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:

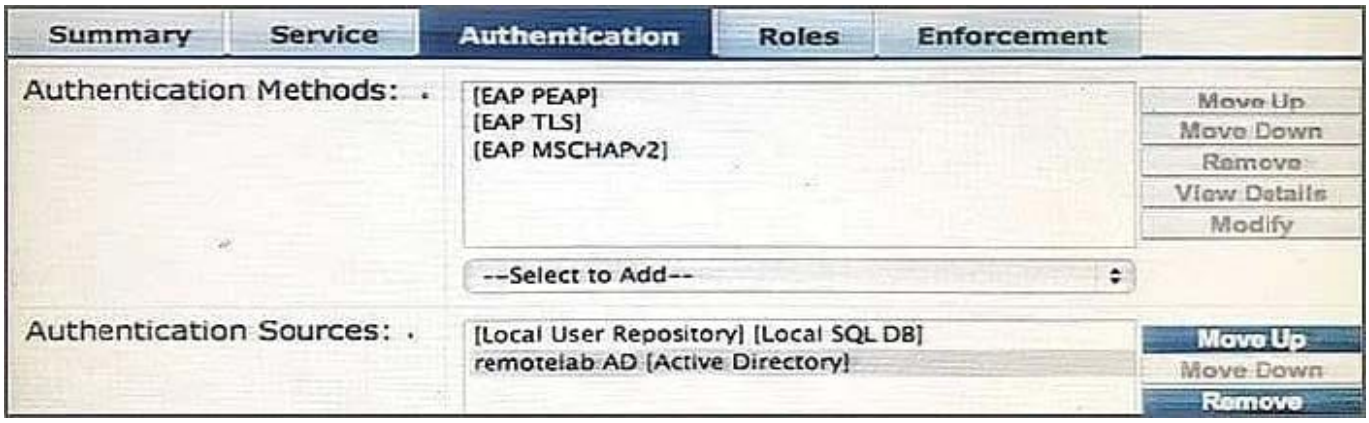
https://www.leads4pass.com/hpe6-a68.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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.

Correct Answer: D

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:

1.

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

2.

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.

3.

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 2

A customer would like to deploy ClearPass with these requirements:

1.

2000 devices need to be Onboarded

2.

2000 corporate devices need to run posture checks daily

3.

500 guest users need to authenticate each day using the web login feature

What is the license mix that customer will need to purchase?

A. CP-HW-5k, 2500 ClearPass Enterprise

B. CP-HW-25k, 4500 ClearPass Enterprise

C. CP-HW-500, 2500 ClearPass Enterprise

D. CP-HW-25k, 4000 ClearPass Enterprise

E. CP-HW-5k, 4500 ClearPass Enterprise

Correct Answer: B

QUESTION 3

A customer wants all guests who access a company\\'s guest network to have their accounts approved by the receptionist, before they are given access to the network. How should the network administrator set this up in ClearPass? (Select two.)

A. Enable sponsor approval confirmation in Receipt actions.

B. Configure SMTP messaging in the Policy Manager.

C. Configure a MAC caching service in the Policy Manager.

D. Configure a MAC auth service in the Policy Manager.

E. Enable sponsor approval in the captive portal authentication profile on the NAD.

Correct Answer: AD

A:

Sponsored self-registration is a means to allow guests to self-register, but not give them full access until a sponsor (could even be a central help desk) has approved the request. When the registration form is completed by the guest/user,

an on screen message is displayed for the guest stating the account requires approval.

Guests are disabled upon registration and need to wait on the receipt page for the confirmation until the login button gets enabled.

D.

Device Mac Authentication is designed for authenticating guest devices based on their MAC address.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 94

https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 4

Refer to the exhibit.

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

Based on the Enforcement Policy configuration shown, when a user with Role Remote Worker connects to the network and the posture token assigned is quarantine, which Enforcement Profile will be applied?

A. RestrictedACL

B. Remote Employee ACL

C. [Deny Access Profile]

D. EMPLOYEE_VLAN

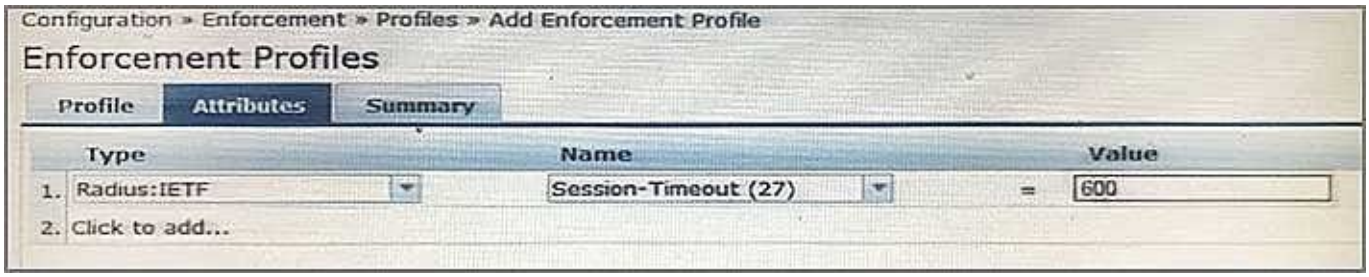
E. HR VLAN

Correct Answer: B

The first rule will match, and the Remote Employee ACL will be used.

QUESTION 5

Refer to the exhibit.



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

B. It 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. It will count down 600 seconds and send a RADUIS CoA message to the NAD to end the user\\'s session after this time is up.

D. It will count down 600 seconds and send a RADUIUS CoA message to the user to end the user\\'s session after this time is up.

E. It 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.

Correct Answer: E