



Free Questions for HPE6-A75 by certsdeals

Shared by Cortez on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement is true about the Endpoint Profiler? (Select two.)

Options:

- A- The Endpoint Profiler uses DHCP fingerprinting for device categorization.
- B- Data obtained from the Endpoint Profiler can be used in Enforcement Policy.
- C- Endpoint Profiler requires a profiling license.
- D- The Endpoint Profiler requires the Onboard license to be enabled.
- E- The Endpoint Profiler can only categorize laptops and desktops.

Answer:

A, B

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

Enforcement Policies - Enterprise Enforcement Policy

Summary	Enforcement	Rules
Enforcement:		
Name:	Enterprise Enforcement Policy	
Description:	Enforcement policies for local and remote employees	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
Rules Evaluation Algorithm:	Evaluate all	
Conditions	Actions	
1. (Tips:Posture EQUALS HEALTHY (0)) AND (Tips:Role MATCHES_ANY Remote Worker Role Engineer testqa) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN, [RADIUS] Remote Employee ACL	
2. (Tips:Role EQUALS Senior_Mgmt) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN	
3. (Tips:Role EQUALS San Jose HR Local) AND (Tips:Posture EQUALS HEALTHY (0))	HR VLAN	
4. (Tips:Role EQUALS [Guest]) AND (Connection:SSID CONTAINS guest)	[RADIUS] WIRELESS_GUEST_NETWORK	
5. (Tips:Role EQUALS Remote Worker) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	RestrictedACL	

Based on the Enforcement Policy configuration, when a user with Role Engineer connects to the network and the posture token assigned is Unknown, which Enforcement Profile will be applied?

Options:

- A- EMPLOYEE_VLAN
- B- RestrictedACL
- C- Deny Access Profile
- D- HR VLAN
- E- Remote Employee ACL

Answer:

C

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

Customize Form Fields

Use this list view to modify the fields of the form **create_user**.







Rank	Field	Type	Label	Description
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this visitor account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this visitor account.
20	visitor_name	text	Visitor's Name:	Name of the visitor.
25	visitor_phone	text	Phone Number:	The visitor's phone number.
 Edit  Edit Base Field  Remove  Insert Before  Insert After  Enable Field				
30	visitor_company	text	Company Name:	Company name of the visitor.
40	email	text	Email Address:	The visitor's email address. This will become their username to log into the network.
50	modify_start_time	dropdown	Account Activation:	Select an option for changing the activation time of this account.

Exhibit:accn67-433

Based on the configuration of me create_user form shown, which statement accurately describes the status?

Options:

- A-** The email field will be visible to guest users when they access the web login page.
- B-** The visitor_company field will be visible to operators creating the account.
- C-** The visitor_company field will be visible to the guest users when they access the web login page.
- D-** The visitor_phone field will be visible to the guest users in the web login page.
- E-** The visitor_phone field will be visible to operators creating the account.

Answer:

A

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

...the organization name is displayed by the device using provisioning.

Identity	
These options control the generation of device credentials	
* Certificate Authority:	Local Certificate Authority ▼ Select the certificate authority that will be used to sign profiles and messages.
* Signer:	Onboard Certificate Authority ▼ Select the source that will be used to sign TLS client certificates.
* Key Type:	1024-bit RSA – created by device ▼ Select the type of private key to use for TLS certificates.
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.

Exhibit: accp67-531

Based on the configuration for the client's certificate private key as shown, which statements accurately describe the settings? (Select two.)

Options:

- A- More bits in the private key will increase security.
- B- The private key for TLS client certificates is not created.
- C- The private key is stored in the ClearPass server.
- D- More bits in the private key will reduce security.
- E- The private key is stored in the user device.

Answer:

A, E

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

Enforcement Policies - Onboard Provisioning - Aruba

Summary	Enforcement	Rules
Enforcement:		
Name:	Onboard Provisioning - Aruba	
Description:	Enforcement policy controlling network access for device provisioning	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Authentication:OuterMethod EQUALS EAP-TLS)	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
2. (Authentication:Source EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
3. (Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Pre-Provisioning - Aruba	

Exhibit:accp67-552

An employee connects a corporate laptop to the network and authenticates for the first time using EAP-TLS. Based on the Enforcement Policy configuration shown, which Enforcement Profile will be sent?

Options:

A- Deny Access Profile

B- Onboard Post-Provisioning - Aruba

C- Onboard Device Repository

D- Onboard Pre-Provisioning - Aruba

Answer:

D

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

Enforcement Profiles

	Profile	Attributes	Summary
Type	Name		Value
1.	Radius:IETF	Session-Timeout (27)	= 600
2.	Click to add...		

Exhibit:accp67-445

An Enforcement Profile has been created in the Policy Manager as shown. Which action will ClearPass take based on this Enforcement Profile?

Options:

- A-** ClearPass will count down 600 seconds and send a RADIUS CoA message to the user to end the user's session after this time is up.
- B-** ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the NAD and the NAD will end the user's session after 600 seconds.
- C-** ClearPass will count down 600 seconds and send a RADIUS CoA message to the NAD to end the user's session after this time is up.
- D-** ClearPass will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD and the NAD will end the user's session after 600 seconds.
- E-** ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the User and the user's session will be terminated after 600 seconds.

Answer:

B

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

User: User1
Vlan: 100
IP: 10.1.100.11
Authenticated 802.1X
Role: employee-corp
ESSID: employee1
BSSID

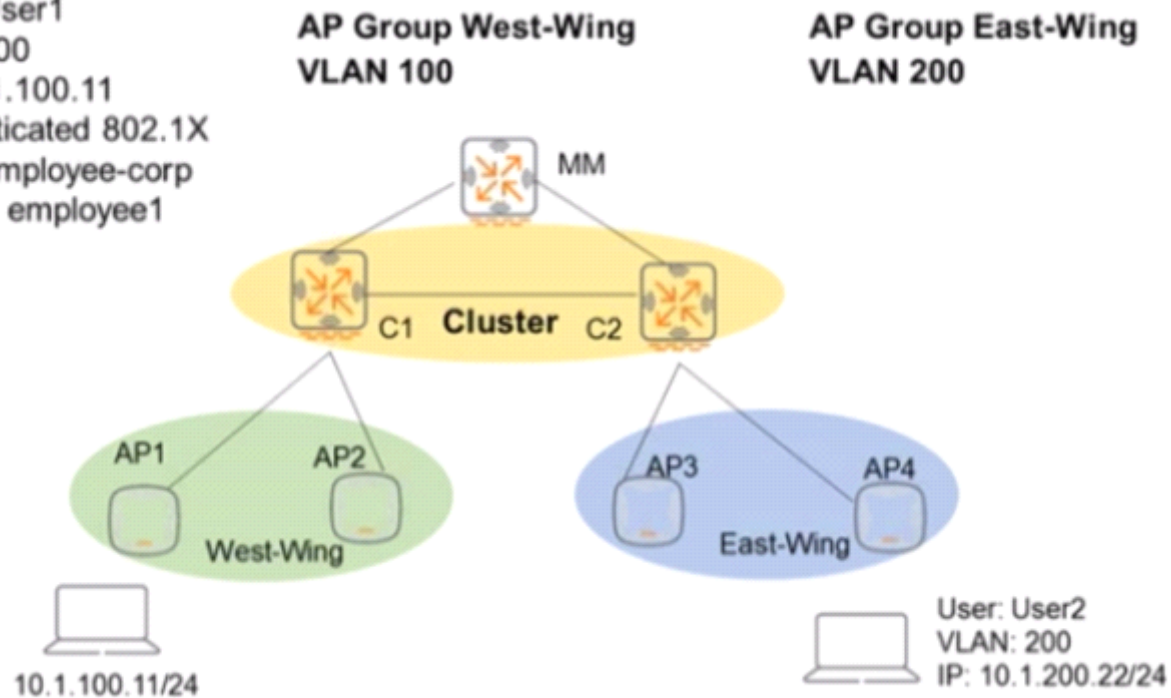


Exhibit:01125754-139

Controllers are configured in a cluster as shown in the exhibit. These are the network details.

- * A Mobility Master (MM) manages the cluster.
- * The cluster contains two controllers: C1 and C2.
- * AP1 and AP2 use C1 as their Active AP Anchor Controller (A-AAC), with C2 as their Standby AAC (S-AAC).
- * AP3 and AP4 use C2 as their A-AAC, with C1 as their S-AAC.

User1 establishes a wireless connection via API, where the Active User Anchor Controller (A-UAC) assigned is C1. with C2 as the standby. What happens when User I roams the wireless network and eventually their session is handled by AP3?

Options:

- A- The AP3's A-AAC switches to C1, and the user's A-UAC remains on C1.
- B- The AP3's A-AAC switches to C2, and the user's A-UAC remains on C2.
- C- The AP3's A-AAC switches to C1, and the user's A-UAC remains on C2.
- D- The AP3's A-AAC switches to C2, and the user's A-UAC remains on C1.

Answer:

B

Question 8

Question Type: MultipleChoice

Which ArubaOS CLI command can an administrator execute to determine if AP load balancing is enabled in a cluster?

Options:

A- show switches

B- show lc-cluster group-membership

C- show aaa cluster essid

D- show ap active

Answer:

B

Question 9

Question Type: MultipleChoice

An administrator needs to authenticate users connected to an ArubaOS Switch where the switch authenticates the user, assigns the firewall policies to the user, and processes some of the users' traffic. Which connection method should the administrator configure on the ArubaOS-Switch?

Options:

- A- Per-user tunneled node
- B- Split-tunneled mode
- C- Per-port tunneled node
- D- VLAN tunneled mode

Answer:

C

To Get Premium Files for HPE6-A75 Visit

<https://www.p2pexams.com/products/hpe6-a75>

For More Free Questions Visit

<https://www.p2pexams.com/hp/pdf/hpe6-a75>

