# Free Questions for NSE7_PBC-7.2

## Shared by Mccoy on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type: MultipleChoice**

How does an administrator secure container environments from newly emerged security threats?

## Options:

**A-** Use distributed network-related application control signatures.

**B-** Use Amazon AWS-related application control signatures

**C-** Use Amazon AWS_S3-related application control signatures

**D-** Use Docker-related application control signatures

## Answer:

D

## Explanation:

Securing container environments from newly emerged security threats involves employing specific security mechanisms tailored to the technology and structure of containers. In this context, the use of Docker-related application control signatures (Option D) is critical for effectively managing and mitigating threats in containerized environments.

Docker-Specific Threats: Docker containers, being a prevalent form of container technology, are targeted by various security threats, including those that exploit vulnerabilities specific to the Docker environment and runtime. Using Docker-related application control signatures means implementing security measures that are specifically designed to detect and respond to anomalies and threats that are unique to Docker containers.

Application Control Signatures: These are sets of definitions that help identify and block potentially malicious activities within application traffic. By focusing on Docker-related signatures, administrators can ensure that the security tools are finely tuned to the operational specifics of Docker containers, thereby providing a robust defense against exploits that target container-specific vulnerabilities.

## Question 2

**Question Type: MultipleChoice**

A customer would like to use FortiGate fabric integration With FortiCNP

When configuring a FortiGate VM to add to FortiCNP, which three mandatory configuration steps must you follow on FortiGate? (Choose three.)

### Options:

**A-** Enable send logs-

**B-** Create and IPS sensor and a firewall policy

**C-** Create an IPsec tunnel.

**D-** Create an SSL]SSH inspection profile.

**E-** Enable two-factor authentication.

## Answer:

A, B, D

## Explanation:

To configure a FortiGate VM to add to FortiCNP, you need to perform three steps on FortiGate:

Enable send logs in FortiGate to allow FortiCNP to receive the IPS logs from FortiGate.

Create an SSL/SSH inspection profile on FortiGate to inspect the encrypted traffic and apply IPS protection.

Create an IPS sensor and a firewall policy on FortiGate to enable IPS detection and prevention for the traffic.

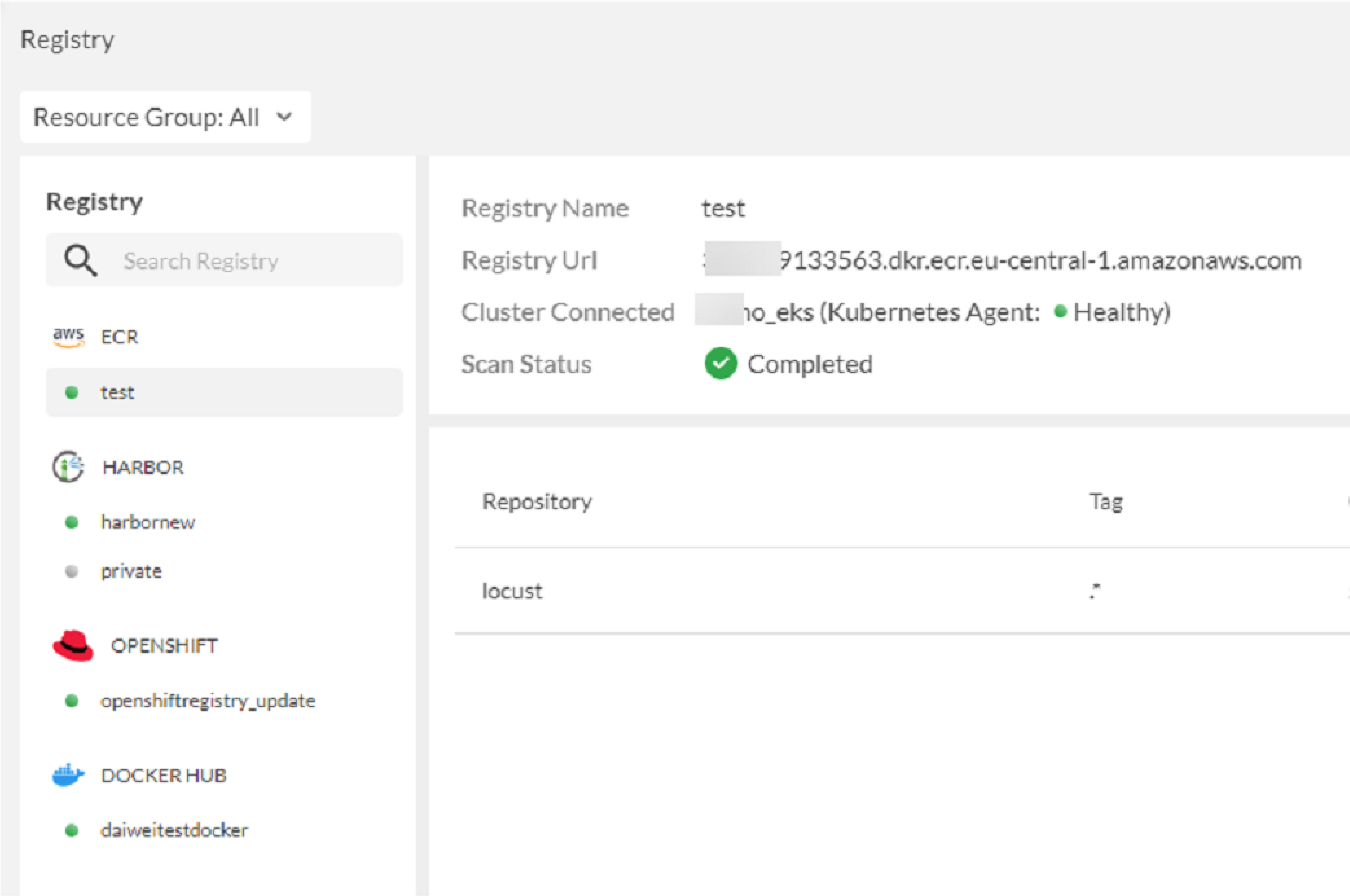
FortiCNP 22.4.a Administration Guide, page 22-24

FortiGate IPS Administration Guide, page 9-10

# Question 3

## Question Type: **MultipleChoice**

Refer to the exhibit



Registry

Resource Group: All

Registry

Search Registry

ECR

- ● test

HARBOR

- ● harbornew
- ● private

OPENSHIFT

- ● openshiftregistry_update

DOCKER HUB

- ● daiweitestdocker

Registry Name test

Registry Url [redacted]9133563.dkr.ecr.eu-central-1.amazonaws.com

Cluster Connected [redacted]o_eks (Kubernetes Agent: ● Healthy)

Scan Status ✓ Completed

| Repository | Tag |
|---|---|
| locust | .* |

The exhibit shows the results of a FortiCNP registry scan

Which two statements are correct? (Choose two )

## Options:

A- When adding a repository, you can leave the Tag section blank to scan all images-

B- The registry scan is part of the FortiCNP cloud protection.

C- The registry scan is part of the FortiCNP container protection.

D- When adding a repository, you can add a minimum number of images to be imported through the CAP section.

## Answer:

A, C

## Explanation:

The exhibit shows the results of a FortiCNP registry scan, which is part of the FortiCNP container protection.FortiCNP's Container Protection provides deep visibility into the security posture of container registries and images1.The registry scan utilizes Common Vulnerabilities and Exposures (CVE) index regularly updated by NVD to detect underlying vulnerabilities, security flaws, and provides security best practices2.The registry scan is performed at the registry level, and it can scan all images in a repository if the Tag section is left blank when adding a repository2.The CAP section stands for Container Assurance Policy, which defines the minimum number of images to be scanned per repository3. Therefore, the correct statements are A and C.Reference:Container Image Scan | FortiCNP

22.3.a,FortiCNP,Cloud Native Application Protection Platform | FortiCNP

# Question 4

**Question Type: MultipleChoice**

When adding the Amazon Web Services (AWS) account to the FortiCNP, which three mandatory configuration steps must you follow? (Choose three.)

## Options:

**A-** Add AWS accounts through FortiCNP.

**B-** Enable cloud protection through AWS Guard Duty and AWS Inspector

**C-** Accept FortiCNP to create CloudTrail for the account

**D-** Enable cross-reg Ion aggregation

**E-** Launch the CloudFormation template.

## Answer:

A, C, E

### Explanation:

When adding the Amazon Web Services (AWS) account to the FortiCNP, you must follow these three mandatory configuration steps:

Add AWS accounts through FortiCNP. This is the first step to enable cloud protection for your AWS account. You can add one or multiple accounts automatically or manually. You need to provide the AWS account ID and a name for the account.You also need to select the optional permissions to be granted to FortiCNP as needed1.

Accept FortiCNP to create CloudTrail for the account. This is required for FortiCNP to collect and analyze the AWS API calls and events. You can choose to let FortiCNP create a CloudTrail for the account or use an existing one.You also need to specify the aggregation region for the CloudTrail1.

Launch the CloudFormation template. This is required for FortiCNP to create a stack and a role in your AWS account. The stack contains the resources that FortiCNP needs to access and monitor your AWS account. The role allows FortiCNP to assume it and perform actions on your behalf.You need to enter a custom or default role name and a unique UUID that is designated for your company on FortiCNP1.

https://docs.fortinet.com/document/forticnp/22.4.a/online-help/246021/add-aws-account-automatically

# Question 5

**Question Type:** MultipleChoice

You are troubleshooting an Azure SDN connectivity issue with your FortiGate VM

Which two queries does that SDN connector use to interact with the Azure management API? (Choose two.)

## Options:

**A-** The first query is targeted to a special IP address to get a token.

**B-** The first query is targeted to IP address 8.8

**C-** There is only one query initiating from FortiGate port1 -

**D-** Some queries are made to manage public IP addresses.

## Answer:

A, D

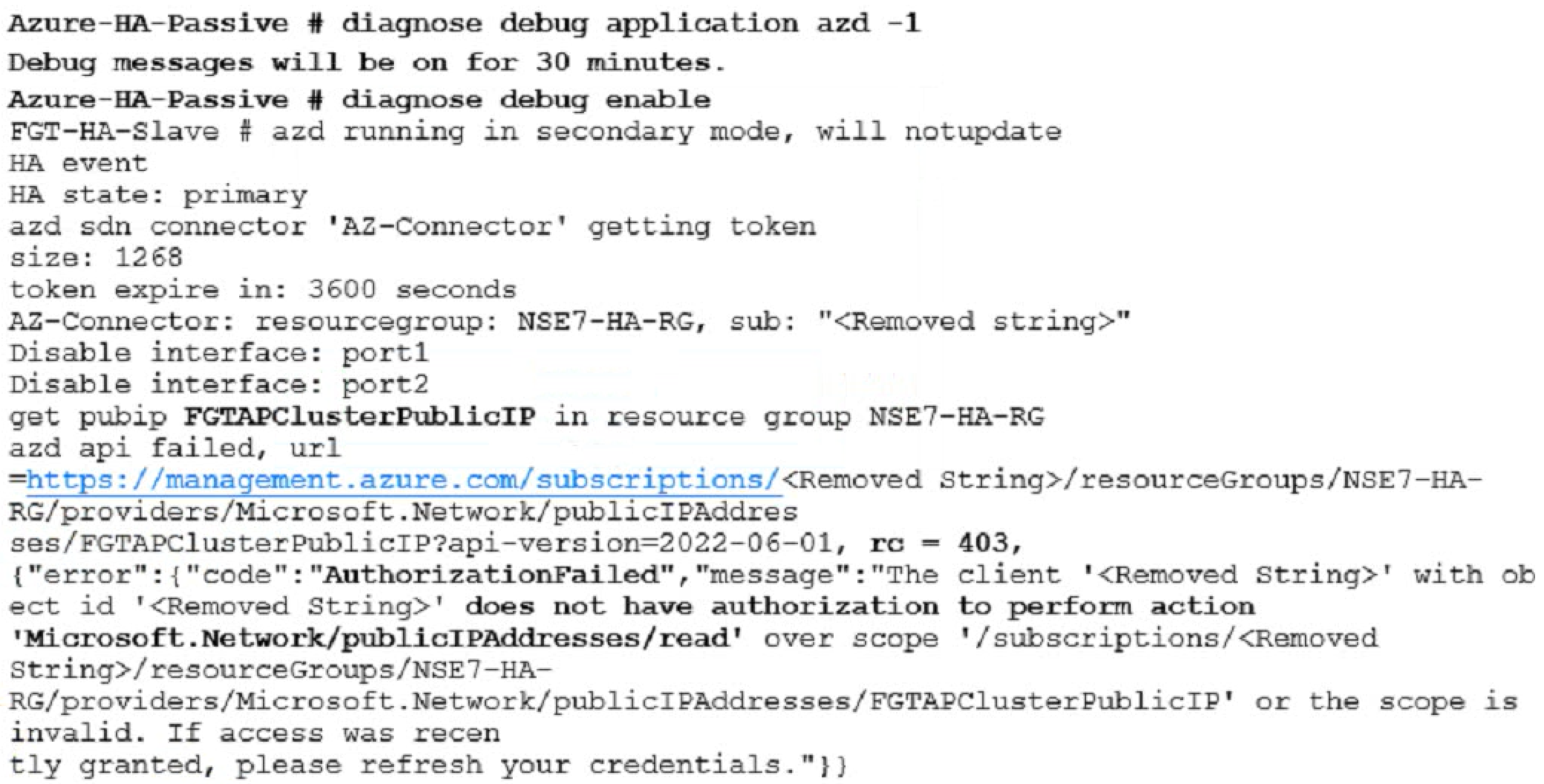
## Explanation:

The Azure SDN connector uses two types of queries to interact with the Azure management API. The first query is targeted to a special IP address to get a token. This token is used to authenticate the subsequent queries. The second type of query is used to retrieve information about the Azure resources, such as virtual machines, network interfaces, network security groups, and public IP addresses. Some queries are made to manage public IP addresses, such as assigning or releasing them from the FortiGate VM.Reference:Configuring an SDN connector in Azure,Azure SDN connector using service principal,Troubleshooting Azure SDN connector

# Question 6

**Question Type: MultipleChoice**

Refer to the exhibit.



```
Azure-HA-Passive # diagnose debug application azd -1
Debug messages will be on for 30 minutes.
Azure-HA-Passive # diagnose debug enable
FGT-HA-Slave # azd running in secondary mode, will notupdate
HA event
HA state: primary
azd sdn connector 'AZ-Connector' getting token
size: 1268
token expire in: 3600 seconds
AZ-Connector: resourcegroup: NSE7-HA-RG, sub: "<Removed string>"
Disable interface: port1
Disable interface: port2
get pubip FGTAPClusterPublicIP in resource group NSE7-HA-RG
azd api failed, url
=https://management.azure.com/subscriptions/<Removed String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddres
ses/FGTAPClusterPublicIP?api-version=2022-06-01, rc = 403,
{"error":{"code":"AuthorizationFailed","message":"The client '<Removed String>' with ob
ect id '<Removed String>' does not have authorization to perform action
'Microsoft.Network/publicIPAddresses/read' over scope '/subscriptions/<Removed
String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddresses/FGTAPClusterPublicIP' or the scope is
invalid. If access was recen
tly granted, please refresh your credentials."}}
```

You are troubleshooting a FortiGate HA floating IP issue with Microsoft Azure. After the failover, the new primary device does not have the previous primary device floating IP

address.

What could be the possible issue With this scenario?

## Options:

**A-** FortiGate port4 does not have internet access.

**B-** A wrong client secret credential is used

**C-** The error is caused by credential time expiration.

**D-** The Azure service principle account must have a contributor role.

## Answer:

D

## Explanation:

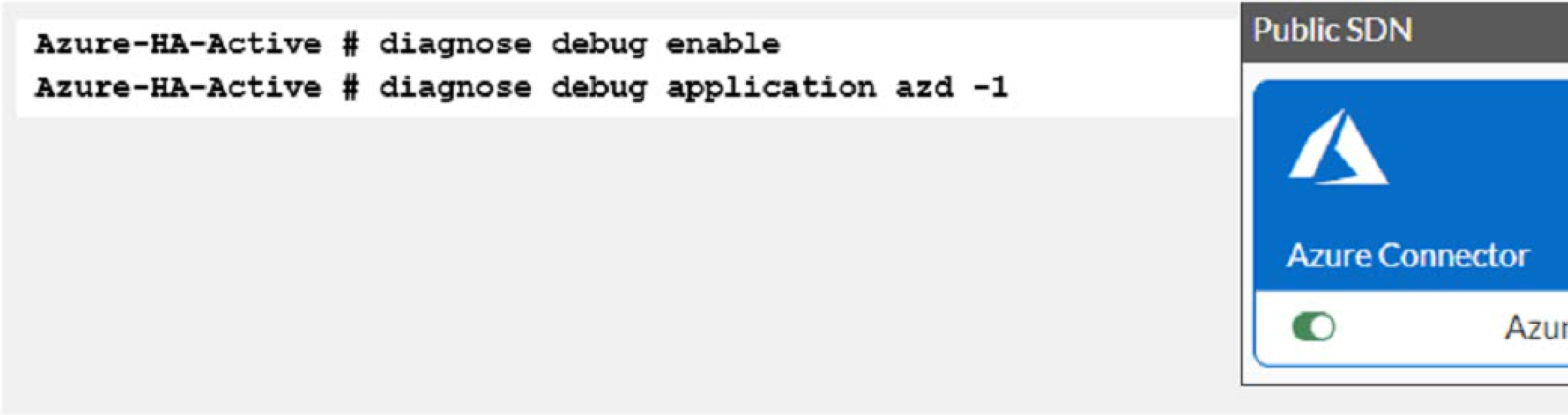
In this scenario, the issue is caused by the Azure service principle account not having a contributor role. This is required for the FortiGate HA floating IP to work properly. Without this role, the new primary device will not have the previous primary device floating IP address after failover.Reference: Fortinet Public Cloud Security knowledge source documents or study guide.

https://docs.fortinet.com/product/fortigate-public-cloud/7.2

# Question 7

**Question Type:** MultipleChoice

Refer to Exhibit:



```
Azure-HA-Active # diagnose debug enable
Azure-HA-Active # diagnose debug application azd -1
```

You are troubleshooting a Microsoft Azure SDN connector issue on your FortiGate VM in Azure

Which three settings should you check while troubleshooting this problem? (Choose three.)

## Options:

**A-** Use the show vdom command to see hidden VDOMs.

**B-** use the diag sys va command.

**C-** Ensure FortiGate port4 can resolve DNS.

**D-** Ensure FortiGate portl has internet access

**E-** Ensure IP address 169.254.169_254 is not blocked

## Answer:

C, D, E

## Explanation:

The three settings that should be checked while troubleshooting this problem are:

Ensure FortiGate port4 can resolve DNS.This is because the Azure SDN connector requires DNS resolution to communicate with the Azure API1. If the FortiGate port4 cannot resolve DNS, the SDN connector will not be able to retrieve the Azure resources and display them in the GUI.

Ensure FortiGate portl has internet access.This is because the Azure SDN connector requires internet access to communicate with the Azure API1. If the FortiGate portl does not have internet access, the SDN connector will not be able to connect to the Azure cloud and display an error in the CLI.

Ensure IP address 169.254.169_254 is not blocked.This is because the Azure SDN connector uses this IP address to obtain metadata information from the Azure instance2. If this IP address is blocked by a firewall policy or a network ACL, the SDN connector will not be able to get the required information and display an error in the CLI.

20%
DISCOUNT