

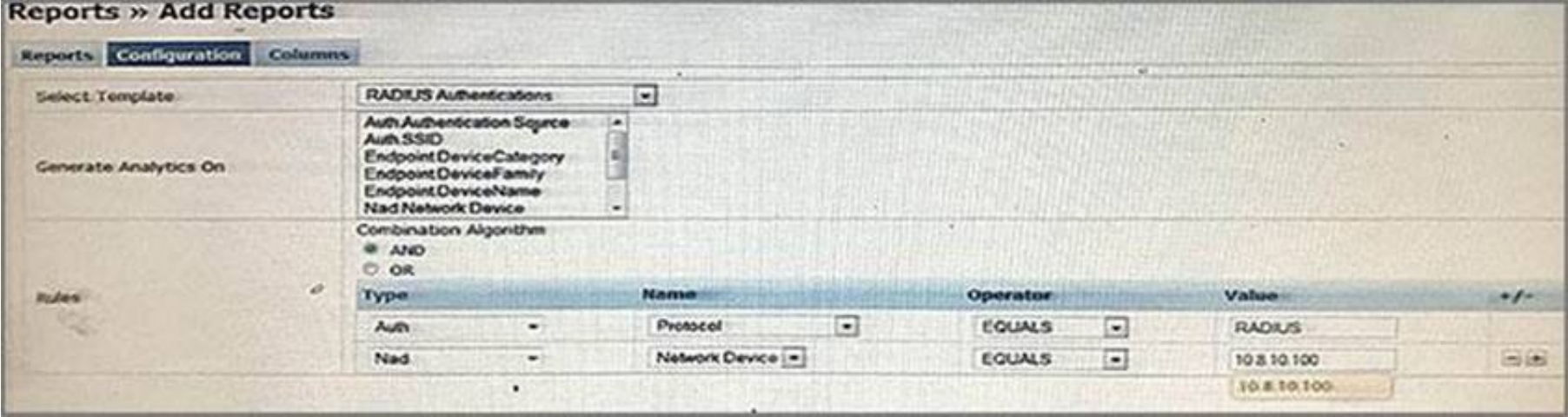
HP

Exam Questions HPE6-A68

Aruba Certified Clearpass Professional 6.7



NEW QUESTION 1
Refer to the exhibit.



Which types of records will the report shown display?

- A. all RADIUS authentications from the 10.8.10.100 NAD to ClearPass
- B. all failed RADIUS authentications through ClearPass
- C. only Windows devices that have authenticated through the 10.8.10.100 NAD
- D. all successful RADIUS authentications through ClearPass
- E. all successful RADIUS authentications from the 10.8.10.100 NAD to ClearPass

Answer: A

NEW QUESTION 2

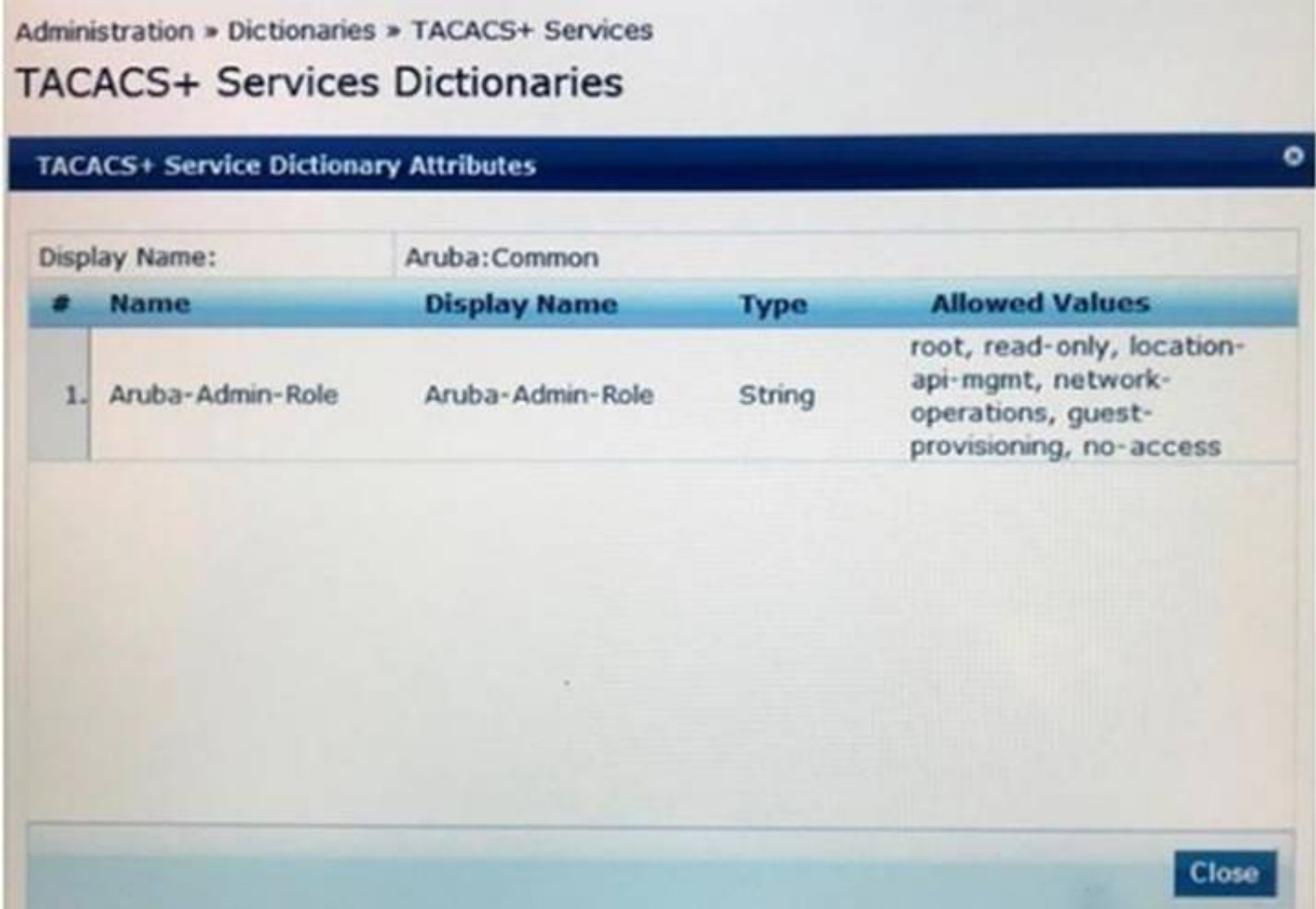
A guest self-registered through a Publisher's Register page.
Which statement accurately describes how the guest's account will be stored?

- A. It will be stored in the Publisher's guest user repository and the Subscriber's Onboard user repository.
- B. It will be stored in the Publisher's local user repository and the Subscriber's guest user repository.
- C. It will be stored in the Publisher's guest user repository permanently, but only for 14 days in the Subscriber's guest user repository,
- D. It will be stored in both the Publisher's guest user repository and the Subscriber's guest user repository.
- E. It will be stored in the Publisher's guest user repository, but not the Subscriber's.

Answer: D

NEW QUESTION 3

Refer to the exhibit.



Based on the Aruba TACACS+ dictionary shown, how is the Aruba-Role attribute used?

- A. The Aruba-Admin-Role on the controller is applies to users using TACACS+ to login to the Policy Manager
- B. To assign different privileges to clients during 802.1X authentication
- C. To assign different privileges to administrators logging into an Aruba NAD
- D. It is used by ClearPass to assign TIPS roles to clients during 802.1X authentication
- E. To assign different privileges to administrators logging into ClearPass

Answer: C

NEW QUESTION 4

Refer to the exhibit.

Summary	Input	Output
Session Identifier:		W00000024-01-515a5f14
Date and Time:		Apr 02, 2013 04:31:17 UTC
End-Host Identifier:		4c60def412ee
Username:		4c60def412ee
Access Device IP/Port:		-
System Posture Status:		HEALTHY (0)
Policies Used -		
Service:		Health Check for clients
Authentication Method:		Not applicable
Authentication Source:		-
Authorization Source:		-
Roles:		[Guest]
Enforcement Profiles:		[Aruba Terminate Session]
Service Monitor Mode:		Disabled

Based on the Access Tracker output for the user shown, which statement describes the status?

- A. The Aruba Terminate Session enforcement profile as applied because the posture check failed.
- B. A Healthy Posture Token was sent to the Policy Manager.
- C. A RADIUS-Access-Accept message is sent back to the Network Access Device.
- D. The authentication method used is EAP-PEAP.
- E. A NAP agent was used to obtain the posture token for the user.

Answer: B

Explanation:

We see System Posture Status: HEALTHY(0)

End systems that pass all SHV tests receive a Healthy Posture Token, if they fail a single test they receive a Quarantine Posture Token.

References: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 13

[https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%](https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%20Configuration%20Guide.pdf)

NEW QUESTION 5

Which authorization servers are supported by ClearPass? (Select two.)

- A. Aruba Controller
- B. LDAP server
- C. Cisco Controller
- D. Active Directory
- E. Aruba Mobility Access Switch

Answer: BD

Explanation:

Authentication Sources can be one or more instances of the following examples:

- * Active Directory
- * LDAP Directory
- * SQL DB
- * Token Server
- * Policy Manager local DB

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 114

[https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%](https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20User%20Reference%20Guide.pdf)

NEW QUESTION 6

Which authentication protocols can be used for authenticating Windows clients that are Onboarded? (Select two.)

- A. EAP-GTC
- B. PAP
- C. EAP-TLS
- D. CHAP
- E. PEAP with MSCHAPv2

Answer: CE

NEW QUESTION 7

Which devices support Apple over-the-air provisioning? (Select two.)

- A. IOS 5
- B. Laptop running Mac OS X 10.8
- C. Laptop running Mac OS X 10.6
- D. Android 2.2
- E. Windows XP

Answer: AB

Explanation:

Apple over-the-air provisioning is supported by IOS and OSX above version 10.6. References:
https://community.arubanetworks.com/aruba/attachments/aruba/tkb@tkb/286/1/BYODwithClearPass_Cameron

NEW QUESTION 8

Refer to the exhibit.

Summary	Policy	Mapping Rules
<u>Policy:</u>		
Policy Name:	WLAN role mapping	
Description:		
Default Role:	[Guest]	
<u>Mapping Rules:</u>		
Rules Evaluation Algorithm:	First applicable	
Conditions		Role Name
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive
2.	(Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor
3.	(Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device
4.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-week NOT_BELONGS_TO Saturday, Sunday)	HR Local
5.	(Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User
6.	(Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee

An AD user’s department attribute value is configured as “QA”. The user authenticates from a laptop running MAC OS X. Which role is assigned to the user in ClearPass?

- A. HR Local
- B. Remote Employee
- C. [Guest]
- D. Executive
- E. IOS Device

Answer: C

Explanation:

None of the Listed Role Name conditions are met.

NEW QUESTION 9

What does a Windows client need for it to perform EAS-PEAP successfully when ‘Validate server Certificate’ is not enabled?

- A. Pre-shared key
- B. Client Certificate
- C. WPA2-PSK
- D. Username and Password
- E. Server Certificate

Answer: D

NEW QUESTION 10

Refer to the exhibit.

Captive Portal Authentication Profile > default

Show Reference

Save As

Reset

Default Role	guest ▼	Default Guest Role	guest ▼
Redirect Pause	10 sec	User Login	✓
Guest Login	<input type="checkbox"/>	Logout popup window	✓
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	<input type="checkbox"/>
Use CHAP (non-standard)	<input type="checkbox"/>	Login page	/auth/index.html
Welcome page	/auth/welcome.html	Show Welcome Page	✓
Add switch IP address in the redirection URL	<input type="checkbox"/>	Allow only one active user session	<input type="checkbox"/>
While List	<div>▲ ▼ Delete Add</div>	Black List	<div>▲ ▼ Delete Add</div>
Show the acceptable use policy page	<input type="checkbox"/>		

Based on the information shown, which field in the Captive Portal Authentication profile should be changed so that guest users are redirected to a page on ClearPass when they connect to the Guest SSID?

- A. both Login and Welcome Page
- B. Default Role
- C. Welcome Page
- D. Default Guest Role
- E. Login Page

Answer: E

Explanation:

The Login page is the URL of the page that appears for the user login. This can be set to any URL.

The Welcome page is the URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.

References:

http://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Captive_Portal/C

NEW QUESTION 10

What does Authorization allow users to do in a Policy Service?

- A. To use attributes in databases in role mapping and Enforcement.
- B. To use attributes stored in databases in Enforcement only, but not role mapping.
- C. To use attributes stored in external databases for Enforcement, but not internal databases.
- D. To use attributes stored in databases in role mapping only, but not Enforcement.
- E. To use attributes sored in internal databases for Enforcement, but not external databases.

Answer: A

NEW QUESTION 13

Refer to the exhibit.

Summary	Policy	Posture Plugins	Rules
Policy Name:	Employee Posture Policy		
Description:			
Posture Agent:	<input type="radio"/> NAP Agent <input checked="" type="radio"/> OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> Mac OS X		

Based on the Posture Policy configuration shown, above, which statement is true?

- A. This Posture Policy can only be applied to an 802.1x wired service not 802.1x wireless.
- B. This Posture Policy checks the health status of devices running Windows, Linux and Mac OS X.
- C. This Posture Policy can use either the persistent or dissolvable Onguard agent to obtain the statement of health.
- D. This Posture Policy checks for presence of a firewall application in Windows devices.
- E. This Posture Policy checks with a Windows NPS server for posture tokens.

Answer: C

NEW QUESTION 14

What is the purpose of the Audit Viewer in the Monitoring section of ClearPass Policy Manager?

- A. to audit client authentications
- B. to display changes made to the ClearPass configuration
- C. to display the entire configuration of the ClearPass Policy Manager
- D. to audit the network for PCI compliance
- E. to display system events like high CPU usage.

Answer: B

NEW QUESTION 17

What are Operator Profiles used for?

- A. to enforce role based access control for Aruba Controllers
- B. to enforce role based access control for ClearPass Policy Manager admin users
- C. to enforce role based access control for ClearPass Guest Admin users
- D. to assign ClearPass roles to guest users
- E. to map AD attributes to admin privilege levels in ClearPass Guest

Answer: C

Explanation:

An operator profile determines what actions an operator is permitted to take when using ClearPass Guest. References:
http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/OperatorLogins/Operato

NEW QUESTION 19

Refer to the exhibit.

Device Provisioning Settings

General

Web Login

iOS iOS & OS X

Legacy OS X

Windows

Android

Onboard Client

*Name:

Local Device Provisioning

Enter a name for this configuration set.

Description:

This is the default configuration set for device provisioning.

Enter a description for the configuration set.

*Organization:

Example Organization

Enter an organization name for this configuration set.

The organization name is displayed by the device during provisioning.

Identity

These options control the generation of device credentials

* Certificate Authority:

Local Certificate Authority

Select the certificate authority that will be used to sign profiles and messages.

* Signer:

Onboard Certificate Authority

Select the source that will be use to sign TLS client certificates.

* Key Type:

1024-bit RSA - created by device

Select the type of private key to use for TLS certificates.

* Unique Device Credentials:

☒

Include the username in unique device credentials

When checked, the username is prefixed to the device's PEAP credentials.

This unique set of credentials is used to identify the user and device on the network.

Based on the configuration for the client's certificate private key as shown, which statements accurately describe the settings? (Select two.)

- A. The private key is stored in the ClearPass server.
- B. The private key is stored in the user device.
- C. The private key for TLS client certificates is not created.
- D. More bits in the private key will increase security.
- E. More bits in the private key will reduce security.

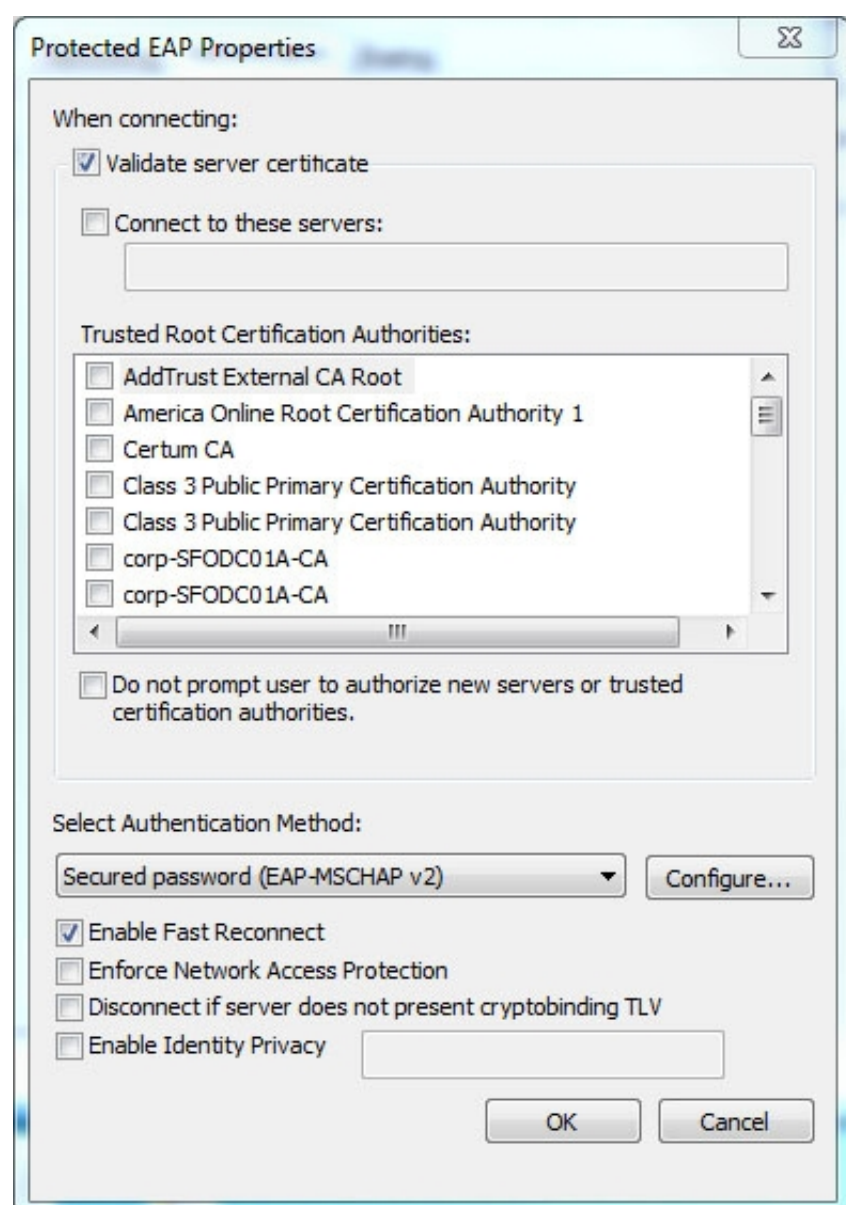
Answer: BD

NEW QUESTION 24

Refer to the exhibit.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>



The image shows the 'Protected EAP Properties' dialog box in Windows. The 'When connecting:' section has 'Validate server certificate' checked. Below it, 'Connect to these servers:' is unchecked. The 'Trusted Root Certification Authorities:' list contains several entries, including 'AddTrust External CA Root' and 'America Online Root Certification Authority 1'. The 'Do not prompt user to authorize new servers or trusted certification authorities.' checkbox is unchecked. The 'Select Authentication Method:' dropdown is set to 'Secured password (EAP-MSCHAP v2)'. Below this, 'Enable Fast Reconnect' is checked, while 'Enforce Network Access Protection', 'Disconnect if server does not present cryptobinding TLV', and 'Enable Identity Privacy' are unchecked. 'OK' and 'Cancel' buttons are at the bottom.

Based on the configuration of a Windows 802.1X supplicant shown, what will be the outcome of selecting 'Validate server certificate'?









- A. The server and client will perform an HTTPS SSL certificate exchange.
- B. The client will verify the server certificate against a trusted CA.
- C. The client will send its private key to the server for verification.
- D. The server will send its private key to the client for verification.
- E. The client will send its certificate to the server for verification.

Answer: B

NEW QUESTION 26

Refer to the exhibit.

Use this list view to modify the fields of the form **create_user**.

<div>  Quick Help  Preview Form </div>				
Rank	Field	Type	Label	Description
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this visitor account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this visitor account.
20	visitor_name	text	Visitor's Name:	Name of the visitor.
25	visitor_phone	text	Phone Number	The visitor's phone number
<div>  Edit  Edit base field  Remove  Insert before  Insert After  Enable Field </div>				
30	visitor_company	text	Company Name:	Company name of the visitor.
40	email	text	Email Address:	The visitor's email address. This will become their username to log into the network.
50	modify_start_time	dropdown	Account Activation:	Select an option for changing the activation time of this account.

Based on the configuration of the create_user form shown, which statement accurately describes the status?

- A. The email field will be visible to guest users when they access the web login page.

- B. The visitor_company field will be visible to operators creating the account.
- C. The visitor_company field will be visible to the guest users when they access the web login page.
- D. The visitor_phone field will be visible to the guest users in the web login page.
- E. The visitor_phone field will be visible to operators creating the account.

Answer: A

Explanation:

References:

<https://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/expire-timezone-field-is-not-showin>

NEW QUESTION 28

Refer to the exhibit.

Based on the configuration for ‘maximum devices’ shown, which statement accurately describes its settings?

- A. The user cannot Onboard any devices.
- B. It limits the total number of devices that can be provisioned by ClearPass.
- C. It limits the total number of Onboarded devices connected to the network.
- D. It limits the number of devices that a single user can Onboard.
- E. It limits the number of devices that a single user can connect to the network.

Answer: D

NEW QUESTION 31

Refer to the exhibit.

Summary		Enforcement		Rules	
Enforcement:					
Name:		Handheld_Wireless_Access_Policy			
Description:		Enforcement policy for handheld wireless access			
Enforcement Type:		RADIUS			
Default Profile:		WIRELESS_CAPTIVE_NETWORK			
Rules:					
Rules Evaluation Algorithm:		First applicable			
Conditions			Actions		
1.	(Tips:Role MATCHES_ANY [guest])		WIRELESS_GUEST_NETWORK		
2.	(Endpoint:OS Version CONTAINS Android)		WIRELESS_HANDHELD_NETWORK		
3.	(Tips:Role MATCHES_ANY conferencelaptop developer senior_mgmt testqa Role_Engineer)		WIRELESS_EMPLOYEE_NETWORK		

A user who is tagged with the ClearPass roles of Role_Engineer and developer, but not testqa, connects to the network with a corporate Windows laptop. Which Enforcement Profile is applied?

- A. WIRELESS_GUEST_NETWORK
- B. WIRELESS_CAPTIVE_NETWORK
- C. WIRELESS_HANDHELD_NETWORK
- D. Deny Access
- E. WIRELESS_EMPLOYEE_NETWORK

Answer: E

Explanation:

MATCHES_ANY: For list data types, true if any of the run-time values in the list match one of the configured values.

Example: Tips:Role MATCHES_ANY HR,ENG,FINANCE

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Rules

NEW QUESTION 34

An employee authenticates using a corporate laptop and runs the persistent Onguard agent to send a health check back the Policy Manager. Based on the health of the device, a VLAN is assigned to the corporate laptop.

Which licenses are consumed in this scenario?

- A. 1 Policy Manager license, 1 Onboard License
- B. 2 Policy Manager licenses, 1 Onguard License
- C. 1 Policy Manager license, 1 Profile License
- D. 2 Policy Manager licenses, 2 Onguard licenses
- E. 1 Policy Manager license, 1 Onguard License

Answer: E

NEW QUESTION 39

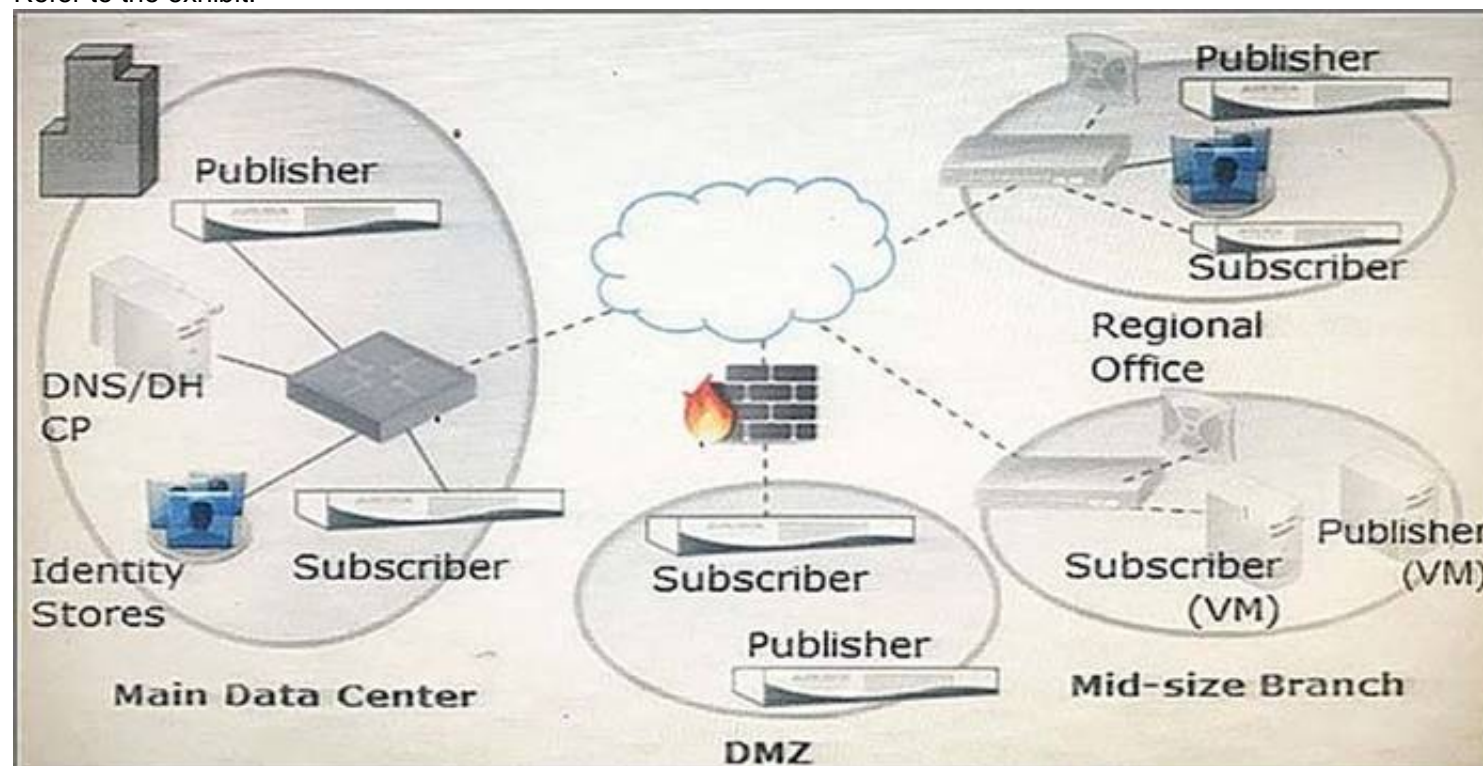
Under which circumstances is it necessary to use an SNMP based Enforcement profile to send a VLAN?

- A. when a VLAN must be assigned to a wired user on an Aruba Mobility Controller
- B. when a VLAN must be assigned to a wireless user on an Aruba Mobility Controller
- C. when a VLAN must be assigned to a wired user on a third party wired switch that does not support RADIUS return attributes
- D. when a VLAN must be assigned to a wired user on an Aruba Mobility Access Switch
- E. when a VLAN must be assigned to a wired user on a third party wired switch that does not support RADIUS accounting

Answer: C

NEW QUESTION 42

Refer to the exhibit.



Based on the network topology diagram shown, how many clusters are needed for this deployment?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 8

Answer: D

Explanation:

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deploy

NEW QUESTION 44

When a third party Mobile Device Management server is integrated with ClearPass, where is the endpoint information from the MDM server stored in ClearPass?

- A. Endpoints repository
- B. Onboard Device repository
- C. MDM repository
- D. Guest User repository
- E. Local User repository

Answer: A

Explanation:

A service running in CPPM periodically polls MDM servers using their exposed APIs. Device attributes obtained from MDM are added as endpoint tags. Profiler related attributes are sent to profiler which uses these attributes to derive final profile.

References: ClearPass Profiling TechNote (2014), page 23

[https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%](https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote)

NEW QUESTION 47

A ClearPass administrator wants to make Enforcement decisions during 802.1x authentication based on a client's Onguard posture token. Which Enforcement profile should be used on the health check service?

- A. RADIUS CoA
- B. Quarantine VLAN
- C. Full Access VLAN
- D. RADIUS Accept
- E. RADIUS Reject

Answer: A

Explanation:

The Health Check Service requires a profile to terminate the session so that the RADIUS 802.1X authentication Service can use the posture token in a new authentication routine. The terminate session profile will utilize the Change of Authorization feature to force a re-authentication.

See step 6) below.

Navigate to the list of Enforcement Profiles by selecting, Configuration > Enforcement > Profiles.

* 2. Click the + Add link in the upper right hand corner.

* 3. From the Template dropdown menu, choose RADIUS Change of Authorization (CoA).

* 4. Name the policy.

This example uses Dell Terminate Session as the profile name.

* 5. Leave all the other settings as default, and click Next > to move to the Attributes tab.

* 6. On the dropdown menu for Select RADIUS CoA Template, choose IETF-Terminate-Session-IETF.

* 7. Click Next > and review the Summary tab (Figure 22).

* 8. Click Save.

References: ClearPass NAC and Posture Assessment for

Campus Networks Configuring ClearPass OnGuard, Switching, and Wireless (v1.0) (September 2015), page 22

<http://en.community.dell.com/cfs-file/ key/telligent-evolution-components-attachments/13-4629-00-00-20-44>

NEW QUESTION 48

Which collectors can be used for device profiling? (Select two.)

- A. Username and Password
- B. ActiveSync Plugin
- C. Client's role on the controller
- D. Onguard agent
- E. Active Directory Attributes

Answer: BD

NEW QUESTION 51

Use the arrows to sort the steps to request a Policy Service on the left into the order they are performed on the right.

Steps to Request a Policy Service Order Performed

ClearPass tests the request against Service Rules to select a Policy Service.

ClearPass applies the Enforcement Policy

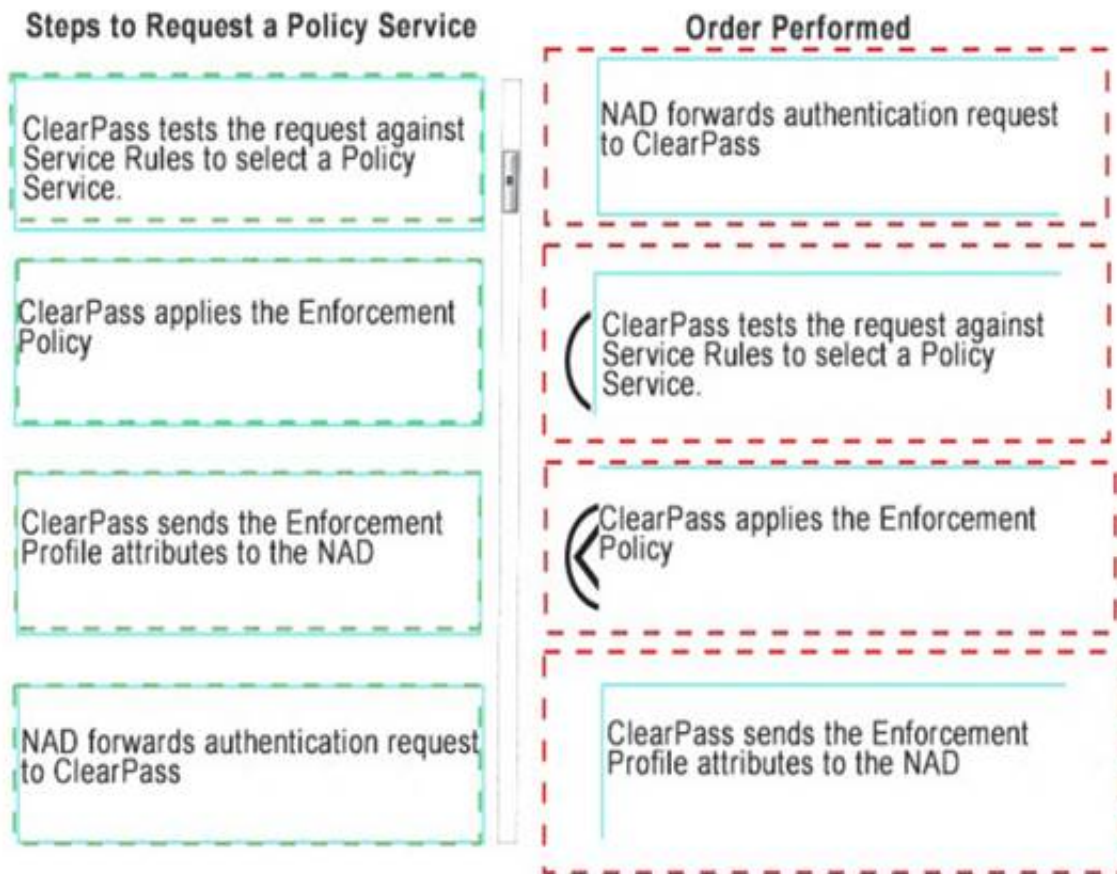
ClearPass sends the Enforcement Profile attributes to the NAD

NAD forwards authentication request to ClearPass

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 53

Refer to the exhibit.



Based on the configuration of the Enforcement Profiles in the Onboard Authorization service shown, which Onboarding action will occur?

- A. The device will be disconnected from the network after Onboarding so that an EAP-TLS authentication is not performed.
- B. The device will be disconnected from and reconnected to the network after Onboarding is completed.
- C. The device's onboard authorization request will be denied.
- D. The device will be disconnected after post-Onboarding EAP-TLS authentication, so a second EAP-TLS authentication is performed.
- E. After logging in on the Onboard web login page, the device will be disconnected from and reconnected to the network before Onboard begins.

Answer: B

NEW QUESTION 57

Which settings need to be validated for a successful EAP-TLS authentication? (Select two.)

- A. Username and Password
- B. Pre-shared key
- C. WPA2-PSK
- D. Server Certificate
- E. Client Certificate

Answer: DE

Explanation:

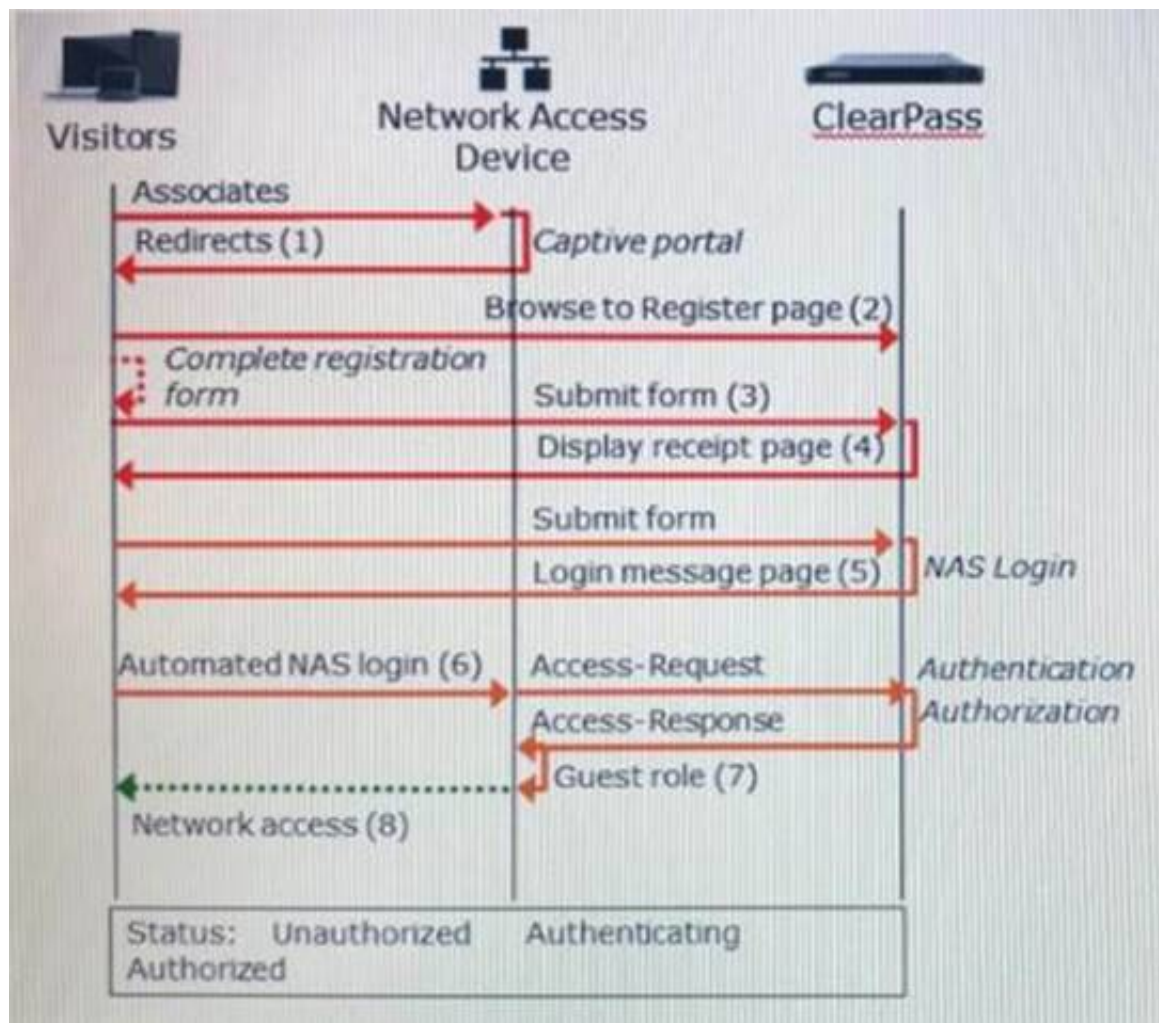
When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements both on the server and on the client for successful authentication.

References:

<https://support.microsoft.com/en-us/help/814394/certificate-requirements-when-you-use-eap-tls-or-peap-with-ea>

NEW QUESTION 59

Refer to the exhibit.



Based on the guest Self-Registration with Sponsor Approval workflow shown, at which stage does the sponsor approve the user's request?

- A. After the RADIUS Access-Request
- B. After the NAS login, but before the RADIUS Access-Request
- C. Before the user can submit the registration form
- D. After the RADIUS Access-Response
- E. After the receipt page is displayed, before the NAS login

Answer: E

NEW QUESTION 62

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

Login Form
Options for specifying the behaviour and content of the login form.

Credentials - Require a username and password ▼
Select the authentication requirement.
Access Code requires a single code (username) to be entered.
Anonymous allows a blank form requiring just the terms or a Log In button. A pre-Access Code and Anonymous require the account to have the Username Authentici

Authentication:

Custom Form: ☐ Provide a custom login form
If selected, you must supply your own HTML login form in the Header or Footer HT

Custom Labels: ☐ Override the default labels and error messages
If selected, you will be able to alter labels and error messages for the current login

*** Pre-Auth Check:** **RADIUS - check using a RADIUS request** ▼
Select how the username and password should be checked before proceeding to th

Terms: ☐ Require a Terms and Conditions confirmation
If checked, the user will be forced to accept a Terms and Conditions checkbox.

A Web Login page is configured in Clear Pass Guest as shown. What is the purpose of the Pre-Auth Check?

- A. To authenticate users after the NAD sends an authentication request to ClerPass
- B. To authenticate users before the client sends the credentials to the NAD
- C. To authenticate users when they are roaming from one NAD to another
- D. To authenticate users before they launch the Web Login Page
- E. To replace the need for the NAD to send an authentication request to ClearPass

Answer: B

NEW QUESTION 66

Refer to the exhibit.

Summary	Policy	Mapping Rules
Policy:		
Policy Name:	WLAN role mapping	
Description:		
Default Role:	[Guest]	
Mapping Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Role Name	
1. (Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive	
2. (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor	
3. (Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device	
4. (Authorization:remotelab AD:UserDN EXISTS)	[Employee]	
5. (Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-week NOT_BELONGS_TO Saturday, Sunday)	HR Local	
6. (Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User	

An AD user's department attribute value is configured as "Product Management". The user connects on Monday to a NAD that belongs to the Device Group HQ. Which role is assigned to the user in ClearPass?

- A. HR Local
- B. [Guest]
- C. [Employee]
- D. Linux User
- E. Executive

Answer: E

Explanation:

The conditions of the Executive Role is met.

NEW QUESTION 70

Refer to the exhibit.

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	NAD-IP-Address	BELONGS_TO_GROUP	HQ
4. Click to add...			

Under which circumstances will ClearPass select the Policy Service named 'Test device group'?

- A. when the NAD belongs to an Airware device group HQ
- B. when the ClearPass IP address is part of the device group HQ
- C. when the Aruba access point that the client is associated to is part of the device group HQ
- D. when an end user IP address is part of the device group HQ
- E. when the IP address of the NAD is part of the device group HQ

Answer: E

NEW QUESTION 73

Which steps are required to use ClearPass as a TACACS+ Authentication server for a network device? (Select two.)

- A. Configure a TACACS Enforcement Profile on ClearPass for the desired privilege level.
- B. Configure a RADIUS Enforcement Profile on ClearPass for the desired privilege level.
- C. Configure ClearPass as an Authentication server on the network device.

- D. Configure ClearPass roles on the network device.
- E. Enable RADIUS accounting on the NAD.

Answer: AC

Explanation:

You need to make sure you modify your policy (Configuration » Enforcement » Policies » Edit - [Admin Network Login Policy]) and add your AD group settings in to the corresponding privilege level.

NEW QUESTION 78

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

HPE6-A68 Practice Exam Features:

- * HPE6-A68 Questions and Answers Updated Frequently
- * HPE6-A68 Practice Questions Verified by Expert Senior Certified Staff
- * HPE6-A68 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HPE6-A68 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The HPE6-A68 Practice Test Here](#)