

HP.HPE6-A82.v2022-04-11.q54

□□□□:	HPE6-A82
□□□□:	Aruba Certified ClearPass Associate Exam
□□□:	HP
□□ □□ □□□:	54
□□:	v2022-04-11
# □□ □:	2037
# □□ □□□:	540
https://www.krdump.com/HP.HPE6-A82.v2022-04-11.q54.html	

NEW QUESTION: 1

RADIUS □□ □□(CoA)□□ □□□□□?

- A. ClearPass □ Dynamic Segmentation □ □□ □□□□ □□□□ □□□ UBT(User-Based Tunnel) □ □□□ □ □□□ □□ □□□ □□□□.
- B. □□□□□□ TACACS+ □ □□□□ □□ RADIUS □ □□□□ ClearPass □ □□ □□ □□□ □□□ □ □□□□.
- C. □□ □□□□ □□□□□ □□□□ □□□ □□□□ □□ □ □□□□□□ □□□ □□□□□□.
- D. ClearPass □ NAD/NAS(Network Attached Device/Network Attached Server) □ □□□□ □□□□ □□□□ □□ □□□ □□□ □ □□□ □□□.

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

NEW QUESTION: 2

ClearPass □□ □□□ □□□ □□□ □□□□□?)

- A. OnGuard □ □□ □□□□ Posture □□□ □□□□□.
- B. □□□□□□ □□ □□ □□ □□
- C. □□□□□ □□□□ Enforcement Profile □□
- D. □□□ □□□ □□□ □□

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

NEW QUESTION: 3

□□□ □□□□□.



Which of the following is a valid condition for a service rule?

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 4

ClearPass Insight can provide posture to validate the security status of devices on your wired, wireless and VPN networks.

Term	Description
ClearPass Insight	can provide posture 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 posture 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: 5

ClearPass can integrate with Cisco Device Sensor via CDP, LLDP, or DTLS. Which of the following is a valid condition for a service rule?

- A. Aruba is SSID
- B. CDP(Cisco Discovery Protocol) is LLDP(Link Layer Discovery Protocol)
- C. DTLS(Datagram Transport Layer Security) is DHCP or HTTP
- D. NAD(Network Access Device) is Cisco Smart Net
- E. RADIUS is DHCP or HTTP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 9

□□□□ □□ □□□ □□□□

□□ □□□ □□ □□□ □□□ □□□□□□. □□□ □ □□ □□□□□□.

Term	Description
Accounting	used to match a credential that is being submitted to an account representing the client
Authentication	applying access decisions based on attributes attached to the user's account
Client	the owner of an endpoint that is providing credentials
Authorization	the device which consumes networks resources
User	gathering the start and stop times of network access and ongoing health checks of an endpoint

Answer:

Term	Description	
Accounting	Authentication	used to match a credential that is being submitted to an account representing the client
Authentication	Authorization	applying access decisions based on attributes attached to the user's account
Client	User	the owner of an endpoint that is providing credentials
Authorization	Client	the device which consumes networks resources
User	Accounting	gathering the start and stop times of network access and ongoing health checks of an endpoint

NEW QUESTION: 10

□□□ □□□□ □□ □□□□ □□ ClearPass□□ □□□ □□ □□ □□□□ □□□ □□ □□□□□□.

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 11

□□□ □□□□□.

Enforcement Policies - Corp SSID Access

Summary Enforcement Rules

Enforcement:
 Name: Corp SSID Access
 Description:
 Enforcement Type: RADIUS
 Default Profile: Allow Internet Only Access

Rules:
 Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Tips:Role EQUALS employee)	Allow Full Access
2. (Tips:Role EQUALS [Contractor])	Corp Secure Contractor
3. (Tips:Role EQUALS Corp BYOD)	Secure Corp BYOD Access

Configurations = Identity + Local Users

Filter: Role contains employee [Go] [Clear Filter]

#	User ID	Name	Role
1.	john	john	[Employee]
2.	mike	mike	[Employee]
3.	neil	neil	[Employee]

Showing 1-3 of 3

Exhibit:ACCA82-345

Which user is not associated with the "neil" role?

- A. John
- B. Corp BYOD
- C. Corp
- D. Mike

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

NEW QUESTION: 12

Which user is not associated with the "neil" role?

Which user is not associated with the "neil" role?

- A. John
- B. Corp BYOD
- C. Corp
- D. Mike

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

NEW QUESTION: 13

Which user is not associated with the "neil" role?

Which user is not associated with the "neil" role?

Term	Description
Accounting	used to match a credential that is being submitted to an account representing the client
Authentication	applying access decisions based on attributes attached to the user's account
Client	the owner of an endpoint that is providing credentials
Authorization	the device which consumes networks resources
User	gathering the start and stop times of network access and ongoing health checks of an endpoint

Answer:

Term	Description
Authentication	used to match a credential that is being submitted to an account representing the client
Authorization	applying access decisions based on attributes attached to the user's account
User	the owner of an endpoint that is providing credentials
Client	the device which consumes networks resources
Accounting	gathering the start and stop times of network access and ongoing health checks of an endpoint

Description

Authentication	used to match a credential that is being submitted to an account representing the client
Authorization	applying access decisions based on attributes attached to the user's account
User	the owner of an endpoint that is providing credentials
Client	the device which consumes networks resources
Accounting	gathering the start and stop times of network access and ongoing health checks of an endpoint

NEW QUESTION: 14

□□□□ □□ □□□ □□ □□□ □□ □□□ □□□□□□.

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

(2□□ □□□□□.)

A. ClearPass Policy Manager □□□□ SMTP(Simple Mail Transport Protocol) □□□ □□□□□.

B. ClearPass □□□ □□□□ SMTP(Simple Mail Transport Protocol) □□□ □□□□□.

C. ClearPass Policy Manager □□□□ SMS(Short Message Service) □□□□□□ □□□□□.

D. ClearPass □□□ □□□□ SMS(Short Message Service) □□□□□□ □□□□□.

E. □□□□ SMTP(Simple Mail Transport Protocol) □□□ □□□□□ □□ □□ □□□□ □□□□□.

Answer: A,E (LEAVE A REPLY)

□□/□□: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Guest/PDFs/Guest_User_Guide.pdf

NEW QUESTION: 15

□□□ □□□□□.

For Login (Guest Network)

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

Web Login Editor	
* Name:	Guest Network <small>Enter a name for this web login page.</small>
Page Name:	arubalogin <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	 <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	Aruba Networks <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated — Guest browser performs HTTP form submit <small>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.</small>
* Address:	securelogin.arubanetworks.com <small>Enter the IP address or hostname of the vendor's product here.</small>
Secure Login:	Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. This address should only be used whenever the controller is not available or fails the requirements below.</small>

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 16

MAC □□ □□□ □□□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□?

(2□□ □□□□□.)

- A. □□□□□□□ MAC-Auth □□ □□ □□ □□□□ □□ □□□ □□ □□□□ □□□.
- B. □□□□□□□ □□ □□□ □□□□□□ □□□□□ □□ □□□ □ "□□□" □□□ □□□□□.
- C. □□□□ □□□ □ □□ □□ SSID□ □□ □□□□□ □□□□ □□□.
- D. □□□ □□□□ MAC □□□ □□□□ □□ □□□ □ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 17

Which protocol is used for authentication in a network environment?

- A. EAP-TLS
- B. RADIUS
- C. TACACS+
- D. MACsec

Answer: (SHOW ANSWER)

NEW QUESTION: 18

ClearPass OnGuard can be used to monitor the health of which of the following?

- A. Network devices
- B. Client devices
- C. Client Health Status
- D. Network devices and client devices
- E. Network devices and client devices

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 19

ClearPass can be used to integrate with which of the following?

- A. Active Directory
- B. ClearPass "Network Access" and "Network Access" policies
- C. ClearPass "Network Access" policies
- D. ClearPass policies and Active Directory policies
- E. ClearPass "Network Access" policies

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 20

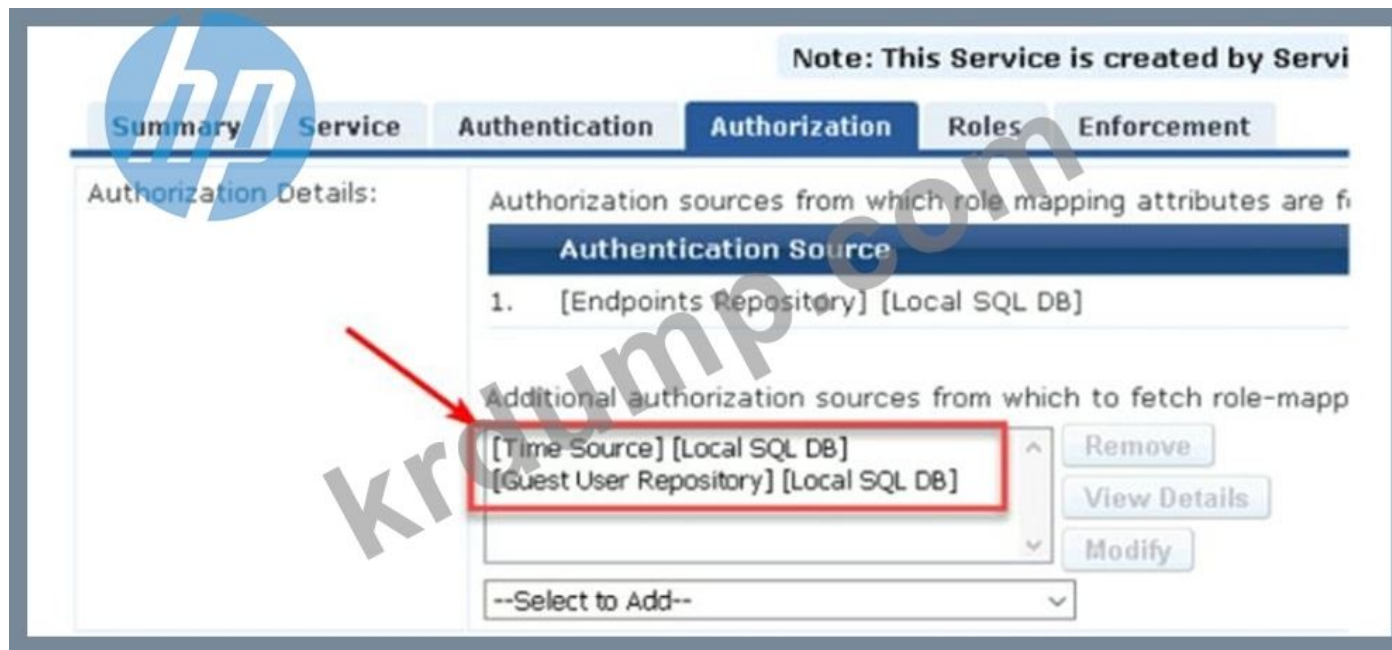
ClearPass can be used to integrate with which of the following?

- A. NAD(Network Access Device) policies
- B. ClearPass policies
- C. ClearPass policies
- D. Accounting Start-Stop policies

Answer: A (LEAVE A REPLY)

NEW QUESTION: 21

ClearPass can be used to integrate with which of the following?



Which of the following is not a valid authorization source for role mapping?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 22

Which of the following is not a valid authorization source for role mapping?

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

Answer: A (LEAVE A REPLY)

URL:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Enforce/EPRADIUS_CoA.htm

NEW QUESTION: 23

Which of the following is not a valid authorization source for role mapping?

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

Answer: C (LEAVE A REPLY)

- B. □□ □□□ □□□
- C. OnGuard □□□
- D. □□□ □□□ □□□

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

NEW QUESTION: 27

□□□ □□□□ □□ □□□□ □□ ClearPass□□ □□□ □□ □□ □□□□ □□□ □□ □□□□□.

□□□ □□□ □□'□ □□□□ □□ □□□ □□□□□? (2□ □□)

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

D18912E1457D5D1DDCB40AB3BF70D5D

- D. □□ □□ □□□□ □□ □□ □□□ □□□ □ □□□□.
- E. □□ □□ □□ □□□ □□□□ □□□□ □□□ □ □□ □□ □□□ □□ □□□ □ □□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 28

□□□□□ □□□ □□ DHCP □□□□□□ □□□□ □□□ □□□□□?

- A. NAD(Network Access Devices)□□ DHCP □□□□ □□□□□ DHCP □□□ ClearPass□ □□
- B. □□□□□□ □□□□□□□ □□ □□□□ Clearpass□ □□□□□ DHCP □□□ □□□□□□.
- C. □□□□□□ □□□ □□ □ DHCP□ □□ □ □□□ ClearPass□□ DHCP □□□ □□
- D. □□□□□ ClearPass□□ DHCP □□□□□□ □□□□□ □□□ NAD(Network Access Device)□□ DHCP □□□ □□□ □□ □□ □□□□.

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

NEW QUESTION: 29

□□□ □□□□□.

Enforcement Policies - Corp SSID Access

Summary Enforcement Rules

Enforcement:
 Name: Corp SSID Access
 Description:
 Enforcement Type: RADIUS
 Default Profile: Allow Internet Only Access

Rules:
 Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Tips:Role [RADIUS] employee)	Allow Full Access
2. (Tips:Role [RADIUS] [Contractor])	Corp Secure Contractor
3. (Tips:Role [RADIUS] Corp BYOD)	Secure Corp BYOD Access

Configurations = Identity + Local Users

Filter: Role contains employee [Go] [Clear Filter]

#	User ID	Name	Role
1.	john	john	[Employee]
2.	mike	mike	[Employee]
3.	ned	ned	[Employee]

Showing 1-3 of 3

Exhibit: ACCA82-345

Which user is not associated with the "employee" role?

- A. Secure Corp BYOD
- B. Allow Full Access
- C. Corp Secure Contractor
- D. Allow Internet Only Access

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

Active Directory authentication is implemented on a network. Which protocol is used for authentication?

- A. Active Directory Authentication Protocol (AD-Auth)
- B. Active Directory Lightweight Directory Services (AD-LDS)
- C. Active Directory Certificate Services (AD-Cert)
- D. Active Directory Federation Services (AD-FS)

Answer: B (LEAVE A REPLY)

NEW QUESTION: 31

Which protocol is used for authentication?

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 <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy			
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	
3. Radius:Aruba	Aruba-Essid-Name	EXISTS		
4. Radius:Aruba	Aruba-Essid-Name	EQUALS	CORP	
5. Click to add...				

Which of the following is a valid configuration for the service rule?

- A. Radius:Aruba SSID EQUALS "CORP"
- B. "CORP" SSID EXISTS
- C. Aruba SSID EQUALS "CORP"
- D. SSID "CORP" Aruba IAP EQUALS

Answer: D (LEAVE A REPLY)

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**)

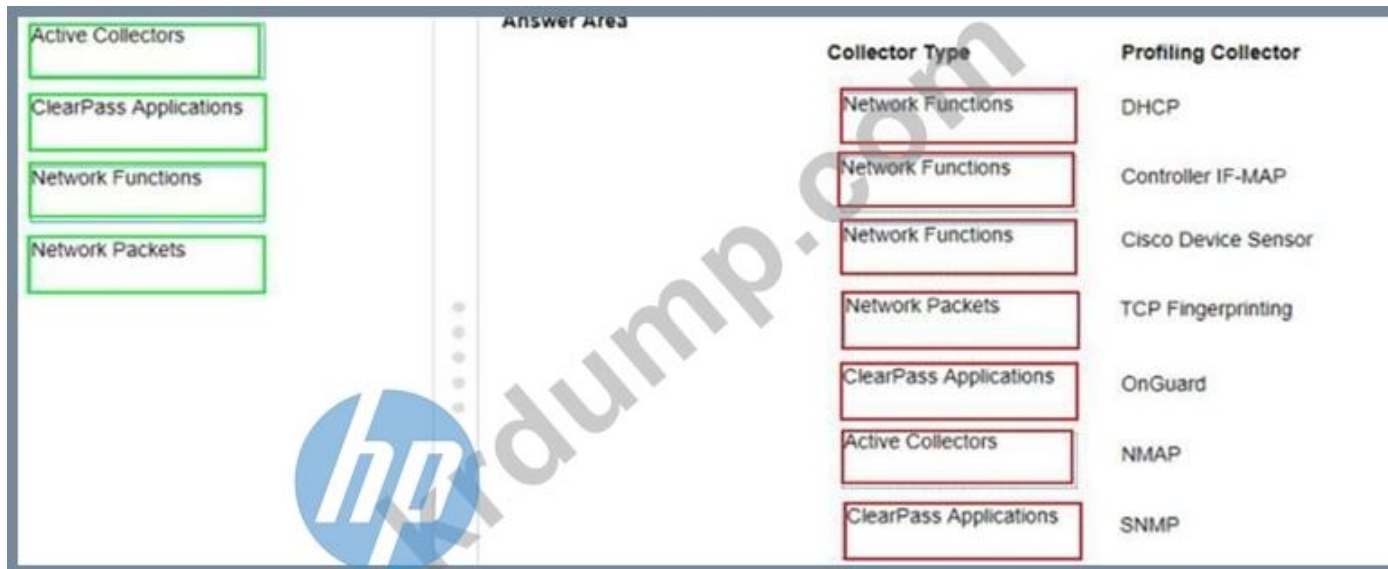
NEW QUESTION: 32

ClearPass is configured to use a RADIUS server for authentication. The RADIUS server is configured to use a shared secret of 'Aruba8021X'. Which of the following is a valid configuration for the service rule?

(2 correct answers.)

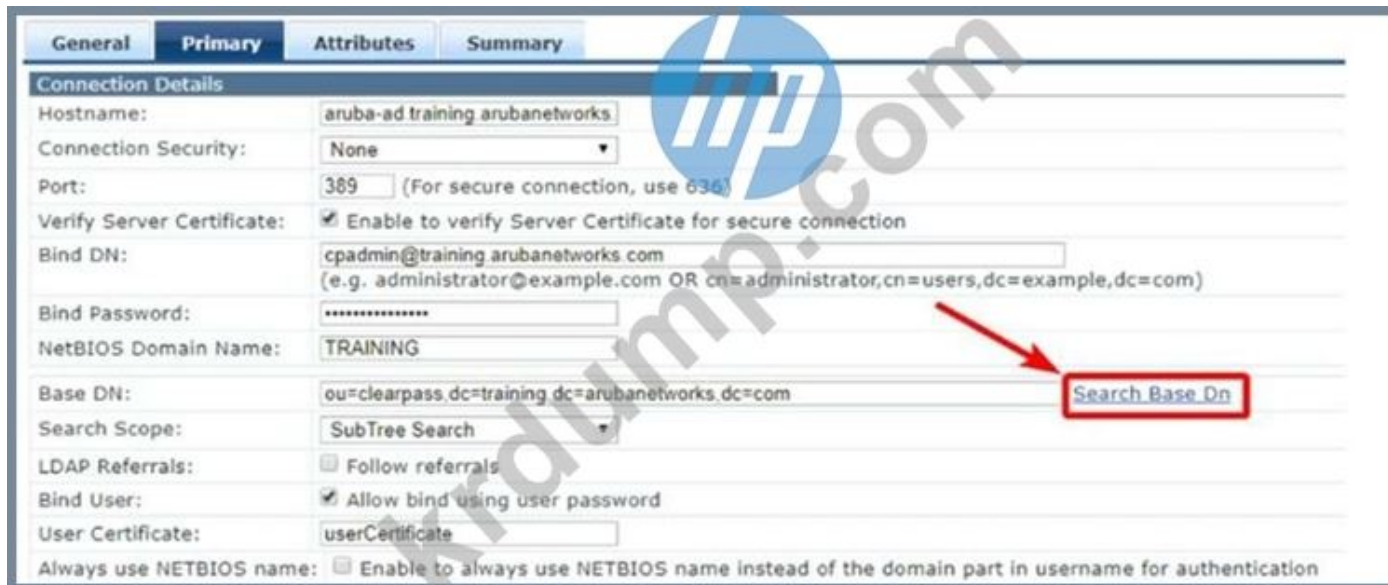
- A. ClearPass RADIUS SSID EQUALS "Aruba8021X"
- B. "Aruba8021X" RADIUS SSID EQUALS
- C. "Aruba8021X" RADIUS SSID EXISTS
- D. RADIUS SSID EQUALS "Aruba8021X"
- E. RADIUS SSID EQUALS "Aruba8021X"

Answer: B,E (LEAVE A REPLY)



NEW QUESTION: 36

□□□ □□□□□.



Active Directory □□□□ □□□ □ Starch Base Dn□ □□□ □□□? {2□□ □□□□□.}

- A. □□ DN(□□ □□) □□□ □□ □□□□ □□□ □□□□ □□□□□.
- B. □□□ □□ DN(□□ □□)□ □□□□ □□ □□□ □□ □□□ □□□□ Active Directory □□□ □□□□□.
- C. □□□ □□□ □□□ □□□□ □□ DN(□□ □□)□ □□□□□.
- D. □□□□ □□□ □□□ Active Directory□ □□ DN(□□ □□)□ □□□□□□□.
- E. □□ □□ □□□ □□□ □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 37

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

- A. ClearPass □□□ □□.
- B. □□□□□ □□□□□□□ □□□ □□.

□□ □□□ □□ □□□ □□□ □□□□□□. □□□ □ □□ □□□□□.

Term	Description
Accounting	used to match a credential that is being submitted to an account representing the client
Authentication	applying access decisions based on attributes attached to the user's account
Client	the owner of an endpoint that is providing credentials
Authorization	the device which consumes networks resources
User	gathering the start and stop times of network access and ongoing health checks of an endpoint

Answer:

Term	Description	
Accounting	Authentication	used to match a credential that is being submitted to an account representing the client
Authentication	Accounting	applying access decisions based on attributes attached to the user's account
Client	User	the owner of an endpoint that is providing credentials
Authorization	Client	the device which consumes networks resources
User	Authorization	gathering the start and stop times of network access and ongoing health checks of an endpoint

NEW QUESTION: 41

□□□ □□□□□.

The screenshot shows the 'ClearPass Policy Manager' interface for configuring an 'Authentication Source - Remote Lab AD'. The breadcrumb trail is 'Configuration > Authentication > Sources > Add - Remote Lab AD'. The page title is 'Authentication Sources - Remote Lab AD'. There are tabs for 'Summary', 'General', 'Primary', 'Attributes', 'Backup 1', and 'Backup 2', with 'General' selected. The configuration fields are as follows:

- Name: Remote Lab AD
- Description: (empty)
- Type: Active Directory
- Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes
- Authorization Sources: (empty list with 'Remove' and 'View Details' buttons, and a '-- Select --' dropdown)
- Server Timeout: 10 seconds
- Cache Timeout: 36000 seconds
- Backup Servers Priority: Backup 1, Backup 2 (with 'Move Up', 'Move Down', 'Add Backup', and 'Remove' buttons)

Remote Lab AD is a Windows authentication source. What is the default server timeout for this source?

- A. ClearPass Remote Lab AD server timeout is 10 seconds.
- B. ClearPass Remote Lab AD server timeout is 36000 seconds.
- C. ClearPass Remote Lab AD server timeout is 10 seconds.
- D. ClearPass Remote Lab AD server timeout is 36000 seconds.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 42

OnGuard is a Windows authentication source. What is the default server timeout for this source?

- A. ClearPass/OnGuard server timeout is 10 seconds.
- B. Antivirus/Antispyware server timeout is 36000 seconds.
- C. 802.1X server timeout is 10 seconds.
- D. Windows Mac OS X server timeout is 36000 seconds.

Answer: (SHOW ANSWER)

NEW QUESTION: 45

□□□ □□□□□.

Configuration > Authentication > Sources > Add - AD1

Authentication Sources - AD1

The screenshot shows the configuration page for an Active Directory authentication source. The 'General' tab is active. The 'Name' field is 'AD1'. The 'Type' is 'Active Directory'. The 'Use for Authorization' checkbox is checked. The 'Cache Timeout' is set to 36000 seconds. The 'Backup Servers Priority' list contains 'Backup 1' and 'Backup 2'. At the bottom, there are buttons for 'Add Backup', 'Remove', 'Move Up', 'Move Down', 'Clear Cache', 'Copy', and 'Save'. A watermark 'krdump.com' is visible over the form.

□□ □□ □□□ 36000□□ □□□□ □ □□ □□□ □□□□□? (2□□ □□□□□.)

- A. ClearPass□ □□□ □□□□ □□□ □□ □□□ □ □□□ □□□□ 10□□□□ AD□ □□ □□□ □ □□□ □□□ □□□□□.
- B. □□□ □□□□ □□□□ Cache Timeout □□□ □□ □□□ □□□□ □□ □□□ AD□□ □□ □□ □□□ □ □ □□□□.
- C. 10□□ □□□ □□□ □ ClearPass□ AD □□ □□ □□□ □□□□ □□□□.
- D. Cache Timeout□ 10□□ □□ □□□ □□ □□□ □□□□ ClearPass□ AD □□ □□ □□□ □□ □□□□ □□□□□□□.
- E. □□ □□ □□ □. ClearPass□ □□□□□□□ □□□□□□□ □□□ □□ 10□□ □□□ □□ □□ □□□ □ □□□ □□□ □□□ □□□.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 46

ClearPass□ □□ IP □□□ □□ □□□ □□□□ □ □□□□ □□ □□□ □□□ □□□□□?

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

Answer: A (LEAVE A REPLY)

Services

Service Authentication Rules Enforcement Summary

Type: Aruba 802.1X Wireless

Name: Test_Service

Description: Aruba 802.1X Wireless Access Service

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Posture Compliance Audit End-hosts Profile Groups Accounting Profile

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:SETF	Network-Type	EQUALS	Wireless-802.11 (19)
2. Radius:SETF	Service-Type	BELONGS_TO	Login-User (1), Framed
3. Radius:Aruba	Aruba-SSID Name	EXISTS	
4. Radius:Aruba	Aruba-SSID Name	EQUALS	CORP
5. Click to add...			

Which of the following SSIDs is associated with the service rule?

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

Which of the following protocols is used for ClearPass authentication? (2 correct answers.)

- A. IF-MAP
- B. SNMP
- C. DHCP
- D. NMAP
- E. HTTP

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 52

Which of the following is a valid IP address?

Services - Aruba 802.1X Secure Wireless

Summary Service Authentication Authorization Roles **Enforcement** Profiler

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

Enforcement Policy: aruba wireless enforcement policy Modify

Enforcement Policy Details

Description: Aruba wireless Enforcement policy
 Default Profile: [Deny Access Profile]
 Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:Category <i>HOT_EXISTS</i>)	assign profile only role
2. (Tips:Role <i>EQUALS</i> corporate_user) AND (Tips:Role <i>EQUALS</i> computer)	assign employee full role
3. (Tips:Role <i>EQUALS</i> corporate_user) AND (Tips:Role <i>EQUALS</i> smart_phone)	assign employee smart role
4. (Tips:Role <i>EQUALS</i> temp_user)	assign temp access role
5. (Tips:Role <i>EQUALS</i> temp_user) AND (Tips:Role <i>EQUALS</i> smart_phone)	assign employee smart role

Which of the following is a valid condition for the enforcement policy?

- A. (Tips:Role EQUALS corporate_user) AND (Tips:Role EQUALS computer)
- B. (Tips:Role EQUALS corporate_user) AND (Tips:Role EQUALS smart_phone)
- C. (Tips:Role EQUALS temp_user)
- D. (Tips:Role EQUALS temp_user) AND (Tips:Role EQUALS smart_phone)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 53

Which of the following is a valid condition for the enforcement policy?

Edit Endpoint

Fingerprints Endpoint Attributes

MAC Address	18ee6952ee34	IP Address	-
Description		Static IP	FALSE
Status	<input checked="" type="radio"/> Known client <input type="radio"/> Unknown client <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

Save Cancel

Which of the following is a valid condition for the enforcement policy? (2 correct answers.)

- A. Exchange Plugging
- B. 3 MDM

