HP

HPE6-A68 Exam

HP Aruba Certified ClearPass Professional (ACCP) 6.7 Exam

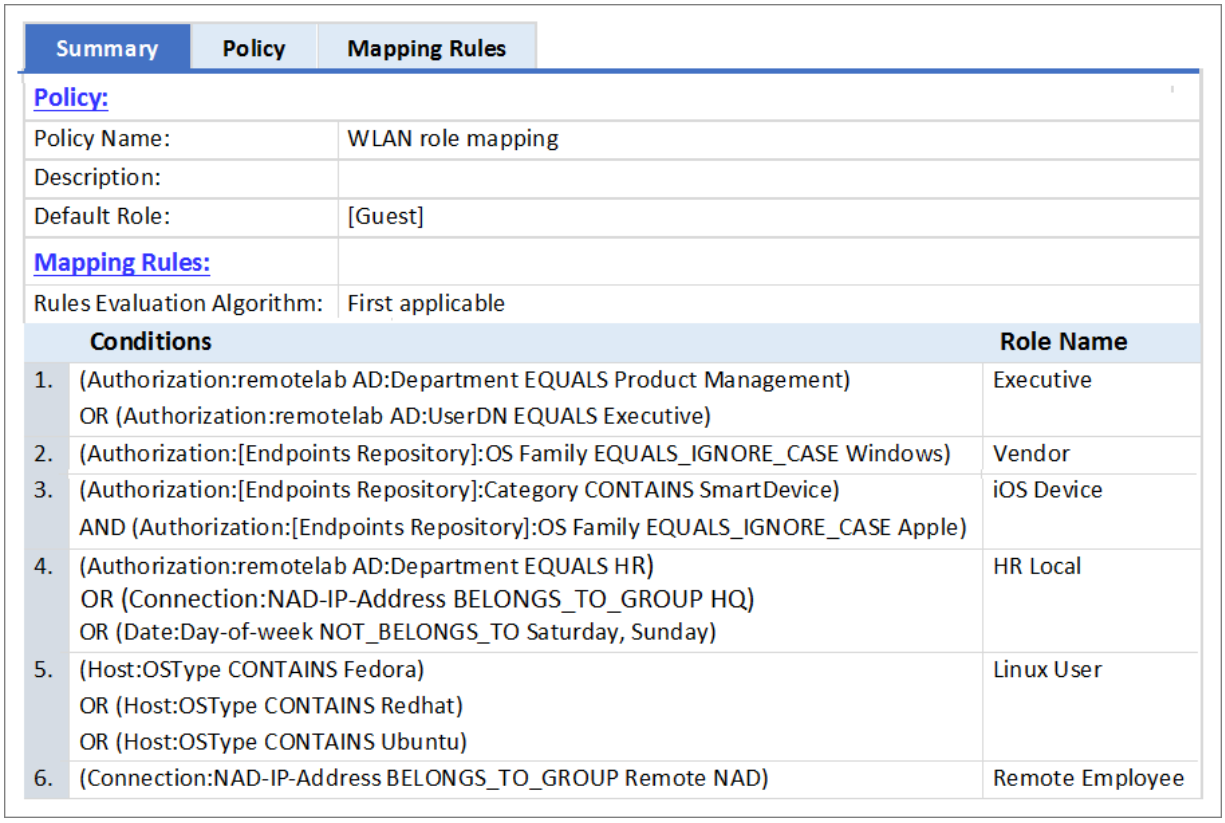
Questions & Answers
(Demo Version – Limited Content)

Thank you for Downloading HPE6-A68 exam PDF Demo

Version: 8.0

Question: 1

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?

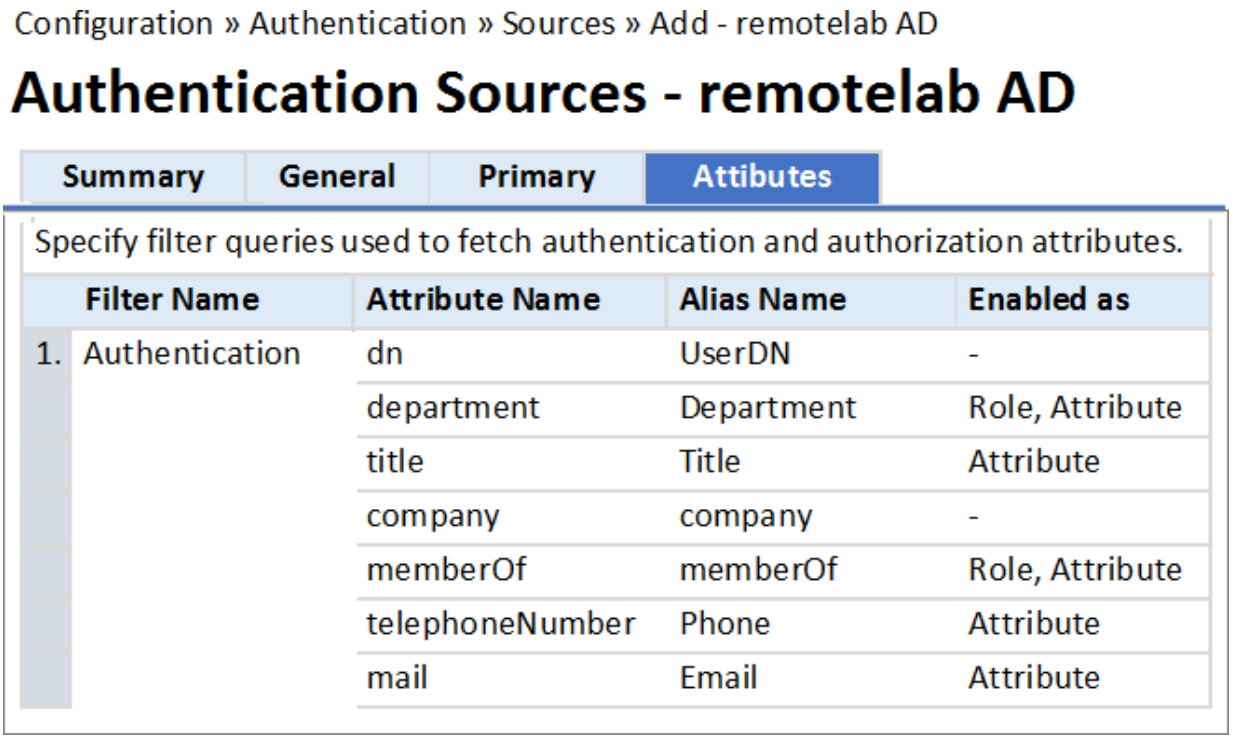
A. HR Local
B. Remote Employee
C. [Guest]
D. Executive
E. IOS Device

Answer: C

Explanation:
None of the Listed Role Name conditions are met.

Question: 2

Refer to the exhibit.



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

Question: 3

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

Answer: C,D

Explanation:
C: Role Mappings Page - Rules Editor Page Parameters

Parameter	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to Namespaces.) In the role mapping context, Policy Manager allows attributes from following namespaces: • 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 • Endpoint • GuestUser • Host • LocalUser • Onboard • TACACS • 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.

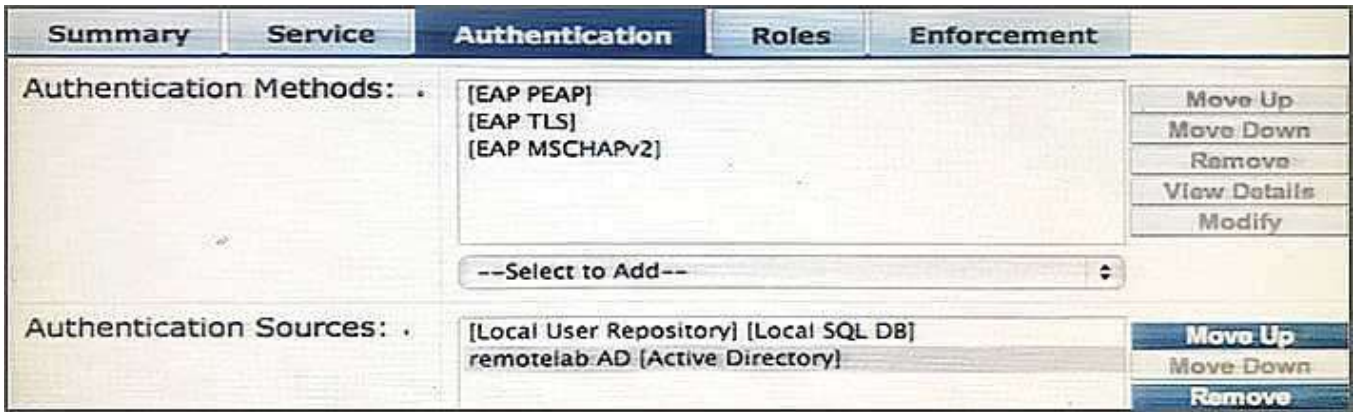
D: Enforcement Policy Attributes tab Parameters

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
• 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/CPPM_UserGuide/identity/RoleMappingPolicies.html
http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/PolicySim/PS_Enforcement_Policy.htm

Question: 4

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.

Answer: D

Explanation:
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:
* On successful authentication, Policy Manager moves on to the next stage of policy evaluation, which
collects role mapping attributes from the authorization sources.
* 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.
* 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: 5

Which authorization servers are supported by ClearPass? (Select two.)

A. Aruba Controller
B. LDAP server
C. Cisco Controller
D. Active Directory
E. Aruba Mobility Access Switch

Answer: B,D

Explanation:
Authentication Sources can be one or more instances of the following examples:
* Active Directory
* LDAP Directory
* SQL DB
* Token Server
* Policy Manager local DB
References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 114
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

Question: 6

Which CLI command is used to upgrade the image of a ClearPass server?

A. Image update
B. System upgrade
C. Upgrade image
D. Reboot
E. Upgrade software

Answer: B

Explanation:
When logged in as appadmin, you can manually install the Upgrade and Patch binaries imported via the CLI using the
following commands:
* system update (for patches)
* system upgrade (for upgrades)
References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 564
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

Question: 7

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: A,C

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.

Question: 8

What are Operator Profiles used for?

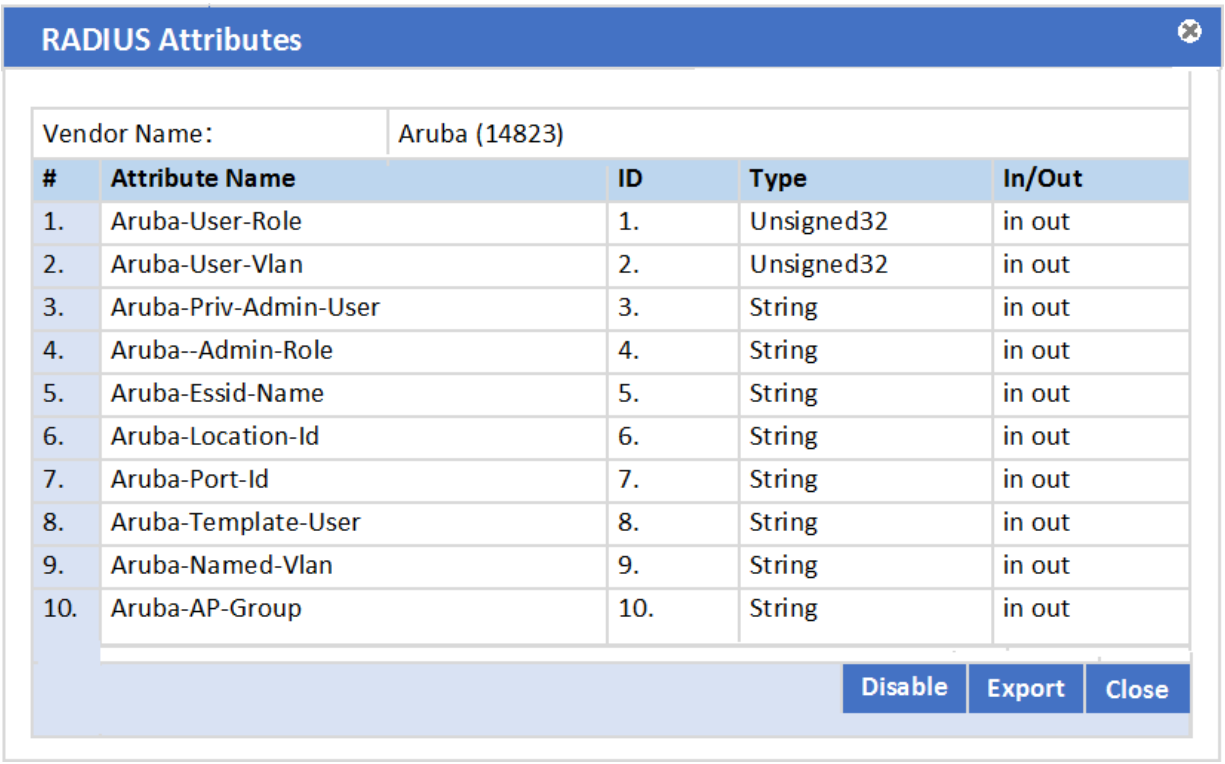
A. to enforce role based access control for Aruba Controllers
B. to enforce role based access control for ClearPass Policy Manager admin users
C. to enforce role based access control for ClearPass Guest Admin users
D. to assign ClearPass roles to guest users
E. to map AD attributes to admin privilege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

Question: 9

Refer to the exhibit.



RADIUS Attributes

Vendor Name: Aruba (14823)

#	Attribute Name	ID	Type	In/Out
1.	Aruba-User-Role	1.	Unsigned32	in out
2.	Aruba-User-Vlan	2.	Unsigned32	in out
3.	Aruba-Priv-Admin-User	3.	String	in out
4.	Aruba--Admin-Role	4.	String	in out
5.	Aruba-Essid-Name	5.	String	in out
6.	Aruba-Location-Id	6.	String	in out
7.	Aruba-Port-Id	7.	String	in out
8.	Aruba-Template-User	8.	String	in out
9.	Aruba-Named-Vlan	9.	String	in out
10.	Aruba-AP-Group	10.	String	in out

Disable Export Close

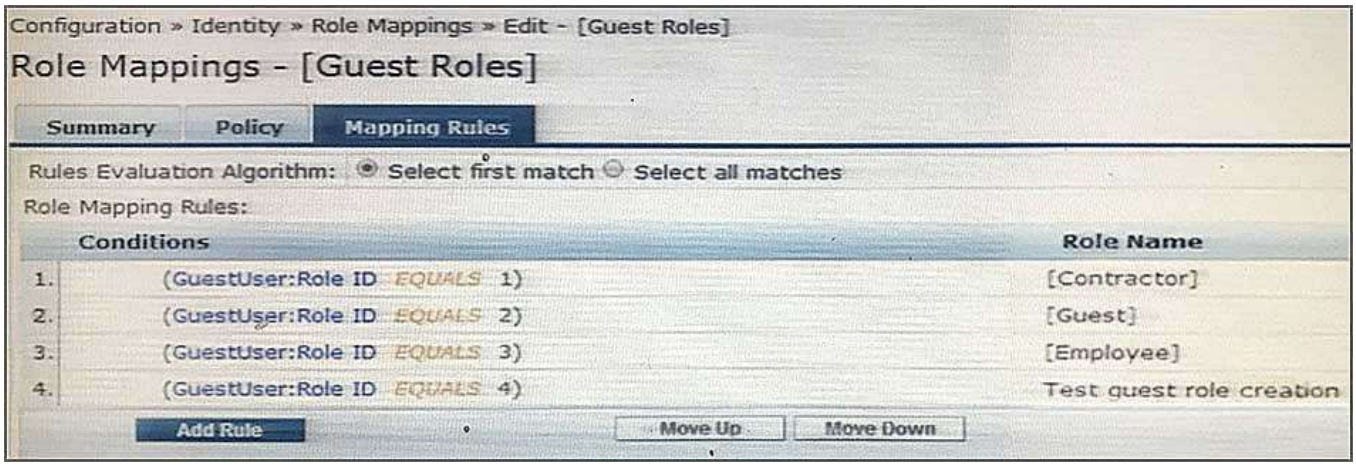
In the Aruba RADIUS dictionary shown, what is the purpose of the RADIUS attributes?
In the Aruba RADIUS dictionary shown, what is the purpose of the RADIUS attributes?

A. to send information via RADIUS packets to Aruba NADs
B. to gather and send Aruba NAD information to ClearPass
C. to send information via RADIUS packets to clients
D. to gather information about Aruba NADs for ClearPass
E. to send CoA packets from ClearPass to the Aruba NAD

Answer: C

Question: 10

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

Thank You for trying HPE6-A68 PDF Demo