

DUMPSBOSS.

Aruba Certified Clearpass Professional v6.2

Aruba ACCP-v6.2

Version Demo

Total Demo Questions: 10

Total Premium Questions: 140

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

What must be configured to enable RADIUS authentication with Clearpass on a network access device (NAD)? (Choose 2)

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

ANSWER: C D

QUESTION NO: 2

Which of the following steps are required to use ClearPass as a TACACS+ Authentication server for a network device? (Choose 2)

- A. Configure the ClearPass Policy Manager as an Authentication server on the network device.
- B. Configure ClearPass roles on the network device.
- C. Configure RADIUS Enforcement Profile for the desired privilege level.
- D. Configure TACACS Enforcement Profile for the desired privilege level.
- E. Enable RADIUS accounting on the NAD device.

ANSWER: A D

QUESTION NO: 3

Which of the following statements is true based on the Access Tracker output shown below?

Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker Jul 12, 2012 10:26:39 PDT

Data Filter: [All Requests] Server: Clearpass6 (10.254.1.176)

Date Range: Last 1 day before Today

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

Server	Type	User	Service Name	Login	Date
10.254.1.176	RADIUS	8C705A065CF0		REJECT	2012/07/12 10:26:39 PDT

Request Details

Summary Input Output Alerts

Error Code: 204

Error Category: Authentication failure

Error Message: Failed to classify request to service

Alerts for this Request

RADIUS Service Categorization failed

- A. The client wireless profile is incorrectly setup.
- B. Clearpass does not have a service enabled for MAC authentication.
- C. The client MAC address is not present in the Endpoints table in the Clearpass database.
- D. The client used incorrect credentials to authenticate to the network.
- E. The RADIUS client on the Windows server failed to categorize the service correctly.

ANSWER: B

QUESTION NO: 4

Below is an Enforcement Profile that has been created in the Policy Manager:

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

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

What is the action that is taken by this Enforcement Profile?

- A. ClearPass will count down 600 seconds and send a RADIUS CoA message to the NAD device 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 User and the user's session will be terminated after 600 seconds.
- C. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the NAD device and the NAD will end the user's session after 600 seconds.

D. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD device and the NAD will end the user's session after 600 seconds.

ANSWER: C

QUESTION NO: 5

If the "Alerts" tab in an authentication session details tab in Access Tracker shows the following error message "Access denied by policy", what could be a possible cause for authentication failure?

- A. Implementation of an Enforcement Policy
- B. Implementation of a firewall policy
- C. Failure to categorize the request in a Clearpass service
- D. Implementation of a Posture Policy
- E. Failure to activate the enforcement policy

ANSWER: A

QUESTION NO: 6

Which of the following is TRUE of dual-SSID onboarding?

- A. The device connects to the secure SSID for provisioning
- B. The Onboard Authorization service is triggered when the user connects to the secure SSID
- C. The Onboard Provisioning service is triggered when the user connects to the Provisioning SSID
- D. The Onboard Authorization service is triggered during the Onboarding process
- E. The Onboard Authorization service is never triggered

ANSWER: D

QUESTION NO: 7

Which of the following conditions can be used for rule creation of an Enforcement Policy? (Choose 3)

- A. System Time
- B. Clearpass IP address
- C. Posture
- D. Switch VLAN

E. Connection Protocol

ANSWER: A C E

QUESTION NO: 8

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 GREATER_THAN 2)	[Deny Access Profile]
2. (Date:Day-of-Week BELONGS_TO 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 [Update Endpoint Known], 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.

ANSWER: A

QUESTION NO: 9

Which of the following components can use Active Directory authorization attributes for the decision-making process? (Choose 2)

- A. Role Mapping Policy
- B. Posture Policy
- C. Enforcement Policy

D. Service Rules

ANSWER: A C

QUESTION NO: 10

A company deployed the guest Self-registration with Sponsor Approval workflow for their guest SSID. The administrator logs into the Policy Manager and sees the following in the Guest User Repository:

Configuration » Identity » Guest Users

Guest Users

Filter: Username contains YOUR

#	<input type="checkbox"/> Username ▲	Sponsor Name	Guest Type	Status
1.	<input type="checkbox"/> YOUREMAIL@gmail.com	YOUREMAIL@gmail.com	USER	Disabled

Showing 1-1 of 1

What can you conclude from the above? (Choose 2)

- A. The guest has submitted the registration form.
- B. The guest has not submitted the registration form yet.
- C. The sponsor has confirmed the guest account.
- D. The sponsor has not confirmed the guest account yet.
- E. The user's account is active.

ANSWER: A D