



Free Questions for HPE6-A84 by vceexamstest

Shared by Gomez on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the scenario.

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

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 Bas](#)

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	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-sacl Rules (i) Drag rows to re

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 Bas](#)

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 (i) Drag rows to re-

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
------------	--------	-------------	---------------------	--------	-------------

What setting not shown in the exhibit must you check to ensure that the requirements of the scenario are met?

Options:

- 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

Explanation:

AppRF and WebCC are features that allow the MCs to classify and control application traffic and web content based on predefined or custom categories¹². These features are required to meet the scenario requirements of denying access to all high-risk websites and denying access to the WLAN for a period of time if they send any SSH or Telnet traffic.

To enable AppRF and WebCC, you need to check the following settings:

On the global level, you need to enable AppRF and WebCC under Configuration > Services > AppRFandConfiguration > Services > WebCC, respectively¹².

On the role level, you need to enable AppRF and WebCC under Configuration > Security > Access Control > Roles > medical-mobile > AppRFandConfiguration > Security > Access Control > Roles > medical-mobile > WebCC, respectively¹².

You also need to make sure that the MCs have valid licenses for AppRF and WebCC, which are included in the ArubaOS PEFNG license³.

Question 2

Question Type: MultipleChoice

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 Enforce

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:c

Device Groups:

-

Description:

RADIUS Shared Secret:

Verify:

TACACS+ Shared Secret:

Verify:

Vendor Name:

Aruba

Enable RADIUS Dynamic Authorization:



Enable RadSec:



Copy

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

How could you fix this issue?

Options:

A- Change the UDP port in the MCs' RFC 3576 server config to 3799.

- B-** Enable RadSec on the MCs' 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

Explanation:

Dynamic authorization is a feature that allows CPPM to send change of authorization (CoA) or disconnect messages to the MC to modify or terminate a user session based on certain conditions or events¹. Dynamic authorization uses the RFC 3576 protocol, which is an extension of the RADIUS protocol².

To enable dynamic authorization on the MC, you need to configure the IP address and UDP port of the CPPM server as the RFC 3576 server on the MC³. The default UDP port for RFC 3576 is 3799, but it can be changed on the CPPM server. The MC and CPPM must use the same UDP port for dynamic authorization to work properly³.

In this scenario, the MC is configured with the IP address of the CPPM server (10.47.47.8) as the RFC 3576 server, but it is using the default UDP port of 3799. However, according to the exhibit, the CPPM server is using a different UDP port of 1700 for dynamic authorization. This mismatch causes the CoA requests from CPPM to fail on the MC, as shown by the statistics.

To fix this issue, you need to change the UDP port in the MCs' RFC 3576 server config to match the UDP port used by CPPM, which is 1700 in this case. Alternatively, you can change the UDP port in CPPM to match the default UDP port of 3799 on the MC. Either way, you need to ensure that both devices use the same UDP port for dynamic authorization³.

Question 3

Question Type: MultipleChoice

Refer to the scenario.

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


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

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	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-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

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	--



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 8 is "ipv4 any any any permit".)

Options:

- A- In the "medical-mobile" policy, move rules 2 and 3 between rules 7 and 8.
- B- In the "medical-mobile" policy, change the subnet mask in rule 3 to 255.255.248.0.
- C- Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.
- D- In the "medical-mobile" policy, change the source in rule 8 to "user."

Answer:

B

Explanation:

The subnet mask in rule 3 of the "medical-mobile" policy is currently 255.255.252.0, which means that the rule denies access to the 10.1.12.0/22 subnet as well as the adjacent 10.1.16.0/22 subnet. This is not consistent with the scenario requirements, which state that only the 10.1.12.0/22 subnet should be denied access, while the rest of the 10.1.0.0/16 range should be permitted access.

To fix this issue, the subnet mask in rule 3 should be changed to 255.255.248.0, which means that the rule only denies access to the 10.1.8.0/21 subnet, which includes the 10.1.12.0/22 subnet. This way, the rule matches the scenario requirements more precisely.

Question 4

Question Type: MultipleChoice

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:

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
2.	(Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam

Enforcement Profiles - written-exam-a

Summary

Profile

Attributes

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS

The gateway cluster has two gateways with these IP addresses:

* 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

* 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

* 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?

Options:

- 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

Answer:

A

Explanation:

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 switch¹. 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 unreachable¹. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery².

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, respectively². 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 gateway³.

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 cluster¹².

Question 5

Question Type: MultipleChoice

You are designing an Aruba ClearPass Policy Manager (CPPM) solution for a customer. You learn that the customer has a Palo Alto firewall that filters traffic between clients in the campus and the data center.

Which integration can you suggest?

Options:

- A-** Sending Syslogs from the firewall to CPPM to signal CPPM to change the authentication status for misbehaving clients
- B-** Importing clients' MAC addresses to configure known clients for MAC authentication more quickly
- C-** Establishing a double layer of authentication at both the campus edge and the data center DMZ
- D-** Importing the firewall's rules to program downloadable user roles for AOS-CX switches more quickly

Answer:

A

Explanation:

This option allows CPPM to receive real-time information about the network activity and security posture of the clients from the firewall, and then apply appropriate enforcement actions based on the configured policies¹². For example, if a client is detected to be infected with malware or violating the network usage policy, CPPM can quarantine or disconnect the client from the network².

Question 6

Question Type: MultipleChoice

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.

ArubaOS-CX REST API

<https://switch.acnsxtest.local/api/v10.10/openapi.json>

RESTful interface for ArubaOS-CX switch software

Change Log: <https://switch.acnsxtest.local/api/v10.10/changelog.html>

AAA_Accounting_Attributes

AAA_Server_Group

AAA_Server_Group_Prio

ACL

ACL_Entry

ACL_Object_Group

ADC_List

What should you do before proceeding?

Options:

- 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.

Answer:

B

Explanation:

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 7

Question Type: MultipleChoice

Refer to the exhibit.

Show:

<All>

Field	Value
 Subject	*.acnsxtest.com, ACNSX Test...
 Public key	RSA (4096 Bits)
 Public key parameters	05 00
 Subject Alternative Name	DNS Name=*.acnsxtest.com
 Enhanced Key Usage	Server Authentication (1.3.6....
 Subject Key Identifier	754c32324ed2035e09c1e4b4...
 Authority Key Identifier	KeyID=5169bb4853ce75f767...
 Thumbprint	f9965493hff18f07c915c49c4a

DNS Name=*.acnsxtest.com

Edit Properties...

Copy to File...

OK

You have been given this certificate to install on a ClearPass server for the RADIUS/EAP and RadSec usages.

What is one issue?

Options:

- A- The certificate has a wildcard in the subject common name.
- B- The certificate uses a fully qualified the '.local' domain name.
- C- The certificate does not have a URI subject alternative name
- D- The certificate does not have an IP subject alternative name

Answer:

B

Explanation:

The exhibit shows a screenshot of a certificate that has the following information:

The subject common name (CN) is *.clearpass.local, which is a wildcard domain name that matches any subdomain under clearpass.local.

The subject alternative names (SANs) are DNS Name=clearpass.local and DNS Name=*.clearpass.local, which are the same as the subject CN.

The issuer CN is clearpass.local, which is the same as the subject domain name.

The key usage (KU) is Digital Signature and Key Encipherment, which are required for RADIUS/EAP and RadSec usages.

The extended key usage (EKU) is Server Authentication and Client Authentication, which are also required for RADIUS/EAP and RadSec usages.

The issue with this certificate is that it uses a fully qualified the '.local' domain name, which is a reserved domain name for local networks that cannot be registered on the public Internet. This means that the certificate cannot be verified by any public certificate authority (CA), and therefore cannot be trusted by any external devices or servers that communicate with ClearPass. This could cause problems for RADIUS/EAP and RadSec usages, as they rely on secure and authenticated connections between ClearPass and other devices or servers.

To avoid this issue, the certificate should use a valid domain name that can be registered on the public Internet, such as clearpass.com or clearpass.net. This way, the certificate can be issued by a public CA that is trusted by most devices and servers, and can be verified by them. Alternatively, if the certificate is intended to be used only within a private network, it should be issued by a private CA that is trusted by all devices and servers within that network.

Question 8

Question Type: MultipleChoice

Refer to the scenario.

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


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

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	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-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

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	--



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 8 is "ipv4 any any any permit".)

Options:

- A- In the "medical-mobile" policy, move rules 2 and 3 between rules 7 and 8.
- B- In the "medical-mobile" policy, change the subnet mask in rule 3 to 255.255.248.0.
- C- Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.
- D- In the "medical-mobile" policy, change the source in rule 8 to "user."

Answer:

B

Explanation:

The subnet mask in rule 3 of the "medical-mobile" policy is currently 255.255.252.0, which means that the rule denies access to the 10.1.12.0/22 subnet as well as the adjacent 10.1.16.0/22 subnet. This is not consistent with the scenario requirements, which state that only the 10.1.12.0/22 subnet should be denied access, while the rest of the 10.1.0.0/16 range should be permitted access.

To fix this issue, the subnet mask in rule 3 should be changed to 255.255.248.0, which means that the rule only denies access to the 10.1.8.0/21 subnet, which includes the 10.1.12.0/22 subnet. This way, the rule matches the scenario requirements more precisely.

Question 9

Question Type: MultipleChoice

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:

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-Auth	Auth-User-Role	...

The gateway cluster has two gateways with these IP addresses:

* 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

* 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

* 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?

Options:

- 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

Explanation:

The UBT solution requires that the VLAN assignments for the wired clients are done by the gateway, not by the switch. Therefore, the role configurations on the gateways should not have any VLAN assignments, as they would override the VLAN 20 that is specified in the enforcement profile. Instead, the role configurations should only have policies that define the access rights for the clients in the "eth-internet" role. This way, the gateway can assign the clients to VLAN 20 and apply the appropriate policies based on their role.

1: Aruba Certified Network Technician (ACNT) | HPE Aruba Networking, section "Get the Edge: An Introduction to Aruba Networking Solutions"

Question 10

Question Type: MultipleChoice

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?

Options:

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 FODN

Answer:

D

Explanation:

An authentication source is a configuration element in CPPM that defines how to connect to an external identity provider and retrieve user or device information . CPPM supports various types of authentication sources, such as Active Directory, LDAP, SQL, Kerberos, and HTTP .

To authenticate wireless and wired clients to Azure AD, you need to set up an authentication source as HTTP type, referencing Azure AD's FQDN . This type of authentication source allows CPPM to use REST API calls to communicate with Azure AD and validate the user or device credentials . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

To use information collected by Intune to make access control decisions, you need to set up another authentication source as HTTP type, referencing the Intune extension . This type of authentication source allows CPPM to use REST API calls to communicate with Intune and retrieve the device compliance status . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

To Get Premium Files for HPE6-A84 Visit

<https://www.p2pexams.com/products/hpe6-a84>

For More Free Questions Visit

<https://www.p2pexams.com/hp/pdf/hpe6-a84>

