VCE & PDF
passapply.com

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.passapply.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

What is the purpose of RADIUS CoA (RFC 3576)?

A. to force the client to re-authenticate upon roaming to a new Controller

B. to apply firewall policies based on authentication credentials

C. to validate a host MAC address against a whitelist or a blacklist

D. to authenticate users or devices before granting them access to a network

E. to transmit messages to the NAD/NAS to modify a user\'s session status

Correct Answer: E

CoA messages modify session authorization attributes such as data filters. References: https://tools.ietf.org/html/rfc3576

QUESTION 2

A customer would like to deploy ClearPass with these requirements:

every day, 100 employees need to authenticate with their corporate laptops using EAP-TLS every Friday, a meeting with business partners takes place and an additional 50 devices need to authenticate using Web Login Guest Authentication

What should the customer do regarding licenses? (Select two.)

A. When counting policy manager licenses, include the additional 50 business partner devices.

B. When counting policy manager licenses, exclude the additional 50 business partner devices.

C. Purchase Onboard licenses.

D. Purchase guest licenses.

E. Purchase Onguard licenses.

Correct Answer: AC

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.

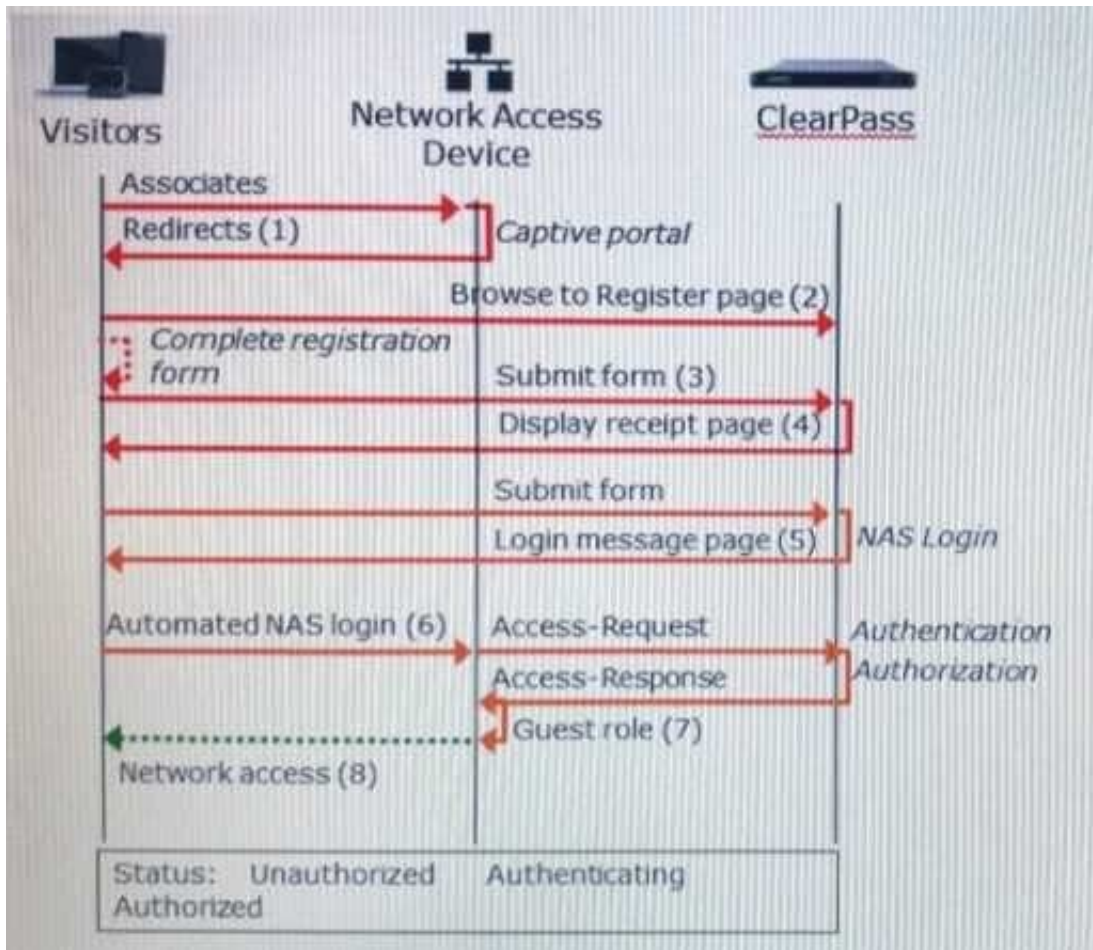C. To use attributes stored in external databases for Enforcement, but not internal databases.

D. To use attributes stored in databases in role mapping only, but not Enforcement.

E. To use attributes sored in internal databases for Enforcement, but not external databases.

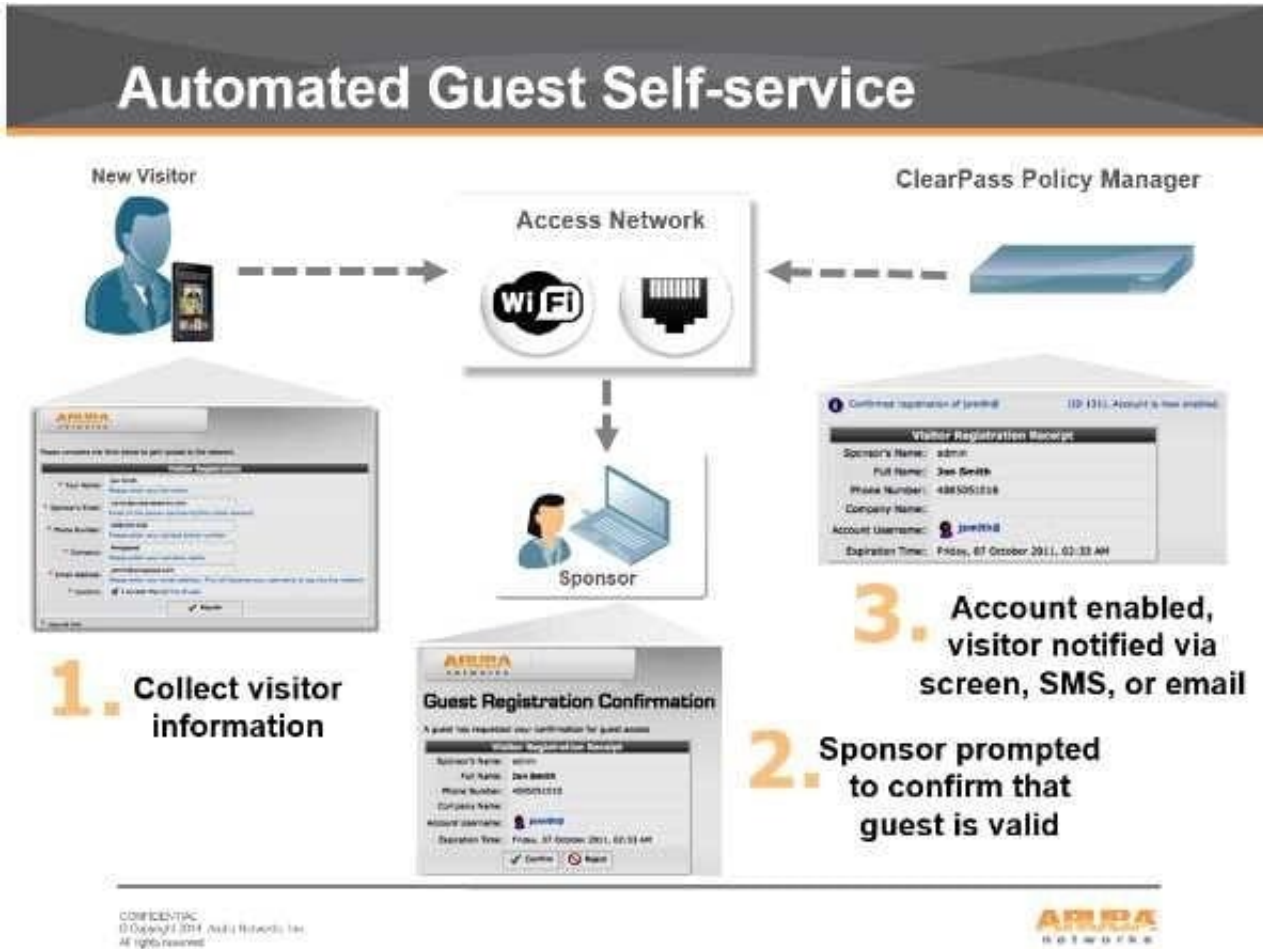Correct Answer: A

QUESTION 4

Refer to the exhibit.

Based on the guest Self-Registration with Sponsor Approval workflow shown, at which stage is an email request sent to the sponsor?

A. after `Guest Role (7)\\'

B. after `Login Message page (5)\\'

C. after `Submit form (3)\\'

D. after `Automated NAS login (6)\\'

E. after `Redirects (1)\\'

Correct Answer: C

There\'s the Self Service part of provisioning one\'s information. Then the sponsor/operator part to confirm that guest is valid. Then the enablement via the sponsor/operator clicking \'confirm\'.

References: https://community.arubanetworks.com/t5/Security/Guest-Captive-Portal-sponsor-approval-architecture/td-p/267625

QUESTION 5

Refer to the exhibit.

Based on the configuration for `maximum devices\' shown, which statement accurately describes its settings?

A. The user cannot Onboard any devices.

B. It limits the total number of devices that can be provisioned by ClearPass.

C. It limits the total number of Onboarded devices connected to the network.

D. It limits the number of devices that a single user can Onboard.

E. It limits the number of devices that a single user can connect to the network.

Correct Answer: D

QUESTION 6

An Android device goes through the single-SSID Onboarding process and successfully connects using EAP-TLS to the secure network. What is the order in which services are triggered?

A. Onboard Authorization, Onboard Provisioning, Onboard Authorization

B. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization, Onboard Provisioning

C. Onboard Provisioning, Onboard Authorization, Onboard Pre-Auth

D. Onboard Provisioning, Onboard Authorization, Onboard Provisioning

E. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization

Correct Answer: D

QUESTION 7

Refer to the exhibit.

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, which statement describes the status?

A. The Aruba Terminate Session enforcement profile as applied because the posture check failed.

B. A Healthy Posture Token was sent to the Policy Manager.

C. A RADIUS-Access-Accept message is sent back to the Network Access Device.

D. The authentication method used is EAP-PEAP.

E. A NAP agent was used to obtain the posture token for the user.

Correct Answer: B

We see System Posture Status: HEALTHY(0)

End systems that pass all SHV tests receive a Healthy Posture Token, if they fail a single test they receive a Quarantine Posture Token.

References: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 13

https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%20config%20Tech%20Note%20v1.pdf

QUESTION 8

Refer to the exhibit.

A user logged in to the Self-Service Portal as shown. What do the traffic received and sent statistics present?

A. These show the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the NAD to ClearPass.

B. These show the total amount of traffic the NAD transmitted to ClearPass, as seen through RADIUS accounting messages from the NAD to ClearPass.

C. These show the total amount of traffic the guest transmitted after account expiration, as seen through RADIUS accounting messages sent from the NAD to ClearPass.

D. These show the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the client to ClearPass.

E. These show the total amount of traffic the guest transmitted, as seen through RADIUS accounting messages sent from the NAD to ClearPass.

Correct Answer: E

QUESTION 9

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

QUESTION 10

Which is a valid policy simul-ation types in ClearPass? (Choose three.)

A. Enforcement Policy

B. Posture token derivation

C. Role Mapping

D. Endpoint Profiler

E. Chained simulation

Correct Answer: ACE

QUESTION 11

A client\\'s authentication is failing and there are no entries in the ClearPass Access tracker. What is a possible reason for the authentication failure?

A. The user account has expired.

B. The client used a wrong password.

C. The shared secret between the NAD and ClearPass does not match.

D. The user\\'s certificate is invalid.

E. The user is not found in the database.

Correct Answer: C

QUESTION 12

Refer to the exhibit.

Summary	Policy	Mapping rules		
Policy:				
Policy Name:		WLAN role mapping		
Description:				
Default Role:		[Guest]		
Mapping Rules:				
Rules Evaluation Algorithm:		Evaluate all		

	Conditions	Role Name
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive
2.	(Authorization: [Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor
3.	(Authorization: [Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization: [Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device
4.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	HR Local
5.	(Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User
6.	Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee

An AD user\\'s department attribute is configured as "HR". The user connects on Monday using an Android phone to an Aruba Controller that belongs to the Device Group Remote NAD. Which roles are assigned to the user in ClearPass? (Select two.)

A. Executive

B. iOS Device

C. Vendor

D. Remote Employee

E. HR Local

Correct Answer: DE

QUESTION 13

A university wants to deploy ClearPass with the Guest module. The university has two types that need to use web login authentication. The first type of users are students whose accounts are in an Active Directory server. The second type of

users are friends of students who need to self-register to access the network.

How should the service be set up in the Policy Manager for this network?

A. Guest User Repository and Active Directory server both as authentication sources

B. Active Directory server as the authentication source, and Guest User Repository as the authorization source

C. Guest User Repository as the authentication source, and Guest User Repository and Active Directory server as authorization sources

D. Either the Guest User Repository or Active Directory server should be the single authentication source

E. Guest User Repository as the authentication source and the Active Directory server as the authorization source

Correct Answer: A

QUESTION 14

A bank would like to deploy ClearPass Guest with web login authentication so that their customers can selfregister on the network to get network access when they have meetings with bank employees. However, they\\'re concerned about

security.

What is true? (Choose three.)

A. If HTTPS is used for the web login page, after authentication is completed guest Internet traffic will all be encrypted as well.

B. During web login authentication, if HTTPS is used for the web login page, guest credentials will be encrypted.

C. After authentication, an IPSEC VPN on the guest\\'s client be used to encrypt Internet traffic.

D. HTTPS should never be used for Web Login Page authentication.

E. If HTTPS is used for the web login page, after authentication is completed some guest Internet traffic may be unencrypted.

Correct Answer: BCE

QUESTION 15

When is the RADIUS server certificate used? (Select two.)

A. During dual SSID onboarding, when the client connects to the Guest network

B. During EAP-PEAP authentication in single SSID onboarding

C. During post-Onboard EAP-TLS authentication, when the client verifies the server certificate

D. During Onboard Web Login Pre-Auth, when the client loads the Onboarding web page

E. During post-Onboard EAP-TLS authentication, when the server verifies the client certificate

Correct Answer: CD