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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

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

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

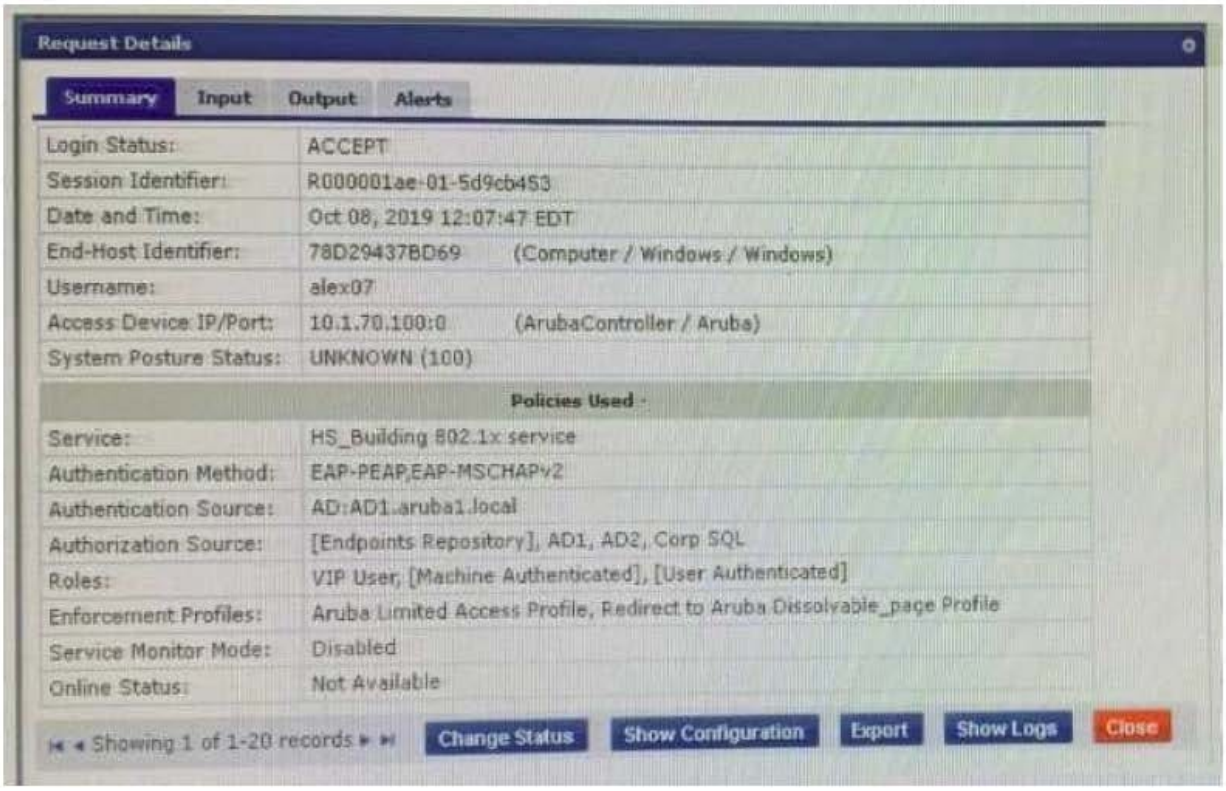
C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

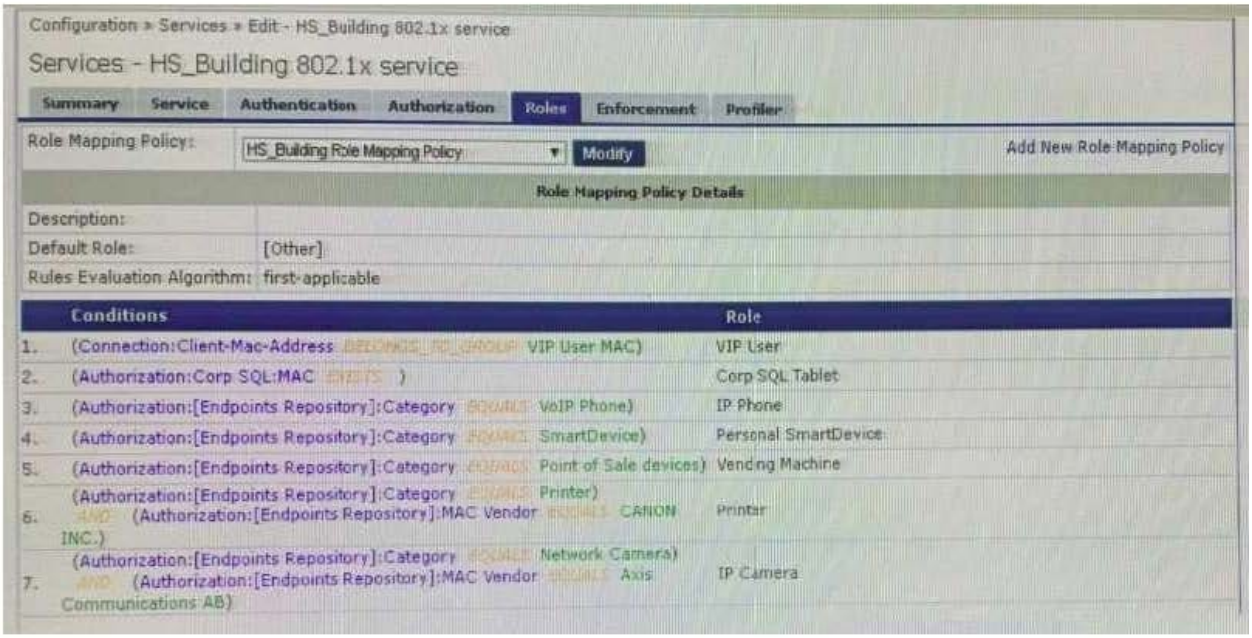
D. OnBoard Authorization RADIUS service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

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: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?

A. Secure Login should use HTTP

B. Change the Vendor Settings to Airespace Networks

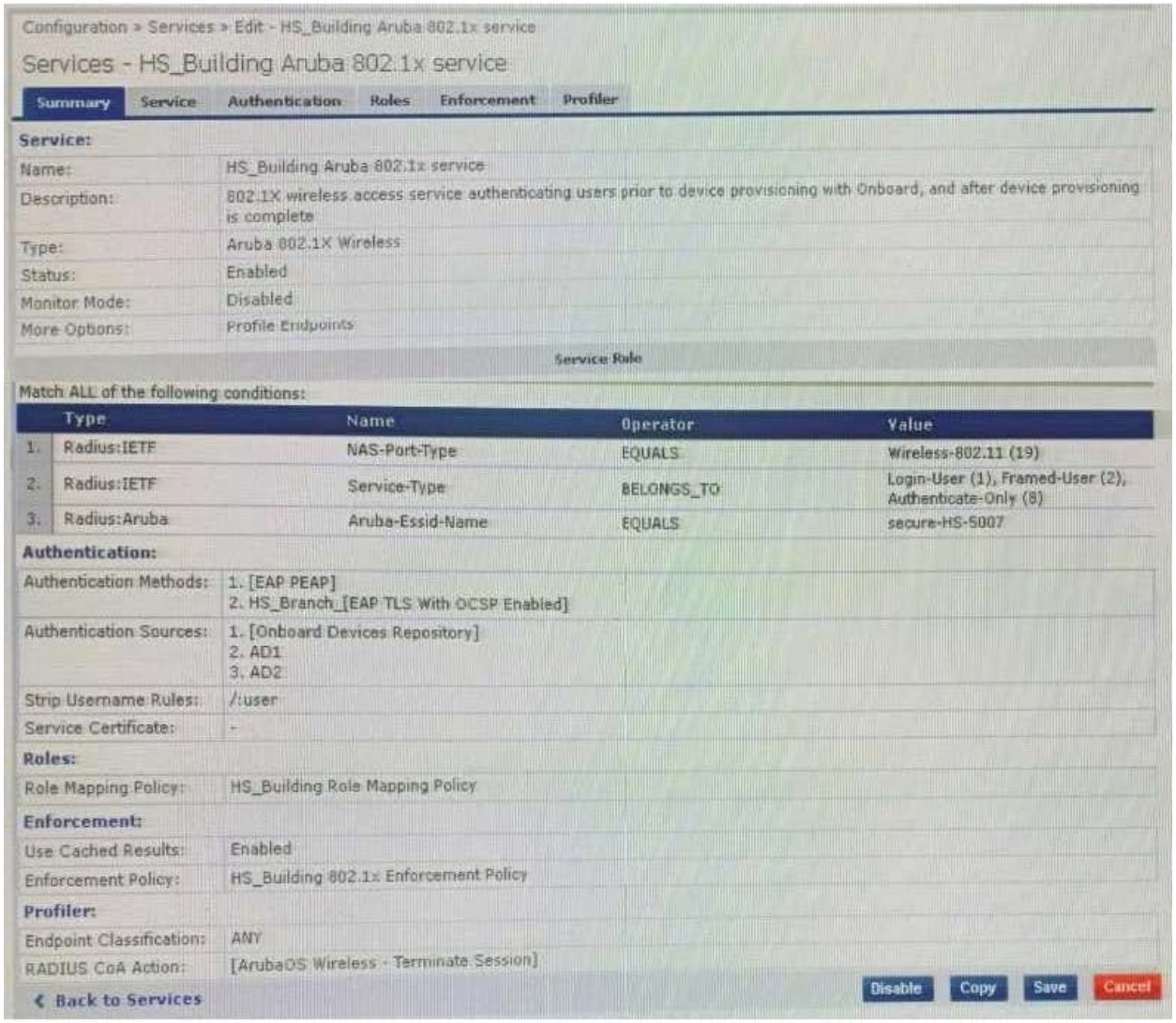
C. Change \he IP Address to the Cisco Controller DNS name

D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

QUESTION 4

Refer to the exhibit:



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 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


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 true)
Aruba Full Access Profile
2. (Authentication:OuterMethod EAP-PEAP) AND (Tips:Role Corp SQL Tablet)
Redirect to Aruba OnBoard Portal
3. (Authentication:OuterMethod EAP-TLS) AND (Tips:Role Corp SQL Tablet)
Aruba Full Access Profile
4. (Tips:Role VIP User)
Aruba VIP Full Access Profile
5. (Tips:Role [User Authenticated] [Machine Authenticated]) AND (Authentication:Source AD1) AND (Tips:Posture HEALTHY (0))
Aruba Full Access Profile
6. (Tips:Role [User Authenticated] [Machine Authenticated]) AND (Authentication:Source AD1) AND (Tips:Posture UNKNOWN (100))
Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7. (Tips:Role [User Authenticated] [Machine Authenticated]) AND (Authentication:Source AD1) AND (Tips:Posture 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 5

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