



0

[← Back to the Course](#)

Level: Advanced

AWS Certified Security Specialty

Active Directory - Quiz

Completed on Sun, 27 Feb 2022

1st
Attempt0/5
Marks Obtained0.00%
Your Score0h 0m 2s
Time TakenFAIL
Result

Domain wise Quiz Performance Report

Join us on [Slack community](#)

No.	Domain	Total Question	Correct	Incorrect	Unattempted
1	Identity and Access Management	1	0	0	0
2	Identity and Access Management	4	0	0	0
Total	All Domains	5	0	0	0



Review the Answers

Filter By [All Questions](#)

Question 1

Unattempted

Domain: Other

A company is planning to move its on-premises workloads to AWS. They are planning to set up their own Active Directory setup on a set of EC2 Instances. They need to ensure that, for the time being, resources from their on-premises data center can access the Active Directory setup. Which of the following implementation steps need to be carried out? Choose 2 answers from the options given below.

- A. Ensure that the Network ACLs have been set for allowing traffic. right
- B. Ensure that VPC Flow logs have been enabled.
- C. Ensure that the Security Groups have been set for allowing traffic. right
- D. Ensure that the AD connector is in place.

Explanation:

Answer – A and C

This is mentioned in the AWS Documentation.

If you're deploying and managing your own AD DS installation, domain controllers and member servers will require several security group rules to allow traffic for services such as AD DS replication, user authentication, Windows Time services, and Distributed File System (DFS), among others. You should also consider restricting these rules to specific IP subnets that are used within your VPC.

Options B and D are incorrect since these are not key requirements for having the Active Directory setup in place.

For more information on ingress traffic for Active Directory, please visit the below URL

<https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html>

[Ask our Experts](#)

 View Queries



Question 2

Unattempted

Domain: Other

A company is planning to move its on-premises workloads to AWS. They are working on setting up their own Active Directory servers on a set of EC2 Instances. You need to ensure that the network connections

between the newly created AWS EC2 servers and the existing on-premises data servers are stable and private. How can you achieve this?

A. Use the Direct Connect. right

B. Provision a NAT gateway in the public subnet.

C. Use the Remote Desktop gateway.

D. Provision a VPN connection.

Explanation:

Answer - A

Remote desktop gateway servers do require internet access. If we would like our EC2 servers not to have internet access, they can be accessed and managed using a remote desktop gateway that has internet access, and that would be the only server that requires internet access.

In case of the remote desktop gateway, EC2 servers will remain in a private subnet that can only communicate with the remote desktop gateway server to be segregated from the internet completely and have no internet access.

Remote desktop gateway is usually configured with full internet access and any IP address on the internet can access it. This can be restricted using security groups.

VPN is a point-to-point (site-to-site) connection that cannot be accessed unless you are on the private network of either end of the VPN connection/tunnel.

Direct Connect is the only service that doesn't require internet and would be faster and more secure than VPN/remote gateway.

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

Ask our Experts



[View Queries](#)

Question 3

Unattempted

Domain: Identity and Access Management

Your company has set up the AWS Managed Microsoft AD directory. Users log in to the AWS console using their AD credentials. They want you to add a security layer for authentication. How can you achieve this?

- A. Allow users to log in with their user name and password.
- B. Enable multi-factor authentication for your AWS Managed Microsoft AD directory. right
- C. Use Access keys along with the user name and password.
- D. Enable multi-factor authentication for the IAM user.

Explanation:

Answer: B

Option A is incorrect because the username and password are the first levels of authentication and the ask would be for an additional layer of authentication after the user credentials.

Option B is CORRECT because you can enable multi-factor authentication (MFA) for your AWS Managed Microsoft AD directory to increase security when your users specify their AD credentials to access Supported Amazon Enterprise Applications. When you enable MFA, your users enter their username and password (first factor) as usual. They must also enter an authentication code (the second factor) they obtain from your virtual or hardware MFA solution. These factors together provide additional security by preventing access to your Amazon Enterprise applications unless users supply valid user credentials and a valid MFA code.

Option C is incorrect because AWS access keys are used for programmatic access to AWS services via CLI or SDK. It cannot provide a second layer of authentication via Microsoft AD.

Option D is incorrect because MFA needs to be enabled on the AD Directory and not on the AWS IAM service.

Reference:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_mfa.html

[Ask our Experts](#)

[View Queries](#)



Question 4

Unattempted

Domain: Other

Your company has set up the AWS Managed Microsoft AD directory. There are on-premises nodes that will be using the AWS Managed Microsoft AD directory for authentication. You need to ensure that all traffic is encrypted in transit. How can you achieve this in the most IDEAL manner?

A. Make use of KMS Keys to encrypt the traffic.

B. Enable LDAP over SSL. right

C. Enable LDAP over HTTPS.

D. Enable Server-side encryption.

Explanation:

Answer – B

This is mentioned in the AWS Documentation.

To mitigate this form of data exposure, AWS Managed Microsoft AD provides an option for you to enable LDAP over Secure Sockets Layer (SSL)/Transport Layer Security (TLS), also known as LDAPS. With LDAPS, you can improve security across the wire and meet compliance requirements by encrypting all communications between your LDAP-enabled applications and AWS Managed Microsoft AD directory.

Since the ideal and correct approach is specified in the AWS Documentation, all other options are incorrect.

For more information on using LDAP in AD, please visit the below URL

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_ldap.html

[Ask our Experts](#)

 [View Queries](#)

**Question 5**

Unattempted

Domain: Other

Your company has set up the AWS Managed Microsoft AD directory service. They need to ensure that users' accounts get locked after a specified number of failed login attempts. How can you achieve this?

- A. Enable LDAP over SSL.
- B. Use Password policies in the directory service. right
- C. Enable MFA for the directory service.
- D. Use IAM Policies.

Explanation:

Answer – B

This is mentioned in the AWS Documentation.

You may also modify the following properties of your password policies to specify if and how Active Directory should lockout an account after login failures:

- Number of failed login attempts allowed
- Account lockout duration
- Reset failed logon attempts after some duration

Option A is incorrect since this is used to encrypt all data in transit.

Option C is incorrect since this is used for adding one more layer of authentication.

Option D is incorrect since this is used for managing access to IAM users.

For more information on supported password policy settings, please visit the below URL

<https://docs.aws.amazon.com/directoryservice/latest/admin-guide/supportedpolicysettings.html>

Ask our Experts

 View Queries



Finish Review

Certification

- Cloud Certification
- Java Certification
- PM Certification
- Big Data Certification

Company

- Become Our Instructor
- Support
- Discussions
- Blog
- Business

Support

- Contact Us
- Help Topics

 **Join us on Slack!**

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!



© 2022, Whizlabs Education INC.

