



HPE6-A81^{Q&As}

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

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

<https://www.passapply.com/hpe6-a81.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

Refer to the exhibit:



Monitoring > Live Monitoring > Access Tracker

Access Tracker Oct 02, 2019 03:43:03 EDT Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] p50-t07-cp1 (10.1.79.1) Last 1 day before Today Edit

Filter: Login Status contains acc Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:13
2.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:07
3.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:00:55

aruba ClearPass Onboard

Guest Onboard

- Start Here
- Certificate Authorities
- Management and Control
 - Start Here
 - View by Device
 - View by Username
 - View by Certificate
 - Usage
- Configuration
 - Start Here
 - Network Settings
 - iOS Settings
 - Windows Applications
- Deployment and Provisioning
 - Start Here
 - Configuration Profiles
 - Provisioning Settings
- Self-Service Portal

Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
mike07	HS_Branch	8	tls-client	2019-10-02 02:45:47-04:00	2020-10-01 03:15:47-04:00	Windows

View certificate Trust Chain Export certificate Delete certificate

Certificate Information

Certificate Details
Details about the certificate and its owner.

Issued To: mike07

Revoked At: Wednesday, 02 October 2019, 3:01 AM

Revoked: This certificate has been revoked.

Valid From: Wednesday, 02 October 2019, 2:45 AM

Valid To: Thursday, 01 October 2020, 3:15 AM

Country US
Locality Sunnyvale
Organization Aruba
Common Name mike07
State California

Subject: mdpUsername mike07
mdpDeviceName Windows 10
mdpDeviceType Windows



Certificate Authorities Create new

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
 p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
 p50-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.

How do I fix this problem?
 Use this list to manage certificate authorities.

Name	Mode	Status	Expiry	OCSP URL
HS_Branch	root	Valid	2029-09-25T03:19:47-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/2
Local Certificate Authority <small>This is the default certificate authority.</small>	root	Valid	2029-06-25T21:25:44-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/1

Refresh 1

Configuration > Services > Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

Summary Service Authentication Authorization Roles Enforcement

Service:

Name: HS_Branch Onboard Provisioning
 Description: 802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
 Type: Aruba 802.1X Wireless
 Status: Enabled
 Monitor Mode: Disabled
 More Options: Authorization

Service Rule:

Match 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. Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

Authentication:

Authentication Methods: 1. [EAP PEAP]
2. [EAP TLS]
 Authentication Sources: 1. [Onboard Devices Repository]
2. AD1
3. AD2
 Strip Username Rules: /user
 Service Certificate: -

Authorization:

Authorization Details: 1. AD1
2. AD2

After the helpdesk revoked the certificate of a device reported to be lost by an employee, the lost device was seen as connected successfully to the secure network. Further testing has shown that device revocation is not working.

What steps should you follow to make device revocations work?

A. Copy the default [EAP-TLS with OSCP Enabled] authentication method and set The Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA. Remove EAP-TLS and map the custom



created method to the OnBoard Authorization Service.

B. copy the default [EAP-TLS with OSCP Enabled] authentication method and set the verify certificate using OSCP: option as "required" then configure the correct OSCF URL link for the OnBoard CA. Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the 802 1X Radius Service.

C. Remove the EAP-TLS authentication method configuration changes are required and add "EAP-TLS with OCSP Enabled" authentication method in the OnBoard Provisioning service. No other configuration changes are required.

D. Edit the default [EAP-TLS with OSCP Enabled] authentication method and set the Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the OnBoard Provisioning Service.

Correct Answer: C

QUESTION 2

A Customer has these requirements:

- *
2,000 IoT endpoints that use MAC authentication
 - *
6,000 endpoints using a mix of username/password and certificate (Corporate/BYOD) based authentication
 - *
1,000 guest endpoints at peak usage that use guest self-registration
 - *
1500 BYOD devices estimated as 3 devices per User (500 users)
 - *
2,500 endpoints that have OnGuard installed and connect on a daily basis
- What licenses should be installed to meet customer requirements?

- A. 11,500 Access, 500 Onboard, 2,500 Onguard
- B. 13,000 Access, 1,500 Onboard, 2,500 Onguard
- C. 11,500 Access, 1,500 Onboard, 2,500 Onguard
- D. 9,000 Access, 500 Onboard. 2,500 Onguard

Correct Answer: C

QUESTION 3



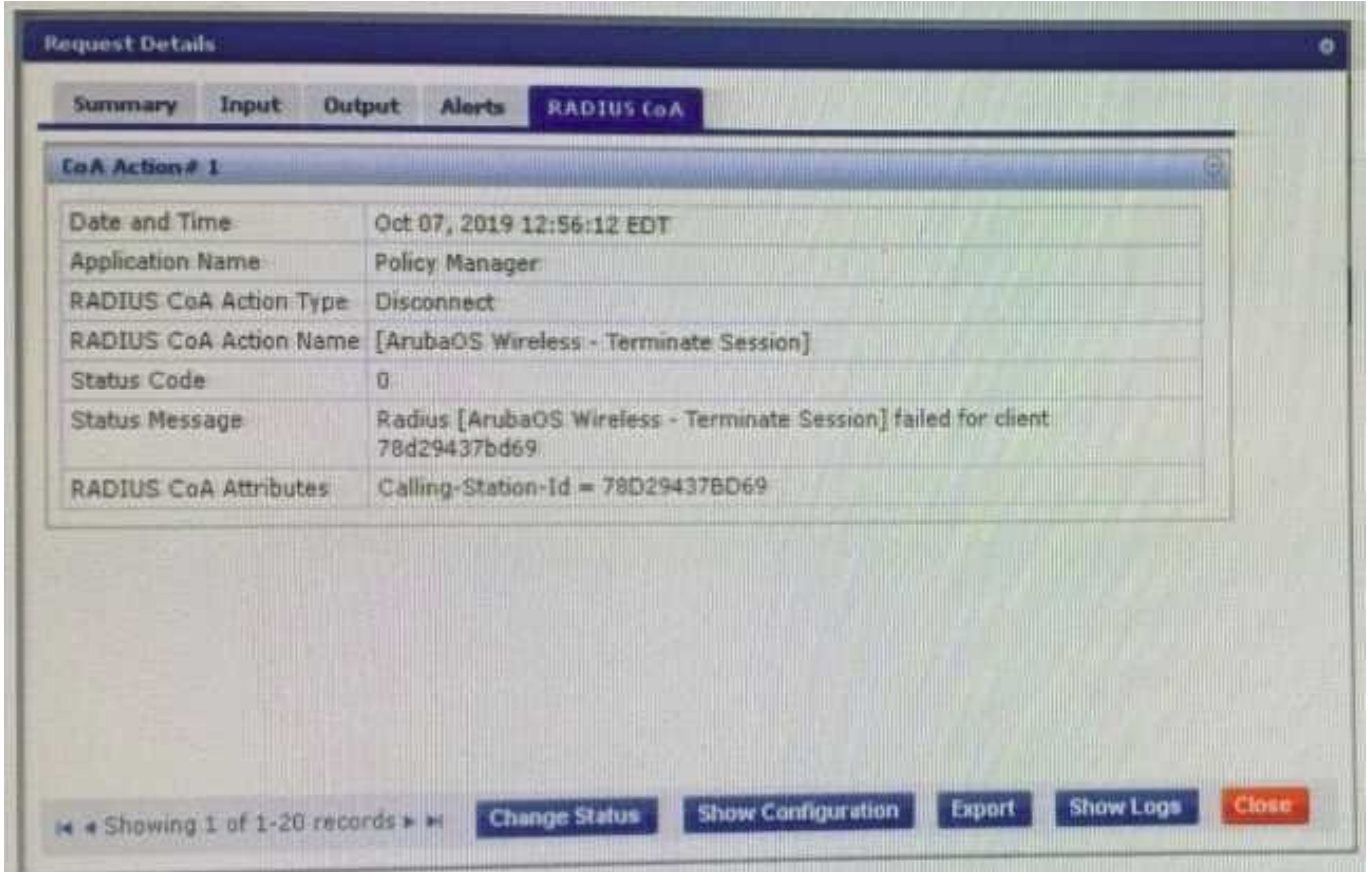
A customer has a ClearPass cluster deployment with one Publisher and one Subscriber configured as a Standby Publisher at the Headquarters DataCenter They also have a large remote site that is connected with an Aruba SD Branch solution over a two Mbps Internet connection. The Remote Site has two ClearPass servers acting as Subscribers. The solution implemented for the customer includes OnGuard, Guest Self Registration, and Employee 802.1x authentication. The client is complaining that users connecting to an IAP Clusters Guest SSID located at the Remote Site are experiencing a significant delay in accessing the Guest Captive Portal page. What could be a possible cause of this behavior?

- A. The configuration of the captive portal is pointing to a link located on one of the servers in the Headquarters
- B. The ClearPass Cluster has no zones defined and the guest captive portal request is being redirected to the Publisher
- C. The guest page is not optimized to work with the client browser and a proper theme should be applied
- D. The captive portal page was only created on the Publisher and requests are getting redirected to a Subscriber

Correct Answer: A

QUESTION 4

Refer to the exhibit: You configuring an 802.1x service endpoint profiling. When the client connects to the network, ClearPass successfully profiles the client and sends Radius Change of Authorization (RCoA) but Radius Change of Authorization (RCoA) fails for the client You manually clicked on the Change Status button in the access tracker to force an RCoA but that failed too. What must you check to ensure that the RCoA will work? (Select two.)





Request Details

No response from network device

Summary | Input | Output | Alerts

Login Status:	ACCEPT
Session Identifier:	R00000180-01-5d9b61af
Date and Time:	Oct 07, 2019 12:02:55 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	HS_Building 802.1x service
Authentication Method:	EAP-PEAP
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL
Roles:	[User Authenticated]
Enforcement Profiles:	Aruba Limited Access for Profiling
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-6 records

Change Status | Show Configuration | Export | Show Logs | Close

- A. RFC 3576 option is enabled for Aruba Controller under Network device in ClearPass.
- B. RFC 3576 server should be mapped in the server group on the Aruba Controller
- C. The RFC 3576 shared secret on ClearPass should match the Authentication Server shared secret
- D. RFC 3576 server IPs and the Authentication server IPs should be same in the AAA profile

Correct Answer: AC

QUESTION 5

Refer to the exhibit: You are doing a ClearPass PoC at a customer site with a single Aruba Mobility Controller. The customer asked for a demonstration of a simple Web Login functionality. You used a service template to create the guest services. During testing, the user gets redirected back to the weblogin page with an Authentication failed message. The guest configurations on the Aruba Mobility Controller are configured correctly. Why would the guest fail to authenticate successfully?



Configuration > Services > Edit - HPE-Aruba Wired Mac auth

Services - HPE-Aruba Wired Mac auth

Summary Service Authentication Authorization Roles **Enforcement** Profiler

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

Enforcement Policy: HPE-ArubaOS Mac auth policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:Category NOT_EXISTS)	Assign Switch role PROFILE
2. (Authorization:[Endpoints Repository]:Category EQUALS Access Points) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Aruba)	Assign Aruba switch role AP-ACCESS

Configuration > Service Templates & Wizards

Service Templates - Guest Authentication with MAC Caching

General Wireless Network Settings **NAC Caching Settings** Posture Settings Access Restrictions

- Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.
- Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.
- At least one of Employee, Guest, and Contractor Access must be provided.

Enforcement Type*: Aruba Role Enforcement

Captive Portal Access*: gueaths-login

Days allowed for access*: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Maximum number of devices allowed per user*: 0

Maximum bandwidth allowed per user*: 0 MB (For unlimited bandwidth, set value to 0)

Employee Access:

Guest Access: Lab-Guest

Contractor Access:

Back to Service Templates & Wizards Delete Next Add Service Cancel

Configuration > Services > Edit - Guest User Authentication with MAC Caching

Services - Guest User Authentication with MAC Caching

Summary Service Authentication Authorization Roles **Enforcement**

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

Enforcement Policy: Guest User Authentication with MAC Caching Enforcement Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Allow Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 0)	[Deny Access Profile]
2. (Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week IS_LONGER_THAN Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	Guest MAC Caching Session Timeout, Guest MAC Caching Bandwidth Limit, Guest MAC Caching Session Limit, Guest Guest MAC Caching, [Update Endpoint Known], Guest MAC Caching Do Expire, Guest MAC Caching Expire Post Login, Guest Guest Profile

A. The authentication source mapped in the service is incorrect, it should be mapped as (Guest Device Repository)



[Local SQL DB].

B. The username and/or password used for authentication is incorrect Re-enter the correct password on the weblogin page.

C. The username used for authentication does not exist in the Guest User Database Create a new user and authenticate again.

D. The Unique-Device-Count does not allow any Client devices. Update the Enforcement policy condition: Unique-Device-Count.

Correct Answer: A

[Latest HPE6-A81 Dumps](#)

[HPE6-A81 VCE Dumps](#)

[HPE6-A81 Exam Questions](#)