HP

Exam Questions HPE6-A68

Aruba Certified Clearpass Professional 6.7

NEW QUESTION 1

Based on the Policy configuration shown, which VLAN will be assigned when a user with ClearPass role Engineer authenticates to the network successfully using connection protocol WEBAUTH?

Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

| Summary | Enforcement | Rules |

Enforcement:

Name:	Vlan enforcement
Description:	
Enforcement Type:	RADIUS
Default Profile:	Internet VLAN

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS Engineer) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Connection:Protocol EQUALS RADIUS)	Full Access VLAN
2.	(Tips:Role EQUALS Manager) AND (Connection:Protocol BELONGS_TO RADIUS, TACACS, WEBAUTH, Application)	Full Access VLAN
3.	(Tips:Role EQUALS Engineer) AND (Connection:Protocol BELONGS_TO WEBAUTH)	Employee Vlan

A. Deny Access
B. Employee VLAN
C. Internet VLAN
D. Full Access VLAN

Answer: B

NEW QUESTION 2

An Android device goes through the single-SSID Onboarding process and successfully connects using EAP-TLS to the secure network.
What is the order in which services are triggered?

A. Onboard Authorization, Onboard Provisioning, Onboard Authorization
B. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization, Onboard Provisioning
C. Onboard Provisioning, Onboard Authorization, Onboard Pre-Auth
D. Onboard Provisioning, Onboard Authorization, Onboard Provisioning
E. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization

Answer: D

NEW QUESTION 3

Refer to the exhibit.

Configuration » Enforcement » Policies » Edit - Onboard Provisioning - Aruba

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

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?

A. Onboard Post-Provisioning – Aruba
B. Onboard Pre-Provisioning – Aruba
C. Deny Access Profile
D. Onboard Device Repository

Answer: A

NEW QUESTION 4

Refer to the exhibit.

Home >> Configuration >> Web Logins

RADIUS Web Login

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

RADIUS Web Login Editor	
* Name:	Guest Network Enter a name for this web login page.
Page Name:	Aruba_login Enter a page name for this web login. The web login 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.
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. The address above will be used whenever the parameter is not available or fails.

When configuring a Web Login Page in ClearPass Guest, the information shown is displayed. What is the Address field value 'securelogin.arubanetworks.com' used for?

A. for ClearPass to send a TACACS+ request to the NAD
B. for appending to the Web Login URL, before the page name
C. for the client to POST the user credentials to the NAD
D. for ClearPass to send a RADIUS request to the NAD
E. for appending to the Web Login URL, after the page name.

Answer: C

NEW QUESTION 5
What is a benefit of ClearPass Onguard?

A. It enables organizations to run advanced endpoint posture assessments.
B. It allows a receptionist in a hotel to create accounts for guest users.
C. It allows employees to self-provision their personal devices on the corporate network.
D. It offers an easy way for users to self-configure their devices to support 802.1X authentication on wired and wireless networks.
E. It allows employees to create temporary accounts for Wi-Fi access.

Answer: A

NEW QUESTION 6
Refer to the exhibit.

Captive Portal Authentication Profile > default   **Show Reference**   **Save As**   **Reset**

Default Role	guest ▼	Default Guest Role	guest ▼
Redirect Pause	10 sec	User Login	✔
Guest Login	☐	Logout popup window	✔
Use HTTP for authentication	☐	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	☐
Use CHAP (non-standard)	☐	Login page	/auth/index.html
Welcome page	/auth/welcome.html	Show Welcome Page	✔
Add switch IP address in the redirection URL	☐	Allow only one active user session	☐
While List	▲ Delete / ▼ Add	Black List	▲ Delete / ▼ Add
Show the acceptable use policy page	☐		

Based on the information shown, which field in the Captive Portal Authentication profile should be changed so that guest users are redirected to a page on ClearPass when they connect to the Guest SSID?

A. both Login and Welcome Page
B. Default Role
C. Welcome Page
D. Default Guest Role
E. Login Page

Answer: E

Explanation:
The Login page is the URL of the page that appears for the user logon. This can be set to any URL.
The Welcome page is the URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.
References:
http://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Captive_Portal/C

NEW QUESTION 7
What does Authorization allow users to do in a Policy Service?

A. To use attributes in databases in role mapping and Enforcement.
B. To use attributes stored in databases in Enforcement only, but not role mapping.
C. To use attributes stored in external databases for Enforcement, but not internal databases.
D. To use attributes stored in databases in role mapping only, but not Enforcement.
E. To use attributes sored in internal databases for Enforcement, but not external databases.

Answer: A

NEW QUESTION 8
What are Operator Profiles used for?

A. to enforce role based access control for Aruba Controllers
B. to enforce role based access control for ClearPass Policy Manager admin users
C. to enforce role based access control for ClearPass Guest Admin users
D. to assign ClearPass roles to guest users
E. to map AD attributes to admin privilege levels in ClearPass Guest

Answer: C

Explanation:
An operator profile determines what actions an operator is permitted to take when using ClearPass Guest. References:
http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/OperatorLogins/Operato

NEW QUESTION 9
Refer to the exhibit.

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

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

Answer: BD

NEW QUESTION 10
When is the RADIUS server certificate used? (Select two.)

A. During dual SSID onboarding, when the client connects to the Guest network
B. During EAP-PEAP authentication in single SSID onboarding
C. During post-Onboard EAP-TLS authentication, when the client verifies the server certificate
D. During Onboard Web Login Pre-Auth, when the client loads the Onboarding web page
E. During post-Onboard EAP-TLS authentication, when the server verifies the client certificate

Answer: CD

NEW QUESTION 10
Refer to the exhibit.

Based on the configuration for 'maximum devices' shown, which statement accurately describes its settings?

A. The user cannot Onboard any devices.
B. It limits the total number of devices that can be provisioned by ClearPass.
C. It limits the total number of Onboarded devices connected to the network.
D. It limits the number of devices that a single user can Onboard.
E. It limits the number of devices that a single user can connect to the network.

Answer: D

NEW QUESTION 12
Refer to the exhibit.

Summary	Enforcement	Rules

Enforcement:

Name:	Handheld_Wireless_Access_Policy
Description:	Enforcement policy for handheld wireless access
Enforcement Type:	RADIUS
Default Profile:	WIRELESS_CAPTIVE_NETWORK

Rules:

Rules Evaluation Algorithm:	First applicable

Conditions	Actions
1. (Tips:Role MATCHES_ANY [guest])	WIRELESS_GUEST_NETWORK
2. (Endpoint:OS Version CONTAINS Android)	WIRELESS_HANDHELD_NETWORK
3. (Tips:Role MATCHES_ANY conferencelaptop developer senior_mgmt testqa Role_Engineer)	WIRELESS_EMPLOYEE_NETWORK

A user who is tagged with the ClearPass roles of Role_Engineer and developer, but not testqa, connects to the network with a corporate Windows laptop.
Which Enforcement Profile is applied?

A. WIRELESS_GUEST_NETWORK
B. WIRELESS_CAPTIVE_NETWORK
C. WIRELESS_HANDHELD_NETWORK
D. Deny Access
E. WIRELESS_EMPLOYEE_NETWORK

Answer: E

Explanation:
MATCHES_ANY: For list data types, true if any of the run-time values in the list match one of the configured values.
Example: Tips:Role MATCHES_ANY HR,ENG,FINANCE
References:
http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Rules

---

NEW QUESTION 13
If the "Alerts" tab in an access tracker entry shows the following error message: "Access denied by policy", what could be a possible cause for authentication failure?

A. Configuration of the Enforcement Policy.
B. An error in the role mapping policy.
C. Failure to select an appropriate authentication method for the authentication request.
D. Implementation of a firewall policy on ClearPass.
E. Failure to find an appropriate service to process the authentication request.

Answer: A

NEW QUESTION 18
An SNMP probe is sent from ClearPass to a network access device, but ClearPass is unable to obtain profiling information.
What are likely causes? (Select three.)

A. Only SNMP read has been configured but SNMP write is needed for profiling information.
B. An external firewall is blocking SNMP traffic.
C. SNMP is not enabled on the NAD.
D. SNMP community string in the ClearPass and NAD configuration is mismatched.
E. SNMP probing is not supported between ClearPass and NADs.

Answer: BCD

Explanation:
Verify firewall port 162 (default) is open between AMP and the controller. SNMP must be enabled on the NAD.
The community string that ClearPass is using to access the NAD might be wrong.
References:
https://community.arubanetworks.com/t5/Monitoring-Management-Location/SNMP-Get-Failed-quot-error-mess

---

NEW QUESTION 22
When a third party Mobile Device Management server is integrated with ClearPass, where is the endpoint information from the MDM server stored in ClearPass?

A. Endpoints repository
B. Onboard Device repository
C. MDM repository
D. Guest User repository
E. Local User repository

Answer: A

Explanation:

A service running in CPPM periodically polls MDM servers using their exposed APIs. Device attributes obtained from MDM are added as endpoint tags. Profiler related attributes are send to profiler which uses these attributes to derive final profile.
References: ClearPass Profiling TechNote (2014), page 23
https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%

NEW QUESTION 23
During a web login authentication, what is expected to happen as part of the Automated NAS login?

A. NAD sends TACACS+ request to ClearPass.
B. ClearPass sends TACACS+ request to NAD.
C. Client device sends RADIUS request to NAD.
D. NAD sends RADIUS request to ClearPass.
E. ClearPass sends RADIUS request to NAD.

Answer: D

NEW QUESTION 25
Refer to the exhibit.

Configuration » Authentication » Sources » Add - remotelab AD

Authentication Sources - remotelab AD

| Summary | General | Primary | **Attributes** |

Specify filter queries used to fetch authentication and authorization attributes.

	Filter Name	Attribute Name	Alias Name	Enabled as
1.	Authentication	dn	UserDN	-
		department	Department	Role, Attribute
		title	Title	Attribute
		company	company	-
		memberOf	memberOf	Role, Attribute
		telephoneNumber	Phone	Attribute
		mail	Email	Attribute

Based on the Attribute configuration shown, which statement accurately describes the status of attribute values?

A. Only the attribute values of department and memberOf can be used in role mapping policies.
B. The attribute values of department, title, memberOf, telephoneNumber, and mail are directly applied as ClearPass.
C. Only the attribute value of company can be used in role mapping policies, not the other attributes.
D. The attribute values of department and memberOf are directly applied as ClearPass roles.
E. Only the attribute values of title, telephoneNumber, and mail can be used in role mapping policies.

Answer: D

NEW QUESTION 27
A hotel chain deployed ClearPass Guest. When hotel guests connect to the Guest SSID, launch a web browser and enter the address www.google.com, they are unable to immediately see the web login page.
What are the likely causes of this? (Select two.)

A. The ClearPass server has a trusted server certificate issued by Verisign.
B. The ClearPass server has an untrusted server certificate issued by the internal Microsoft Certificate server.
C. The ClearPass server does not recognize the client's certificate.
D. The DNS server is not replying with an IP address for www.google.com.

Answer: BD

Explanation:
You would need a publicly signed certificate.
References:
http://community.arubanetworks.com/t5/Security/Clearpass-Guest-certificate-error-for-guest-visitors/td-p/22199

NEW QUESTION 30
Refer to the exhibit.

What is the purpose of the 'Clock Skew Allowance' setting? (Select two.)

A. to ensure server certificate validation does not fail due to client clock sync issues
B. to set start time in client certificate to a few minutes before current time
C. to adjust clock time on client device to a few minutes before current time
D. to ensure client certificate validation does not fail due to client clock sync issues
E. to set expiry time in client certificate to a few minutes longer than the default setting

Answer: D

Explanation:
Clock Skew Allowance adds a small amount of time to the start and end of the client certificate's, not the server certificate's, validity period. This permits a newly issued certificate to be recognized as valid in a network where not all devices are perfectly synchronized.
References:
http://www.arubanetworks.com/techdocs/ClearPass/6.6/Guest/Content/Onboard/EditingCASettings.htm

NEW QUESTION 35
Refer to the exhibit.

Based on the Endpoint information shown, which collectors were used to profile the device as Apple iPad? (Select two.)

A. HTTP User-Agent
B. SNMP
C. DHCP fingerprinting
D. SmartDevice
E. Onguard Agent

Answer: AC

Explanation:
 HTTP User-Agent
In some cases, DHCP fingerprints alone cannot fully classify a device. A common example is the Apple family of smart devices; DHCP fingerprints cannot distinguish between an Apple iPad and an iPhone. In these scenarios, User-Agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.
User-Agent strings are collected from:
* ClearPass Guest
* ClearPass Onboard
* Aruba controller through IF-MAP interface
Note: Collectors are network elements that provide data to profile endpoints.
The following collectors send endpoint attributes to Profile:
* DHCP
DHCP snooping Span ports
* ClearPass Onboard
* HTTP User-Agent
*MAC OUI – Acquired via various auth mechanisms such as 802.1X, MAC auth, etc.
* ActiveSync plugin
* CPPM OnGuard
*SNMP
* Subnet Scanner
* IF-MAP

* Cisco Device Sensor (Radius Accounting)
* MDM
References: Tech Note: ClearPass Profiling (2014), page 11
https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%

NEW QUESTION 39
Refer to the exhibit.

Based on the Guest Role Mapping Policy shown, what is the purpose of the Role Mapping Policy?

A. to display a role name on the Self-registration receipt page
B. to send a firewall role back to the controller based on the Guest User's Role ID
C. to assign Controller roles to guests
D. to assign three roles of [Contractor], [Guest] and [Employee] to every guest user
E. to create additional account roles for guest administrators to assign to guest accounts

Answer: C

NEW QUESTION 43
An administrator enabled the Pre-auth check for their guest self-registration. At what stage in the registration process in this check performed?

A. after the user clicks the login button and after the NAD sends an authentication request
B. after the user self-registers but before the user logs in
C. after the user clicks the login button but before the NAD sends an authentication request
D. when a user is re-authenticating to the network
E. before the user self-registers

Answer: C

Explanation:
The Onboard template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials before starting the device provisioning process. This also creates an authorization service that checks whether a user's device can be provisioned using Onboard.

NEW QUESTION 46
Use this form to make changes to the RADIUS Web Login Guest Network.
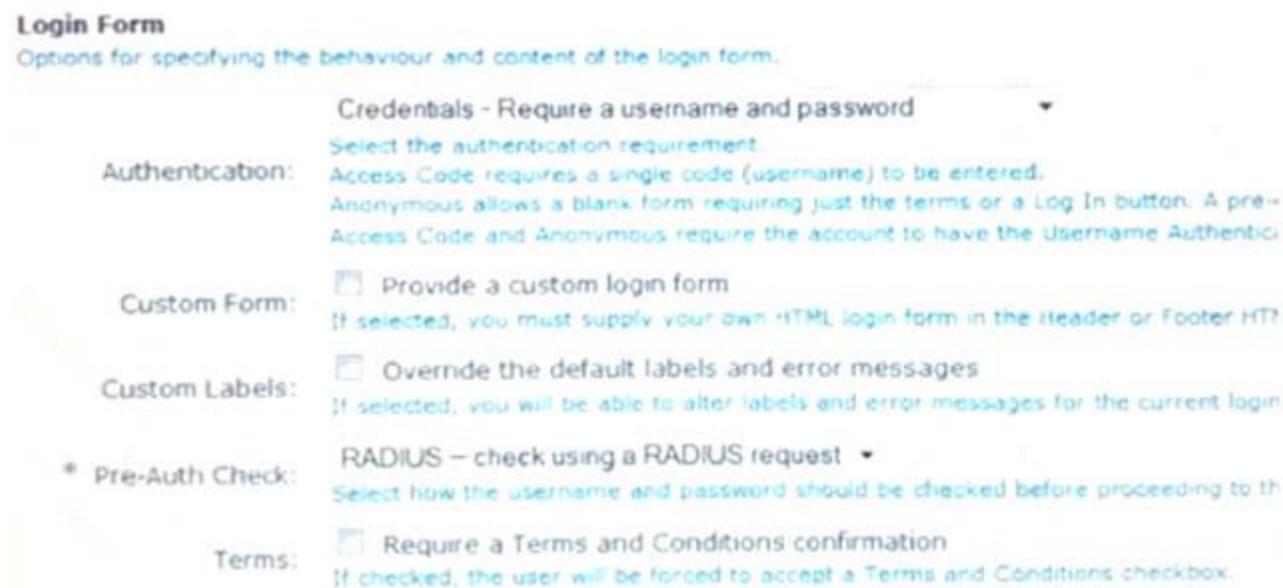
A Web Login page is configured in Clear Pass Guest as shown. What is the purpose of the Pre-Auth Check?

A. To authenticate users after the NAD sends an authentication request to ClerPass
B. To authenticate users before the client sends the credentials to the NAD
C. To authenticate users when they are roaming from one NAD to another
D. To authenticate users before they launch the Web Login Page
E. To replace the need for the NAD to send an authentication request to ClearPass

Answer: B

NEW QUESTION 49
Which steps are required to use ClearPass as a TACACS+ Authentication server for a network device? (Select two.)

A. Configure a TACACS Enforcement Profile on ClearPass for the desired privilege level.
B. Configure a RADIUS Enforcement Profile on ClearPass for the desired privilege level.
C. Configure ClearPass as an Authentication server on the network device.
D. Configure ClearPass roles on the network device.
E. Enable RADIUS accounting on the NAD.

Answer: AC

Explanation:
You need to make sure you modify your policy (Configuration » Enforcement » Policies » Edit - [Admin Network Login Policy]) and add your AD group settings in to the corresponding privilege level.

NEW QUESTION 53
......