DUMPSQUEEN

Aruba Certified ClearPass Expert Written Exam

HP HPE6-A81

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

A customer has multiple Aruba Controllers integrated with ClearPass for guest access using a controller-initialed login method. The customer is aware that a public CA-signed captive portal certificate is required in Aruba controllers for controller-initiated workflows. The customer has purchased unique public CA-signed server certificates for each controller.

What configuration steps would you suggest to the customer to complete the deployment?

(Select three.)

A. From the weblogin/ self-registration page NAS Vendor settings, enable the check box for "The controller will send the IP to submit credentials" under Dynamic address.

B. Edit the HTML header in the weblogin/ self-registration register page with a script to match the controllers IP and captive portal certificate CN names respectively.

C. From the Aruba controller, enable the option "Add switch IP address in the redirection URL" under the respective L3 Authentication profile mapped in the initial role

D. From the Aruba controller, enable the option 'Add switch ip address in the redirection URL' under the respective guest AAA profile mapped in the VAP profile.

E. Add all the controller IP address and its certificate common names in the DNS server's Forward Lookup Zones and Reverse Lookup Zones to resolve queries from client.

F. From the weblogin/ self-registration page Login form settings, enable the check box for "The controller will send the IP to submit credentials" under Dynamic address.

ANSWER: A D F

QUESTION NO: 2

Refer to the exhibit.

Configuration > Services > Edit - HPE-Aruba Wired Mac auth

Services - HPE-Aruba Wired Mac auth

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Service:

Name:	HPE-Aruba Wired Mac auth
Description:	MAC-based Authentication Service
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	1. Authorization 2. Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	HPE-Aruba Switches

Authentication:

Authentication Methods:	[Allow All MAC AUTH]
Authentication Sources:	[Local User Repository]
Strip Username Rules:	-

Authorization:

Authorization Details:	[Endpoints Repository]

Roles:

Role Mapping Policy:	HS_Building Role Mapping Policy

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	HPE-ArubaOS Mac auth policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Switching - Bounce Switch Port]

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 | 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 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 - HPE-Aruba Wired Mac auth

Services - HPE-Aruba Wired Mac auth

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

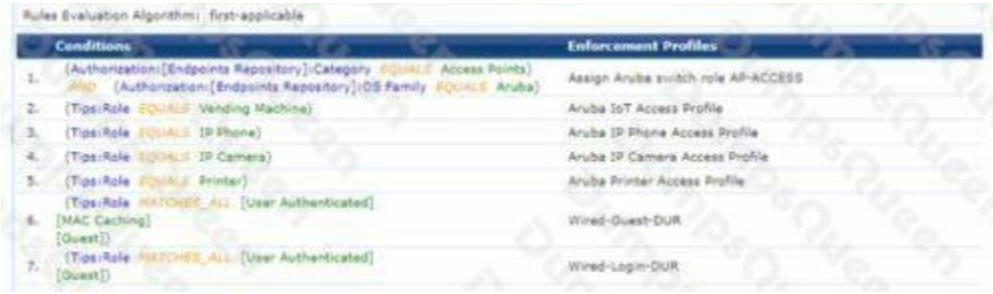
Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HPE-ArubaOS Mac auth policy | Modify | Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Category EQUALS Access Points) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Aruba)	Assign Aruba switch role AP-ACCESS



Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Category EQUALS Access Points) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Aruba)	Assign Aruba switch role AP-ACCESS
2.	(Tips:Role EQUALS Vending Machine)	Aruba IoT Access Profile
3.	(Tips:Role EQUALS IP Phone)	Aruba IP Phone Access Profile
4.	(Tips:Role EQUALS IP Camera)	Aruba IP Camera Access Profile
5.	(Tips:Role EQUALS Printer)	Aruba Printer Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [MAC Caching] [Guest])	Wired-Guest-DUR
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Guest])	Wired-Login-DUR

You configured the Wired MAC - Auth service enforcement conditions with the Endpoint profiling data When mac-auth based clients connect to the network, ClearPass assigns Deny access profile. The customer has sent you the above screenshots How would you resolve the issue?

A. Change the Rules evaluation algorithm in the Enforcement policy of HPE ArubaOS Mac auth policy as "select all matches" and add the CoA action as HPE Bounce switch port in the profiler tab.

B. Create a new condition in last position with Type and operator as Tips:Role EQUALS [User Authenticated] with action as Allow access profile permitting any services and any ports to do profiling.

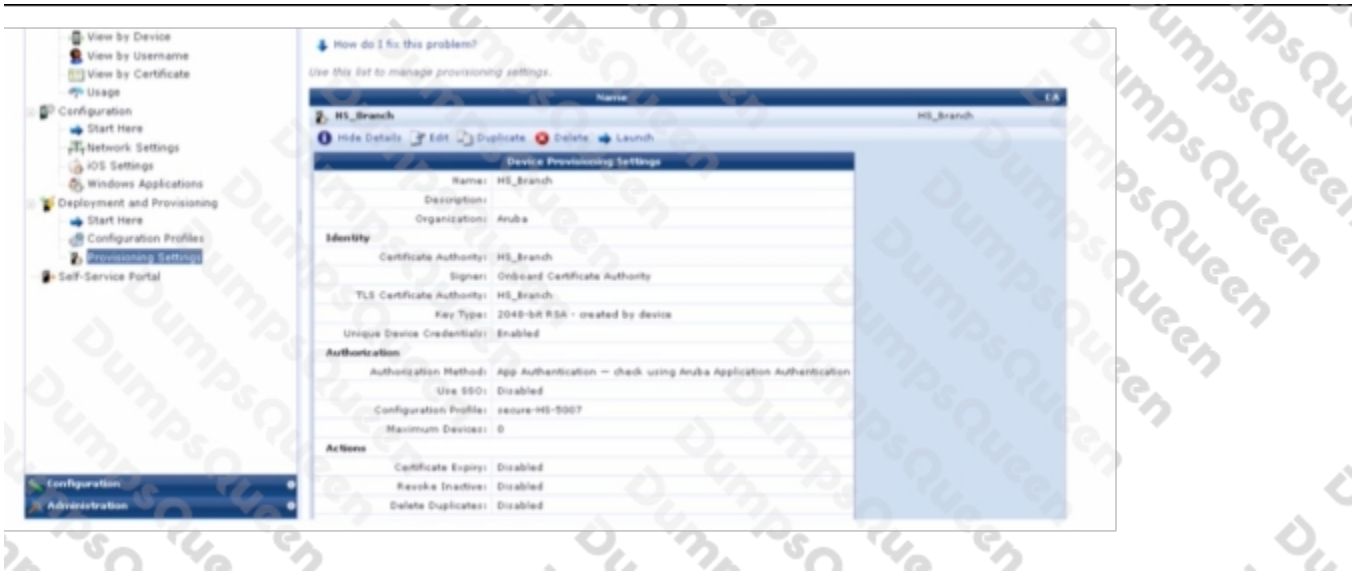
C. Create a new condition in first position with Type and operator as Authorization (Endpoint Repository]:Category NOT_EXISTS with action as Limited access profile allowing only DHCP service.

D. Create a new condition in the first position with Type and operator as Authorization [Endpoint Repository] Category NOT_EXISTS with action as Limited access profile and ArubaOS wireless terminate session

ANSWER: A

QUESTION NO: 3

Refer to the exhibit.



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. Install a public signed HTTPS web server certificate on the ClearPass server

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

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

ANSWER: B

QUESTION NO: 4

What is used to validate the EAP Certificate? (Select two.)

A. Key usage

B. Date

C. Server Identity

D. SAN entries

E. Common Name

ANSWER: A D

QUESTION NO: 5

A customer has a Clear Pass cluster deployment with four servers, two servers at the data center and two servers at a large remote site connected over an SO-WAN solution. The customer would like to implement OnGuard. Guest Self-Registration, and 802.1 X authentication across their entire environment. During testing the customer is complaining that users connecting to an Instant Cluster Employee S5ID 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 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 SO-WAN solution.

B. 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.

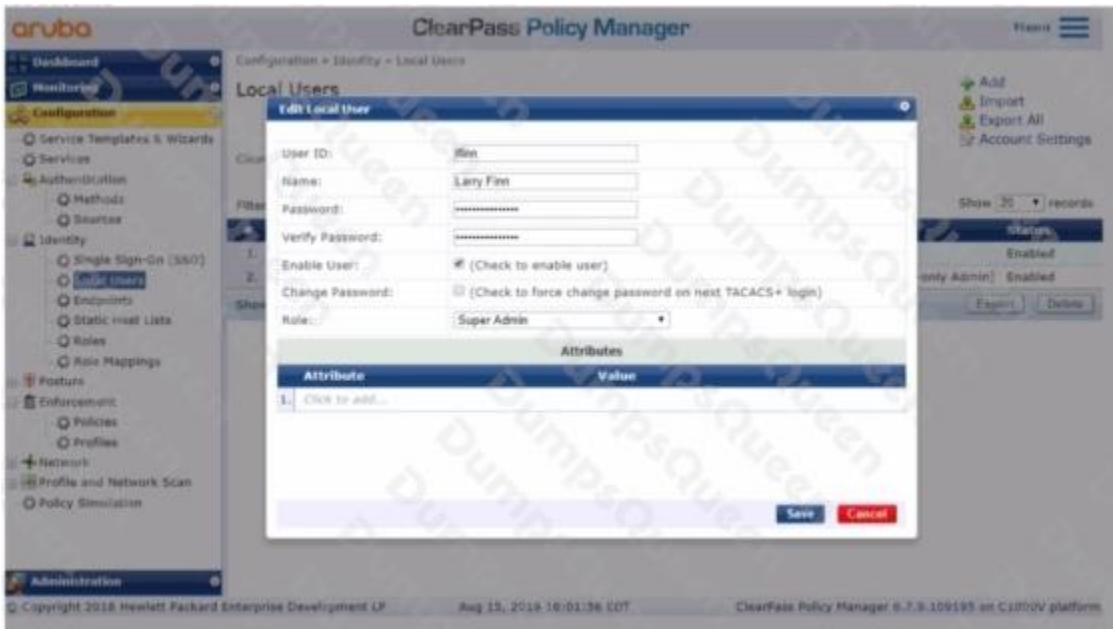
C. The Aruba-user-role received by the IAP is filtering the TCP port 6658 to the Clear Pass servers and after 10 seconds the SSL fallback gets activated and randomly generates the issue

D. The ClearPass Policy Manager zones have been defined but the local IP subnets have not but properly mapped to the zones and the OnGuard Agent might connect to any of the servers in the cluster.

ANSWER: A

QUESTION NO: 6

Refer to the exhibit.



The customer complains that the user shown cannot log into the ClearPess Server at an administrator using the [Policy Manager Admin Network Login Service]. What could be the reason for this?

A. The mapping on the role should be changed to [RADIUS Super Admin]

B. The user might be used for a TACACS authentication.

C. The account created does not fit this purpose.

D. The local user authentication might be disabled.

ANSWER: C

QUESTION NO: 7

A corporate Clear Pass Cluster with two servers located at a single site, has both

Management and Data port IP addresses configured. The Management port IPs art 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. Using the one Virtual IP can provide failover.

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

C. By using the Virtual IP, the failover wait time is faster than using individual server IPs.

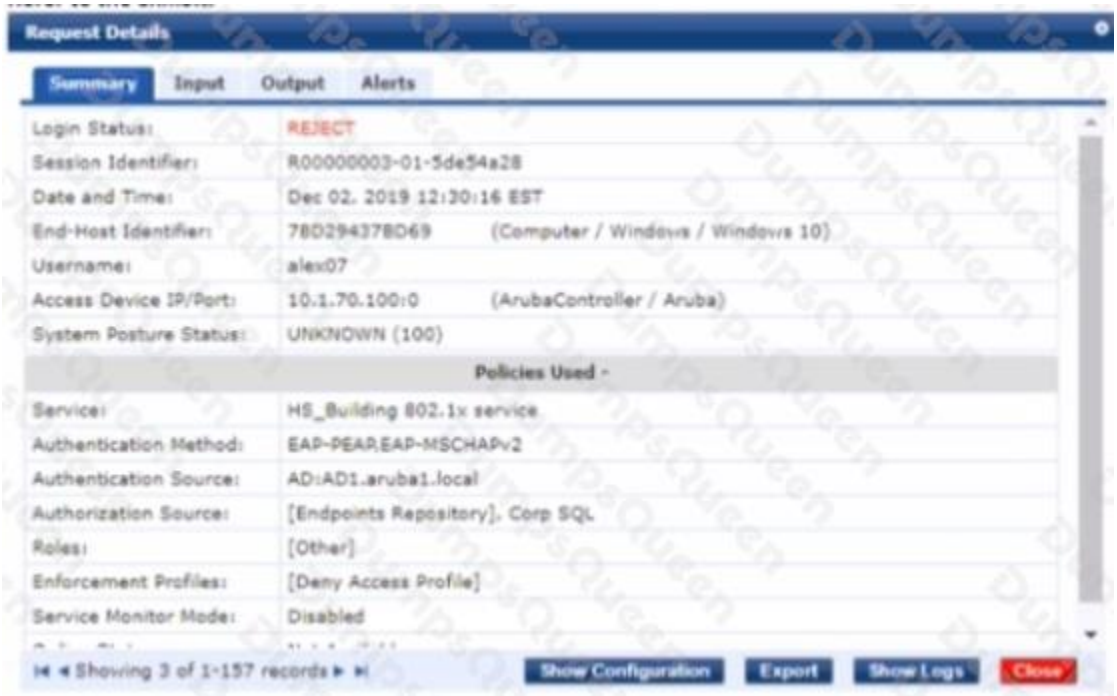
D. The failover can be accomplished only by using Virtual IP

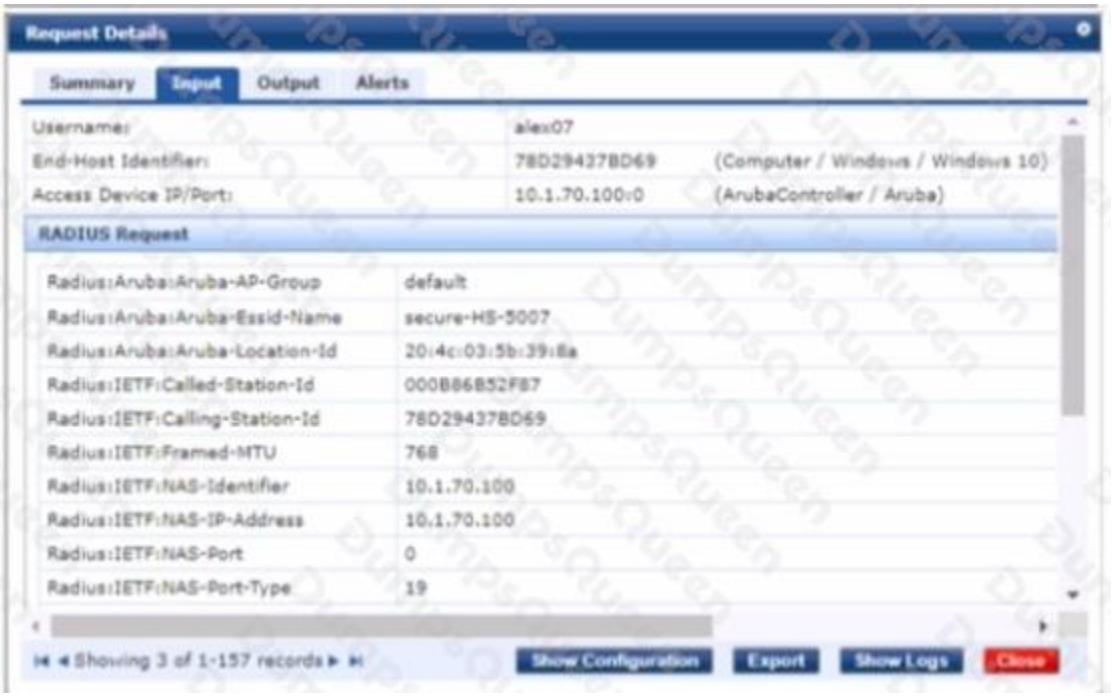
E. The Individual IPs can provide failover and load balancing.

ANSWER: A C

QUESTION NO: 8

Refer to the exhibit.




Request Details
Summary
Input
Output
Alerts
Username:
alex07
End-Host Identifier:
78D29437BD69
(Computer / Windows / Windows 10)
Access Device IP/Port:
10.1.70.100:0
(ArubaController / Aruba)
RADIUS Request
Radius:Aruba:Aruba-AP-Group
default
Radius:Aruba:Aruba-Essid-Name
secure-HS-5007
Radius:Aruba:Aruba-Location-Id
20:4c:03:5b:39:8a
Radius:IETF:Called-Station-Id
000B86B52F87
Radius:IETF:Calling-Station-Id
78D29437BD69
Radius:IETF:Framed-MTU
768
Radius:IETF:NAS-Identifier
10.1.70.100
Radius:IETF:NAS-IP-Address
10.1.70.100
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Showing 3 of 1-157 records
Show Configuration
Export
Show Logs
Close

The users connecting to a wireless SSIO "secure-HS-5007" were being processed by an incorrect 802.1 X service created for VIP access and the user gets deny access. The customer has sent you the screenshot to get your support to resolve the issue What changes will you suggest to fix it?

A. To the HS_Building 802.1 X service, add another service rule condition with VIP access Aruba-Essid-Name and leave it in same position

B. In the HS_Building 802.1X service, remove the service rule condition with Aruba controller location name and leave it in same position

C. Delete the HSBuilding 802 IX service, odd VIP access Aruba-Essid-Name as fourth condition to WSBuilding Aruba 802 1X service

D. In the HSBuilding 802. IXservice. change the Authentication method for AMCAuth for VIP access and leave it in same position

ANSWER: B

QUESTION NO: 9

You art deploying Cleat Pass Policy Manager with Guest functionality for a customer with multiple Aruba Networks Mobility Controllers. The customer wants to avoid SSL errors during guest access but due to company security policy cannot use a wildcard certificate on

ClearPass or the Controllers.

What is the most efficient way to configure the customer's guest solution? (Select two.)

A. Install the same public certificate on all Controllers with the common name "controller.{company domain)

B. Build multiple Web Login pages with vendor settings configured for each controller C. Build one Web Login page with vendor settings for captiveportal-controller (company domain)

C. Build one Web Login page with vendor settings for controller (company domain)

D. Install multiple public certificates with a different Common Name on each controller

ANSWER: C D

QUESTION NO: 10

Which statements are true about that integration between ClearPass Policy Manager and

ClearPass Device Insight? (Select two)

A. Policy Manager stops using ClearPass Profiler for fingerprinting and uses Device Insight Analyzer instead for endpoint in-depth data analysis.

B. ClearPass Device Insight updates ClearPass Policy Manager every 60 minutes if it detects a change in device classification like device spoofing.

C. To provide enhanced profiling and reporting. additional configuration is required to transmit data in both directions between CPPM and Device Insight.

D. When Device Insight integration mode is enabled. you can still use Update Fingerprint button to Update Endpoints at Configuration > Identity > Endpoints

E. An attribute named Device Insight Tags art added to the Endpoints that art available to use in service, role-mapping, and enforcement policy Rules

ANSWER: C D