

DUMPS ARENA

Aruba Certified ClearPass Professional (ACCP) 6.7

HP HPE6-A68

Version Demo

Total Demo Questions: 10

Total Premium Questions: 115

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Summary Enforcement Rules

Enforcement:

Name:	Vlan enforcement
Description:	
Enforcement Type:	RADIUS
Default Profile:	Internet VLAN

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Tips:Role EQUALS Engineer) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Connection:Protocol EQUALS RADIUS)	Full Access VLAN
2. (Tips:Role EQUALS Manager) AND (Connection:Protocol BELONGS_TO RADIUS, TACACS, WEBAUTH, Application)	Full Access VLAN
3. (Tips:Role EQUALS Engineer) AND (Connection:Protocol BELONGS_TO WEBAUTH)	Employee Vlan

Based on the Policy configuration shown, which VLAN will be assigned when a user with ClearPass role Engineer authenticates to the network successfully using connection protocol WEBAUTH?

- A. Deny Access
- B. Employee VLAN
- C. Internet VLAN
- D. Full Access VLAN

ANSWER: B

QUESTION NO: 2

Refer to the exhibit.

Authentication Sources - remotelab AD

Summary	General	Primary	Attributes
Name:	retemotelab AD		
Description:			
Type:	Active Directory		
User for Authorization:	<input checked="" type="checkbox"/> Enable to use this authentication source to		
Authorization Sources:	<div style="border: 1px solid #ccc; padding: 2px;">-- Select --</div>		
Server Timeout:	<input type="text" value="10"/>	seconds	
Cache Timeout:	<input type="text" value="36000"/>	seconds	
Backup Servers Priority:			

What does the Cache Timeout Value refer to?

- A. The amount of time the Policy Manager caches the user credentials stored in the Active Directory.
- B. The amount of time the Policy Manager waits for a response from the Active Directory before checking the backup authentication source.
- C. The amount of time the Policy Manager caches the user attributes fetched from Active Directory.
- D. The amount of time the Policy Manager waits for response from the Active Directory before sending a timeout message to the Network Access Device.
- E. The amount of time the Policy Manager caches the user's client certificate.

ANSWER: C

QUESTION NO: 3

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.	
Authentication:	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 Authentic
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HT
Custom Labels:	<input type="checkbox"/> 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:	<input type="checkbox"/> 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 ClearPass
- 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

QUESTION NO: 4

An employee provisions a personal smart phone using the Onboard process. In addition, the employee has a corporate laptop provided by IT that connects to the secure network.

How many licenses does the employee consume?

- A. 1 Policy Manager license, 2 Guest Licenses
- B. 2 Policy Manager licenses, 1 Onboard License
- C. 1 Policy Manager license, 1 Onboard License
- D. 1 Policy Manager license, 1 Guest License

E. 2 Policy Manager licenses, 2 Onboard Licenses

ANSWER: B

QUESTION NO: 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: B D

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%206.5%20User%20Guide%20-%20October%202015.pdf)

QUESTION NO: 6

Refer to the exhibit.

Summary	Policy	Mapping rules
Policy:		
Policy Name:	WLAN role mapping	
Description:		
Default Role:	[Guest]	
Mapping Rules:		
Rules Evaluation Algorithm:	Evaluate all	
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 is configured as "HR". The user connects on Monday using an Android phone to an Aruba Controller that belongs to the Device Group Remote NAD.

Which roles are assigned to the user in ClearPass? (Select two.)

- A. Executive
- B. iOS Device
- C. Vendor
- D. Remote Employee
- E. HR Local

ANSWER: D E

QUESTION NO: 7

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: A C

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.

QUESTION NO: 8

Refer to the exhibit.

Certificate Issuing	
These options control how certificates are issued by this certificate authority.	
* Authority Info Access:	<input type="text" value="Include OCSP Responder URL"/> Select the information about the certificate authority to include in the client certificate. Note that when an OCSP URL is provided, clients may need to access this URL in order to determine if the certificate is still valid.
OCSP URL:	<input type="text" value="http://cp62-server1/quest/mcps_ocsp.php/4"/> The OCSP URL to be included in certificates.
* Validity Period:	<input type="text" value="365"/> days Maximum validity period for client certificates (in days).
* Clock Skew Allowance:	<input type="text" value="15"/> Amount to pre/post date certificate validity period (in minutes).
Subject Alternative Name:	<input checked="" type="checkbox"/> Include device information in TLS client certificates Store information about the device in the subjectAltName extension of the certificate. Note: Aruba OS version 5.1 or later is required to enable this feature.

What is the purpose of the 'Clock Skew Allowance' setting? (Select two.)

- A. to ensure server certificate validation does not fail due to client clock sync issues
- B. to set start time in client certificate to a few minutes before current time
- C. to adjust clock time on client device to a few minutes before current time
- D. to ensure client certificate validation does not fail due to client clock sync issues
- E. to set expiry time in client certificate to a few minutes longer than the default setting

ANSWER: D

Explanation:

Clock Skew Allowance adds a small amount of time to the start and end of the client certificate's, not the server certificate's, validity period. This permits a newly issued certificate to be recognized as valid in a network where not all devices are perfectly synchronized.

References:

<http://www.arubanetworks.com/techdocs/ClearPass/6.6/Guest/Content/Onboard/EditingCASettings.htm>

QUESTION NO: 9

Refer to the exhibit.

Device Provisioning Settings	
General Web Login iOS iOS & OS X Legacy OS X Windows Android Onboard Client	
*Name:	<input type="text" value="Local Device Provisioning"/> <small>Enter a name for this configuration set.</small>
Description:	<input type="text" value="This is the default configuration set for device provisioning."/> <small>Enter a description for the configuration set.</small>
*Organization:	<input type="text" value="Example Organization"/> <small>Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.</small>
Identity	
<small>These options control the generation of device credentials</small>	
* Certificate Authority:	<input type="text" value="Local Certificate Authority"/> <small>Select the certificate authority that will be used to sign profiles and messages.</small>
* Signer:	<input type="text" value="Onboard Certificate Authority"/> <small>Select the source that will be use to sign TLS client certificates.</small>
* Key Type:	<input type="text" value="1024-bit RSA - created by device"/> <small>Select the type of private key to use for TLS certificates.</small>
* Unique Device Credentials:	<input checked="" type="checkbox"/> <input type="text" value="Include the username in unique device credentials"/> <small>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.</small>

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: B D

QUESTION NO: 10

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: B D