



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.geekcert.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

Refer to the exhibit.

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

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

- 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.

Correct Answer: E

Session Timeout (in seconds) - Configure the agent session timeout interval to re-evaluate the system health again. OnGuard triggers auto-remediation using this value to enable or disable AV-RTP status check on endpoint. Agent re-

authentication is determined based on session-time out value. You can specify the session timeout interval from 60 ?600 seconds. Setting the lower value for session timeout interval results numerous authentication requests in Access

Tracker page. The default value is 0.

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Enforce/EPAgent_Enforcement.htm

QUESTION 2

Refer to the exhibit.



Data Retention
Import Configuration
Operator Logins
Start Here
Login Configuration
Profiles
Servers
Translation Rules
Plugin Manager
SMS Services
Support

4 **MatchAdmin** *memberOf contains CN=Administrators*

Edit Delete Duplicate Disable Move Up Move Down

Edit Translation Rule

*Name:	MatchAdmin <small>Enter a name for this translation rule.</small>
Enabled:	<input checked="" type="checkbox"/> Use this rule when processing reply attributes
Attribute Name:	memberOf <small>Enter the name of the attribute (e.g. memberOf). Use * for all attributes.</small>
Matching Rule:	contains <small>Select the matching rule to apply to the value of the attribute.</small>
Value:	CN=Administrators <small>Enter the value to match the attribute against.</small>
On Match:	Assign fixed operator profile <small>Select what happens when this translation rule matches an attribute.</small>
Operator Profile:	IT Administrators <small>Select the operator profile to assign.</small>
Fallthrough:	<input type="checkbox"/> Continue translation if rule matches <small>Check this box if you want to apply multiple translation rules.</small>

Save Changes Cancel

Based on the Translation Rule configuration shown, what will be the outcome?

- A. An AD user from group Administrators will be assigned the operator profile of IT Administrators.
- B. All ClearPass Policy Manager admin users who are members of the Administrators AD group will be assigned the TACACS profile of IT Administrators.
- C. All active directory users will be assigned the operator profile of IT Administrators.
- D. A user from AD group MatchAdmin will be assigned the operator profile of IT Administrators.

Correct Answer: A

QUESTION 3

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 stored in internal databases for Enforcement, but not external databases.

Correct Answer: A

QUESTION 4

Refer to the exhibit.



Based on the information shown, what will be the outcome when the administrator chooses "Deny Access to this Device"? (Select two.)

- A. EAP-TLS Authentication will be unaffected
- B. The user can Onboard their device again
- C. A new device certificate will be automatically pushed out to the device
- D. The user cannot Onboard their device again
- E. EAP-TLS Authentication will fail

Correct Answer: DE

The Device Management (View by Device) page lists all devices and lets you manage the devices' access to the network. For each device, you can allow or deny network access. When you select the Deny option, a message advises you that any certificates associated with it will be revoked. The device cannot be re-enrolled as long as access is denied. To re-enroll the device, you must use this field to allow access again.

References: <http://www.arubanetworks.com/techdocs/ClearPass/6.6/Guest/Content/Onboard/DeviceManagement.htm>



QUESTION 5

What must be configured to enable RADIUS authentication with ClearPass on a network access device (NAD)? (Select two.)

- A. the ClearPass server must have the network device added as a valid NAD
- B. the ClearPass server certificate must be installed on the NAD
- C. a matching shared secret must be configured on both the ClearPass server and NAD
- D. an NTP server needs to be set up on the NAD
- E. a bind username and bind password must be provided

Correct Answer: AC

[Latest HPE6-A68 Dumps](#)

[HPE6-A68 VCE Dumps](#)

[HPE6-A68 Braindumps](#)