

HPE6-A68^{Q&As}

Aruba Certified ClearPass Professional (ACCP) V6.7

Pass HP HPE6-A68 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.certbus.com/hpe6-a68.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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

Correct Answer: A

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%20TechNote.pdf>

QUESTION 2

Refer to the exhibit.

Filter: ▼ contains

#	<input type="checkbox"/>	User ID ▲	Name	Role
1.	<input type="checkbox"/>	john	john	[Employee]
2.	<input type="checkbox"/>	mike	mike	[Employee]
3.	<input type="checkbox"/>	neil	neil	[Employee]

Showing 1-3 of 3

Based on the Local User repository in ClearPass shown, which Aruba firewall role will be assigned to "mike" when this user authenticates Aruba Controller?

- A. We can't know this from the screenshot above.
- B. mike
- C. Employee
- D. john

Correct Answer: A

QUESTION 3

What is the purpose of RADIUS CoA (RFC 3576)?

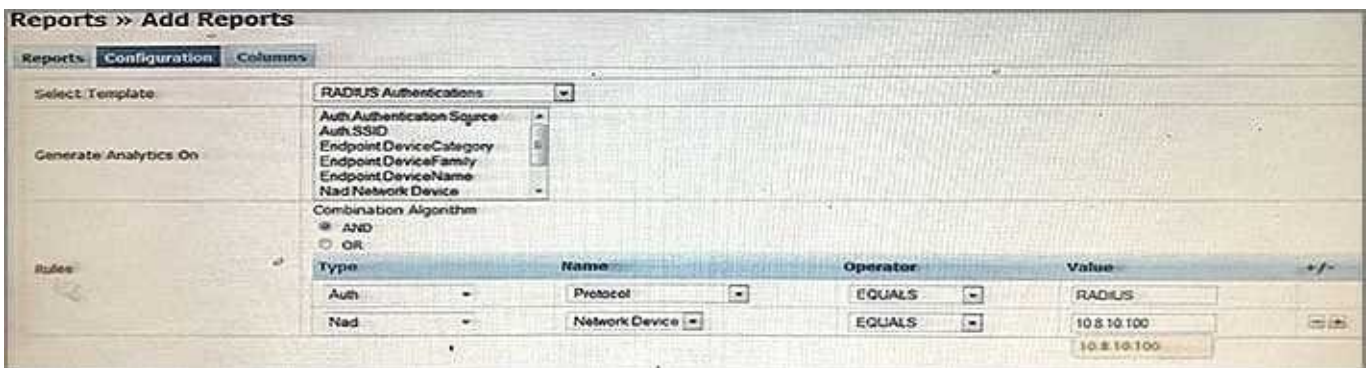
- A. to force the client to re-authenticate upon roaming to a new Controller
- B. to apply firewall policies based on authentication credentials
- C. to validate a host MAC address against a whitelist or a blacklist
- D. to authenticate users or devices before granting them access to a network
- E. to transmit messages to the NAD/NAS to modify a user's session status

Correct Answer: E

CoA messages modify session authorization attributes such as data filters. References:
<https://tools.ietf.org/html/rfc3576>

QUESTION 4

Refer to the exhibit.



Which types of records will the report shown display?

- A. all RADIUS authentications from the 10.8.10.100 NAD to ClearPass
- B. all failed RADIUS authentications through ClearPass
- C. only Windows devices that have authenticated through the 10.8.10.100 NAD
- D. all successful RADIUS authentications through ClearPass
- E. all successful RADIUS authentications from the 10.8.10.100 NAD to ClearPass

Correct Answer: A

QUESTION 5

Refer to the exhibit.

Administration » Server Manager » Server Configuration

Server Configuration

✕
Cluster-Wide Parameters

General

Cleanup Intervals

Notifications

Standby Publisher

Virtual IP Configuration

Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	TRUE ▼	FALSE
Designated Standby Publisher	cp82.clearpass ▼	0
Failover Wait Time	10 ▼ minutes	10

Restore Defaults
Save
Cancel

Which statements accurately describe the cp82 ClearPass node? (Select two.)

- A. It becomes the Publisher when the primary Publisher fails.
- B. It operates as a Publisher in the same cluster as the primary Publisher when the primary is active.
- C. It operates as a Publisher in a separate cluster when the Publisher is active.
- D. It operates as a Subscriber when the Publisher is active.
- E. It stays as a Subscriber when the Publisher fails.

Correct Answer: AD

ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.

When a Publisher failure is detected, the designated subscriber node is promoted to active Publisher status.

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deployment/Standby_publisher.htm

QUESTION 6

Which components can use Active Directory authorization attributes for the decision-making process? (Select two.)

- A. Profiling policy
- B. Certificate validation policy
- C. Role Mapping policy

D. Enforcement policy

E. Posture policy

Correct Answer: CD

C: Role Mappings Page - Rules Editor Page Parameters

Parameter	Description
Type	<p>The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context (Refer to Namespaces.)</p> <p>In the role mapping context, Policy Manager allows attributes from following namespaces:</p> <ul style="list-style-type: none"> Application Application:ClearPass Authentication Authorization Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (See Adding and Modifying Authentication Sources). Only those attributes that have been configured to be fetched are shown in the attributes drop-down list. Certificate Connection Date Device Fingerprint GuestUser Host LocalUser Onboard IACACS RADIUS - All enabled RADIUS vendor dictionaries.
Name	Displays the drop-down list of attributes present in the selected namespace
Operator	Displays the drop-down list of context-appropriate (with respect to the attribute data type) operators. Operators have the obvious meaning; for stated definitions of operator meaning, refer to Operators .
Value	Depending on attribute data type this may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget.

D: Enforcement Policy Attributes tab Parameters

Attribute	Description
Type:	Select the type of attributes from the drop-down list.
Host	See Host Namespaces
Authentication	See Authentication Namespaces
Connection	See Connection Namespaces
Application	See Application Namespace
<ul style="list-style-type: none"> Radius:IETF Radius:Cisco Radius:Microsoft Radius:Avenda Radius:Aruba 	See RADIUS Namespaces
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

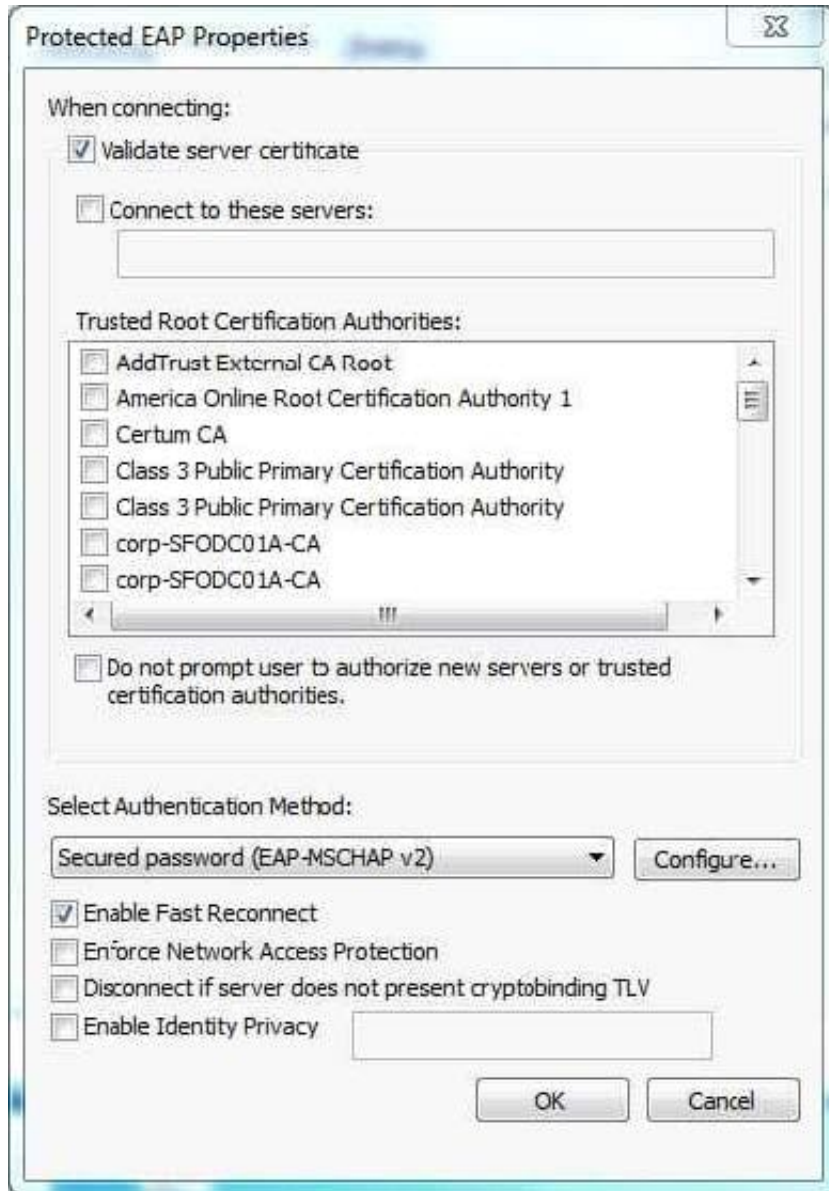
References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPM_UserGuide/identity/RoleMappingPolicies.html http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/

CPPM_UserGuide/PolicySim/PS_Enforcement_Policy.htm

QUESTION 7

Refer to the exhibit.



Based on the configuration of a Windows 802.1X supplicant shown, what will be the outcome of selecting 'Validate server certificate'?

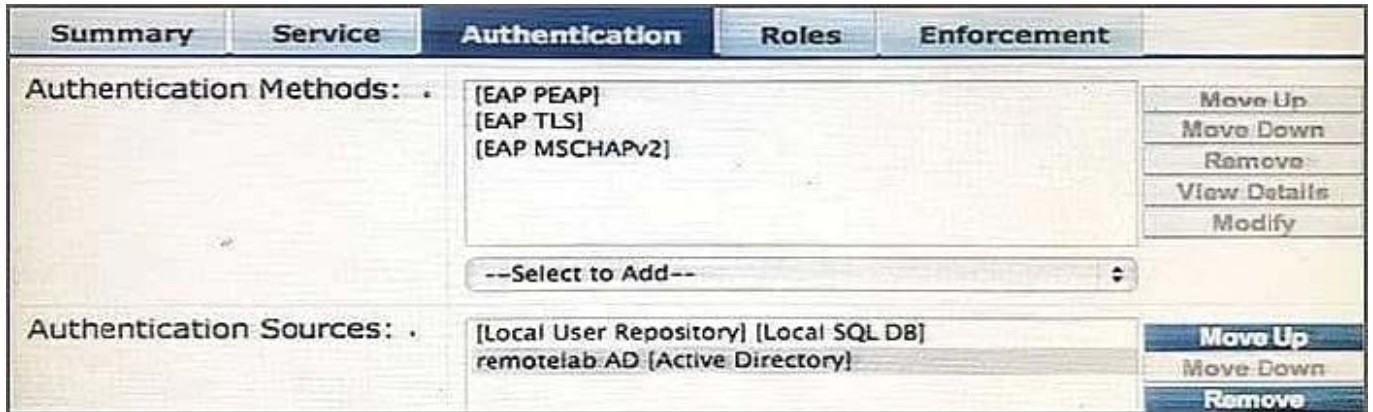
- A. The server and client will perform an HTTPS SSL certificate exchange.
- B. The client will verify the server certificate against a trusted CA.
- C. The client will send its private key to the server for verification.
- D. The server will send its private key to the client for verification.

E. The client will send its certificate to the server for verification.

Correct Answer: B

QUESTION 8

Refer to the exhibit.



Based on the Authentication sources configuration shown, which statement accurately describes the outcome if the user is not found?

- A. If the user is not found in the remotelab AD but is present in the local user repository, a reject message is sent back to the NAD.
- B. If the user is not found in the local user repository but is present in the remotelab AD, a reject message is sent back to the NAD.
- C. If the user is not found in the local user repository a reject message is sent back to the NAD.
- D. If the user is not found in the local user repository and remotelab AD, a reject message is sent back to the NAD.
- E. If the user is not found in the local user repository a timeout message is sent back to the NAD.

Correct Answer: D

Policy Manager looks for the device or user by executing the first filter associated with the authentication source.

After the device or user is found, Policy Manager then authenticates this entity against this authentication source. The flow is outlined below:

1.

On successful authentication, Policy Manager moves on to the next stage of policy evaluation, which collects role mapping attributes from the authorization sources.

2.

Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this service.

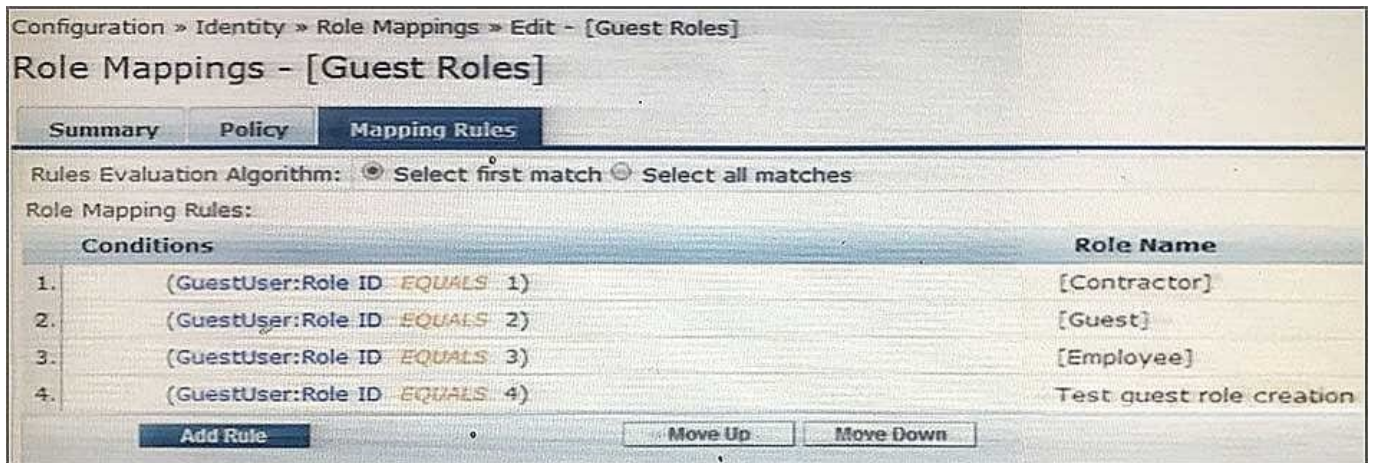
3.

If Policy Manager does not find the connecting entity in any of the configured authentication sources, it rejects the request.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 134 <https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf>

QUESTION 9

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

Correct Answer: C

QUESTION 10

Refer to the exhibit.

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	

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

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

Correct Answer: B

QUESTION 11

Refer to the exhibit.



The ClearPass Event Viewer displays an error when a user authenticates with EAP-TLS to ClearPass through an Aruba Controller Wireless Network. What is the cause of this error?

- A. The controller's shared secret used during the certificate exchange is incorrect.
- B. The NAS source interface IP is incorrect.
- C. The client sent an incorrect shared secret for the 802.1X authentication.
- D. The controller used an incorrect shared secret for the RADIUS authentication.
- E. The client's shared secret used during the certificate exchange is incorrect.

Correct Answer: D

QUESTION 12

Refer to the exhibit.

Summary	Policy	Mapping Rules
Policy:		
Policy Name:	WLAN role mapping	
Description:		
Default Role:	[Guest]	
Mapping Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Role Name	
1. (Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive	
2. (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor	
3. (Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device	
4. (Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-week NOT_BELONGS_TO Saturday, Sunday)	HR Local	
5. (Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User	
6. (Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee	

An AD user's department attribute value is configured as "QA". The user authenticates from a laptop running MAC OS X. Which role is assigned to the user in ClearPass?

- A. HR Local
- B. Remote Employee
- C. [Guest]
- D. Executive
- E. IOS Device

Correct Answer: C

None of the Listed Role Name conditions are met.

QUESTION 13

Refer to the exhibit.



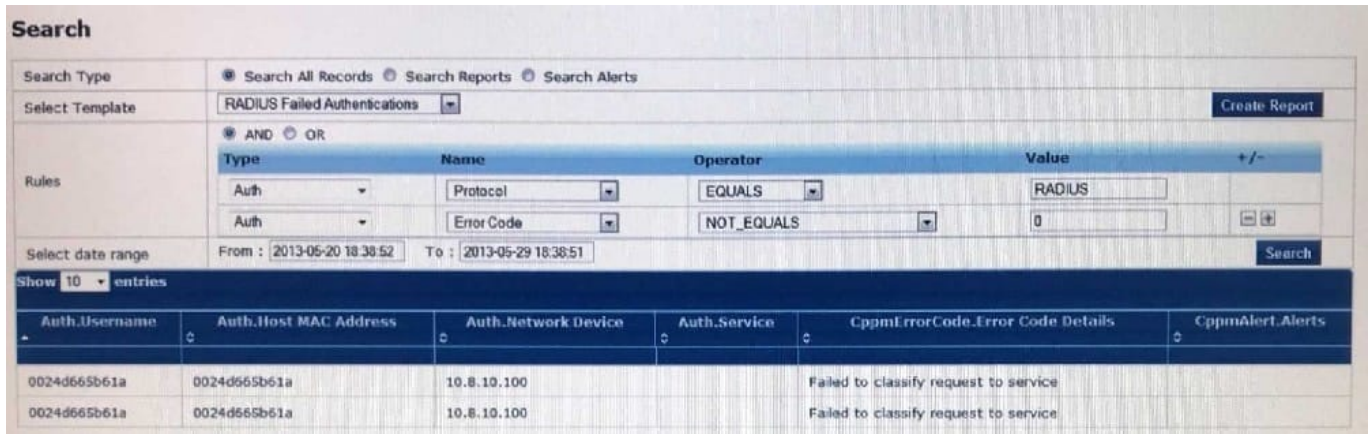
Based on the configuration for `maximum devices` shown, which statement accurately describes its settings?

- 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.

Correct Answer: D

QUESTION 14

Refer to the exhibit.



An administrator configured a service and tested authentication, but was unable to complete authentication successfully. The administrator performs a Search using insight and the information displays as shown. What is a possible reason for the ErrorCode `Failed to classify request to service` shown?

- A. The user failed authentication due to an incorrect password.
- B. ClearPass could not match the authentication request to a service, but the user passed authentication.
- C. ClearPass service authentication sources were not configured correctly.

- D. The NAD did not send the authentication request.
- E. ClearPass service rules were not configured correctly.

Correct Answer: E

QUESTION 15

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.

Correct Answer: D