



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.pass4itsure.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: 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.)

CoA Action# 1	
Date and Time	Oct 07, 2019 12:56:12 EDT
Application Name	Policy Manager
RADIUS CoA Action Type	Disconnect
RADIUS CoA Action Name	[ArubaOS Wireless - Terminate Session]
Status Code	0
Status Message	Radius [ArubaOS Wireless - Terminate Session] failed for client 78d29437bd69.
RADIUS CoA Attributes	Calling-Station-Id = 78D29437BD69

Showing 1 of 1-20 records

Change Status Show Configuration Export Show Logs Close



The screenshot shows a 'Request Details' window with a status message 'No response from network device'. It contains a table with the following data:

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		

At the bottom, there are navigation buttons: 'Change Status' (highlighted with a red box), 'Show Configuration', 'Export', 'Show Logs', and 'Close'. A status bar at the bottom left indicates 'Showing 1 of 1-6 records'.

- 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 2

Refer to the Exhibit:



Configuration > Services > Edit - HeathCheck-Service

Services - HeathCheck-Service

Summary Service Roles Posture **Enforcement**

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

Enforcement Policy: T2-OnGuard-Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [ArubaOS Wireless - Terminate Session]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Posture - ONBOARD HEALTHY (0))	T2-Emp-Healthy, [ArubaOS Wireless - Terminate Session], [Cisco - Terminate Session]
2. (Tips:Posture - ONBOARD QUARANTINE (20))	T2-Emp-Unhealthy, [ArubaOS Wireless - Terminate Session], [Cisco - Terminate Session]

Exhibit A77-01126930-347

Configuration > Posture > Posture Policies > Edit - T2-OnGuard-Posture-Policy

Posture Policies - T2-OnGuard-Posture-Policy

Summary Policy Posture Plugins **Roles**

Rules Evaluation Algorithm: First applicable

Conditions	Posture Token
1. Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
2. Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE

Add Role Move Up Move Down Edit Rule Remove Role

Configuration > Services > Edit - Aruba 802.1X Wireless

Services - Aruba 802.1X Wireless

Summary Service **Authentication** Authorization Roles **Enforcement**

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

Enforcement Policy: secure1-2x Aruba 802.1X Wireless Enforcement Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access-Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role - ANYONE T2-Staff-User) [Machine Authenticated] T2-SOL-Device	T2-Employee-Auth
2. (Tips:Posture - ONBOARD HEALTHY (0)) (Tips:Role - ANYONE T2-Staff-User) [User Authenticated] T2-SOL-Device	T2-Employee-Auth
3. (Tips:Role - ANYONE T2-Staff-User) (Tips:Posture - ONBOARD HEALTHY (0))	T2-Employee-Auth
4. (Tips:Role - ANYONE T2-MDM-Device) [User Authenticated]	T2-Quarantine-Profile
5. (Tips:Posture - ONBOARD QUARANTINE (20)) (Tips:Role - ANYONE T2-Staff-User) [User Authenticated]	T2 - Unknown - Profile
6. (Tips:Posture - ONBOARD UNKNOWN (100))	

A customer wants to integrate posture validation into an Aruba Wireless 802.1X authentication service

During testing, the client connects to the Aruba Employee Secure SSID and is redirected to the Captive Portal page where the user can download the OnGuard Agent After the Agent is installed, the client receives the Healthy token the client remains connected to the Captive Portal page ClearPass is assigning the endpoint the following roles: T2-Staff-User. (Machine Authenticated! and T2-SOL-Device. What could cause this behavior?

- A. The Enforcement Policy conditions for rule 1 are not configured correctly.
- B. Used Cached Results: has not been enabled In the Aruba 802.1X Wireless Service
- C. RFC-3576 Is not configured correctly on the Aruba Controller and does not update the role.



D. The Enforcement Profile should bounce the connection instead of a Terminate session

Correct Answer: B

QUESTION 3

A customer has completed all the required configurations in the Windows server in order for Active Directory Certificate Services (ADCS) to sign Onboard device TLS certificates. The Onboard portal and the Onboard services are also configured. Testing shows that the Client certificates are still signed by the Onboard Certificate Authority and not ADCS. How can you help the customer with the situation?

A. Educate the customer that, when integrating with Active Directory Certificate Services (ADCS) the Onboard CA will be the same authority used for signing the final TLS certificate of the device.

B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL `http://ADCSVVeoEnrollmentServmostname/certsrv` in the OnBoard Provisioning settings.

C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C

QUESTION 4

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 5

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