

## HP.HPE6-A82.v2022-08-01.q54

|                                                                                                                               |                                          |
|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| □□□□:                                                                                                                         | HPE6-A82                                 |
| □□□□:                                                                                                                         | Aruba Certified ClearPass Associate Exam |
| □□□:                                                                                                                          | HP                                       |
| □□ □□ □□□:                                                                                                                    | 54                                       |
| □□:                                                                                                                           | v2022-08-01                              |
| # □□ □:                                                                                                                       | 964                                      |
| # □□ □□□:                                                                                                                     | 540                                      |
| <a href="https://www.krdump.com/HP.HPE6-A82.v2022-08-01.q54.html">https://www.krdump.com/HP.HPE6-A82.v2022-08-01.q54.html</a> |                                          |

### NEW QUESTION: 1

□□□□□ □□□□□□ □□□□□.

| Edit Endpoint   |                                                                                                                                |                  |                           |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------------|
| Fingerprints    | Endpoint                                                                                                                       | Attributes       |                           |
| MAC Address     | 18ee6952ee34                                                                                                                   | IP Address       | -                         |
| Description     |                                                                                                                                | Static IP        | FALSE                     |
| Status          | <input checked="" type="radio"/> Known client<br><input type="radio"/> Unknown client<br><input type="radio"/> Disabled client | Hostname         | faculty:iOS 11.3:PDA 25   |
| MAC Vendor      | Apple, Inc.                                                                                                                    | Device Category  | SmartDevice               |
| Added by        | clusteradmin                                                                                                                   | Device OS Family | Apple                     |
| Online Status   | Not Available                                                                                                                  | Device Name      | Apple iPad                |
| Connection Type | Unknown                                                                                                                        | Added At         | Feb 15, 2019 14:40:32 PST |
|                 |                                                                                                                                | Last Profiled At | Feb 15, 2019 14:40:32 PST |

□□□□□□ □□□ □□□ □□□□□□? (2□□ □□□□□.)

- A. Cisco □□ □□
- B. 3□ MDM
- C. DNS □□
- D. Exchange Plugging □□□□
- E. NAD ARP □□ □□□

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 2

□□□ □□□□□□□.

Note: This Service is created by Servi

Summary Service Authentication **Authorization** Roles Enforcement

Authorization Details:

Authorization sources from which role mapping attributes are fi

**Authentication Source**

1. [Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapp

[Time Source] [Local SQL DB] Remove  
 [Guest User Repository] [Local SQL DB] View Details  
 Modify

--Select to Add--

ClearPass [Time Source] ClearPass

- A. NTP(Network Time Protocol)
- B. ClearPass
- C.
- D. Insight Master ClearPass

Answer: (SHOW ANSWER)

NEW QUESTION: 3

Web Login (Guest Network)

Use this form to make changes to the Web Login **Guest Network**.

Web Login Editor

\* Name: Guest Network  
 Enter a name for this web login page.

Page Name: arubalogin  
 Enter a page name for this web login.  
 The web login will be accessible from "/guest/page\_name.php".

Description:   
 Comments or descriptive text about the web login.

\* Vendor Settings: Aruba Networks  
 Select a predefined group of settings suitable for standard network configurations.

Login Method: Controller-initiated — Guest browser performs HTTP form submit  
 Select how the user's network login will be handled.  
 Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

\* Address: securelogin.arubanetworks.com  
 Enter the IP address or hostname of the vendor's product here.

Secure Login: Use vendor default  
 Select a security option to apply to the web login process.

Dynamic Address:  The controller will send the IP to submit credentials  
 In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection.  
 The address shown will be used whenever the controller is not available or fails the authentication test.

- A. Aruba Central can be used to manage Aruba switches.
- B. Aruba Central can be used to manage Aruba access points.
- C. ClearPass can be used to manage Aruba switches.
- D. Aruba Central can be used to manage Aruba controllers.

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 4**

A customer with 985 employees would like to authenticate employees using a captive portal guest web login page. Employees should use their AD credentials to login on this page. Which statement is true?

- A. Employees must be taken to a separate web login page on the guest network.
- B. The customer needs to add the AD servers RADIUS certificate to the guest network.
- C. The customer needs to add the AD server as an authentication source in a guest service.
- D. The customer needs to add second guest service in the policy manager for the guest network.

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 5**

Which of the following is a valid MAC address?

- A. 00:00:00:00:00:00
- B. 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
- C. 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
- D. MAC address must be 12 hexadecimal digits.

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 6**

ClearPass can be used to manage Aruba switches, Aruba access points, Aruba controllers, NMAP, DHCP, and OnGuard. Which of the following is a valid MAC address?

- A. OnGuard can be used to manage Aruba switches.
- B. ClearPass can be used to manage Aruba access points.
- C. ClearPass can be used to manage Aruba controllers.
- D. NMAP can be used to manage Aruba switches.

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 7**

Which of the following is a valid MAC address?

- A. DHCP can be used to manage ClearPass.
- B. DHCP can be used to manage Aruba access points.
- C. ClearPass can be used to manage DHCP.
- D. DHCP can be used to manage ClearPass. ClearPass can be used to manage DHCP.

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 8**



## Web Login (Guest Network)

Use this form to make changes to the Web Login Guest Network.

**Web Login Editor**

\* Name:   
Enter a name for this web login page.

Page Name:   
Enter a page name for this web login.  
The web login will be accessible from "/guest/page\_name.php".

Description:   
Comments or descriptive text about the web login.

\* Vendor Settings:   
Select a predefined group of settings suitable for standard network configurations.

Login Method:   
Select how the user's network login will be handled.

\* Address:   
Enter the IP address or hostname of the vendor's product here.

Secure Login:   
Select a security option to apply to the web login process.

The controller will send the IP to submit credentials

Dynamic Address:  In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirecti

□□ □□ □□□ □□ □□ □□□ □□□□□ □□□ □□□□□□□□?

- A. □□□□ □□□ □□□□ □□ □□□□□.
- B. □□□□□ Aruba Central□□ □□□□□ □□ □□ □□□
- C. ClearPass□□ □□□□□ □□ □□ □□□
- D. Aruba □□□□□□ □□□□□ □□ □□ □□□

Answer: C (LEAVE A REPLY)

### NEW QUESTION: 12

Which option support DHCP profiling for devices in a network?

- A. enabling DHCP relay on our network access devices so DHCP requests are forwarded to ClearPass
- B. enabling the DHCP server to profile endpoints and forward meta-data to ClearPass
- C. DHCP profiling is enabled on ClearPass by default configuration of the network access devices is not necessary
- D. configuring ClearPass as a DHCP relay for the client

Answer: A (LEAVE A REPLY)

Reference:

<https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf>

### NEW QUESTION: 13

Active Directory□ □□ □□□ □□□□ 802.1x □□□□□ □□ □□ □□□ □□ □□□□ □□□?

- A. Active Directory □□□ □□ □□□ □□ □□□□□□ □□.
- B. Active Directory □□□ ClearPass □□□ □□ □ □□□□□ □□.
- C. Active Directory □□□ Aruba □□□□ □□□ □□□ Aruba □□□ □□□ □□□□□□ □□.
- D. □□ □□□ □□□□ □□ □□□ □□□ □□ □□□□□□ □□

Answer: (SHOW ANSWER)

**NEW QUESTION: 14**

ClearPass Cisco Device Sensor □□□ □□ □□□□ □□ □□ □□? (2□□ □□□□□.)

- A. □□ □ DTLS(Datagram Transport Layer Security) □□□□ □□□□ DHCP □ HTTP □□□ □□□□ □□□ ClearPass□ □□□ □□.
- B. CDP(Cisco Discovery Protocol) □ LLDP(Link Layer Discovery Protocol)□□ □□ □□□□□ □□□ □□
- C. Aruo□ □□□ □□ AP□ □□□□□ □□□ □□□□ Cisco □□□ □□□□ □□□□ □□□. □□ □□ !□ □□□ □□□□□.
- D. □□□ □□□□ NAD(Network Access Device)□ Cisco Smart Net □□□□□ □□□□ □□□.
- E. RADIUS □□ □□□ □□□□ DHCP □ HTTP □□□ □□□□ □□□ ClearPass□ □□

**Answer: B,D (LEAVE A REPLY)**

**NEW QUESTION: 15**

□□□ 345□□ □□□ □□□□ □□ WLAN□ □□□□□ □□ □□□ □□□ □□□□ □□□ □□□. □□□ □□□□ □□ □□□ □ □□□□ □□ □□□□□ □□ □□□ □□□□. □□□ □□ □□□ □□□□ □□ □□ ClearPass □□□ □□□ □ □□□□□?

- A. □□□□□ □□□□□ □□ □□
- B. □□□ □□□ □□ □□□ □□□ □□
- C. ClearPass □□□ □□
- D. MAC □□□ □□ □□□ □□□

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 16**

OnGuard□ □□ □□□□ □□ □□? (2□□ □□□□□.)

- A. 802 1X □□□ □□
- B. Doth Windows □ Mac OS X □□□□□□ □□□□□.
- C. □□□□/□□□□□ □□□□ □□□□ □ □□□□□.
- D. Antivirus/Antispyware □□□□□ □□□□ □□□ □□□□ □□ □□□□□.

**Answer: B,D (LEAVE A REPLY)**

**HPE6-A82** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ HPE6-A82 □□! DumpTop □ □□ **HPE6-A82** □□ □□ □ □□□□□□, DumpTop HPE6-A82 □□ □□□ □□□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ □□□□□□□□ □□□ □□□□□. <https://www.dumptop.com/HP/HPE6-A82-dump.html> (61 Q&As Dumps, **30%OFF Special Discount: KrDump**)

**NEW QUESTION: 17**

□□□ □□□□□.



## Web Login (Guest Network)

Use this form to make changes to the Web Login Guest Network.

### Web Login Editor

\* Name:   
Enter a name for this web login page.

Page Name:   
Enter a page name for this web login.  
The web login will be accessible from "/guest/page\_name.php".

Description:   
Comments or descriptive text about the web login.

\* Vendor Settings:   
Select a predefined group of settings suitable for standard network configurations.

Login Method:   
Select how the user's network login will be handled.

\* Address:   
Enter the IP address or hostname of the vendor's product here.

Secure Login:   
Select a security option to apply to the web login process.

The controller will send the IP to submit credentials

Dynamic Address:   
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirecti

Where will the guests browser be redirected during a captive portal login attempt?

- A. The captive portal page hosted on ClearPass
- B. The captive portal page hosted on Aruba Central in the cloud
- C. The redirect will time out and fan to resolve
- D. The captive portal page hosted on the Aruba controller

Answer: (SHOW ANSWER)

### NEW QUESTION: 20

□□ □□□ "□□ □□ □□ □□" □□ □□ □□□□□ □□ □□□□ □□□□ □□ □□□□□?

- A. □ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ Enforcement □□□□ □□ Enforcement □□□□ □□ □□□□ □□.
- B. □ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ Enforcement □□□□ □□□□ □□ □□□ □□□□□.
- C. □□ □□□ □□□□□. □□□□ □□□ □□□ □□ □□□□ □□□□ □□□□.
- D. □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)

### NEW QUESTION: 21

□□□ □□□□□.

| Summary                                                                                                | Service                                                                                                                                                                                                             | Authentication   | Roles      | Enforcement            |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------|------------------------|
| Type:                                                                                                  | Aruba 802.1X Wireless                                                                                                                                                                                               |                  |            |                        |
| Name:                                                                                                  | Test_Service                                                                                                                                                                                                        |                  |            |                        |
| Description:                                                                                           | Aruba 802.1X Wireless Access Service                                                                                                                                                                                |                  |            |                        |
| Monitor Mode:                                                                                          | <input type="checkbox"/> Enable to monitor network access without enforcement                                                                                                                                       |                  |            |                        |
| More Options:                                                                                          | <input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts<br><input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy |                  |            |                        |
| <b>Service Rule</b>                                                                                    |                                                                                                                                                                                                                     |                  |            |                        |
| Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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 |
| 3.                                                                                                     | Radius:Aruba                                                                                                                                                                                                        | Aruba-Essid-Name | EXISTS     |                        |
| 4.                                                                                                     | Radius:Aruba                                                                                                                                                                                                        | Aruba-Essid-Name | EQUALS     | CORP                   |
| 5.                                                                                                     | Click to add...                                                                                                                                                                                                     |                  |            |                        |

Which of the following SSIDs will be allowed to connect to the wireless network?

- A. CORP-CORP-CORP-CORP-CORP-CORP-CORP-CORP
- B. "CORP" SSID
- C. SSID "CORP" Aruba IAP
- D. Aruba SSID

Answer: [\(SHOW ANSWER\)](#)

### NEW QUESTION: 22

Refer to the exhibit.

## Service One

| Service Rule                                                                                           |               |            |                                                        |  |
|--------------------------------------------------------------------------------------------------------|---------------|------------|--------------------------------------------------------|--|
| Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions: |               |            |                                                        |  |
| Type                                                                                                   | Name          | Operator   | Value                                                  |  |
| 1. Radius:IETF                                                                                         | NAS-Port-Type | EQUALS     | Ethernet (15)                                          |  |
| 2. Radius:IETF                                                                                         | Service-Type  | BELONGS_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |  |
| 3. Connection                                                                                          | SSID          | EQUALS     | Secure-Corporate                                       |  |

## Service Two

| Service Rule                                                                                           |               |            |                                                        |  |
|--------------------------------------------------------------------------------------------------------|---------------|------------|--------------------------------------------------------|--|
| Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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. Connection                                                                                          | SSID          | EQUALS     | secure-corporate                                       |  |

## Service Three

| Service Rule                                                                                           |                    |            |                                                        |  |
|--------------------------------------------------------------------------------------------------------|--------------------|------------|--------------------------------------------------------|--|
| Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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. Connection                                                                                          | Client-Mac-Address | NOT_EQUALS | %{Radius:IETF:User-Name}                               |  |

Which of the following is a valid configuration for Service One on an Aruba Access Point? (Select three.)

- A. Service-Type: Login-User
- B. Service-Type: Framed-User
- C. SSID: Secure-Corporate
- D. SSID: secure-corporate

Answer: C (LEAVE A REPLY)

### NEW QUESTION: 23

Which of the following is a valid configuration for Service Two on an Aruba Access Point? (Select three.)

Active Collectors

ClearPass Applications

Network Functions

Network Packets

Answer Area

| Collector Type | Profiling Collector |
|----------------|---------------------|
|                | DHCP                |
|                | Controller IF-MAP   |
|                | Cisco Device Sensor |
|                | TCP Fingerprinting  |
|                | OnGuard             |
|                | NMAP                |
|                | SNMP                |

Answer:

Active Collectors

ClearPass Applications

Network Functions

Network Packets

Answer Area

| Collector Type         | Profiling Collector |
|------------------------|---------------------|
| Network Functions      | DHCP                |
| Network Functions      | Controller IF-MAP   |
| Network Functions      | Cisco Device Sensor |
| Network Packets        | TCP Fingerprinting  |
| ClearPass Applications | OnGuard             |
| Active Collectors      | NMAP                |
| ClearPass Applications | SNMP                |

**NEW QUESTION: 24**

Which of the following is a feature of Aruba ClearPass?

- A. ClearPass provides a centralized location for user authentication and authorization.
- B. ClearPass provides a centralized location for user authentication and authorization.
- C. MDM(Mobile Device Manager) is a feature of ClearPass.
- D. ClearPass provides a centralized location for user authentication and authorization.

Answer: (SHOW ANSWER)

**NEW QUESTION: 25**

Which of the following is a feature of Aruba ClearPass? (3 correct answers)

- A. ClearPass provides a centralized location for user authentication and authorization.
- B. ClearPass provides a centralized location for user authentication and authorization.
- C. ClearPass provides a centralized location for user authentication and authorization.
- D. ClearPass provides a centralized location for user authentication and authorization.

E. □□ □□

Answer: A,D,E ([LEAVE A REPLY](#))

**NEW QUESTION: 26**

□□□□ □□ □□□□ □□□ □□ □□□ □□□□□□. □□□ □□□□□ □□ □□□ □ □□□ □□□□ □□ □□□ □□□□□  
□□□ □ □□ □□□ □□□□□? (2□ □□)

- A. ClearPass Policy Manager □□□□ SMTP(Simple Man Transport Protocol) □□ □□
- B. ClearPass □□□ □□□□ SMS(Short Message Service) □□□□□□ □□□□□.
- C. ClearPass □□□ □□□□ SMTP(Simple Mail Transport Protocol) □□□ □□□□□.
- D. ClearPass Policy Manager □□□□ SMS(Short Message Service) □□□□□□ □□□□□.
- E. □□□□ SMTP(Simple Mali Transport Protocol) □□□□ □□□□□ □□ □□ □□□□ □□□□□.

Answer: B,D ([LEAVE A REPLY](#))

**NEW QUESTION: 27**

□□ □□ □□□ □□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□□?

- A. □□□□ □ □□ □□ □□□□ □□□□ □□□ □□□ □□□□.
- B. □□ □□□ □□ □□□□ □□□ □□ □□□□□ □□□ □ □□□□.
- C. □□ □□□ □□ □□□□□□ □□ □□□□ □□□□□.
- D. □□□ □□ □□□□ □□ □□□□□ □ □□□ □□□ □□□□□.

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 28**

□□□ □□□□ □□ □□□□ □□ ClearPass□□ □□□ □□ □□ □□□□ □□□ □□ □□□□□. □□□ □□□ □□'□ □□□  
□ □□ □□□ □□□□□? (2□ □□)

- A. □□ □□ □□□□ □□ □□ □□□ □□□ □ □□□□.
- B. □□ □□ □□ □□□ □□□□ □□□□ □□□ □ □□ □□ □□□ □□ □□□ □ □□□□.
- C. □□□ □□□□ □□□ □□□ □□□ □□□ □□□ □ □□□□.
- D. □□ □□ □□□ □□ □□□□□ □□□□ □ □□□□.
- E. □ □□□ □□□ □□□ □□ □□□ □□□ □□□□□ □□ □□ □□□□□ □□□□□.

Answer: A,C ([LEAVE A REPLY](#))

**NEW QUESTION: 29**

□□ □□□□ □ □□□□□ □□ □□□ □□□□□ ClearPass □□□ □□□□□?

- A. □□□
- B. □□ □□
- C. □□
- D. □□□□□

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 30**

Refer to the exhibit.



- A. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- B. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- C. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- D. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 34**

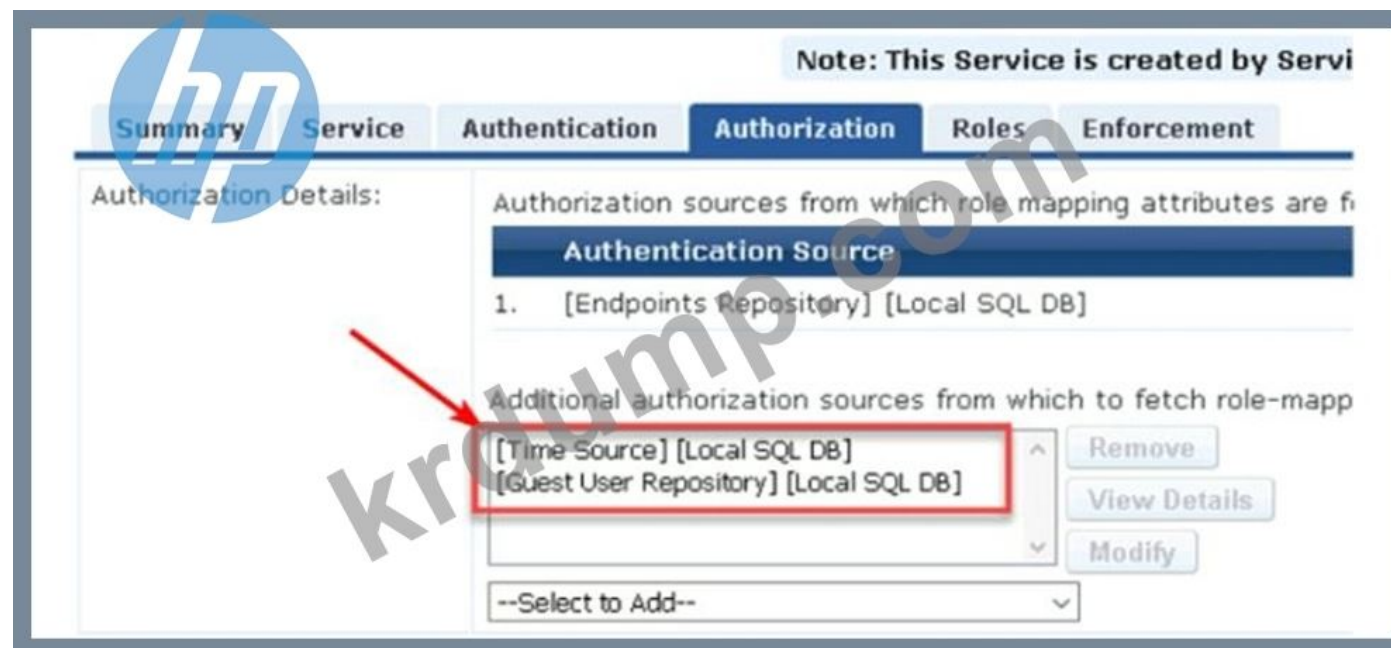
802.1X authentication and DHCP fingerprinting are both Layer-3 functions. Which of the following is true?

- A. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- B. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- C. Because DHCP fingerprinting is a Layer-3 function, it cannot be used with an 802.1X authentication service.
- D. The client needs to connect to an open network first to be profiled, then shifted to the secure 802.1x network.

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 35**

ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.



ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.

- A. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- B. Insight Master can integrate with TACACS+ and RADIUS. Insight Master can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- C. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.
- D. ClearPass can integrate with TACACS+ and RADIUS. ClearPass can also integrate with NAD/NAS (Network Attached Device/Network Attached Server) and Dynamic Segmentation.

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 36**

A customer is setting up Guest access with ClearPass. They are considering using 802.1X for both the Employee network and the Guest network. What are two issues the customer may encounter when deploying 802.1X with the Guest network? (Select two)

- A. the lack of encryption during the authentication process
- B. Guests will not be able to be uniquely identified.
- C. difficult to maintain in an environment with a large number of transient guest users
- D. ClearPass will not be able to enforce individual Access Control policies.
- E. the high level of complexity for users to join the guest network

Answer: (SHOW ANSWER)

**NEW QUESTION: 37**

Which two ClearPass policies can be used to enforce MAC-based authentication? (Select two)

- A. ClearPass Policy Engine
- B. ClearPass Policy Manager
- C. ClearPass Policy Server
- D. ClearPass Policy System

Answer: D (LEAVE A REPLY)

00/00:

**NEW QUESTION: 38**

Which two ClearPass policies can be used to enforce MAC-based authentication? (Select two)

- A. ClearPass Policy Engine
- B. ClearPass Policy Manager
- C. ClearPass Policy Server
- D. ClearPass Policy System
- E. ClearPass Policy System

Answer: B,E (LEAVE A REPLY)

**NEW QUESTION: 39**

RADIUS CoA (CoA) can be used to...

- A. ClearPass NAD/NAS (Network Attached Device/Network Attached Server) can be used to...
- B. ClearPass TACACS+ can be used to...
- C. ClearPass Dynamic Segmentation can be used to...
- D. ClearPass can be used to...

Answer: (SHOW ANSWER)

00:

[http://www.arubanetworks.com/techdocs/ClearPass/Aruba\\_CPPMOnlineHelp/Content/CPMM\\_UserGuide/Enforce/EPRADIUS\\_CoA.htm](http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPMM_UserGuide/Enforce/EPRADIUS_CoA.htm)

**NEW QUESTION: 40**

Which DHCP option is used to support ClearPass?

- A. DHCP option 43 ClearPass
- B. DHCP option 43 ClearPass
- C. DHCP option 43 ClearPass
- D. DHCP option 43 ClearPass

Answer: B (LEAVE A REPLY)

#### NEW QUESTION: 41

Which MAC address is used to identify a device?

- A. MAC address
- B. MAC address
- C. MAC address
- D. MAC address

Answer: D (LEAVE A REPLY)

0/0:

[https://www.arubanetworks.com/techdocs/Instant\\_83\\_WebHelp/Content/Instant\\_UG/Authentication/AuthenticationMethods.htm](https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/Instant_UG/Authentication/AuthenticationMethods.htm)

#### NEW QUESTION: 42

Which of the following is a security risk?

- A. Profiling
- B. Posturing
- C. Profiling
- D. Posturing

Answer: C (LEAVE A REPLY)

#### NEW QUESTION: 43

What are "Known" endpoints in ClearPass?

- A. The label "Known" indicates rogue endpoints labeled as "friendly" or "ignore"
- B. "Known" endpoints can be authenticated based on MAC address to bypass the captive portal login.
- C. These are endpoints whose beacons have been detected but have never completed authentication
- D. "Known" endpoints have been fingerprinted to determine their operating system and manufacturer.

Answer: B (LEAVE A REPLY)

#### NEW QUESTION: 44

Refer to the exhibit.

# ClearPass Policy Manager

Configuration » Authentication » Sources » Add - Remote Lab AD

## Authentication Sources - Remote Lab AD

| Summary                  | General                                                                                                                                                                                                                                                                                                                                                                                                       | Primary | Attributes | Backup 1 | Backup 2 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------------|----------|----------|
| Name:                    | Remote Lab AD                                                                                                                                                                                                                                                                                                                                                                                                 |         |            |          |          |
| Description:             |                                                                                                                                                                                                                                                                                                                                                                                                               |         |            |          |          |
| Type:                    | Active Directory                                                                                                                                                                                                                                                                                                                                                                                              |         |            |          |          |
| Use for Authorization:   | <input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes                                                                                                                                                                                                                                                                                            |         |            |          |          |
| Authorization Sources:   | <div style="border: 1px solid gray; padding: 2px;"><div style="display: flex; justify-content: space-between;"><span>Remove</span><span>View Details</span></div><div style="border: 1px solid gray; height: 20px; margin: 2px;"></div><div style="display: flex; justify-content: space-between;"><span>-- Select --</span><span>▼</span></div></div>                                                        |         |            |          |          |
| Server Timeout:          | 10 seconds                                                                                                                                                                                                                                                                                                                                                                                                    |         |            |          |          |
| Cache Timeout:           | 36000 seconds                                                                                                                                                                                                                                                                                                                                                                                                 |         |            |          |          |
| Backup Servers Priority: | <div style="border: 1px solid gray; padding: 2px;"><div style="display: flex; justify-content: space-between;"><span>Backup 1</span><span>Move Up ↑</span></div><div style="display: flex; justify-content: space-between;"><span>Backup 2</span><span>Move Down ↓</span></div></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Add Backup</span> <span>Remove</span></div> |         |            |          |          |

Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds. Backup servers are Backup 1 and Backup 2.

- A. ClearPass Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds.
- B. ClearPass Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds.
- C. ClearPass Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds.
- D. ClearPass Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds. Backup servers are Backup 1 and Backup 2.

Answer: [\(SHOW ANSWER\)](#)

### NEW QUESTION: 45

Active Directory is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds.

- A. ClearPass Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds.
- B. Cache Timeout is 36000 seconds for ClearPass A/D Active Directory source.
- C. Cache Timeout is 36000 seconds for ClearPass A/D Active Directory source.
- D. ClearPass Remote Lab AD is a Windows Active Directory source. It is used for authentication and authorization. The server timeout is 10 seconds and the cache timeout is 36000 seconds.

Answer: C ([LEAVE A REPLY](#))

□□

<https://community.arubanetworks.com/blogs/arunkumar1/2020/10/20/what-is-the-difference-between-authentication-cache-timeout-and-machine-authentication-cache-timeout>

#### NEW QUESTION: 46

ClearPass OnGuard□□ □□□ □□□ □□□ □□□□□? (2□ □□)

A. □□□□ □□□□ □□ □□□□ □□□□□.

B. □□ □□ □□□□□ □□□□□.

C. Client□ Health Status□ □□□□□.

D. □□□ □□□□ □□ □□□□□□ □□□□□.

E. □□□ □□□□□□ □□ □□□ □□

Answer: A,C ([LEAVE A REPLY](#))

**HPE6-A82** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ HPE6-A82 □□! DumpTop □ □□ **HPE6-A82** □□ □□ □□□□□□□, DumpTop HPE6-A82 □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ □□□□□□□□□□□□. <https://www.dumptop.com/HP/HPE6-A82-dump.html> (61 Q&As Dumps, **30%OFF Special Discount: KrDump**)

#### NEW QUESTION: 47

An organization wants to have guests connect their own personal devices to the wireless network without requiring a receptionist setting up a guest account. Which ClearPass feature can be used to meet the organization's requirements?

A. Policy Manager Enforcement

B. MAC authentication with profiling

C. ClearPass Onboard

D. □□□ □□□ □□□

Answer: D ([LEAVE A REPLY](#))

#### NEW QUESTION: 48

Match the ClearPass system description to the best term Options are used only once.

| Term                     | Description                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------|
| ClearPass Insight        | can provide posturing to validate the security status of devices on your wired, wireless and VPN networks |
| ClearPass Onboard        | provides an intuitive way to securely assign an individual client certificate to each device              |
| ClearPass OnGuard        | gathers endpoint context from passively received data to fingerprint devices                              |
| ClearPass Policy Manager | has the ability to integrate with external systems through APIs or HTTP/REST calls                        |
| ClearPass Profiler       | provides multiple customizable reports and in-depth information about each of the other modules           |

Answer:

| Term                     | Description                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------|
| ClearPass Insight        | can provide posturing to validate the security status of devices on your wired, wireless and VPN networks |
| ClearPass Onboard        | provides an intuitive way to securely assign an individual client certificate to each device              |
| ClearPass OnGuard        | gathers endpoint context from passively received data to fingerprint devices                              |
| ClearPass Policy Manager | has the ability to integrate with external systems through APIs or HTTP/REST calls                        |
| ClearPass Profiler       | provides multiple customizable reports and in-depth information about each of the other modules           |

### NEW QUESTION: 49

□□□ □□□□□.

web Login (Guest network)

Use this form to make changes to the Web Login Guest Network.

**Web Login Editor**

**\* Name:**   
Enter a name for this web login page.

**Page Name:**   
Enter a page name for this web login.  
The web login will be accessible from "/guest/page\_name.php".

**Description:**   
Comments or descriptive text about the web login.

**\* Vendor Settings:**   
Select a predefined group of settings suitable for standard network configurations.

**Login Method:**   
Select how the user's network login will be handled.  
Controller-initiated: The user's browser is redirected to the vendor's login page, usually from the captive portal redirection process.

**\* Address:**   
Enter the IP address or hostname of the vendor's product here.

**Secure Login:**   
Select a security option to apply to the web login process.

**Dynamic Address:**  The controller will send the IP to submit credentials  
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

□□ □□ □□□ □□ □□ □□□□ □□□□□ □□□ □□□□□□□□?

- A. Aruba □□□□□□ □□□□□□ □□ □□ □□□□
- B. □□□□ □□□ □□□□ □□ □□□□□□.
- C. ClearPass□□ □□□□□□ □□□□ □□ □□□□
- D. □□□□□ Aruba Central□□ □□□□□□ □□ □□ □□□□

Answer: (SHOW ANSWER)

### NEW QUESTION: 50

Match the ClearPass system description to the best term Options are used only once.

| Term                     | Description                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------|
| ClearPass Insight        | can provide posturing to validate the security status of devices on your wired, wireless and VPN networks |
| ClearPass Onboard        | provides an intuitive way to securely assign an individual client certificate to each device              |
| ClearPass OnGuard        | gathers endpoint context from passively received data to fingerprint devices                              |
| ClearPass Policy Manager | has the ability to integrate with external systems through APIs or HTTP/REST calls                        |
| ClearPass Profiler       | provides multiple customizable reports and in-depth information about each of the other modules           |

**Answer:**

| Term                     | Description                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------|
| ClearPass Onboard        | can provide posturing to validate the security status of devices on your wired, wireless and VPN networks |
| ClearPass Policy Manager | provides an intuitive way to securely assign an individual client certificate to each device              |
| ClearPass OnGuard        | gathers endpoint context from passively received data to fingerprint devices                              |
| ClearPass Profiler       | has the ability to integrate with external systems through APIs or HTTP/REST calls                        |
| ClearPass Insight        | provides multiple customizable reports and in-depth information about each of the other modules           |

### Description

|                          |                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------|
| ClearPass Onboard        | can provide posturing to validate the security status of devices on your wired, wireless and VPN networks |
| ClearPass Policy Manager | provides an intuitive way to securely assign an individual client certificate to each device              |
| ClearPass OnGuard        | gathers endpoint context from passively received data to fingerprint devices                              |
| ClearPass Profiler       | has the ability to integrate with external systems through APIs or HTTP/REST calls                        |
| ClearPass Insight        | provides multiple customizable reports and in-depth information about each of the other modules           |

### NEW QUESTION: 51

Refer to the Endpoint in the screenshot.



- A. Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.
- B. Profiling describes categorizing the user based on their department while Posturing validates the user as authenticated.
- C. Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.
- D. Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 54**

Which of the following is a valid ClearPass role assignment? (Select two)

- A. Posturing
- B. Profiling
- C. MAC(Media Access Control)
- D. ClearPass

Answer: D ([LEAVE A REPLY](#))

**HPE6-A82** DumpTop HPE6-A82! DumpTop HPE6-A82  
 DumpTop HPE6-A82, DumpTop HPE6-A82  
 DumpTop HPE6-A82. <https://www.dumptop.com/HP/HPE6-A82-dump.html> (61 Q&As Dumps, **30%OFF Special Discount: KrDump**)