HPE6-A84 Q&As

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/hpe6-a84.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

You are working with a developer to design a custom NAE script for a customer. You are helping the developer find the correct REST API resource to monitor.

Refer to the exhibit below.

What should you do before proceeding?

A. Go to the v1 API documentation interface instead of the v10.10 interface.

B. Use your Aruba passport account and collect a token to use when trying out API calls.

C. Enable the switch to listen to REST API calls on the default VRF.

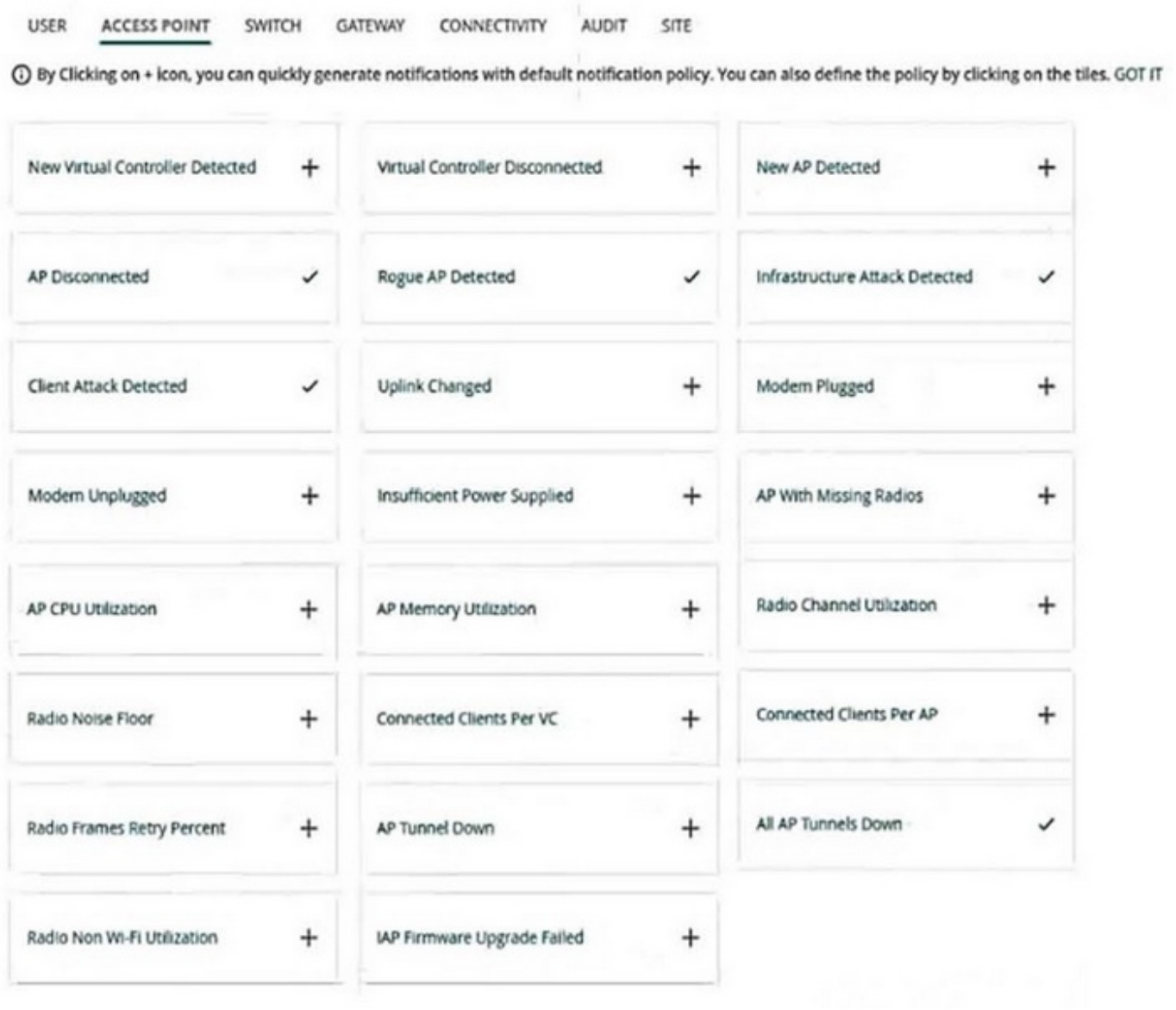
D. Make sure that your browser is set up to store authentication tokens and cookies.

Correct Answer: B

The exhibit shows the ArubaOS-CX REST API documentation interface, which allows you to explore the available resources and try out the API calls using the "Try it out" button. However, before you can use this feature, you need to authenticate yourself with your Aruba passport account and collect a token that will be used for subsequent requests. This token will expire after a certain time, so you need to refresh it periodically. You can find more details about how to use the documentation interface and collect a token in the ArubaOS-CX REST API Guide1.

QUESTION 2

A customer has an AOS 10 architecture, which includes Aruba APs. Admins have recently enabled WIDS at the high level. They also enabled alerts and email notifications for several events, as shown in the exhibit.



Admins are complaining that they are getting so many emails that they have to ignore them, so they are going to turn off all notifications.

What is one step you could recommend trying first?

A. Send the email notifications directly to a specific folder, and only check the folder once a week.

B. Disable email notifications for Roque AP, but leave the Infrastructure Attack Detected and Client Attack Detected notifications on.

C. Change the WIDS level to custom, and enable only the checks most likely to indicate real threats.

D. Disable just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert.

Correct Answer: C

According to the AOS 10 documentation1, WIDS is a feature that monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. WIDS can be configured at different levels, such

as low, medium, high, or custom. The higher the level, the more checks are enabled and the more alerts are generated. However, not all checks are equally relevant or indicative of real threats. Some checks may generate false positives or unnecessary alerts that can overwhelm the administrators and reduce the effectiveness of WIDS. Therefore, one step that could be recommended to reduce the number of email notifications is to change the WIDS level to custom, and enable only the checks most likely to indicate real threats. This way, the administrators can fine-tune the WIDS settings to suit their network environment and security needs, and avoid getting flooded with irrelevant or redundant alerts.
Option C is the correct answer. Option A is incorrect because sending the email notifications directly to a specific folder and only checking the folder once a week is not a good practice for security management. This could lead to missing or ignoring important alerts that require immediate attention or action. Moreover, this does not solve the problem of getting too many emails in the first place. Option B is incorrect because disabling email notifications for Rogue AP, but leaving the Infrastructure Attack Detected and Client Attack Detected notifications on, is not a sufficient solution. Rogue APs are unauthorized access points that can pose a serious security risk to the network, as they can be used to intercept or steal sensitive data, launch attacks, or compromise network performance. Therefore, disabling email notifications for Rogue APs could result in missing critical alerts that need to be addressed. Option D is incorrect because disabling just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert, is not a valid assumption. The Infrastructure Attack Detected alert covers a broad range of attacks that target the network infrastructure, such as deauthentication attacks, spoofing attacks, denial-of-service attacks, etc. The Rogue AP and Client Attack Detected alerts are more specific and focus on detecting and classifying rogue devices and clients that may be involved in such attacks. Therefore, disabling these alerts could result in losing valuable information about the source and nature of the attacks.

QUESTION 3

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients\\' privileges, ClearPass also should use information collected by Intune to make access control decisions.

You are planning to use Azure AD as the authentication source in 802.1X services.

What should you make sure that the customer understands is required?

A. An app registration on Azure AD that references the CPPM\\'s FQDN

B. Windows 365 subscriptions

C. CPPM\\'s RADIUS certificate was imported as trusted in the Azure AD directory

D. Azure AD Domain Services

Correct Answer: A

To use Azure AD as the authentication source in 802.1X services, you need to configure CPPM as a SAML service provider and Azure AD as a SAML identity provider. This allows CPPM to use Azure AD for user authentication and role mapping. To do this, you need to create an app registration on Azure AD that references the CPPM\\'s FQDN as the reply URL and the entity ID. You also need to grant the app registration the required permissions to access user information from Azure AD1

QUESTION 4

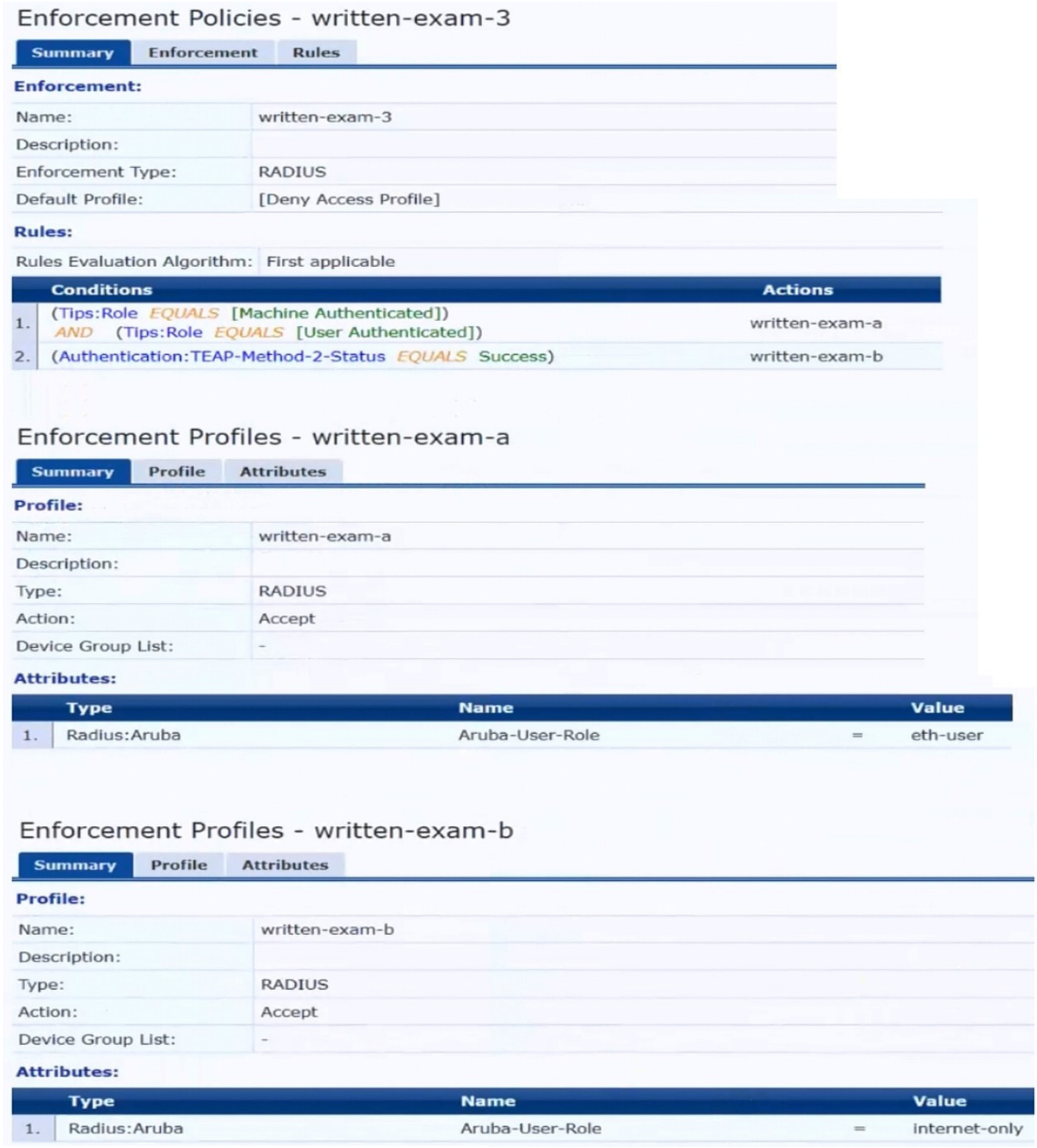
Refer to the scenario.

A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the "eth- internet" role. The gateway should also handle assigning clients to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below: The gateway cluster has two gateways with these IP addresses:



Enforcement Policies - written-exam-3

Summary | Enforcement | Rules

Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [Machine Authenticated]) AND (Tips:Role EQUALS [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam-b

Enforcement Profiles - written-exam-a

Summary | Profile | Attributes

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	eth-user

Enforcement Profiles - written-exam-b

Summary | Profile | Attributes

Profile:

Name:	written-exam-b
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	internet-only

Gateway 1

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

VLAN 4094 (WAN) = 198.51.100.12

VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

You are setting up the UBT zone on an AOS-CX switch.

Which IP addresses should you define in the zone?

A. Primary controller = 10.20.4.21; backup controller = 10.20.4.22

B. [Primary controller = 198.51.100.14; backup controller = 10.20.4.21

C. Primary controller = 10 20 4 21: backup controller not defined

D. Primary controller = 10.20.20.254; backup controller, not defined

Correct Answer: A

To configure user-based tunneling (UBT) on an AOS-CX switch, you need to specify the IP addresses of the mobility gateways that will receive the tunneled traffic from the switch 1. The primary controller is the preferred gateway for the switch to establish a tunnel, and the backup controller is the alternative gateway in case the primary controller fails or becomes unreachable 1. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery 2. In this scenario, the customer has a gateway cluster with two gateways, each with a system IP address on VLAN 4085. Therefore, the switch should use these system IP addresses as the primary and backup controllers for UBT. The IP addresses of the gateways on VLAN 20 and VLAN 4094 are not relevant for UBT, as they are used for user traffic and WAN connectivity, respectively 2. The VRRP IP address on VLAN 20 is also not applicable for UBT, as it is a virtual IP address that is not associated with any specific gateway 3. Therefore, the best option is to use 10.20.4.21 as the primary controller and 10.20.4.22 as the backup controller for UBT on the switch. This will ensure high availability and cluster discovery for the tunneled traffic from the switch to the gateway cluster.

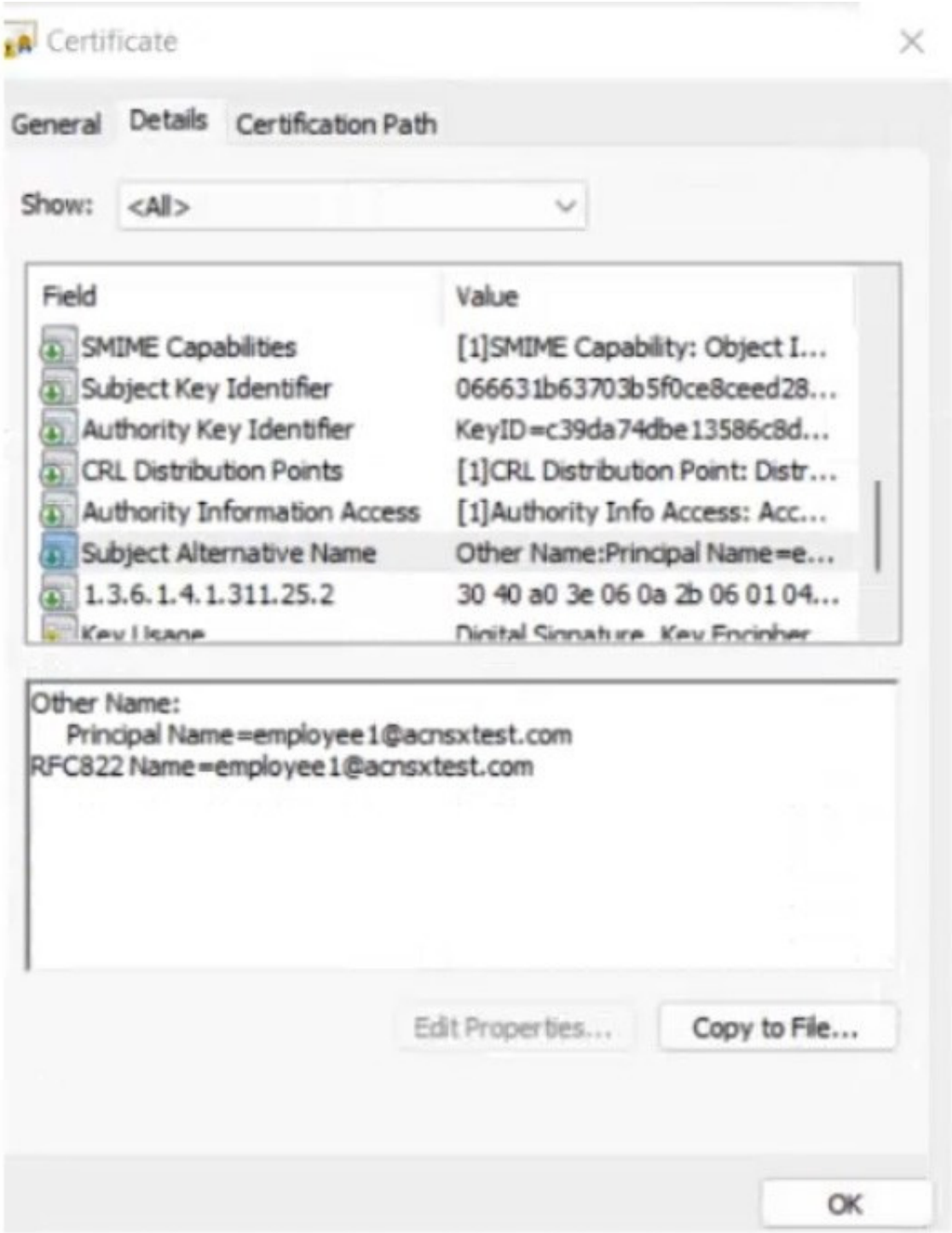
QUESTION 5

Refer to the scenario.

Introduction to the customer

You are helping a company add Aruba ClearPass to their network, which uses Aruba network infrastructure devices.

The company currently has a Windows domain and Windows CA. The Window CA issues certificates to domain computers, domain users, and servers such as domain controllers. An example of a certificate issued by the Windows CA is shown here.



The company is in the process of adding Microsoft Endpoint Manager (Intune) to manage its mobile clients. The customer is maintaining the on-prem AD for now and uses Azure AD Connect to sync with Azure AD.

Requirements for issuing certificates to mobile clients

The company wants to use ClearPass Onboard to deploy certificates automatically to mobile clients enrolled in Intune. During this process, Onboard should communicate with Azure AD to validate the clients. High availability should also be

provided for this scenario; in other words, clients should be able to get certificates from Subscriber 2 if Subscriber 1 is

down.

The Intune admins intend to create certificate profiles that include a UPN SAN with the UPN of the user who enrolled the device.

Requirements for authenticating clients

The customer requires all types of clients to connect and authenticate on the same corporate SSID.

The company wants CPPM to use these authentication methods:

1.

EAP-TLS to authenticate users on mobile clients registered in Intune

2.

TEAR, with EAP-TLS as the inner method to authenticate Windows domain computers and the users on them To succeed, EAP-TLS (standalone or as a TEAP method) clients must meet these requirements:

1.

Their certificate is valid and is not revoked, as validated by OCSP

2.

The client\\'s username matches an account in AD # Requirements for assigning clients to roles After authentication, the customer wants the CPPM to assign clients to ClearPass roles based on the following rules:

1.

Clients with certificates issued by Onboard are assigned the "mobile-onboarded" role

2.

Clients that have passed TEAP Method 1 are assigned the "domain-computer" role

3.

Clients in the AD group "Medical" are assigned the "medical-staff" role

4.

Clients in the AD group "Reception" are assigned to the "reception-staff" role The customer requires CPPM to assign authenticated clients to AOS firewall roles as follows:

1.

Assign medical staff on mobile-onboarded clients to the "medical-mobile" firewall role

2.

Assign other mobile-onboarded clients to the "mobile-other" firewall role

3.

Assign medical staff on domain computers to the "medical-domain" firewall role

4.

All reception staff on domain computers to the "reception-domain" firewall role

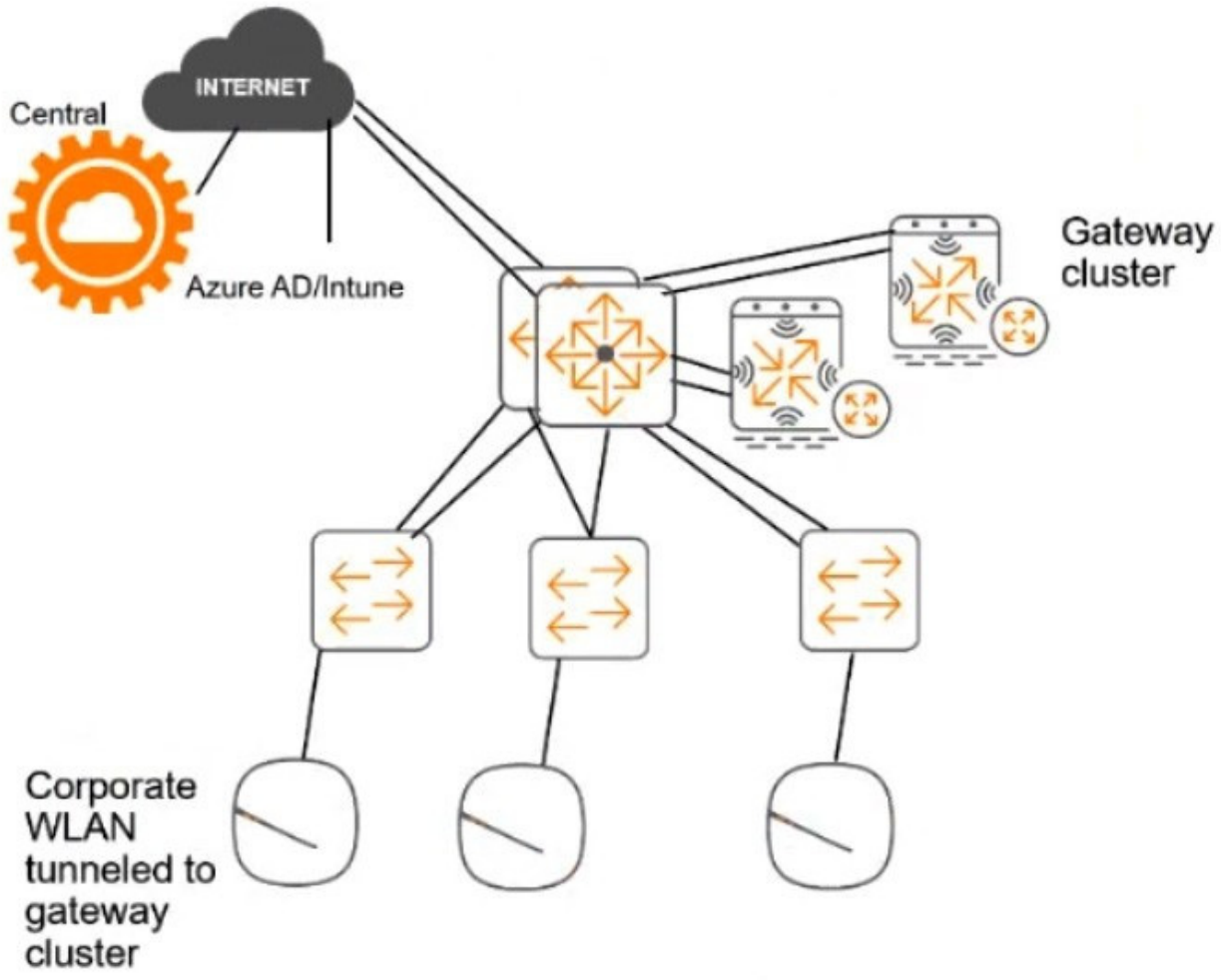
5.

All domain computers with no valid user logged in to the "computer-only" firewall role

6.

Deny other clients\\' access # Other requirements Communications between ClearPass servers and on-prem AD domain controllers must be encrypted. # Network topology For the network infrastructure, this customer has Aruba APs and Aruba gateways, which are managed by Central. APs use tunneled WLANs, which tunnel traffic to the gateway cluster. The customer also has AOS-CX switches that are not

managed by Central at this point.



ClearPass cluster IP addressing and hostnames A customer\\'s ClearPass cluster has these IP addresses:

1.

Publisher = 10.47.47.5

2.

Subscriber 1 = 10.47.47.6

3.

Subscriber 2 = 10.47.47.7

4.

Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8

The customer\\'s DNS server has these entries

1.

cp.acnsxtest.com = 10.47.47.5

2.

cps1.acnsxtest.com = 10.47.47.6

3.

cps2.acnsxtest.com = 10.47.47.7

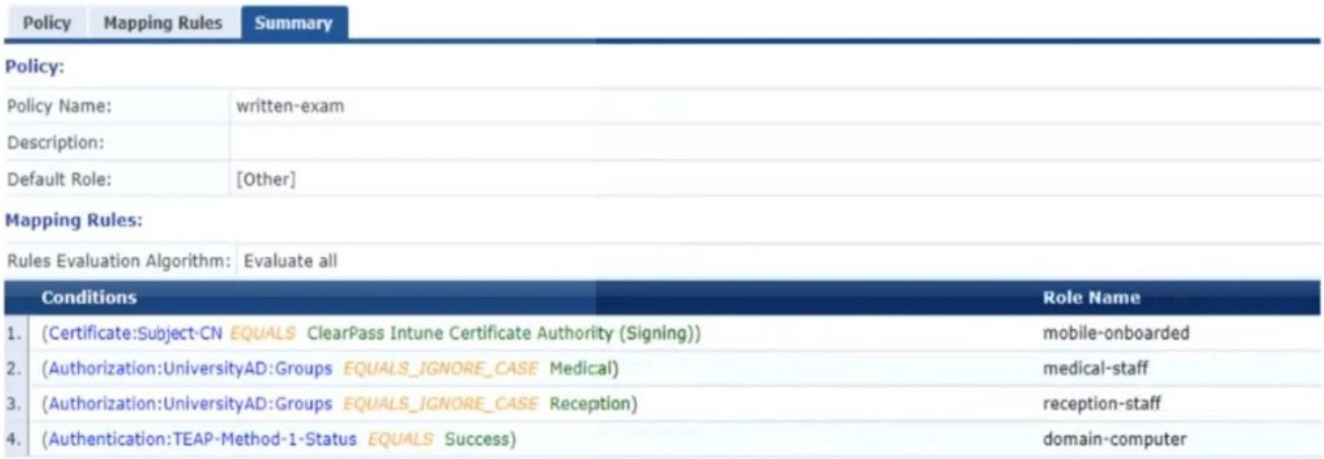
4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

You have created a role mapping policy as shown in the exhibits below.


Policy | Mapping Rules | Summary

Policy:

Policy Name:	written-exam
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Role Name
1.	(Certificate:Subject-CN EQUALS ClearPass Intune Certificate Authority (Signing))	mobile-onboarded
2.	(Authorization:UniversityAD:Groups EQUALS_IGNORE_CASE Medical)	medical-staff
3.	(Authorization:UniversityAD:Groups EQUALS_IGNORE_CASE Reception)	reception-staff
4.	(Authentication:TEAP-Method-1-Status EQUALS Success)	domain-computer

What is one change that you need to make to this policy?

A. In rule 1 change Subject-CN to Issuer-CN.

B. Move rules 2 and 3 to the top of the list.

C. Change the rules evaluation mechanism to first applicable.

D. Change the default role to \\'mobile-onboarded*

Correct Answer: A