



*Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.*



HPE6-A84 Dumps  
HPE6-A84 Braindumps  
HPE6-A84 Real Questions  
HPE6-A84 Practice Test  
HPE6-A84 Actual Questions



**HP**

# HPE6-A84

*Aruba Certified Network Security Expert Written*



<https://killexams.com/pass4sure/exam-detail/HPE6-A84>

Question: 114

A company has an Aruba ClearPass server at 10.47.47.8, FQDN radius.acnsxtest.local. This exhibit shows ClearPass Policy Manager's (CPPM's) settings for an Aruba Mobility Controller (MC).

Edit Device Details

Device

RadSec Settings

SNMP Read Settings

SNMP Write Settings

CLI Settings

OnConnect Enforcement

Attributes

Name:

ExamMC

IP or Subnet Address:

10.47.40.4

(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)

Device Groups:

-

Description:

RADIUS Shared Secret:

\*\*\*\*\*

Verify:

\*\*\*\*\*

TACACS+ Shared Secret:

Verify:

Vendor Name:

Aruba

Enable RADIUS Dynamic Authorization:

☒

Enable RadSec:

☒

Copy

Save

Cancel

The MC is already configured with RADIUS authentication settings for CPPM, and RADIUS requests between the MC and CPPM are working. A network admin enters and commits this command to enable dynamic authorization on the MC: `aaa rfc-3576-server 10.47.47.8`

But when CPPM sends CoA requests to the MC, they are not working.

This exhibit shows the RFC 3576 server statistics on the MC:

RADIUS RFC 3576 Statistics

Server	Disconnect Req	Disconnect Acc	Disconnect Req	No Secret	No Sess ID	Bad Auth
Invalid Req	Pkts Dropped	Unknown service	CoA Req	CoA Acc	CoA Req	No perm
10.47.47.8	0	0	0	0	0	0
0	0	0	0	0	0	0

How could you fix this issue?

- A. Change the UDP port in the MCsâ RFC 3576 server config to 3799.
- B. Enable RadSec on the MCsâ RFC 3676 server config.
- C. Configure the MC to obtain the time from a valid NTP server.
- D. Make sure that CPPM is using an ArubaOS Wireless RADIUS CoA enforcement profile.

Answer: A

Question: 115

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

Permitted to receive IP addresses with DHCP

Permitted access to DNS services from 10.8.9.7 and no other server

Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22

Denied access to other 10.0.0.0/8 subnets

Permitted access to the Internet

Denied access to the WLAN for a period of time if they send any SSH traffic

Denied access to the WLAN for a period of time if they send any Telnet traffic

Denied access to all high-risk websites

External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

The exhibits below show the configuration for the role.

medical-mobile

Policies

Bandwidth

Captive Portal

More

Show Basic View

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-saci	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

+

medical-mobile > Policy > apprf-medical-mobile-saci Rules

Drag rows to re-order

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
IPv4	user	any	web-cc-reputation high-risk	deny_opt	--

medical-mobile

Policies

Bandwidth

Captive Portal

More

Show Basic View

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-saci	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-saci	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

+

medical-mobile > Policy > medical-mobile Rules

Drag rows to re-order

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
IPv4	user	any	svc-dhcp	permit	--
IPv4	user	any	svc-ssh	deny_opt	--
IPv4	user	any	svc-telnet	deny_opt	--
IPv4	user	10.8.9.7	svc-dns	permit	--
IPv4	user	10.1.12.0 255.255.254.0	any	deny_opt	--
IPv4	user	10.1.0.0 255.255.0.0	any	permit	--
IPv4	user	10.0.0.0 255.0.0.0	any	deny_opt	--
IPv4	any	any	any	permit	--

+

- What setting not shown in the exhibit must you check to ensure that the requirements of the scenario are met?
- A. That denylisting is enabled globally on the MCs' firewalls
  - B. That stateful handling of traffic is enabled globally on the MCs' firewalls and on the medical-mobile role
  - C. That AppRF and WebCC are enabled globally and on the medical-mobile role
  - D. That the MCs are assigned RF Protect licenses

Answer: C

### Question: 116

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 "ethernet" 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:

### 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



The gateway cluster has two gateways with these IP addresses:

â€ Gateway 1

- o VLAN 4085 (system IP) = 10.20.4.21
- o VLAN 20 (users) = 10.20.20.1
- o VLAN 4094 (WAN) = 198.51.100.14

â€ Gateway 2

- o VLAN 4085 (system IP) = 10.20.4.22
- o VLAN 20 (users) = 10.20.20.2
- o VLAN 4094 (WAN) = 198.51.100.12

â€ 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.

Assume that you have configured the correct UBT zone and port-access role settings. However, the solution is not working.

What else should you make sure to do?

- A. Assign VLAN 20 as the access VLAN on any edge ports to which tunneled clients might connect.
- B. Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLA
- C. Assign sufficient VIA licenses to the gateways based on the number of wired clients that will connect.
- D. Change the port-access auth-mode mode to client-mode on any edge ports to which tunneled clients might connect.

**Answer: C**

### Question: 117

A company has Aruba gateways and wants to start implementing gateway IDS/IPS. The customer has selected Block for the Fail Strategy.

What might you recommend to help minimize unexpected outages caused by using this particular fail strategy?

- A. Configuring a relatively high threshold for the gateway threat count alerts
- B. Making sure that the gateways have formed a cluster and operate in default gateway mode
- C. Setting the IDS or IPS policy to the least restrictive option, Lenient
- D. Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors

**Answer: B**

### Question: 118

A company has Aruba gateways that are implementing gateway IDS/IPS in IDS mode. The customer complains that admins are receiving too frequent of repeat email notifications for the same threat. The threat itself might be one that the admins should investigate, but the customer does not want the email notification to repeat as often.

Which setting should you adjust in Aruba Central?

- A. Report scheduling settings
- B. Alert duration and threshold settings
- C. The IDS policy setting (strict, medium, or lenient)
- D. The allowlist settings in the IDS policy

**Answer: B**

### Question: 119

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.

Assume that the Azure AD deployment has the proper prerequisites established.

You are planning the CPPM authentication source that you will reference as the authentication source in 802.1X services.

How should you set up this authentication source?

- A. As Kerberos type
- B. As Active Directory type
- C. As HTTP type, referencing the Intune extension
- D. AS HTTP type, referencing Azure AD's FQDN

**Answer: D**

### Question: 120

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

Permitted to receive IP addresses with DHCP

Permitted access to DNS services from 10.8.9.7 and no other server

Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22

Denied access to other 10.0.0.0/8 subnets

Permitted access to the Internet

Denied access to the WLAN for a period of time if they send any SSH traffic

Denied access to the WLAN for a period of time if they send any Telnet traffic

Denied access to all high-risk websites

External devices should not be permitted to initiate sessions with medical-mobile clients, only send return traffic.

The exhibits below show the configuration for the role.

medical-mobile	Policies	Bandwidth	Captive Portal	More	Show Basic View
NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION	
global-saci	0	session	logon, guest, ap-role, stat...	--	
apprf-medical-mobile-s...	1	session	medical-mobile	--	
medical-mobile	8	session	medical-mobile	--	
+					
medical-mobile > Policy > apprf-medical-mobile-saci Rules					Drag rows to re-order
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
IPv4	user	any	web-cc-reputation high-risk	deny_opt	--

medical-mobile	Policies	Bandwidth	Captive Portal	More	Show Basic View
NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION	
global-saci	0	session	logon, guest, ap-role, stat...	--	
apprf-medical-mobile-saci	1	session	medical-mobile	--	
medical-mobile	8	session	medical-mobile	--	
+					
medical-mobile > Policy > medical-mobile Rules					Drag rows to re-order
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
IPv4	any	any	svc-dhcp	permit	--
IPv4	user	10.8.9.7	svc-dns	permit	--
IPv4	user	10.1.12.0 255.255.252.0	any	deny_opt	--
IPv4	user	10.1.0.0 255.255.0.0	any	permit	--
IPv4	user	10.0.0.0 255.0.0.0	any	deny_opt	--
IPv4	user	any	svc-telnet	deny_opt	--
IPv4	user	any	svc-ssh	deny_opt	--
IPv4	any	any	any	permit	--
+					

There are multiple issues with the configuration.

What is one of the changes that you must make to the policies to meet the scenario requirements? (In the options, rules



in a policy are referenced from top to bottom. For example, âmedical-mobileâ rule 1 is âipv4 any any svc-dhcp permit,â and rule 8 is âipv4 any any any permit.â.)

- A. In the âmedical-mobileâ policy, change the source in rule 1 to âuser.â
- B. In the âmedical-mobileâ policy, change the subnet mask in rule 3 to 255.255.248.0.
- C. In the âmedical-mobileâ policy, move rules 6 and 7 to the top of the list.
- D. Move the rule in the âappprf-medical-mobile-saclâ policy between rules 7 and 8 in the âmedical-mobileâ policy.

Answer: B

Question: 121

What is a common characteristic of a beacon between a compromised device and a command and control server?

- A. Use of IPv6 addressing instead of IPv4 addressing
- B. Lack of encryption
- C. Use of less common protocols such as SNAP
- D. Periodic transmission of small, identically sized packets

Answer: D

Question: 122

Refer to the scenario.

A hospital has an AOS10 architecture that is managed by Aruba Central. The customer has deployed a pair of Aruba 9000 Series gateways with Security licenses at each clinic. The gateways implement IDS/IPS in IDS mode.

The Security Dashboard shows these several recent events with the same signature, as shown below:

RAPIDS Gateway IDS/IPS					
Threats List (20)					
Occurred On	Gateway	Type	Source	Destination	
2023-01-12 01:01:08	gw2	DNS	10.1.36.152	10.254.1.21	
2023-01-12 01:01:04	gw2	DNS	10.1.36.152	10.254.1.21	
2023-01-12 01:01:02	gw2	DNS	10.1.36.152	10.254.1.21	
2023-01-12 01:01:01	gw2	DNS	10.1.36.152	10.254.1.21	
2023-01-12 01:01:01	gw2	DNS	10.1.36.152	10.254.1.21	
2023-01-12 00:50:56	gw2	DNS	10.1.36.150	10.254.1.21	
2023-01-12 00:50:52	gw2	DNS	10.1.36.150	10.254.1.21	
2023-01-12 00:50:50	gw2	DNS	10.1.36.150	10.254.1.21	
2023-01-12 00:50:49	gw2	DNS	10.1.36.150	10.254.1.21	

Which step could give you valuable context about the incident?

- A. View firewall sessions on the APs and record the threat sourcesâ type and O
- B. View the user-table on APs and record the threat sourcesâ 802.11 settings.
- C. View the RAPIDS Security Dashboard and see if the threat sources are listed as rogues.
- D. Find the Central client profile for the threat sources and note their category and family.

**Answer: C**

### **Question: 123**

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 "ethernet-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:

## Enforcement Policies - written-exam-3

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	written-exam-3	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	

<b>Rules:</b>		
Rules Evaluation Algorithm: First applicable		
Conditions	Actions	
1. (Tips:Role EQUALS [Machine Authenticated])	written-exam-a	
AND (Tips:Role EQUALS [User Authenticated])		
2. (Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam-b	

## Enforcement Profiles - written-exam-a

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	written-exam-a	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

<b>Attributes:</b>			
Type	Name		Value
1. Radius:Aruba	Aruba-User-Role		= eth-user

## Enforcement Profiles - written-exam-b

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	written-exam-b	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

<b>Attributes:</b>			
Type	Name		Value
1. Radius:Aruba	Aruba-User-Role		= Internet-only

The gateway cluster has two gateways with these IP addresses:

â€¢ Gateway 1

o VLAN 4085 (system IP) = 10.20.4.21

o VLAN 20 (users) = 10.20.20.1

o VLAN 4094 (WAN) = 198.51.100.14

â€ Gateway 2

o VLAN 4085 (system IP) = 10.20.4.22

o VLAN 20 (users) = 10.20.20.2

o VLAN 4094 (WAN) = 198.51.100.12

â€ 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.

What is one change that you should make to the solution?

- A. Change the ubt-client-vlan to VLAN 13.
- B. Configure edge ports in VLAN trunk mode.
- C. Remove VLAN assignments from role configurations on the gateways.
- D. Configure the UBT solution to use VLAN extend mode.

**Answer: C**

## **Question: 124**

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 "ethernet-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:

## Enforcement Policies - written-exam-3

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	written-exam-3	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	

<b>Rules:</b>		
Rules Evaluation Algorithm: First applicable		
Conditions	Actions	
1. (Tips:Role EQUALS [Machine Authenticated])	written-exam-a	
AND (Tips:Role EQUALS [User Authenticated])		
2. (Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam-b	

## Enforcement Profiles - written-exam-a

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	written-exam-a	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

<b>Attributes:</b>			
Type	Name	Value	
1. Radius:Aruba	Aruba-User-Role	=	eth-user

## Enforcement Profiles - written-exam-b

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	written-exam-b	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

<b>Attributes:</b>			
Type	Name	Value	
1. Radius:Aruba	Aruba-User-Role	=	Internet-only

The gateway cluster has two gateways with these IP addresses:

â€¢ Gateway 1



o VLAN 4085 (system IP) = 10.20.4.21

o VLAN 20 (users) = 10.20.20.1

o VLAN 4094 (WAN) = 198.51.100.14

â€ Gateway 2

o VLAN 4085 (system IP) = 10.20.4.22

o VLAN 20 (users) = 10.20.20.2

o VLAN 4094 (WAN) = 198.51.100.12

â€ 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.

Assume that you are using the âmyzoneâ name for the UBT zone.

Which is a valid minimal configuration for the AOS-CX port-access roles?

- A. port-access role eth-internet gateway-zone zone myzone gateway-role eth-user
- B. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet
- C. port-access role eth-internet gateway-zone zone myzone gateway-role eth-internet vlan access 20
- D. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet vlan access 20

**Answer: B**

**Question: 125**

Refer to the scenario.

A customer requires these rights for clients in the âmedical-mobileâ AOS firewall role on Aruba Mobility Controllers (MCs):

Permitted to receive IP addresses with DHCP

Permitted access to DNS services from 10.8.9.7 and no other server

Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22

Denied access to other 10.0.0.0/8 subnets

Permitted access to the Internet

Denied access to the WLAN for a period of time if they send any SSH traffic

Denied access to the WLAN for a period of time if they send any Telnet traffic

Denied access to all high-risk websites

External devices should not be permitted to initiate sessions with medical-mobile clients, only send return traffic.

The line below shows the effective configuration for the role.

medical-mobile	Policies	Bandwidth	Captive Portal	More	Show Basic View
NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION	
global-sacl	0	session	logon, guest, ap-role, stat...	--	
apprf-medical-mobile-sacl	1	session	medical-mobile	--	
medical-mobile	8	session	medical-mobile	--	
+					
medical-mobile > Policy > apprf-medical-mobile-sacl Rules					
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
IPv4	user	any	web-cc-reputation high-risk	deny_opt	--

medical-mobile	Policies	Bandwidth	Captive Portal	More	Show Basic View
NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION	
global-sacl	0	session	logon, guest, ap-role, stat...	--	
apprf-medical-mobile-sacl	1	session	medical-mobile	--	
medical-mobile	8	session	medical-mobile	--	
+					
medical-mobile > Policy > medical-mobile Rules					
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
IPv4	any	any	svc-dhcp	permit	--
IPv4	user	10.8.9.7	svc-dns	permit	--
IPv4	user	10.1.12.0 255.255.252.0	any	deny_opt	--
IPv4	user	10.1.0.0 255.255.0.0	any	permit	--
IPv4	user	10.0.0.0 255.0.0.0	any	deny_opt	--
IPv4	user	any	svc-telnet	deny_opt	--
IPv4	user	any	svc-ssh	deny_opt	--
IPv4	any	any	any	permit	--
+					

- There are multiple issues with this configuration.
- What is one change you must make to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, medical-mobile rule 1 is IPv4 any any svc-dhcp permit, and rule 6 is IPv4 any any permit.)
- A. Apply the "apprf-medical-mobile-sacl" policy explicitly to the medical-mobile user-role under the medical-mobile policy.
  - B. In the medical-mobile policy, change the action for rules 2 and 3 to reject.
  - C. In the medical-mobile policy, move rule 5 under rule 6.
  - D. In the medical-mobile policy, change the subnet mask in rule 5 to 255.255.252.0.

Answer: D

### Question: 126

A customer requires a secure solution for connecting remote users to the corporate main site. You are designing a client-to-site virtual private network (VPN) based on Aruba VIA and Aruba Mobility Controllers acting as VPN Concentrators (VPNCs). Remote users will first use the VIA client to contact the VPNCs and obtain connection settings.

The users should only be allowed to receive the settings if they are the customer's "Remote Employees" AD group. After receiving the settings, the VIA clients will automatically establish VPN connections, authenticating to CPPM with certificates.

What should you do to help ensure that only authorized users obtain VIA connection settings?

- A. Set up the VPNCs' VIA web authentication profile to use CPPM as the authentication server; set up a service on CPPM that uses AD as the authentication source.
- B. Set up the VPNCs' VIA web authentication profile to use an AD domain controller as the LDAP server.
- C. Set up the VPNCs' VIA connection profile to use two authentication profiles, one RADIUS profile to CPPM and one LDAP profile to A
- D. Set up the VPNCs' VIA connection profile to use one authentication profile, which is set to the AD domain controller's hostname.

**Answer: A**

### Question: 127

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.

The customer wants you to configure CPPM to collect information from Intune on demand during the authentication process.

What should you tell the Intune admins about the certificates issued to clients?

- A. They must be issued by a well-known, trusted C
- B. They must include the Intune ID in the subject name.
- C. They must include the client MAC address in the subject name.
- D. They must be issued by a ClearPass Onboard C

**Answer: A**

### Question: 128

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

**Answer: A**

### **Question: 192**

You are configuring gateway IDS/IPS settings in Aruba Central.

For which reason would you set the Fail Strategy to Bypass?

- A. To permit traffic if the IPS engine fails to inspect it
- B. To enable the gateway to honor the allowlist settings configured in IDS/IPS policies
- C. To tell gateways to stop enforcing IDS/IPS policies if they lose connectivity to the Internet
- D. To avoid wasting IPS engine resources on filtering traffic for unauthenticated clients

**Answer: A**

### **Question: 130**

How does Aruba Central handle security for site-to-site connections between AOS 10 gateways?

- A. It uses an Aruba proprietary integrity and encryption technologies to secure site-to-site connections, making them resistant to zero day attacks.
- B. It automatically establishes IPsec tunnels for all site-to-site (all HUBs and Branches) connections using keys securely distributed by Central.
- C. It automatically steers traffic away from Internet-based connections to more secure MPLS connections to reduce encryption overhead.
- D. It automatically establishes simple-to-manage and highly secure TLSv1.3 tunnels between gateways.

**Answer: B**



# SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

*Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:*

**Actual Exam Questions:** *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

**Exam Dumps:** *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

**Practice Tests:** *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

**Guaranteed Success:** *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

**Updated Content:** *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

**Technical Support:** *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>  
Kill your exam at First Attempt....Guaranteed!