

# ACCP-V6.2<sup>Q&As</sup>

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

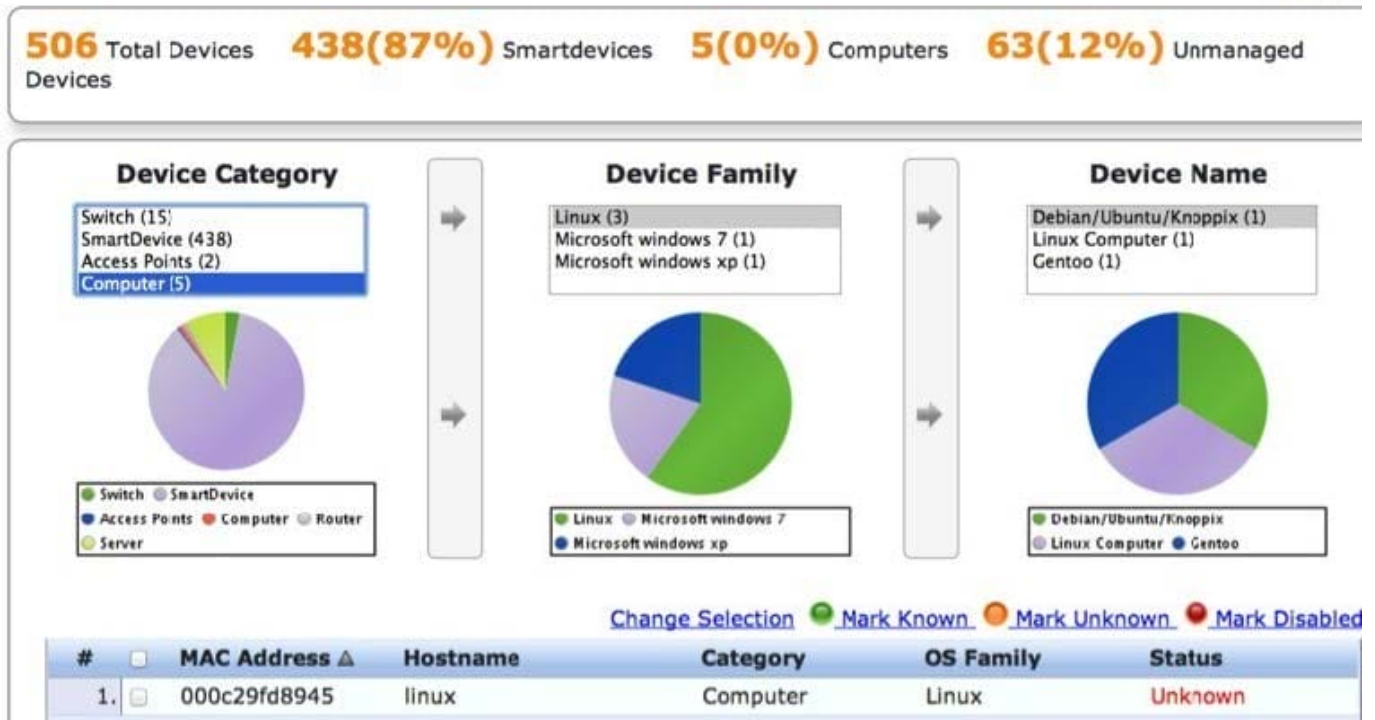


**QUESTION 1**

Refer to the screen capture below:

**Endpoint Profiler**

[Change](#)



Based on the Endpoint Profiler output shown here, which of the following statements is true?

- A. The devices have been profiled using DHCP fingerprinting.
- B. There are 5 devices profiled in the Computer Device Category.
- C. Apple devices will be profiled in the SmartDevice category.
- D. There is only 1 Microsoft Windows device present in the network.
- E. The linux device with MAC address 000c29fd8945 has not been profiled.

Correct Answer: B

**QUESTION 2**

Refer to the screenshot below:

Which of the following statements is true regarding the above configuration for network settings? (Choose 2)

- A. Onboarded devices will connect to Employee\_Secure SSID after provisioning.
- B. Onboarded devices will connect to secure\_emp SSID after provisioning.
- C. Users will connect to Employee\_Secure SSID for provisioning their devices.
- D. Users must enter a Pre-shared key to connect to the network.
- E. Users will do 802.1X authentication when connecting to the SSID.

Correct Answer: BE

**QUESTION 3**

Refer to the diagram below.

Configuration » Services » Add

## Services

Service	Authentication	Roles	Enforcement	Summary
Type:	802.1X Wireless			
Name:	Test device group			
Description:	802.1X Wireless Access Service			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints			
<b>Service Rule</b>				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	
3. Connection	NAD-IP-Address	BELONGS_TO_GROUP	HQ	
4. Click to add...				

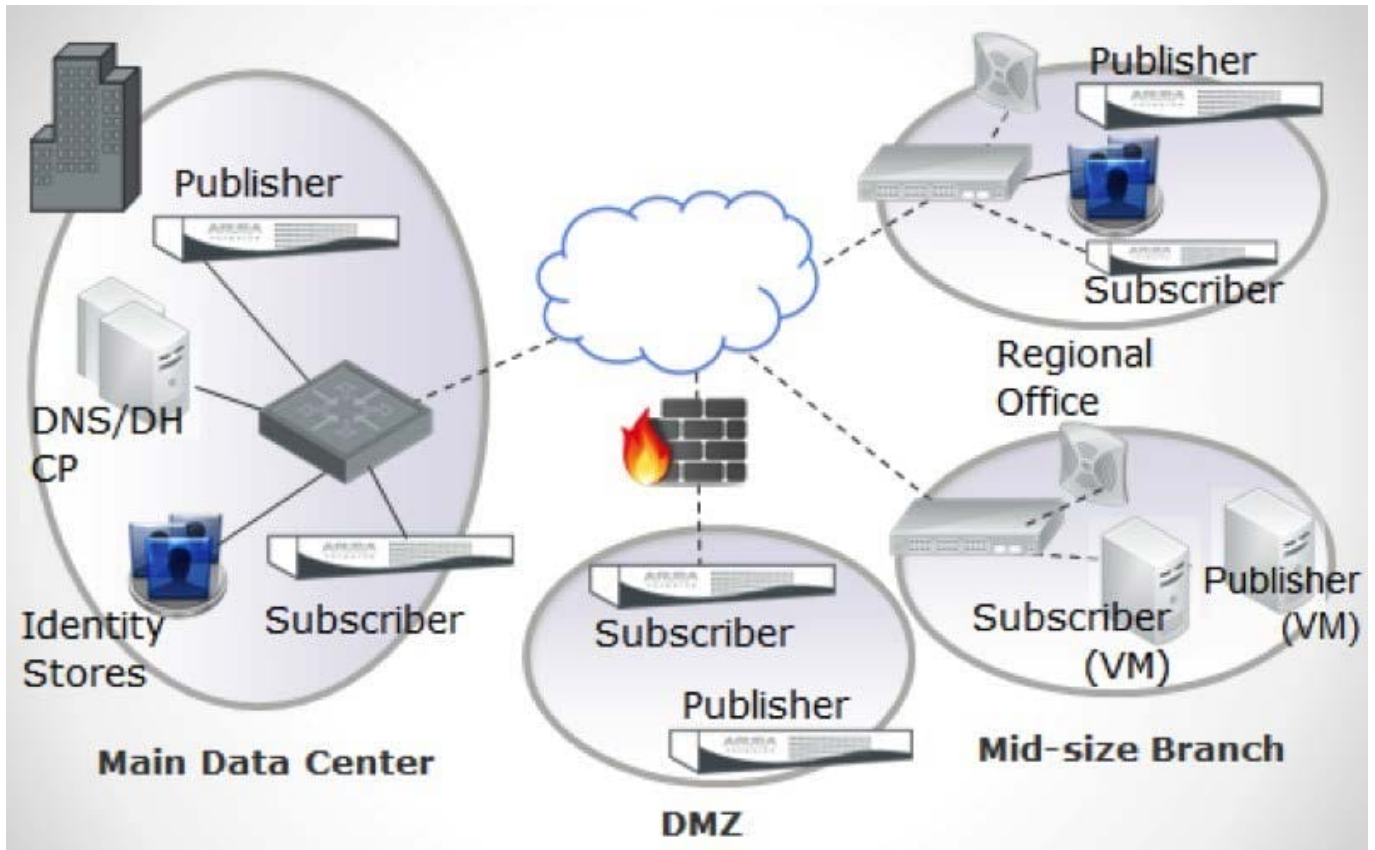
In which of the following scenarios will ClearPass select the Policy Service named "Test device group"?

- A. If an end user IP address is part of the device group HQ.
- B. If the IP address of the NAD device is part of the device group HQ.
- C. If the ClearPass IP address is part of the device group HQ.
- D. If the client's NAD IP address is part of the device group HQ.
- E. If the client's Network Authentication Distribution server's IP address belongs to device group HQ.

Correct Answer: B

### QUESTION 4

Below is a network topology diagram: How many clusters are needed for this deployment?



- A. 1
- B. 3
- C. 4
- D. 8
- E. 2

Correct Answer: C

**QUESTION 5**

Refer to the screenshot below of a MAC Caching service:

Configuration » Services » Edit - MAC Caching - Guest Access With MAC Caching

### Services - MAC Caching - Guest Access With MAC Caching

Summary Service Authentication Authorization Roles Enforcement

Use Cached Results:  Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: MAC Caching - Guest Access With MAC Caching Modify [Add new Enforcement Policy](#)

#### Enforcement Policy Details

Description: Limits guests to maximum n device for MAC caching purposes

Default Profile: [Allow Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:Unique-Device-Count <b>GREATER_THAN 2</b> )	[Deny Access Profile]
2. (Date:Day-of-Week <b>BELONGS_TO</b> Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	MAC Caching - Guest Session Timeout, MAC Caching - Guest Bandwidth Limit, MAC Caching - Guest Session Limit, MAC Caching - Guest MAC Caching <b>[Update Endpoint Known]</b> , MAC Caching - Guest Do Expire, MAC Caching - Guest Expire Post Login

A guest connects to the Guest SSID and authenticates successfully using the guest.php web login page. Which of the following is true?

- A. Their MAC address will be visible in the Endpoints table with Known Status.
- B. Their MAC address will be visible in the Endpoints table with Unknown Status.
- C. Their MAC address will be visible in the Guest User Repository with Known Status.
- D. Their MAC address will be visible in the Guest User Repository with Unknown Status.
- E. Their MAC address will be deleted from the Endpoints table.

Correct Answer: A

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

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

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