passed with each request ✔
- **C.** Ensure the right resource link is passed in each request
- **D.** Ensure the right acccount number is passed in each request

Explanation :

Answer – B
The permission policy of the role that is being assumed determines the permissions for the temporary security credentials returned by AssumeRole, AssumeRoleWithSAML, and AssumeRoleWithWebIdentity. You define these permissions when you create or update the role.
Optionally, you can pass a separate policy as a parameter of the AssumeRole, AssumeRoleWithSAML, or AssumeRoleWithWebIdentity API call. You use the passed policy to scope down the permissions assigned to the temporary security credentials—that is, to allow only a subset of the permissions that are allowed by the permission policy of the role.
For more information on permissions and STS please refer to the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_assumerole.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_assumerole.html)

Ask our Experts

QUESTION 5 CORRECT

Topic : Implementation and Deployment

You are configuring cross account access for users from one AWS account on another AWS account. Before the user assumes a role , you want to add one more layer of security. What can you do in such a scenario

- A. Ensure Cross Account access is configured at the region level
- B. Add MFA to the security process ✔
- C. Use the AssumeRoleWithSAML
- D. Use Web Identity federation as an extra level of security

Explanation :

Answer – B
With IAM policies, you can specify which APIs a user is allowed to call. In some cases, you might want the additional security of requiring a user to be authenticated with AWS multi-factor authentication (MFA) before the user is allowed to perform particularly sensitive actions.
For example, you might have a policy that allows a user to perform the Amazon EC2RunInstances, DescribeInstances, and StopInstances actions. But you might want to restrict a destructive action like TerminateInstances and ensure that users can perform that action only if they authenticate with an AWS MFA device.
For more information on configuring MFA please refer to the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html)

Ask our Experts

QUESTION 6 INCORRECT

Topic : Implementation and Deployment

You have a web application that uses facebook as a login mechanism. This application needs to access a DynamoDB table. Which of the following methods would be used for the application to access the data in the DynamoDB table.

- A. AssumeRoleWithSAML
- B. AssumeRole
- C. AssumeRoleWithWebIdentity ✔
- D. AssumeRoleWithAD ✖

Explanation :

Answer – C
The AssumeRoleWithWebIdentity Returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider.
Option A is invalid because this is used for federated access if you have an on-premise identity store.
Option B is invalid because this is the general assumerole
Option D is invalid because there is no such case as AssumeRoleWithAD
For more information on AssumeRoleWithwebIdentity please refer to the below URL:

- http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html (http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html)

Ask our Experts

QUESTION 7 CORRECT

Topic : Implementation and Deployment

If you need temporary security credentials that could last for more than an hour, which of the following methods can be used for this.

- A. Use the GetCallerIdentity
- B. Use the AssumeRoleWithSAML
- C. Use the GetSessionToken ✔
- D. Use the AssumeRoleWithWebIdentity

Explanation :

Answer - C

The GetSessionToken action must be called by using the long-term AWS security credentials of the AWS account or an IAM user. Credentials that are created by IAM users are valid for the duration that you specify, from 900 seconds (15 minutes) up to a maximum of 129600 seconds (36 hours), with a default of 43200 seconds (12 hours); credentials that are created by using account credentials can range from 900 seconds (15 minutes) up to a maximum of 3600 seconds (1 hour), with a default of 1 hour.
For more information on GetSessionToken please refer to the below URL:

- http://docs.aws.amazon.com/STS/latest/APIReference/API_GetSessionToken.html (http://docs.aws.amazon.com/STS/latest/APIReference/API_GetSessionToken.html)

Ask our Experts

QUESTION 8 INCORRECT

Topic : Designing highly available, cost-efficient, fault-tolerant, scalable systems

A photo-sharing service stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider. Which AWS Security Token Service approach to temporary access should you use for the Amazon S3 operations?

- A. SAML-based Identity Federation ✖
- B. Cross-Account Access
- C. AWS Identity and Access Management roles
- D. Web Identity Federation ✔

Explanation :

Answer – D
With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, 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) (http://openid.net/connect/)-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. Using an IdP helps you keep your AWS account secure, because you don't have to embed and distribute long-term security credentials with your application.
For more information on Web Identity federation please refer to the below URL:

- 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)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14570)

Certification

- Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)
- Java Certification (https://www.whizlabs.com/oracle-java-certifications/)
- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Company

- Support (https://help.whizlabs.com/hc/en-us)
- Discussions (http://ask.whizlabs.com/)
- Blog (https://www.whizlabs.com/blog/)

Mobile App

Android Coming Soon

iOS Coming Soon

Follow us

(https://www.facebook.com/whizlabs.software/)

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

(https://plus.google.com/+WhizlabsSoftware)