HPE6-A77Q&As

Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

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

https://www.geekcert.com/hpe6-a77.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

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 ate 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 the same authority used for signing me final TLS certificate of the device.

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

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

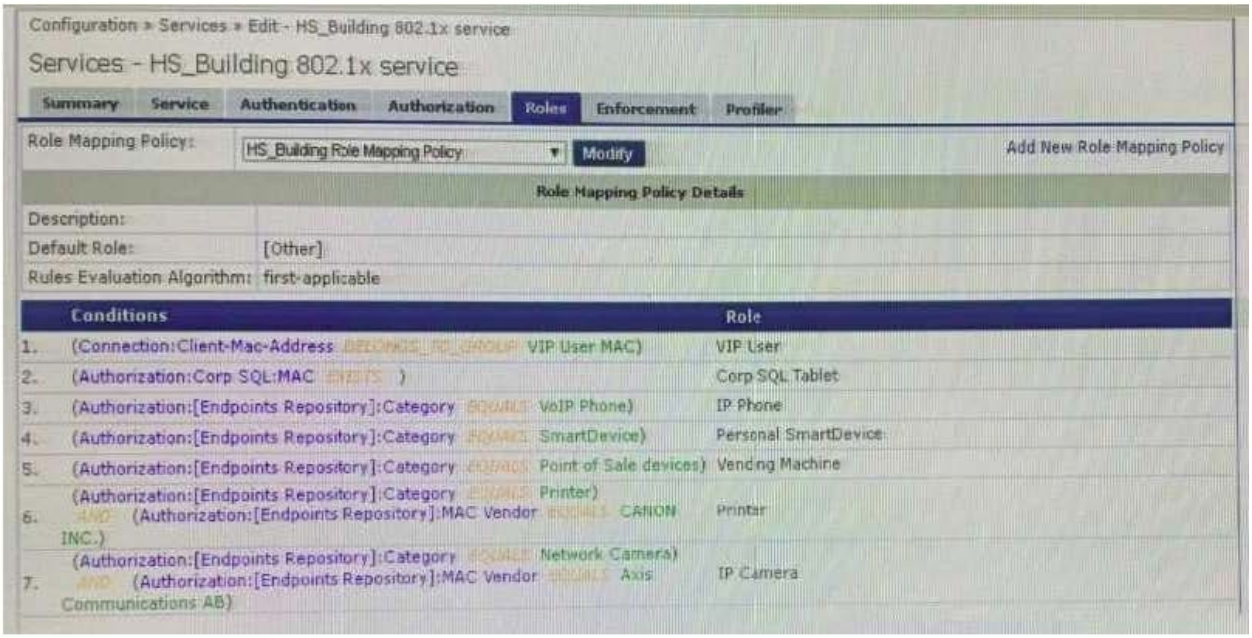
D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C

QUESTION 2

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: ACCEPT
Session Identifier: R000001ae-01-5d9cb453
Date and Time: Oct 08, 2019 12:07:47 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,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: [Endpoints Repository], AD1, AD2, Corp SQL
Roles: VIP User, [Machine Authenticated], [User Authenticated]
Enforcement Profiles: Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Configuration » Services » Edit - HS_Building 802.1x service
Services - HS_Building 802.1x service
Summary
Service
Authentication
Authorization
Roles
Enforcement
Profiler
Role Mapping Policy:
HS_Building Role Mapping Policy
Modify
Add New Role Mapping Policy
Role Mapping Policy Details
Description:
Default Role: [Other]
Rules Evaluation Algorithm: first-applicable
Conditions
Role
1. (Connection:Client-Mac-Address VIP User MAC) VIP User
2. (Authorization:Corp SQL:MAC) Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category VoIP Phone) IP Phone
4. (Authorization:[Endpoints Repository]:Category SmartDevice) Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category Point of Sale devices) Vending Machine
6. (Authorization:[Endpoints Repository]:Category Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor CANON INC.) Printer
7. (Authorization:[Endpoints Repository]:Category Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor Axis Communications AB) IP Camera

The customer created a new enforcement policy condition to allow VIP Users access without additional security compliance checks hut cannot gel it working. The customer has sent you the above screenshots. How would you resolve the issue?

A. Ask the VIP user to complete the one time web health check to get the VIP profile.

B. Set the Enforcement Policy rules evaluation algorithm to evaluate all.

C. Include VIP User role along with the Healthy posture enforcement condition.

D. Modify the Enforcement Policy and re-order the VIP user condition to the lop.

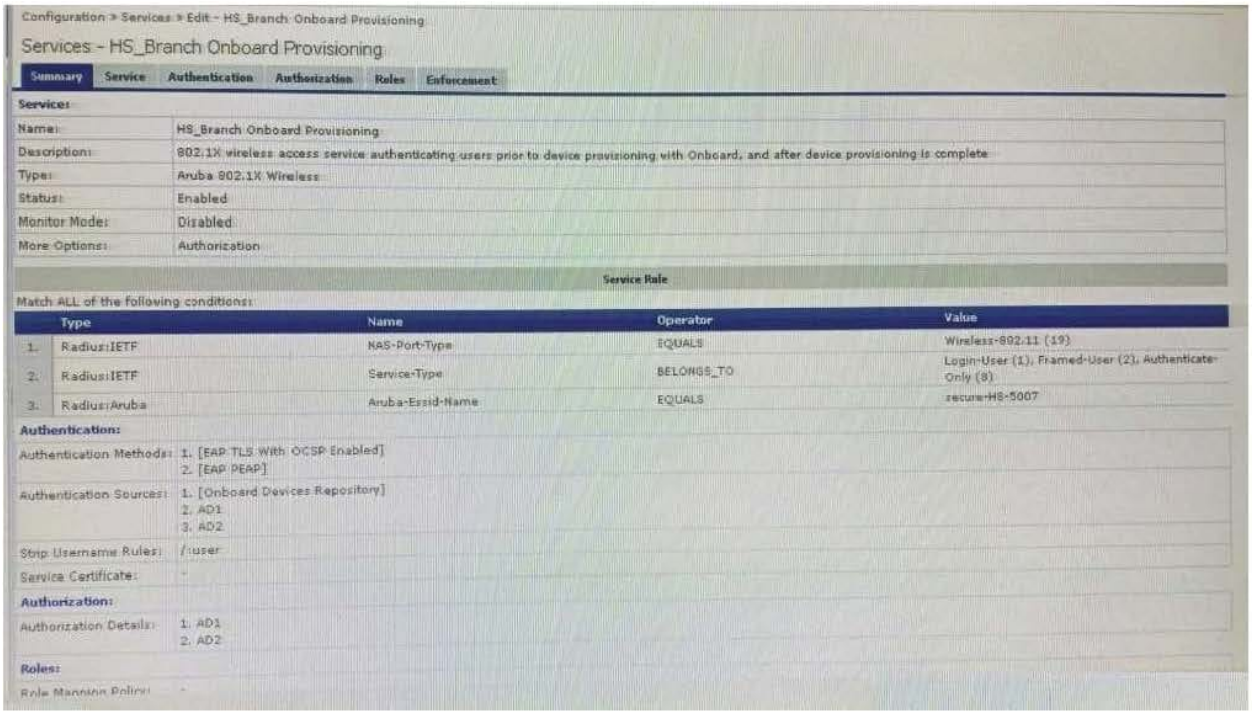
Correct Answer: C

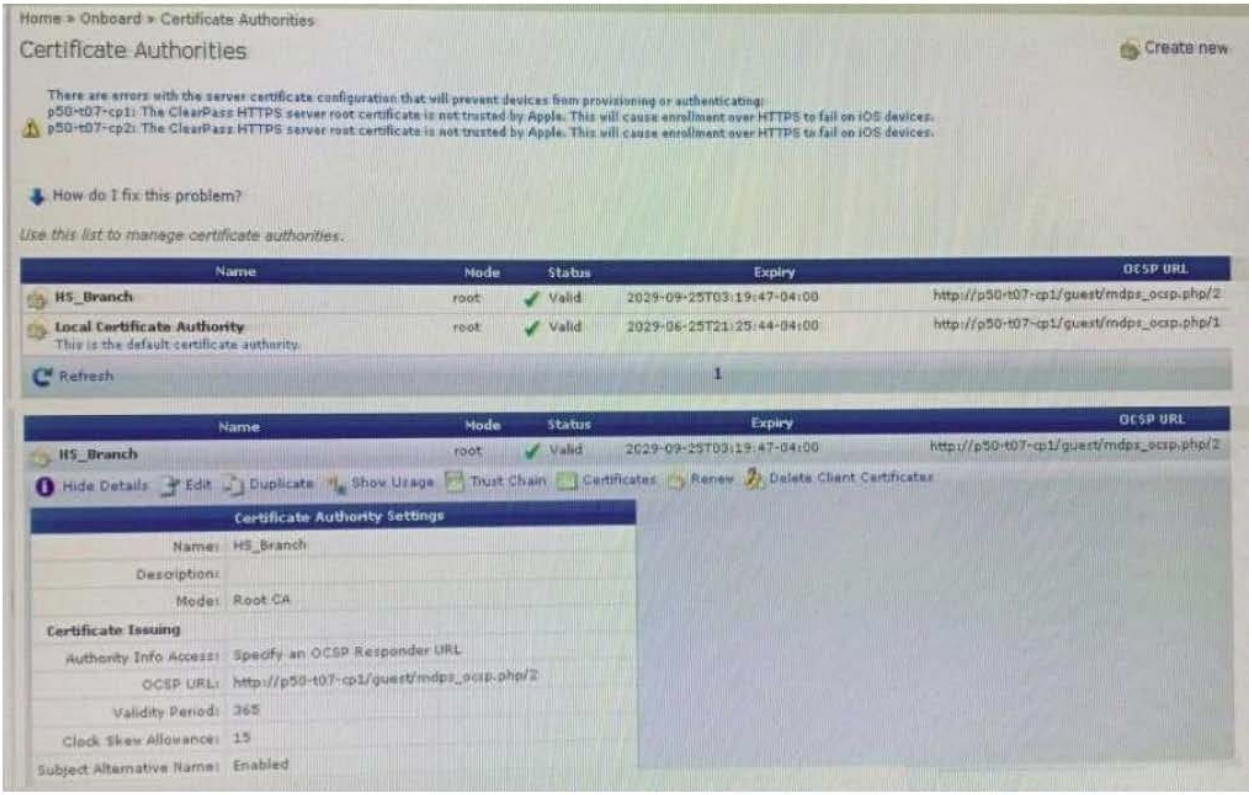
QUESTION 3

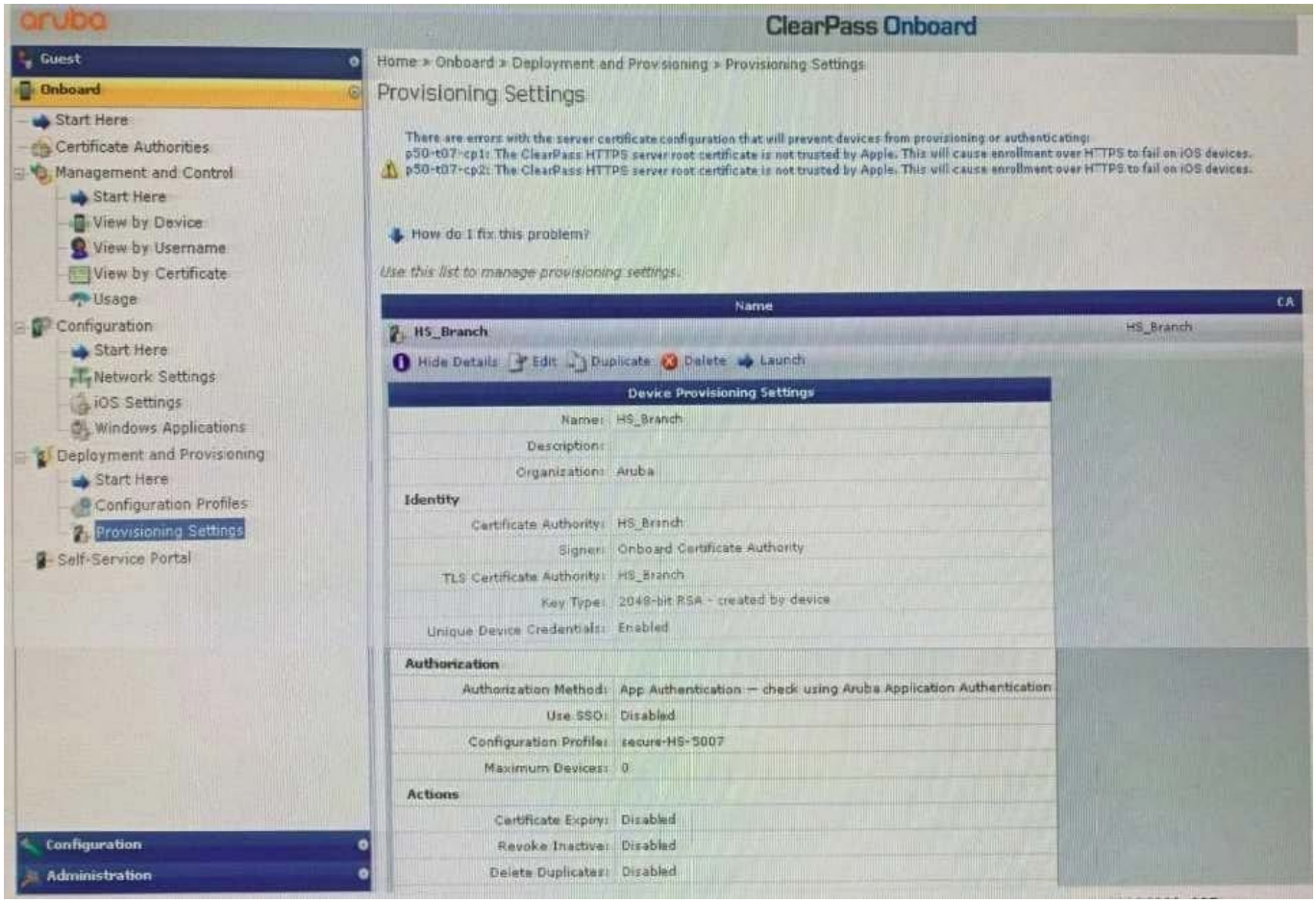
Refer to the exhibit:


QuickConnect by Aruba Networks, Inc.
aruba
NETWORKS
Onboard Wizard
Welcome
Configure
Connect
Summary
Securely Connect to Network
Authentication in progress ...
QuickConnect
Could not authenticate with wireless network
OK
Aruba


Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: R00000002-01-5d6b2731
Date and Time: Sep 25, 2019 04:37:06 EDT
End-Host Identifier: 780294992613 (Computer / Windows / Windows 10)
Username: mike07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Branch Onboard Provisioning
Authentication Method: EAP-TLS
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1, AD2
Roles: -
Enforcement Profiles: [Allow Access Profile], HS_Branch Onboard Post-Provisioning
Service Monitor Mode: Disabled
Showing 1 of 1-7 records
Show Configuration
Export
Show Logs
Close
Request Details
Summary
Input
Output
Alerts
Error Code: 215
Error Category: Authentication failure
Error Message: TLS session error
Alerts for this Request
RADIUS Certificate Status unknown. Reason (UNKNOWN)
EAP-TLS: fatal alert by server - (internal_error
TLS Handshake failed in SSL_read with error:14089086:SSL
routines:ssl3_get_client_certificate:certificate verify failed
eap-tls: Error in establishing TLS session


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 TLS With OCSP Enabled]
2. [EAP PEAP]
Authentication Sources: 1. [Onboard Devices Repository]
2. AD1
3. AD2
Strip Username Rules: /:user
Service Certificate: -
Authorization:
Authorization Details: 1. AD1
2. AD2
Roles:


Home » Onboard » Certificate Authorities
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 root Valid 2029-06-25T21:25:44-04:00 http://p50-t07-cp1/guest/mdps_ocsp.php/1
This is the default certificate authority.
Refresh
1
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
Hide Details Edit Duplicate Show Usage Trust Chain Certificates Renew Delete Client Certificates
Certificate Authority Settings
Name: HS_Branch
Description:
Mode: Root CA
Certificate Issuing
Authority Info Access: Specify an OCSP Responder URL
OCSP URL: http://p50-t07-cp1/guest/mdps_ocsp.php/2
Validity Period: 365
Clock Skew Allowance: 15
Subject Alternative Name: Enabled



You have configured Onboard and cannot get it working The customer has sent you the above screenshots.

How would you resolve the issue?

A. Re-provision the client by running the QuickConnect application as Administrator

B. Install a public signed server authentication certificate on the ClearPass server for EAP

C. Reconnect the client and select the correct certificate when prompted

D. Copy the [EAP-TLS with OSCP Enabled] authentication method and set the correct OCSP URL

Correct Answer: A

QUESTION 4

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 5

There is an Aruba Controller configured to send Guest AAA requests to ClearPass. If the customer would like the most effective way to ensure the lowest license usage counts, how should the controller be configured?

A. Aruba Controller will send stop messages only if EAP termination and Interim accounting are enabled.

B. Aruba Controller will send stop messages if RADIUS Accounting Server Group is defined in the authentication profile.

C. Aruba Controller will send stop messages only if both accounting and interim accounting are enabled.

D. Configure EAP Termination on the Aruba Controller and the client will send a stop message.

Correct Answer: D

HPE6-A77 PDF Dumps HPE6-A77 Exam Questions HPE6-A77 Braindumps