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.pass4itsure.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

You have Integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment to sign the Anal device TLS certificates The Onboard provisioning process completes successfully but when the user finally clicks connect, the user falls to connect to the network with an unknown_ca certificate error. What steps will you follow to complete the requirement?

A. Make sure that the ClearPass servers are using the default self-signed certificates for both SSL and RADIUS server identity

B. Add the ADCS root certificate to both the CPPM Certificate trust list and to the Onboard Certificate Store trust list

C. Make sure both the ClearPass servers have different certificates used for both SSL and RADIUS server identity.

D. Export the self-signed certificate from the ClearPass servers and manually add them as trusted certificates in clients

Correct Answer: A

QUESTION 2

What is the Secure SSID {otherwise referred to as Single SSID) OnBoard deployment service workflow?

A. OnBoard Provisioning RADIUS service, OnBoard Authorization RADIUS service. OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

B. OnBoard Provisioning RADIUS service, OnBoard Pre-Auth RADIUS service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

C. OnBoard Provisioning RADIUS service, OnBoard Pre-Auth Application service. OnBoard Authorization Application service, OnBoard Provisioning RADIUS service

D. OnBoard Provisioning RADIUS service, OnBoard Authorization Application service, OnBoard Pre- Auth Application service, OnBoard Provisioning RADIUS service

Correct Answer: A

QUESTION 3

A customer is complaining that some of the devices, in their manufacturing network, are not getting profiled while other loT devices from the same subnet have been correctly profiled. The network switches have been configured for DHCP IP helpers and IF-MAP has been configured on the Aruba Controllers. What can the customer do to discover those devices as well? (Select two.)

A. Update the Fingerprints Dictionary to the latest in case new devices have been added.

B. Open a TAC case to help you troubleshoot the DHCP device profile functionality.

C. Add the ClearPass Server IP as an IP helper address on the default gateway as well.

D. Allow time for IF-MAP service on the controller to discover the new devices as well.

E. Manually create a new device fingerprint for the devices that are not being profiled.

Correct Answer: DE

QUESTION 4

You are integrating a Postgres SQL server with the ClearPass Policy Manager. What steps will you follow to complete the integration process? (Select three)

A. Click on the default filter name with pre-defined filter queries and check box to enable as role.

B. Specify a new filter with filter queries to fetch authentication and authorization attributes.

C. Attribute Name under filter configuration must match one of the columns being requested from the database table.

D. Create a new Endpoint context server and add the SQL server IP, credentilas and the database name.

E. Alias Name under filter configuration must match one of the columns being requested from the database table.

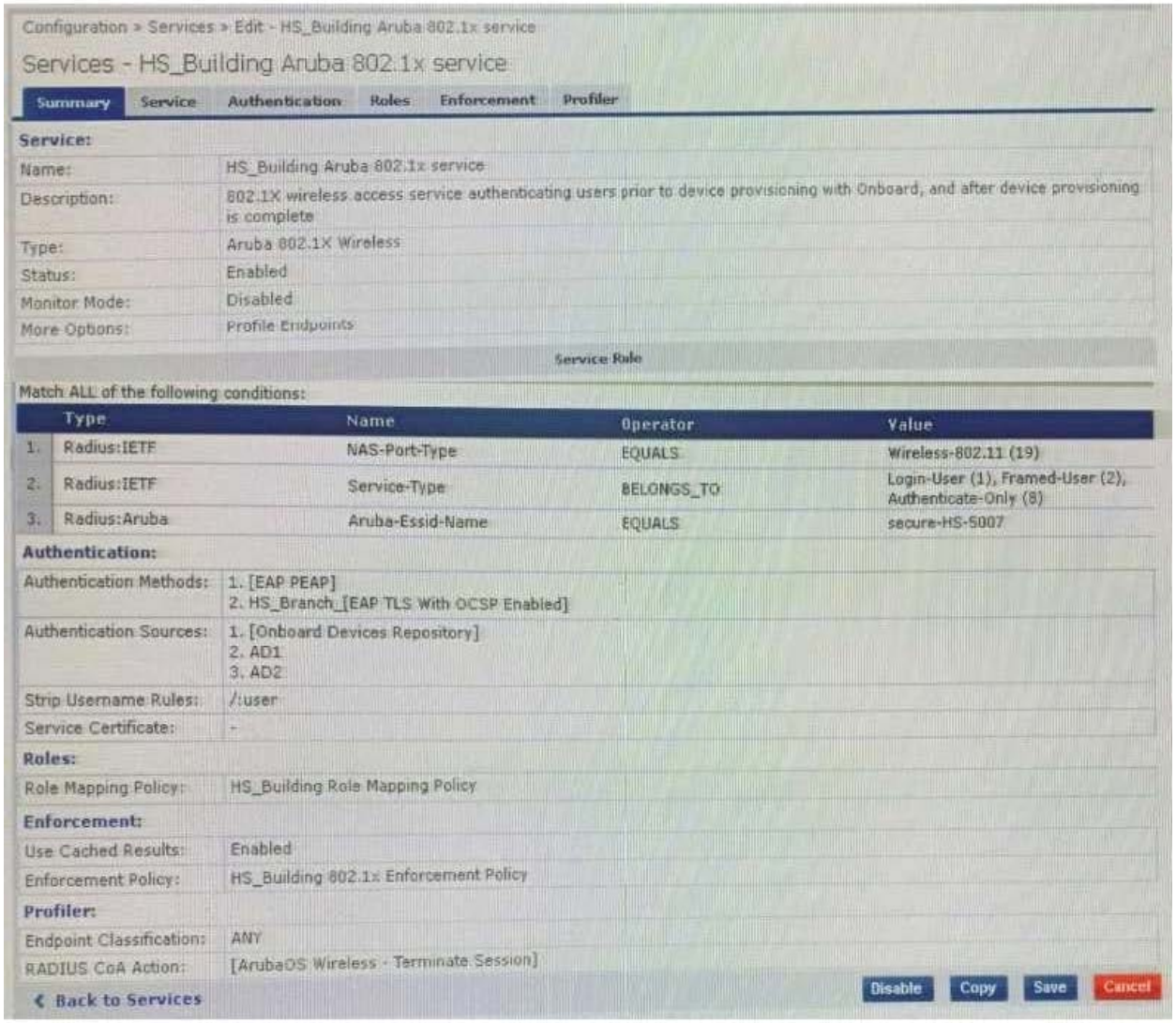
F. Create a new authentication source and add the SQL server IP, credentials and the database name.

Correct Answer: BDF

QUESTION 5

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: R00000218-01-5d9db68b
Date and Time: Oct 09, 2019 06:29:34 EDT
End-Host Identifier: 78D29437BD68 (Computer / Windows / Windows 10)
Username: andy07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Building Aruba 802.1x service
Authentication Method: EAP-PEAP,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1
Roles: [Other], [User Authenticated]
Enforcement Profiles: [Deny Access Profile]
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Show Configuration
Export
Show Logs
Close
Request Details
Summary
Input
Output
Alerts
Error Code: 206
Error Category: Authentication failure
Error Message: Access denied by policy
Alerts for this Request
RADIUS Applied 'Reject' profile



Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Service:

Name:	HS_Building Aruba 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:	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:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-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
Strip Username Rules:	/:user
Service Certificate:	-

Roles:

Role Mapping Policy:	HS_Building Role Mapping Policy

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Building 802.1x Enforcement Policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]

« Back to Services

Disable | Copy | Save | Cancel

Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | 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 BELONGS_TO_GROUP VIP User MAC)	VIP User
2.	(Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3.	(Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4.	(Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5.	(Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6.	(Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)	Printer
7.	(Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	IP Camera

Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

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

Enforcement Policy: HS_Building 802.1x 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.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
4.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	Redirect to Aruba Quarantine Profile

Your company has a postgres SQL database with the MAC addresses of the company-owned tablets You have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.

B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.

C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

D. Enable authorization tab in the service and add the SQL server as an authorization source.

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

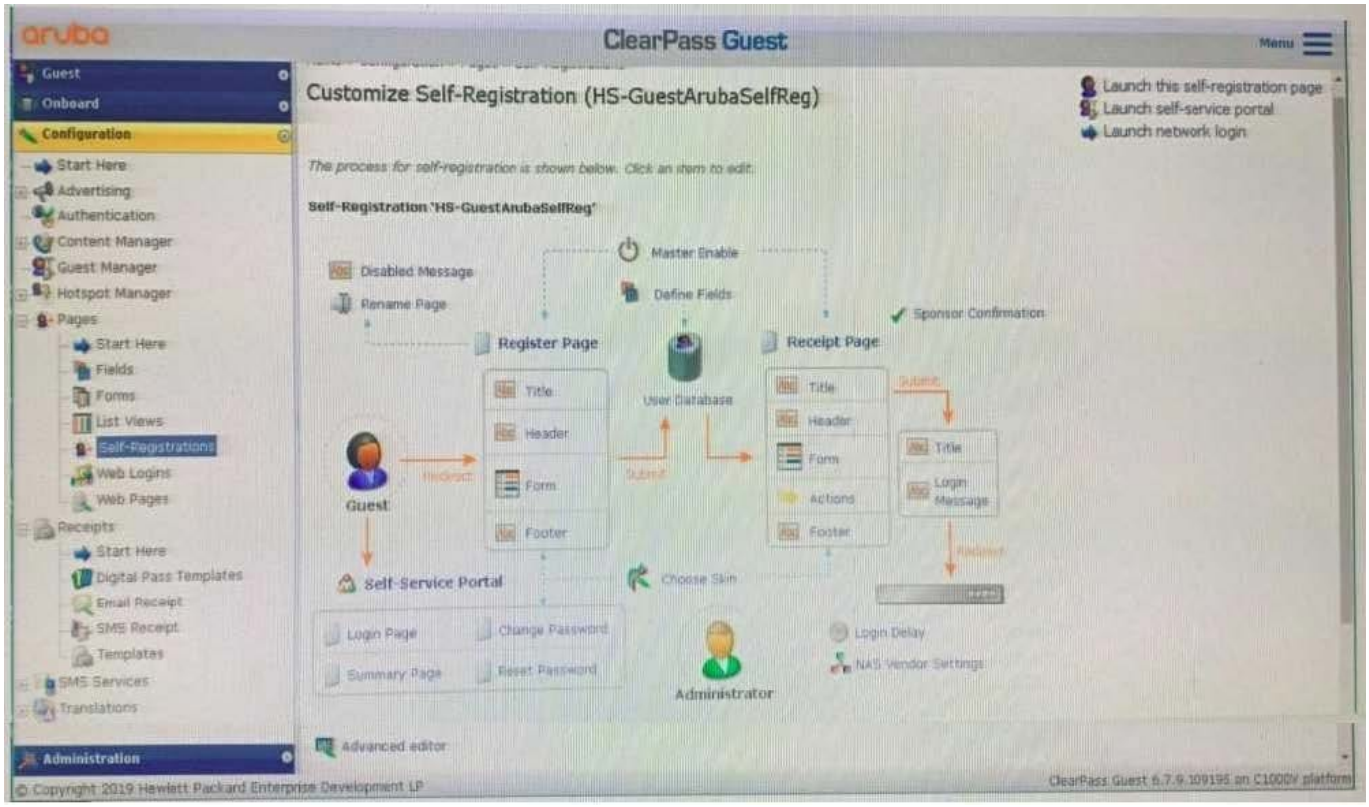
C. insight database

D. ClearPass system cache

Correct Answer: D

QUESTION 7

Refer to the exhibit:



A customer is deploying Guest Self-Registration with Sponsor Approval but does not like the format of the sponsor email. Where can you change the sponsor email?

A. in the Receipt Page - Actions

B. in the Sponsor Confirmation section

C. in me Configuration - Receipts - Email Receipts

D. in the Configuration - Receipts - Templates

Correct Answer: B

QUESTION 8

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

QUESTION 9

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 10

Under Onboard management and control, which option will deny the user from re-provisioning the device a second time?

A. Revoke and Delete certificate

B. Delete user

C. Revoke certificate

D. Delete certificate

Correct Answer: D