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

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.

B. Using the same certificate to Onboard clients and the Guest Captive Portal on a single ClearPass server.

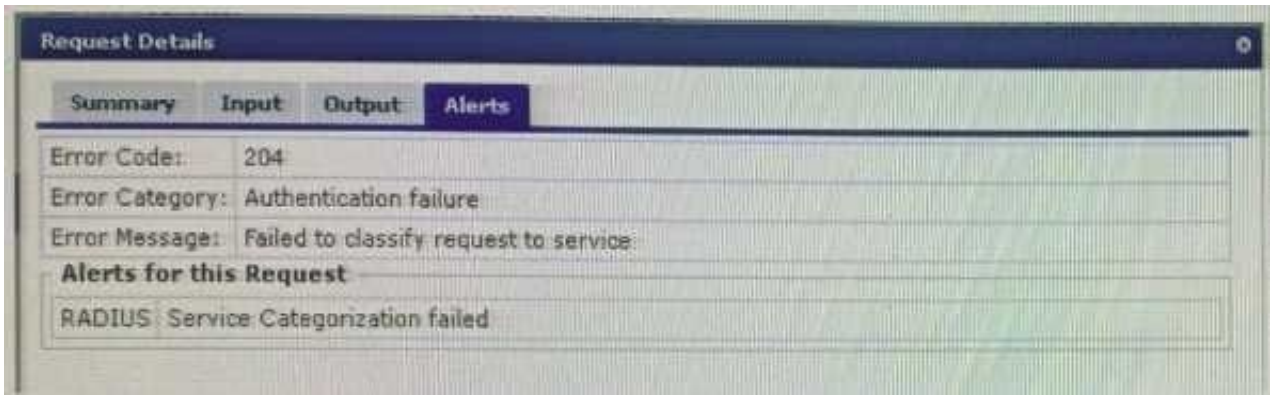
C. The primary authentication server Is not available to authenticate the users.

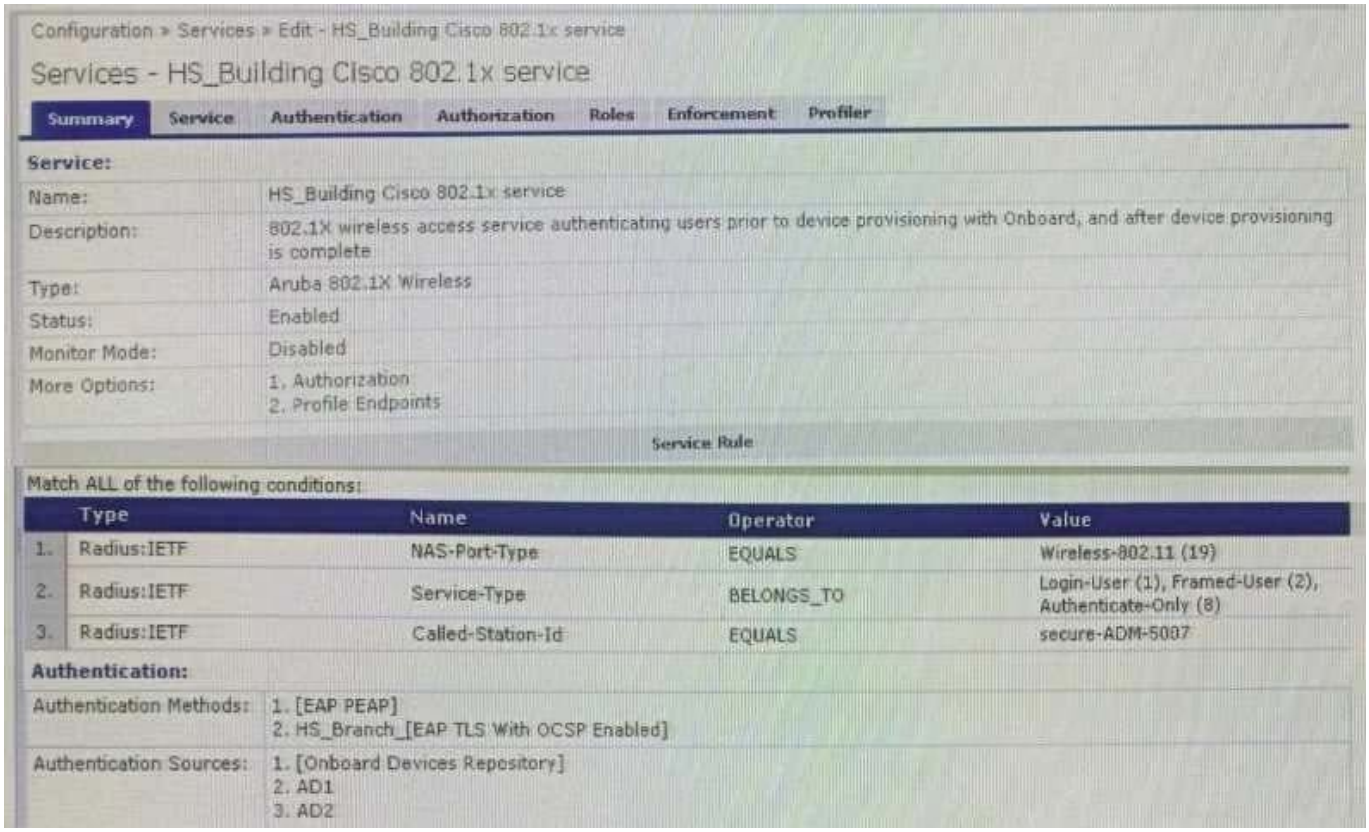
D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

QUESTION 2

Refer to the exhibit: You configured a new Wireless 802.1X service for a Cisco WLC broadcasting the Secure-ADM-5007 SSID. The client falls to connect to the SSID. Using the screenshots as a reference, how would you fix this issue? (Select two.)




Configuration » Services » Edit - HS_Building Cisco 802.1x service

Services - HS_Building Cisco 802.1x service

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Service:

Name:	HS_Building Cisco 802.1x service
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:	1. Authorization 2. Profile Endpoints

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:IETF	Called-Station-Id	EQUALS	secure-ADM-5007

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. HS_Branch_[EAP TLS With OCSP Enabled]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2

A. Update the service condition Radius:IETF Called-Station-Id CONTAINS secure-adm-5007

B. Make sure that the Network Devices entry for the Cisco WLC has a vendor setting of "Airspace"

C. Remove the service condition Radius:lETF Service-Type BELONGSJTO Login-User (1). 2. 8

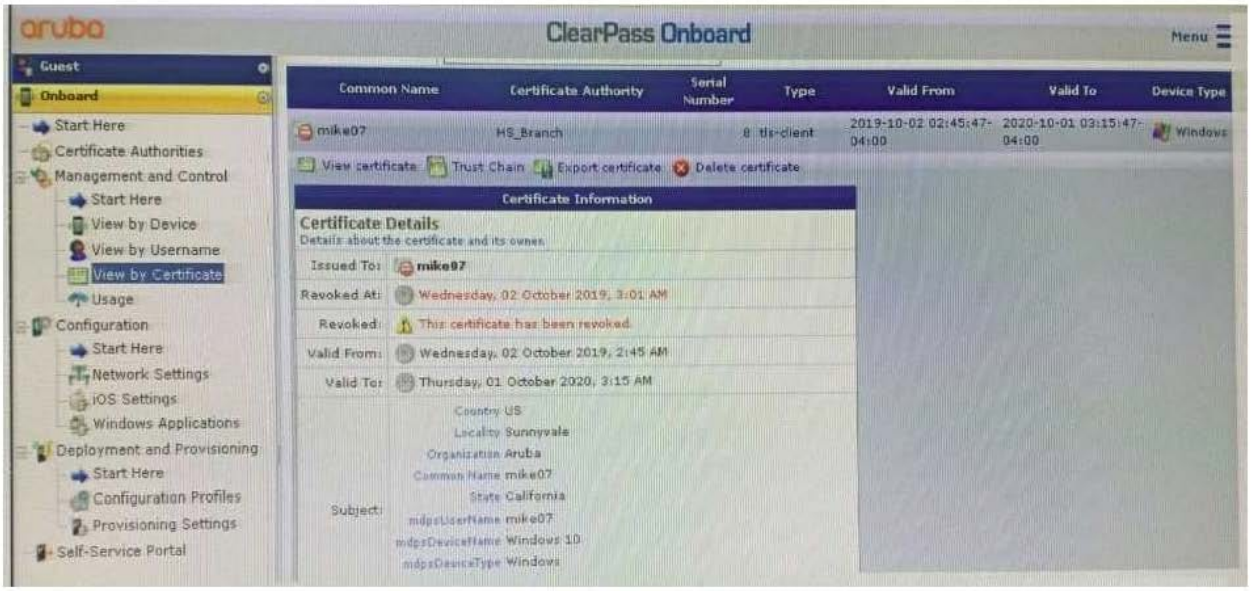
D. Change the service condition to Radius:lETF Calling-Station-Id EQUALS Secure-ADM-5007

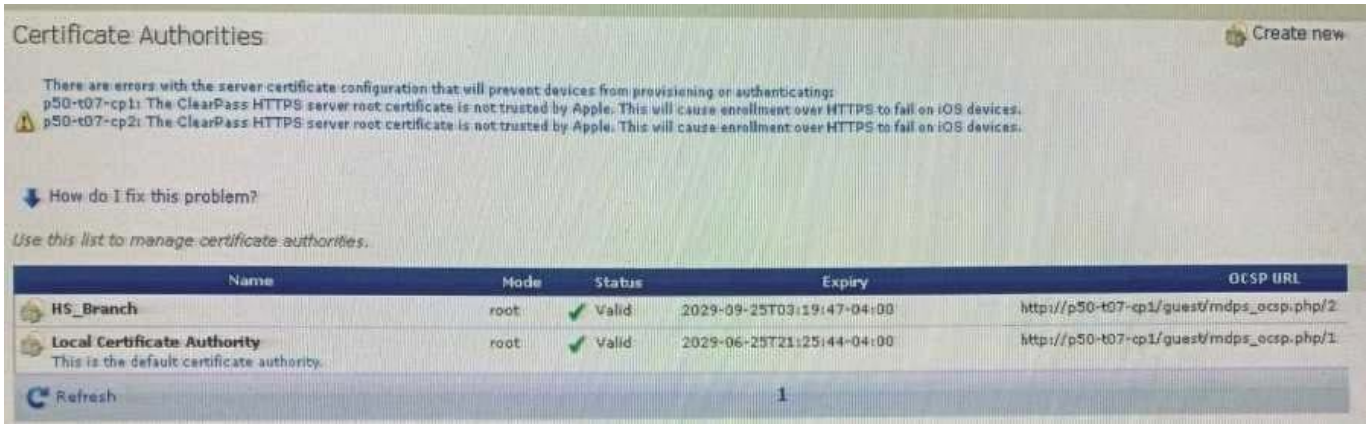
Correct Answer: AC

QUESTION 3

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
Menu
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
Subject: Country US
Locality Sunnyvale
Organization Aruba
Common Name mike07
State California
mdpsUserName mike07
mdpsDeviceName Windows 10
mdpsDeviceType Windows


Certificate Authorities

Create new

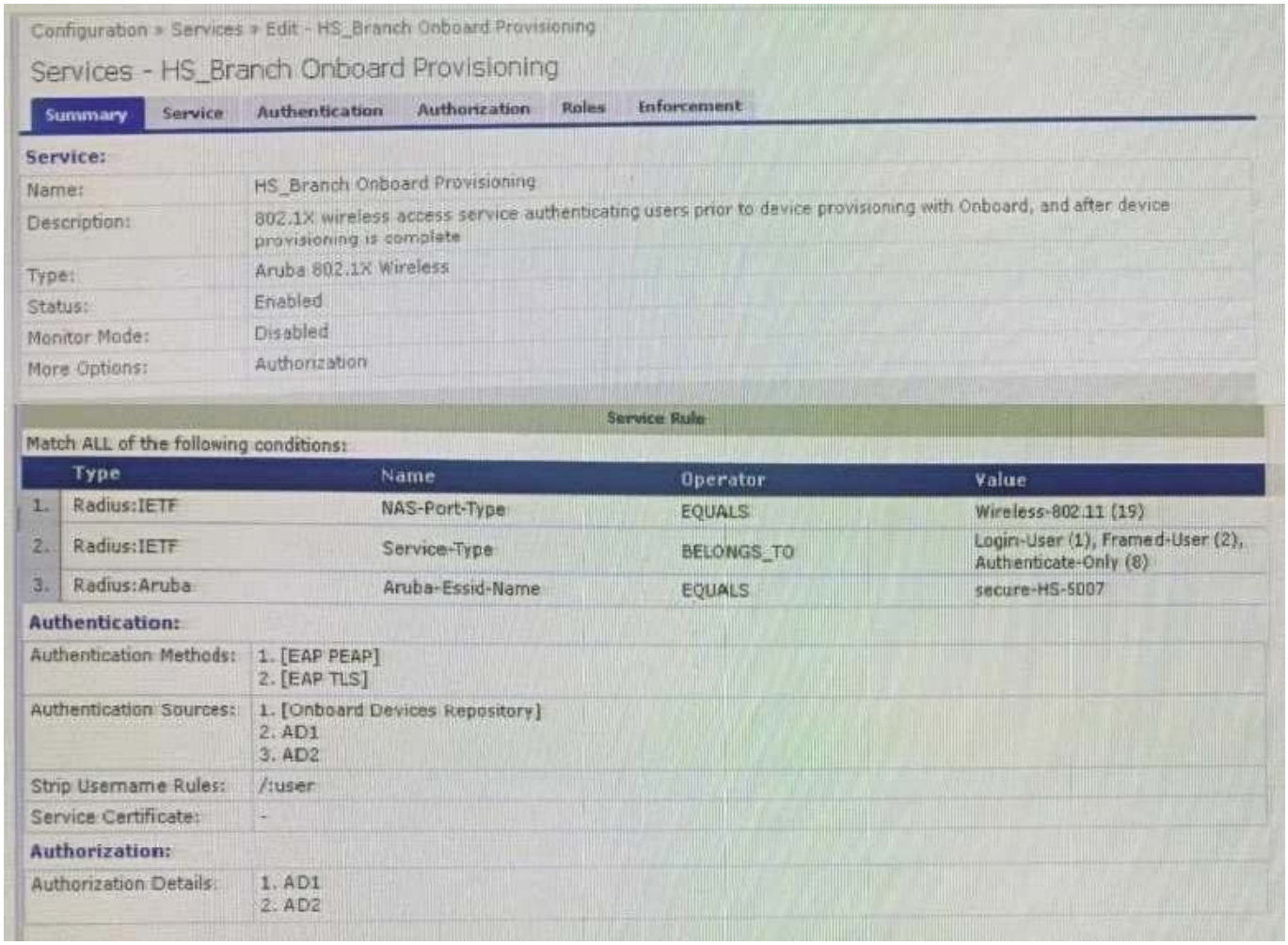
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
p50-t07-cp2: The ClearPass HTTPS server 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 This is the default certificate authority.	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 oy 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 4

A customer has deployed an OnGuard Solution to all the corporate devices using a group policy rule to push the OnGuard Agents. The network administrator is complaining that some of the agents are communicating to the ClearPass server that is located in a DMZ, outside the firewall The network administrator wants all of the agents System Health Validation traffic to stay inside the Management subnets. What can the ClearPass administrator do to move the traffic only to the ClearPass Management Ports?

A. Edit the agent.conf file being deployed to the clients to use the ClearPass Management Port for SHV updates.

B. Select the correct OnGuard Agent installer, and use the one configured for Management Port for the clients.

C. Configure a Policy Manager Zone mapping so the OnGuard agent will use the Management Port IP.

D. Filter TCP port 6658 on the firewall, forcing the OnGuard agent to use the ClearPass Management port.

Correct Answer: C

QUESTION 5

What is used to validate the EAP Certificate? (Select three.)

A. Common Name

B. Date

C. Key usage

D. Server Identity

E. SAN entries

F. Trust chain

Correct Answer: ACF

HPE6-A81 PDF Dumps HPE6-A81 Study Guide HPE6-A81 Exam Questions