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 customer has a ClearPass cluster deployment with four servers, two servers at the data center and two servers at a large remote site connected over an SD-WAN solution The customer would like to implement OnGuard, Guest Self-Registration, and 802.1x authentication across their entire environment. During testing the customer is complaining that users connecting to an Instant Cluster Employee SSID at the remote site, with the OnGuard Persistent Agent installed are randomly getting their health check missed. What could be a possible cause of this behavior?

A. The OnGuard Clients are automatically mapped to the Policy Manager Zone based on their IP range but an ACL on the switch could be blocking access.

B. The traffic on the TCP port 6658 is congested due to the fact that this port is also used by the IPsec keep-alive packets of the SD-WAN solution.

C. The ClearPass Policy Manager zones have been defined but the local IP sub-nets have not been property mapped to the zones and the OnGuard Agent might connect to any of the servers in the cluster.

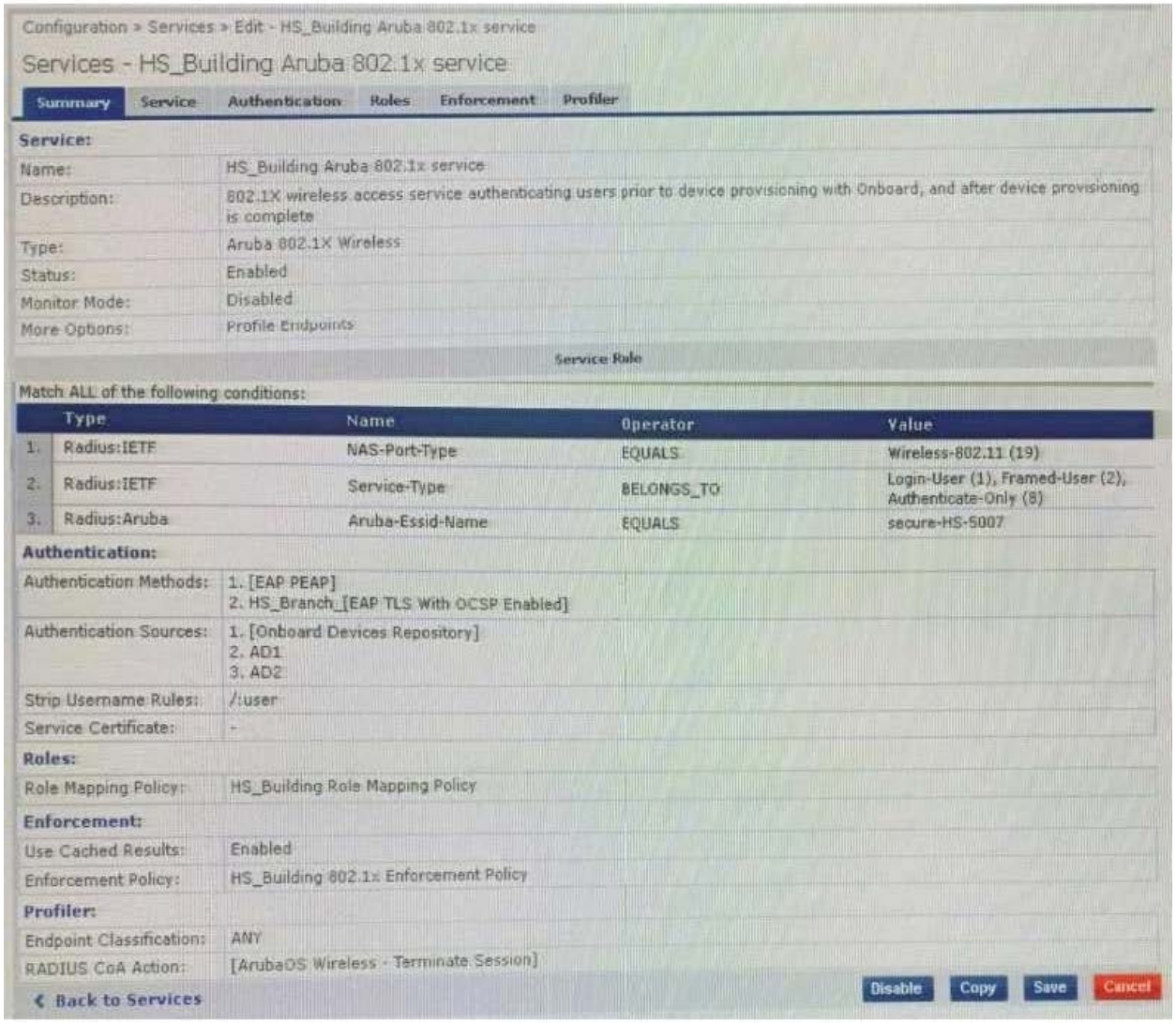
D. The Aruba-user-role received by the IAP is filtering the TCP port 6658 to the ClearPass servers and after 10 seconds the SSL fallback gets activated and randomly generates the issue.

Correct Answer: D

QUESTION 2

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.

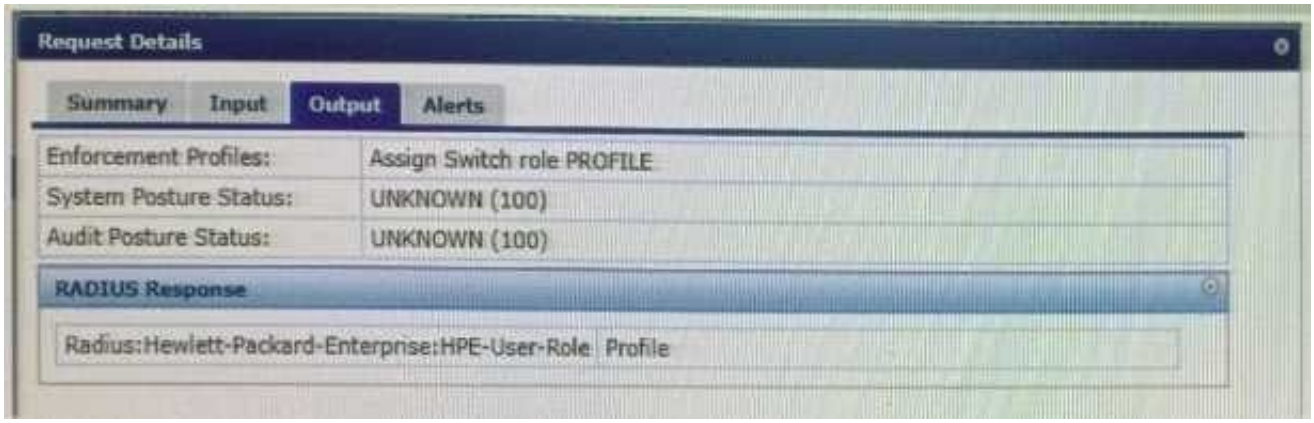
C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

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

Correct Answer: B

QUESTION 3

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Enforcement Profiles:
Assign Switch role PROFILE
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Hewlett-Packard-Enterprise:HPE-User-Role Profile


P50-T7-2930(config)# sho port-access clients
Port Access Client Status
Port Client Name MAC Address IP Address User Role Type
VLAN
3 204c035b4ad2 204c03-5b4ad2 n/a denyall MAC
70
P50-T7-2930(config)# show user-role
User Roles
Enabled : Yes
Initial Role : denyall
Type Name
local PROFILE
predefined denyall
local AP-ACCESS
P50-T7-2930(config)#

You have been asked to help a Customer troubleshoot an issue. They have configured an Aruba OS switch (Aruba 2930 with 16.09) to do MAC authentication with profiling using ClearPass as the authentication source. They cannot get it working.

Using the screenshots as a reference, how will you fix the issue?

A. Delete the initial role in the Aruba OS switch to force the device to get the server derived user roles

B. Use a CoA to bounce the switch port to force the port to change to the correct Aruba user role

C. Change the Vendor settings for the Aruba OS switch to "Aruba" so that the enforcement will use the correct VSAs

D. Modify the enforcement profile conditions with Aruba Vendor specific attributes and Aruba-user- roles

E. User-roles are case sensitive, update the correct role with correct case in the enforcement profile

Correct Answer: D

QUESTION 4

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

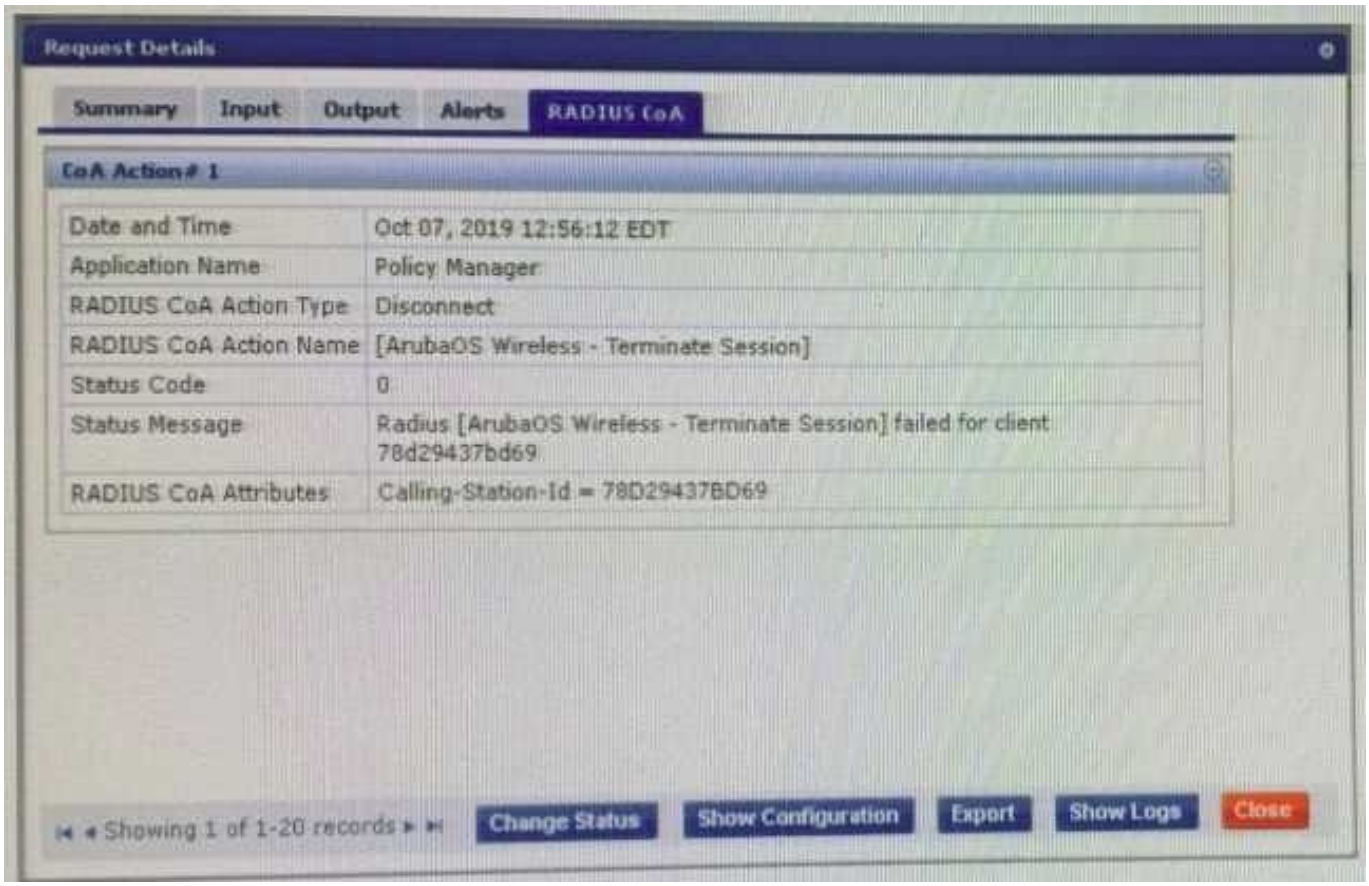
C. Revoke certificate

D. Delete certificate

Correct Answer: D

QUESTION 5

Refer to the exhibit: You configuring an 802 1x service endpoint profiling. When the client connects to the network, ClearPass successfully profiles the client and sends Radius Change of Authorization (RCoA) but Radius Change of Authorization {RCoA) fails for the client You manually clicked on the Change Status button in the access tracker to force an RCoA but that failed too. What must you check to ensure that the RCoA will work? (Select two.)



A. RFC 3576 option is enabled for Aruba Controller under Network device in ClearPass.

B. RFC 3576 server should be mapped in the server group on the Aruba Controller

C. The RFC 3576 shared secret on ClearPass should match the Authentication Server shared secret

D. RFC 3576 server IPs and the Authentication server IPs should be same in the AAA profile

Correct Answer: AC