HP

HPE6-A82 Exam

Aruba Certified ClearPass Associate Exam

Version: 4.0

Question: 1

What is RADIUS Change of Authorization (CoA)?

A. It allows ClearPass to transmit messages to the Network Attached Device/Network Attached Server (NAD/NAS) to modify a user's session status
B. It allows clients to issue a privilege escalation request to ClearPass using RADIUS to switch to TACACS+
C. It is a mechanism that enables ClearPass to assigned a User-Based Tunnel (UBT) between a switch and controller for Dynamic Segmentation
D. It forces the client to re-authenticate upon roaming to an access point controlled by a foreign mobility controller.

Answer: A

Reference:
http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_User Guide/Enforce/EPRADIUS_CoA.htm

Question: 2

Which Authorization Source support device profile enforcement?

A. Local user Repository
B. Endpoint Repository
C. OnGuard Repository
D. Gust User Repository

Answer: A

Question: 3

Refer to the exhibit.

Web Login (Guest Network)

Use this form to make changes to the Web Login Guest Network.

Web Login Editor	
* Name:	Guest Network Enter a name for this web login page.
Page Name:	arubalogin Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks ▼ Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit ▼ Select how the user's network login will be handled. ...ually from the captive portal redirection process.
* Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default ▼ Select a security option to apply to the web login process.
Dynamic Address:	☐ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Where will the guests browser be redirected during a captive portal login attempt?

A. The captive portal page hosted on the Aruba controller
B. The redirect will time out and fan to resolve
C. The captive portal page hosted on ClearPass
D. The captive portal page hosted on Aruba Central in the cloud

Answer: D

Question: 4

DRAG DROP
Match the ClearPass system description to the best term Options are used only once.

Term		Description
ClearPass Insight		can provide posturing to validate the security status of devices on your wired, wireless and VPN networks
ClearPass Onboard		provides an intuitive way to securely assign an individual client certificate to each device
ClearPass OnGuard		gathers endpoint context from passively received data to fingerprint devices
ClearPass Policy Manager		has the ability to integrate with external systems through APIs or HTTP/REST calls
ClearPass Profiler		provides multiple customizable reports and in-depth information about each of the other modules

Answer:

Term		Description
ClearPass Insight	ClearPass OnGuard	can provide posturing to validate the security status of devices on your wired, wireless and VPN networks
ClearPass Onboard	ClearPass Insight	provides an intuitive way to securely assign an individual client certificate to each device
ClearPass OnGuard	ClearPass Policy Manager	gathers endpoint context from passively received data to fingerprint devices
ClearPass Policy Manager	ClearPass Profiler	has the ability to integrate with external systems through APIs or HTTP/REST calls
ClearPass Profiler	ClearPass Onboard	provides multiple customizable reports and in-depth information about each of the other modules

Question: 5

What are "Known" endpoints in ClearPass?

A. These are endpoints whose beacons have been detected but have never completed authentication
B. The label "Known" indicates rogue endpoints labeled as "friendly" or "ignore"
C. "Known" endpoints have be fingerprinted to determine their operating system and manufacturer.
D. "Known" endpoints can be authenticated based on MAC address to bypass the captive portal login.

Answer: D