

ACCP-V6.2^{Q&As}

Aruba Certified Clearpass Professional v6.2

Pass Aruba ACCP-V6.2 Exam with 100% Guarantee

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

<https://www.pass2lead.com/accp-v6-2.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

Refer to the screenshot below:



Which of the following statements is correct regarding the above configuration for 'maximum devices'?

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

Correct Answer: C

QUESTION 2

Refer to the screen capture below:

Filter: Type contains [] + Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.254.5.80	RADIUS	test1	Copy_of_Aruba Corporate Wireless	ACCEPT	2013/04/02 04:31:39
10.254.5.80	RADIUS	test1	Copy_of_Aruba Corporate Wireless	TIMEOUT	2013/04/02 04:31:21
10.254.5.80	WEBAUTH	4c60def412ee	Health Check for clients	ACCEPT	2013/04/02 04:31:17

Request Details		
Summary	Input	Output
Session Identifier:	W00000024-01-515a5f14	
Date and Time:	Apr 02, 2013 04:31:17 UTC	
End-Host Identifier:	4c60def412ee	
Username:	4c60def412ee	
Access Device IP/Port:	-	
System Posture Status:	HEALTHY (0)	
Policies Used -		
Service:	Health Check for clients	
Authentication Method:	Not applicable	
Authentication Source:	-	
Authorization Source:	-	
Roles:	[Guest]	
Enforcement Profiles:	[Aruba Terminate Session]	
Service Monitor Mode:	Disabled	

Based on the Access Tracker output for the user shown above, which of the following statements is true?

- A. A NAP agent was used to obtain the posture token for the user.
- B. The authentication method used is EAP-PEAP.
- C. A Healthy Posture Token was sent to the Policy Manager.
- D. A RADIUS-Access-Accept message is sent back to the Network Access Device.
- E. The Aruba Terminate Session enforcement profile is applied because the posture check failed.

Correct Answer: C

QUESTION 3

Refer to the screen capture below: Based on the Enforcement Policy configuration, if a user with Role Remote Worker connects to the network and the posture token assigned is quarantine, what Enforcement Profile will be applied?

Enforcement Policies - Enterprise Enforcement Policy

Summary	Enforcement	Rules
Enforcement:		
Name:	Enterprise Enforcement Policy	
Description:	Enforcement policies for local and remote employees	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
Rules Evaluation Algorithm:	Evaluate all	
Conditions	Actions	
1. (Tips:Posture EQUALS HEALTHY (0)) AND (Tips:Role MATCHES_ANY Remote Worker Role Engineer testqa) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN, [RADIUS] Remote Employee ACL	
2. (Tips:Role EQUALS Senior_Mgmt) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN	
3. (Tips:Role EQUALS San Jose HR Local) AND (Tips:Posture EQUALS HEALTHY (0))	HR VLAN	
4. (Tips:Role EQUALS [Guest]) AND (Connection:SSID CONTAINS guest)	[RADIUS] WIRELESS_GUEST_NETWORK	
5. (Tips:Role EQUALS Remote Worker) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	RestrictedACL	

- A. EMPLOYEE_VLAN
- B. Remote Employee ACL
- C. RestrictedACL
- D. Deny Access Profile
- E. HR VLAN

Correct Answer: C

QUESTION 4

Refer to the screenshot below:

The screenshot shows a 'Request Details' window with a blue header and four tabs: Summary, Input, Output, and Accounting. The 'Summary' tab is selected. Below the tabs is a table with the following data:

Session Identifier:	R0000028d-01-51565341
Date and Time:	Mar 30, 2013 10:51:45 SGT
End-Host Identifier:	00216A64F294
Username:	00216a64f294
Access Device IP/Port:	192.168.0.233:0
System Posture Status:	UNKNOWN (100)

Below this table is a section titled 'Policies Used -' with a blue header. It contains another table with the following data:

Service:	Returning Clients - MAC Authentication
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Endpoints Repository], [Insight Repository]
Roles:	[MAC Caching], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled

Why is the Insight Repository used as an authorization source for this MAC authentication service?

- A. To check how long ago the last web login authentication was done
- B. To check how many sessions ago the last web login authentication was done
- C. To check how long ago the last MAC authentication was done
- D. To run a report when the user authenticates
- E. To validate the user's MAC address against the endpoints table

Correct Answer: A

QUESTION 5

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

- A. Before the user self-registers.
- B. After the user self-registers; before the user logs in.
- C. After the user logs in; before the NAD sends an authentication request.
- D. After the user logs in; after the NAD sends an authentication request.
- E. When a user is re-authenticating to the network.

Correct Answer: C

[Latest ACCP-V6.2 Dumps](#)

[ACCP-V6.2 PDF Dumps](#)

[ACCP-V6.2 Study Guide](#)