HPE6-A77 Q&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.passapply.com/hpe6-a77.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

A corporate ClearPass Cluster with two servers located at a single site, has both Management and Data port IP addresses configured. The Management port IPs are in the DataCenter networks subnet, while the Data port IPs are in the DMZ. What is the difference between using one Virtual IP for the AAA traffic versus sending AAA requests to the physical IPs for each server? (Select two.)

A. The failover can be accomplished only by using Virtual IP.

B. The Individual IPs can provide failover and load balancing.

C. One Virtual IP can be used together with the individual server IPs for load balancing.

D. By using the Virtual IP, the failover convergence is faster than using individual server IPs.

E. Using the one Virtual IP can provide failover and load balancing.

Correct Answer: BE

QUESTION 2

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. ix 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 3

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

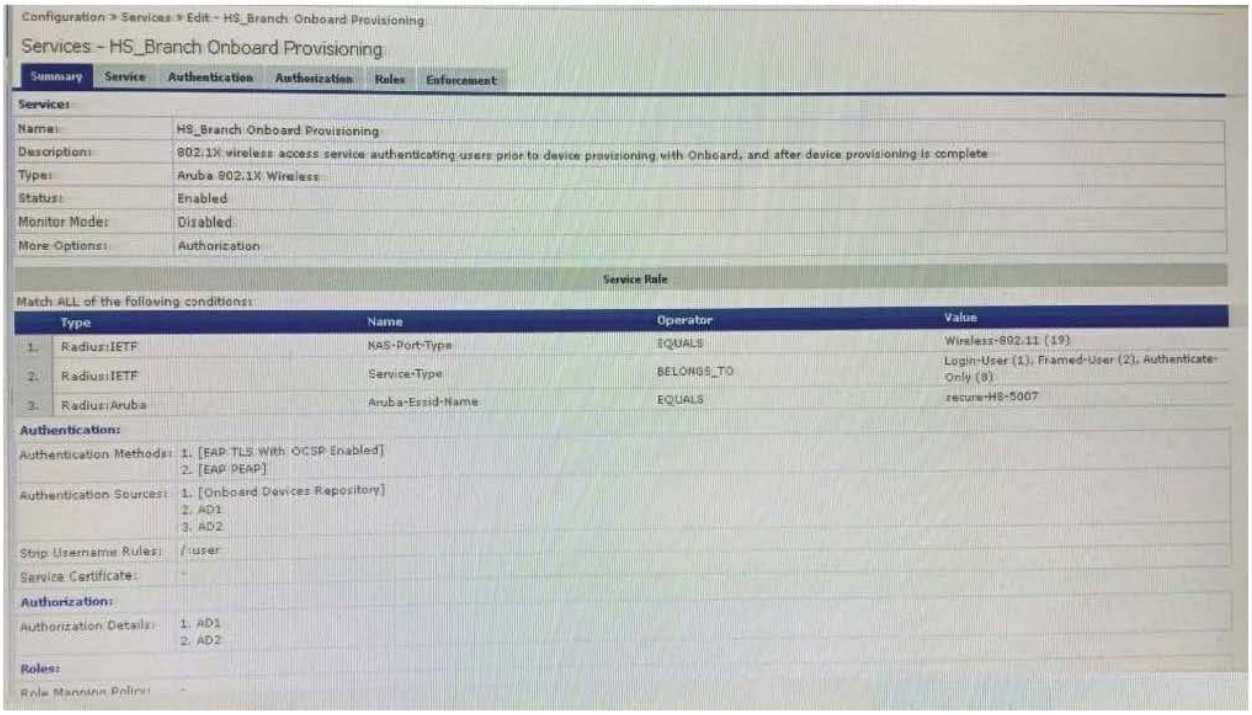
Correct Answer: A

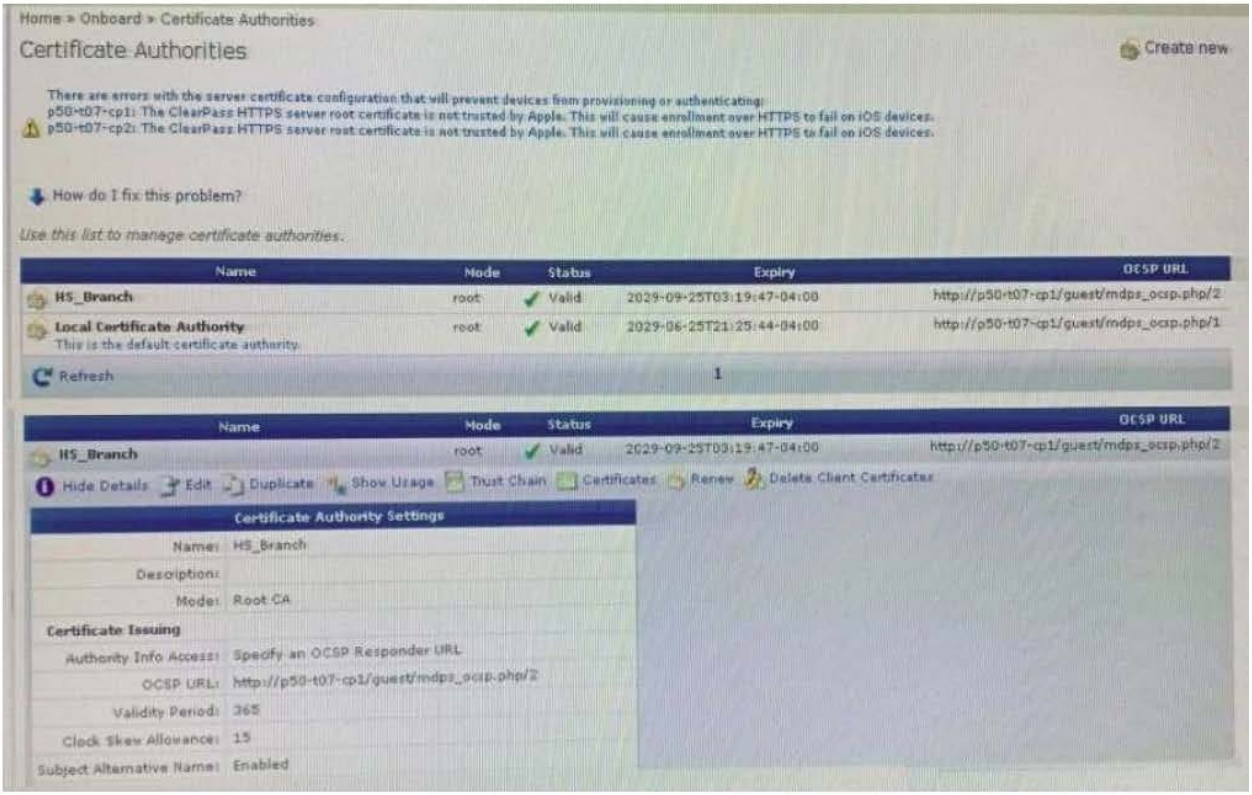
QUESTION 4

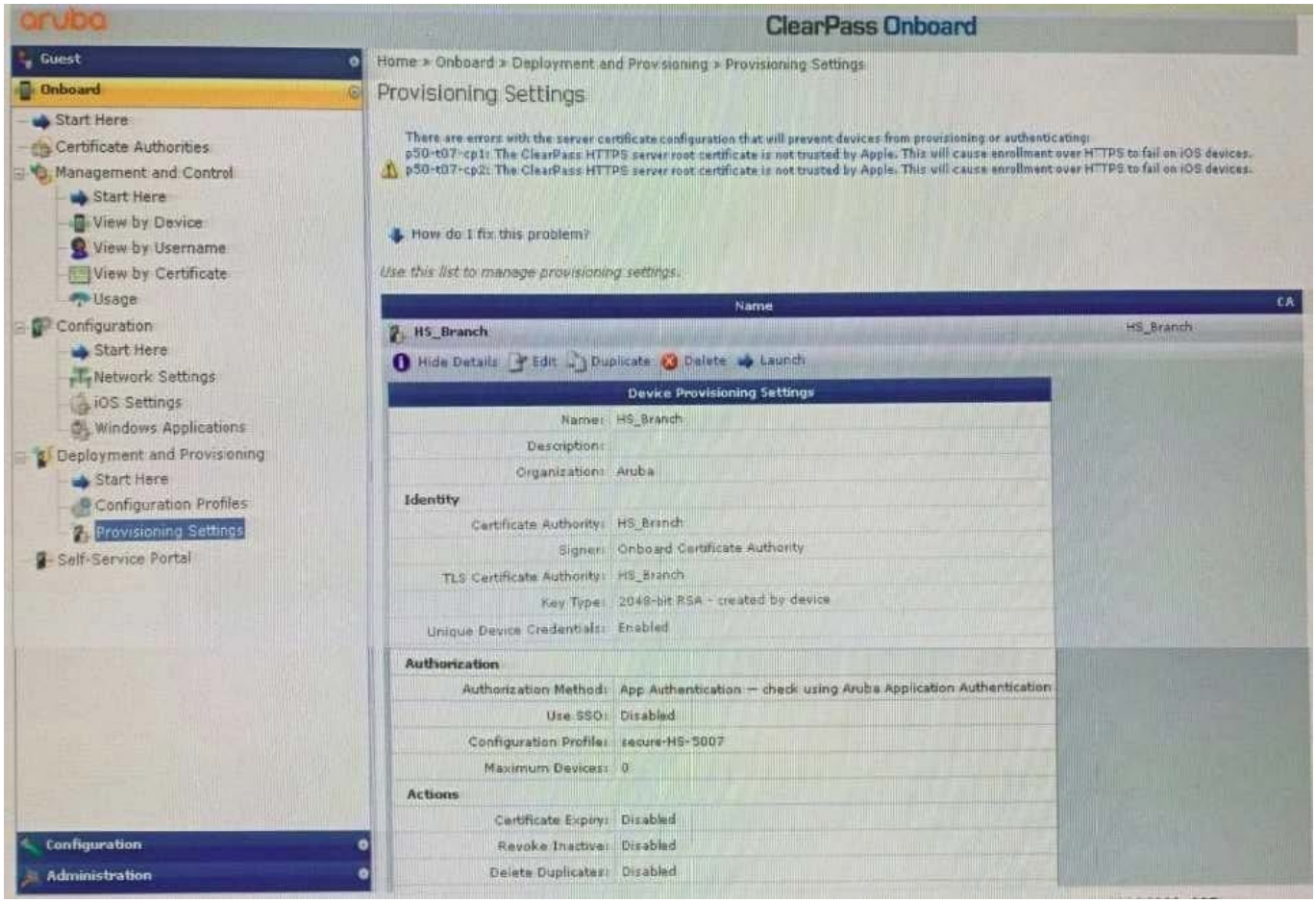
Refer to the exhibit:


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

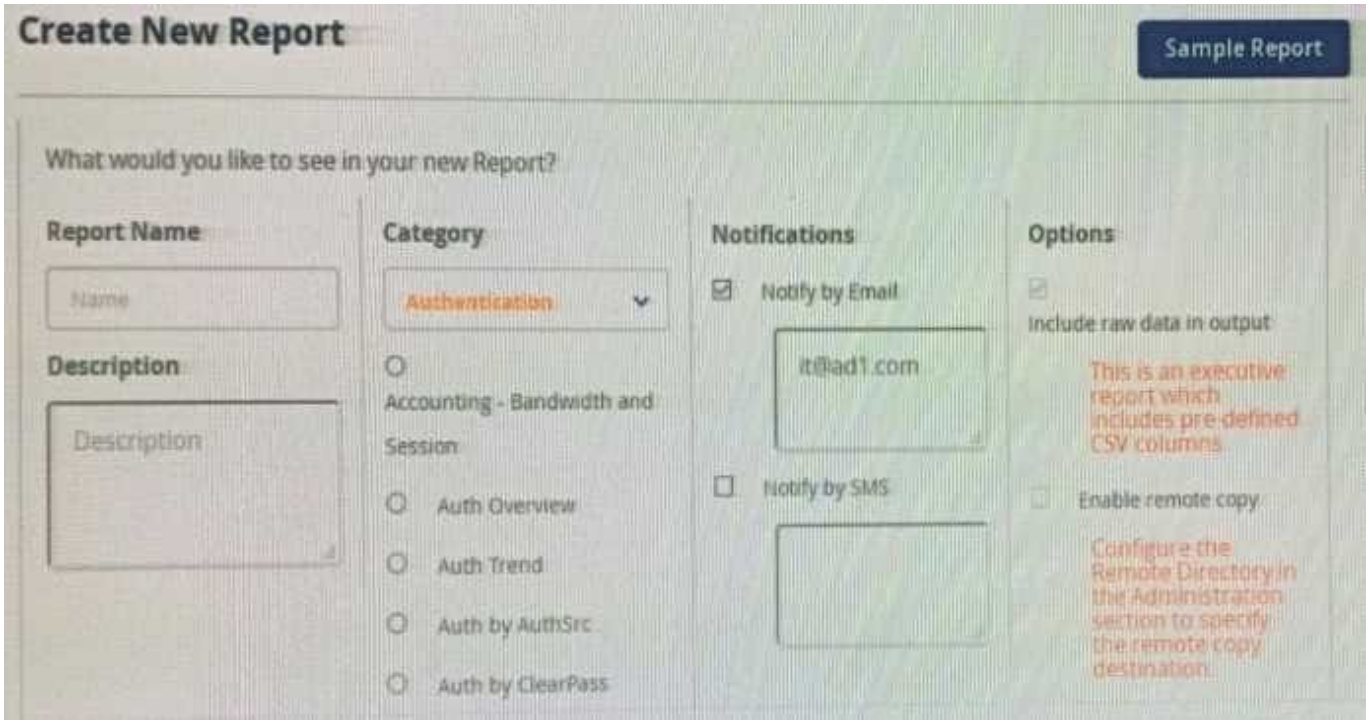
C. Reconnect the client and select the correct certificate when prompted

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

Correct Answer: A

QUESTION 5

Refer to the exhibit:



When creating a new report, there is an option to send report Notifications by Email. Where is the email server configured?

A. In the ClearPass Policy Manager Endpoint Context servers under Administration.

B. In the Insight Reports Interface under Administration on the sidebar menu.

C. In the insight report on the next screen of the report definition.

D. In the ClearPass Policy Manager Messaging setup under Administration.

Correct Answer: B

QUESTION 6

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard

3.

Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

A. Multi-Master cache

B. Endpoint database

C. insight database

D. ClearPass system cache

Correct Answer: D

QUESTION 7

While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

A. expire_after

B. do_expire

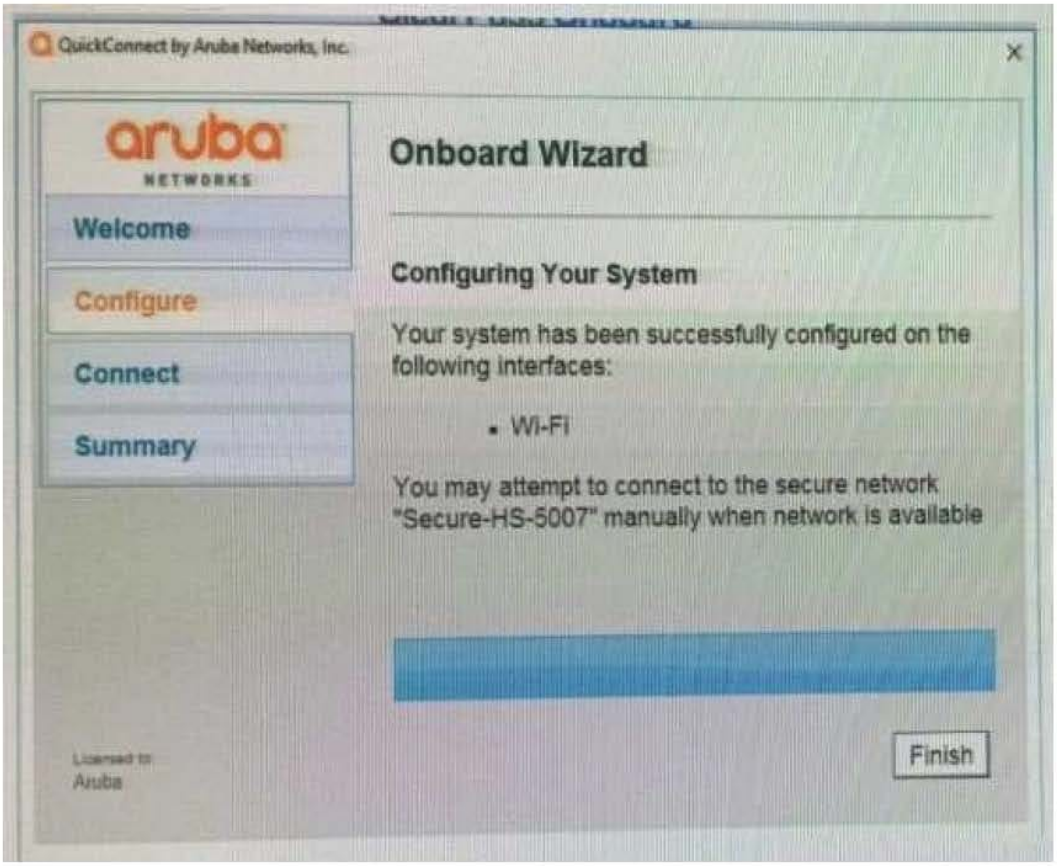
C. expire_time

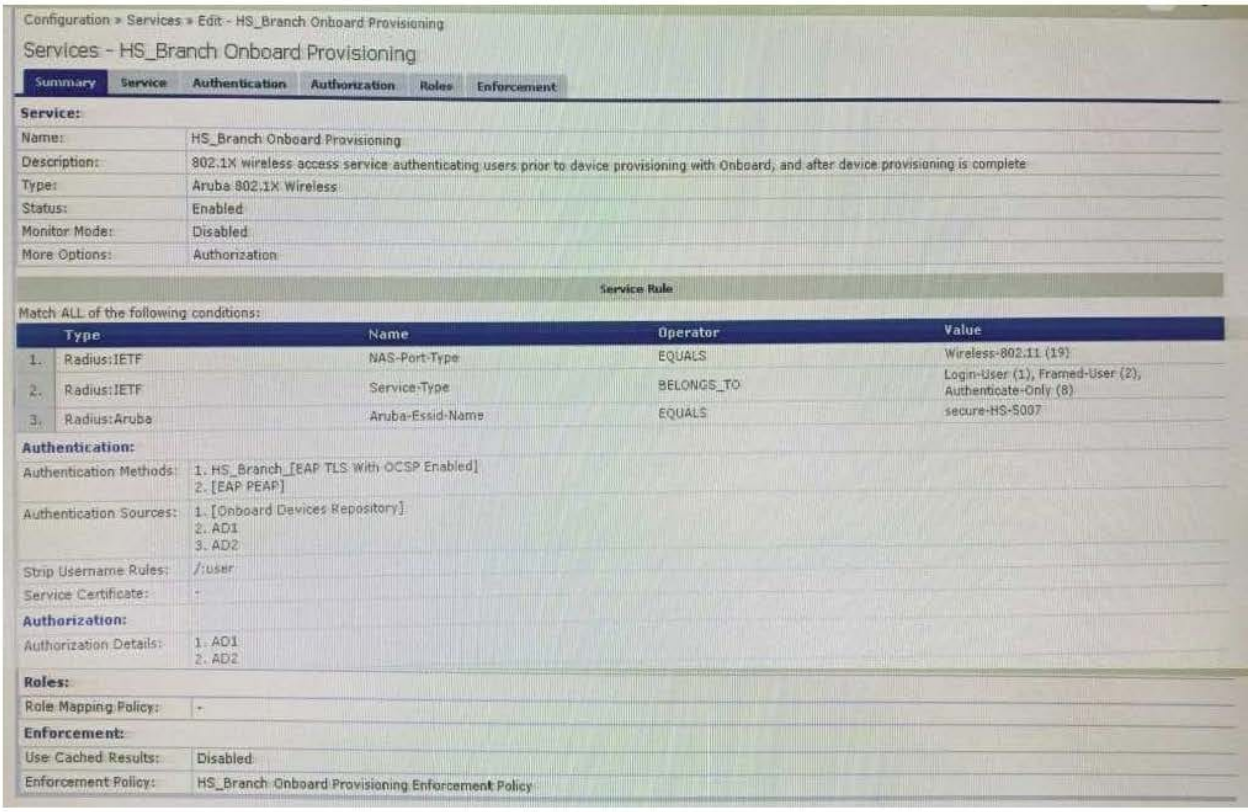
D. expire_ postlogin

Correct Answer: A

QUESTION 8

Refer to the exhibit:





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. HS_Branch_[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:

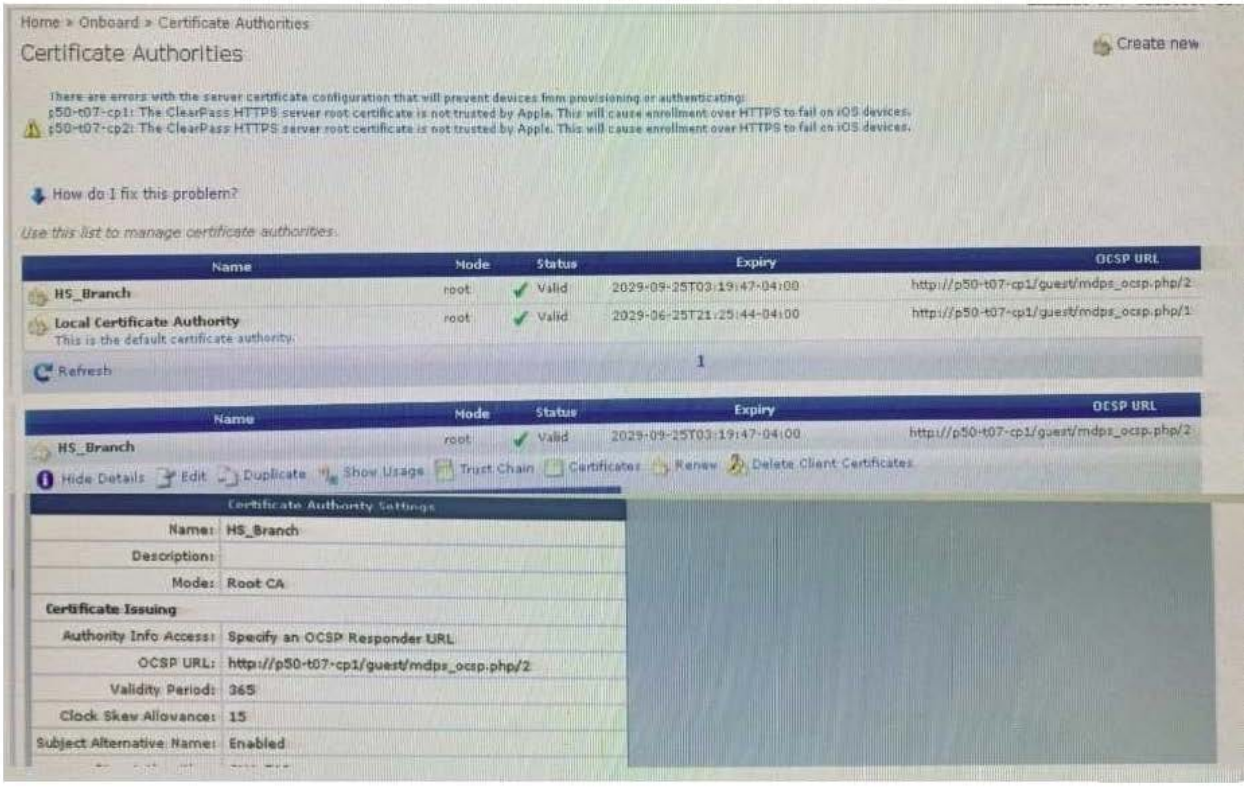
Authorization Details:	1. AD1 2. AD2

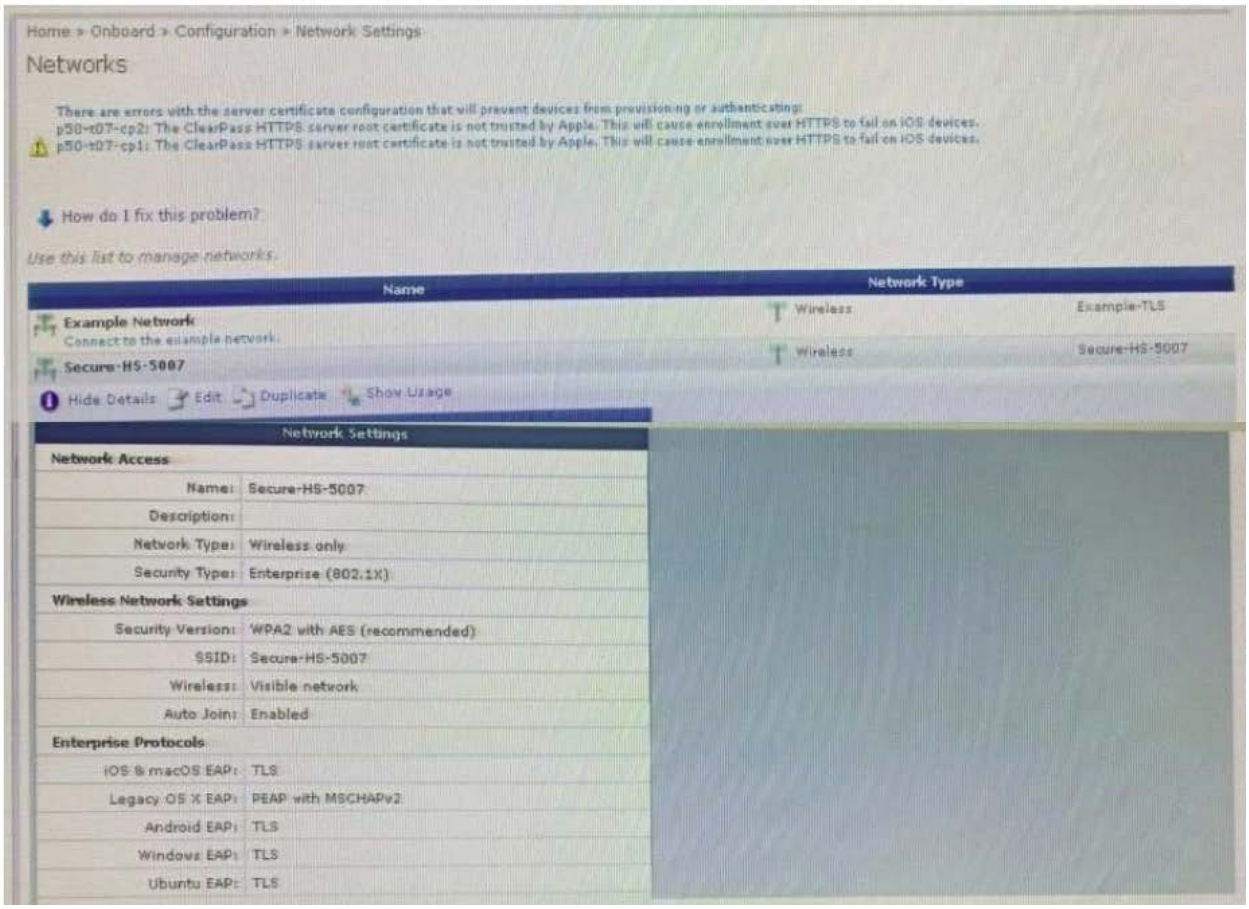
Roles:

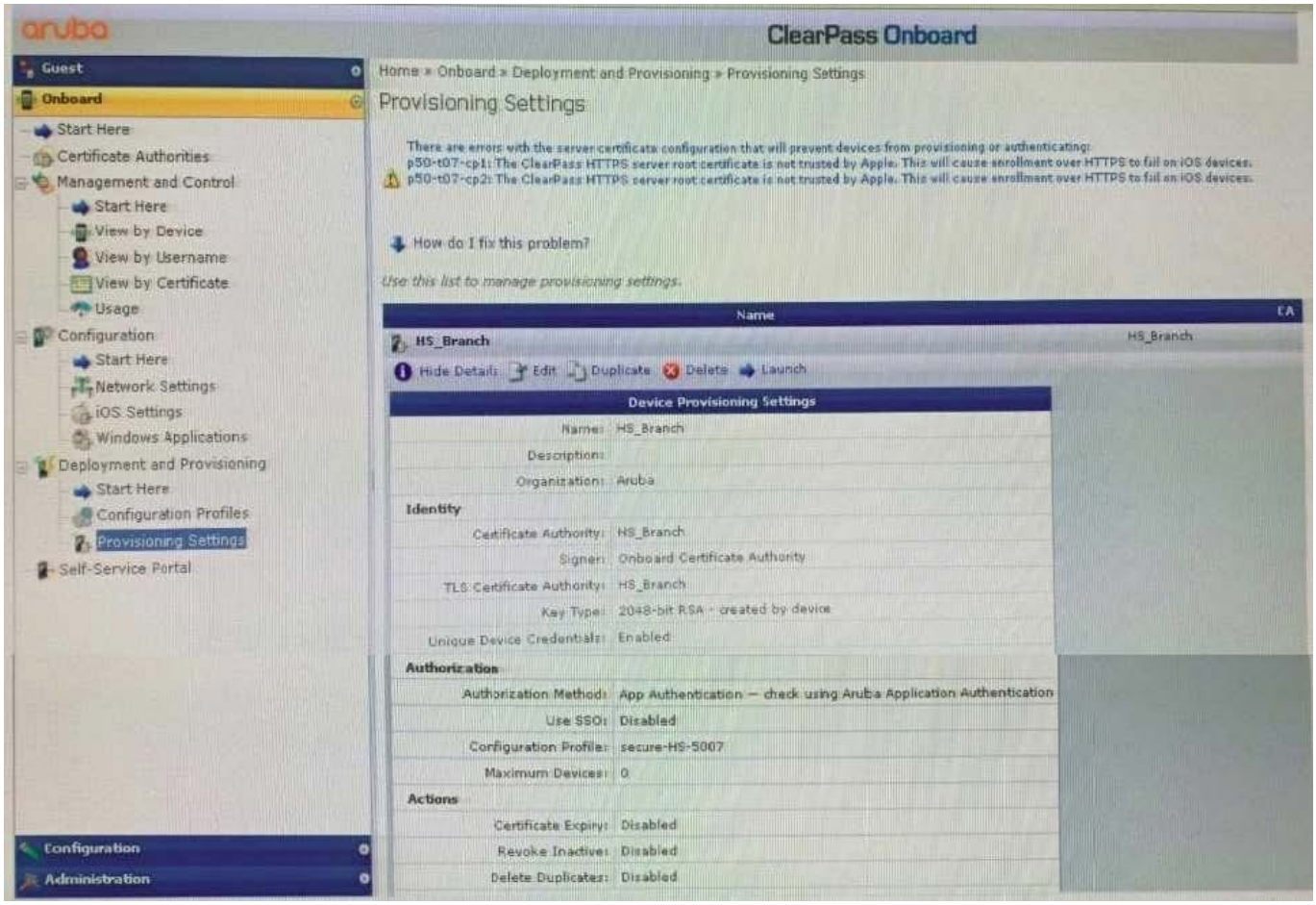
Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	HS_Branch Onboard Provisioning Enforcement Policy


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
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
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


Home » Onboard » Configuration » Network Settings
Networks
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
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.
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.
How do I fix this problem?
Use this list to manage networks.
Name
Network Type
Example Network
Connect to the example network.
Wireless
Example-TLS
Secure-HS-5007
Wireless
Secure-HS-5007
Hide Details
Edit
Duplicate
Show Usage
Network Settings
Network Access
Name: Secure-HS-5007
Description:
Network Type: Wireless only
Security Type: Enterprise (802.1X)
Wireless Network Settings
Security Version: WPA2 with AES (recommended)
SSID: Secure-HS-5007
Wireless: Visible network
Auto Join: Enabled
Enterprise Protocols
iOS & macOS EAP: TLS
Legacy OS X EAP: PEAP with MSCHAPv2
Android EAP: TLS
Windows EAP: TLS
Ubuntu EAP: TLS



You have configured an Onboard portal for single SSID provision. During testing you notice that the QuickConnect Application did not display the "Connect" button, only the finish button. To get connected the test user had to manually connect to the secure-HS-5007 SSID but was prompted for a username and password. Using the screenshots as a reference, how would you fix this issue?

A. Check the network settings for the correct SSID name spelling.

B. Change the network settings to use EAP-TLS for the authentication protocol.

C. Install a public signed HTTPs web server certificate on the ClearPass server.

D. Configure the SSID to support both EAP-PEAP and EAP-TLS authentication method.

Correct Answer: A

QUESTION 9

How does the RadSec improve the RADIUS message exchange? (Select two.)

A. It can be used on an unsecured network or the Internet.

B. It builds a TTLS tunnel between the NAD and ClearPass.

C. Only the NAD needs to trust the ClearPass Certificate.

D. It encrypts the entire RADIUS message.

E. It uses UDP to exchange the radius packets.

Correct Answer: DE

QUESTION 10

Refer to the exhibit:

A customer with multiple Aruba Controllers has just installed a new certificate for "*.customerdomain com" on all Aruba Controllers. While testing the existing guest Self-Registration page the customer noticed that the logins are failing. While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests. Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page. From the screen shown, how can you fix the errors?

A. Change the "IP Address: field to" securelogin.customerdomain.com.

B. Change the "Secure Login:" field to "Use Vendor Default".

C. Change the "IP Address field to "captiveportal-login.customerdomain.com".

D. Add PTR records on the DNS server for "securelogin.arubanetworks.com".

Correct Answer: B