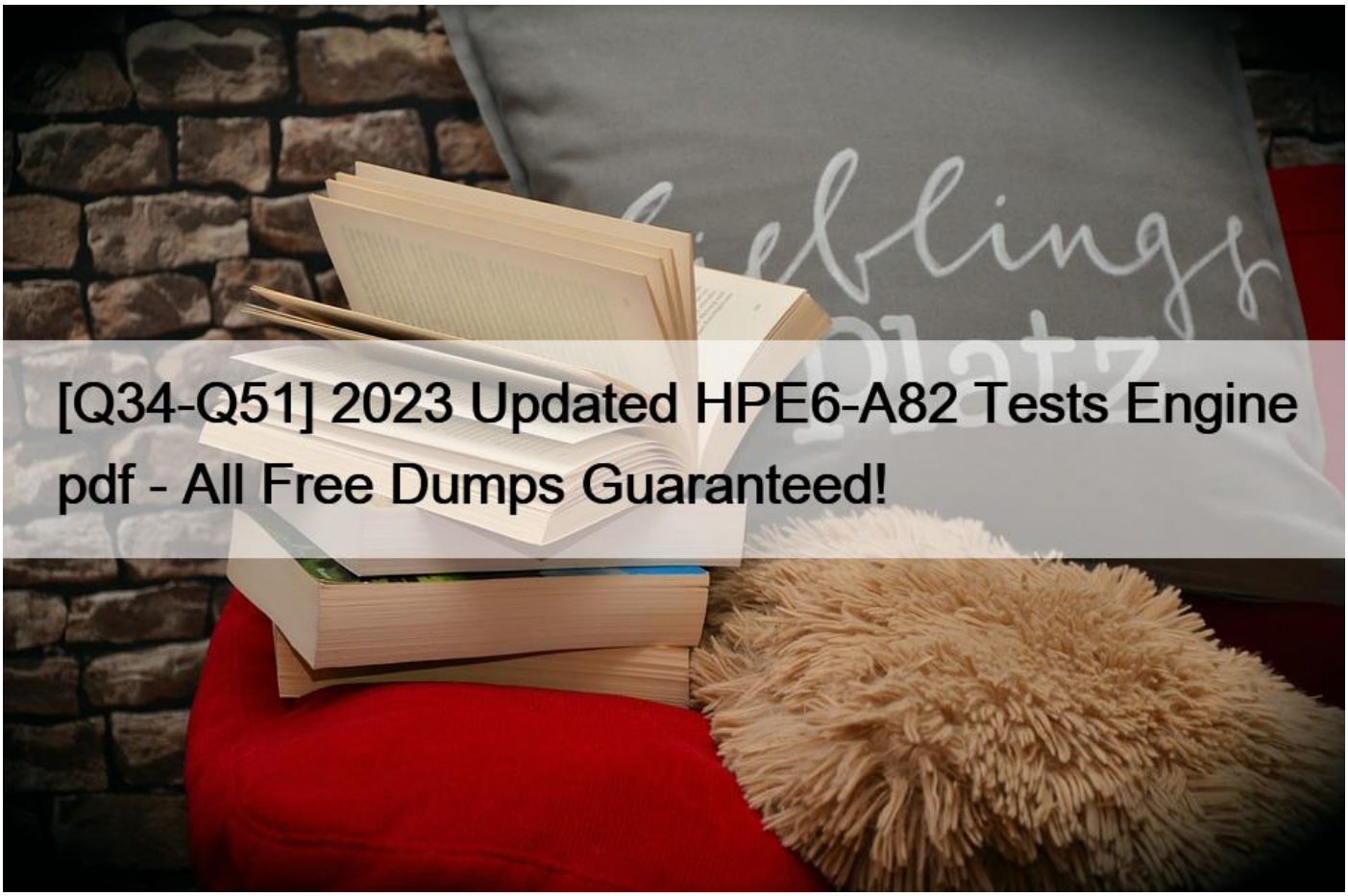
[Q34-Q51 2023 Updated HPE6-A82 Tests Engine pdf - All Free Dumps Guaranteed!



2023 Updated HPE6-A82 Tests Engine pdf - All Free Dumps Guaranteed!
Latest Aruba Certified ClearPass Associate (ACCA) V6.7 HPE6-A82 Actual Free Exam Questions

NO.34 When should a role mapping policy be used in an 802.1x service with Active Directory as the authentication source?
* When you want to match Active Directory attributes directly to an enforcement policy.
* When you want to match Active Directory attributes to an Aruba firewall role on an Aruba Network Access Device.
* When you want to translate and combine Active Directory attributes into ClearPass roles.
* When you want to enable attributes as roles directly without combining multiple attributes.

NO.35 What services are recommended to be allowed by the pre-authenticated role assigned to the Client during the Captive Portal process? (Choose three.)
* HTTPS to the internet
* DHCP options 43 and 150
* DHCP address assignment
* RADIUS to ClearPass
* HTTPS to ClearPass
* DNS resolution

NO.36 Refer to the exhibit.

what will be the enforcement for the user “nell”?
* Corp Secure Contractor
* Allow Full Access
* Secure Corp BYOD Access
* Allow internet Only Access

NO.37 An organization wants guests to be able to create their own guest accounts for access to the public WLAN.

Guests do not want to have to repeatedly log in multiple times through the day.

Which ClearPass feature can meet these requirements?
* ClearPass Onboard Portal.
* Guest access with Media Access Control (MAC) caching.
* Enforcement based on endpoint profiling.
* Guest self-registration with sponsor approval.

NO.38 Which authentication method requires a client certificate?
* EAP-TLS
* Guest self-registration
* PEAP
* MAC Authentication

NO.39 What is true regarding Posturing and Profiling?
* Both Posturing and Profiling describe the same thing, what is the health of the client endpoinst?
* Profiling describes categorizing the user based on their department while Posturing validates the user as authenticated

* Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.
* Profiling is the act of identifying the endpoint type while Posturing is assigning a status as to the health of the endpoint

NO.40 What is an effect of the Cache Timeout setting on the authentication source settings for Active Directory?
* ClearPass will validate the user credentials, then, for the duration of the cache. ClearPass will just fetch account attributes.
* The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the A/D server by caching the credentials
* The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the A/D server by caching the attributes.
* ClearPass will validate the user credentials on the first attempt, then will always fetch the account attributes

NO.41 What is true regarding Posturing and Profiling?
* Both Posturing and Profiling describe the same thing, what is the health of the client endpoinst?
* Profiling describes categorizing the user based on their department while Posturing validates the user as authenticated
* Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.
* Profiling is the act of identifying the endpoint type while Posturing is assigning a status as to the health of the endpoint

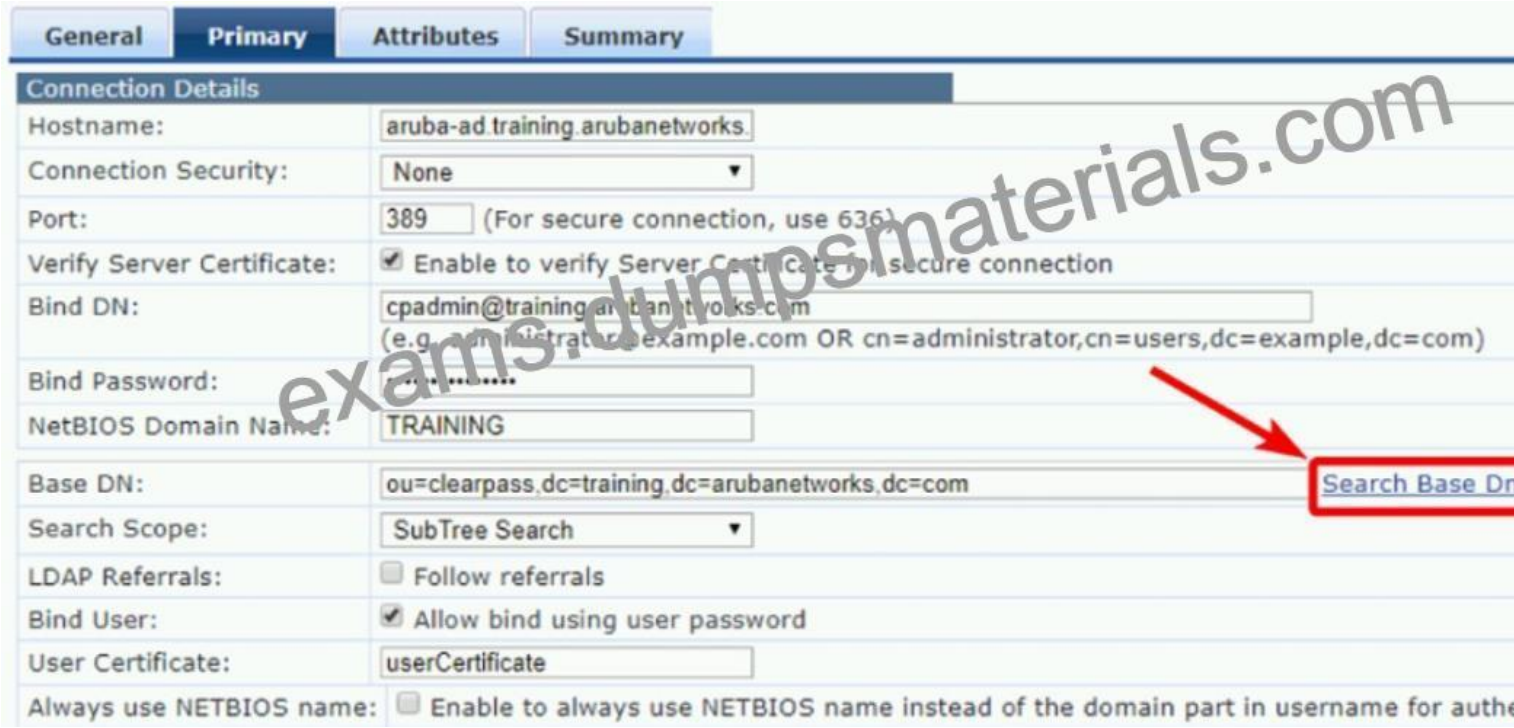
NO.42 What are “Known” endpoints in ClearPass?
* These are endpoints whose beacons have been detected but have never completed authentication
* The label “Known” indicates rogue endpoints labeled as “friendly” or “ignore”
* “Known” endpoints have be fingerprinted to determine their operating system and manufacturer.
* “Known” endpoints can be authenticated based on MAC address to bypass the captive portal login.

NO.43 Refer to the exhibit.

Rank	Field	Type	Label	Description
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
15	**sponsor_email**	text	Sponsor's Email:	Email of the person sponsoring this account.
20	**visitor_name**	text	Your Name:	Please enter your full name.
25	visitor_phone	phone	Phone Number:	Please enter your contact phone number.
30	visitor_company	text	Company Name:	Please enter your company name.
40	**email**	text	Email Address:	Please enter your email address. This will become your username to log into the network.
50	start_time	datetime	Activation Time:	Scheduled date and time at which to enable the account. If blank, the account will be enabled immediately.

What does a bold field indicate?
* The field is currently enabled.
* The field is a non-system field
* The field has been customized
* The field Is required

NO.44 Refer to the exhibit.



What does Starch Base Dn do when joining an Active Directory domain? {Select two.)
* sets the starting point in the directory tree for the Base DN (Distinguished Name) search
* searches for the Base DN (Distinguished Name) based on what was typed in the field
* runs an Active Directory query that returns all results along with any matching the entered Base DN (Distinguished Name)
* validates the connection details entered in the Connection Details
* updates the Base DN (Distinguished Name) in Active Directory if no match is found

NO.45 ClearPass receives fingerprinting profile data for a client device that is based on MAC OUl. NMAP. DHCP, and OnGuard Which fingerprint or fingerprints are used?
* All fingerprints are applied
* The last fingerprint gathered
* NMAP because it is actively obtained
* OnGuard because it is application based

Reference:

ClearPass_Policy_Manager_User_Guide-1.pdf

NO.46 Which authentication method requires a client certificate?
* PEAP
* Guest serf-registration
* EAP-TLS
* MAC Authentication

NO.47 Your boss suggests configuring a guest self-registration page in ClearPass for an upcoming conference event. What are the benefits of using guest serf-registration’? (Select two)
* This strategy effectively stops employees from putting their own corporate devices on the guest network.
* This will enable additional information to be gathered about guests during the conference.

* This allows guest users to create and manage their own login account.
* This will allow employee personal devices to be Onboarded to the corporate network
* This will allow conference employees to pre-load additional device information as guests arrive and register

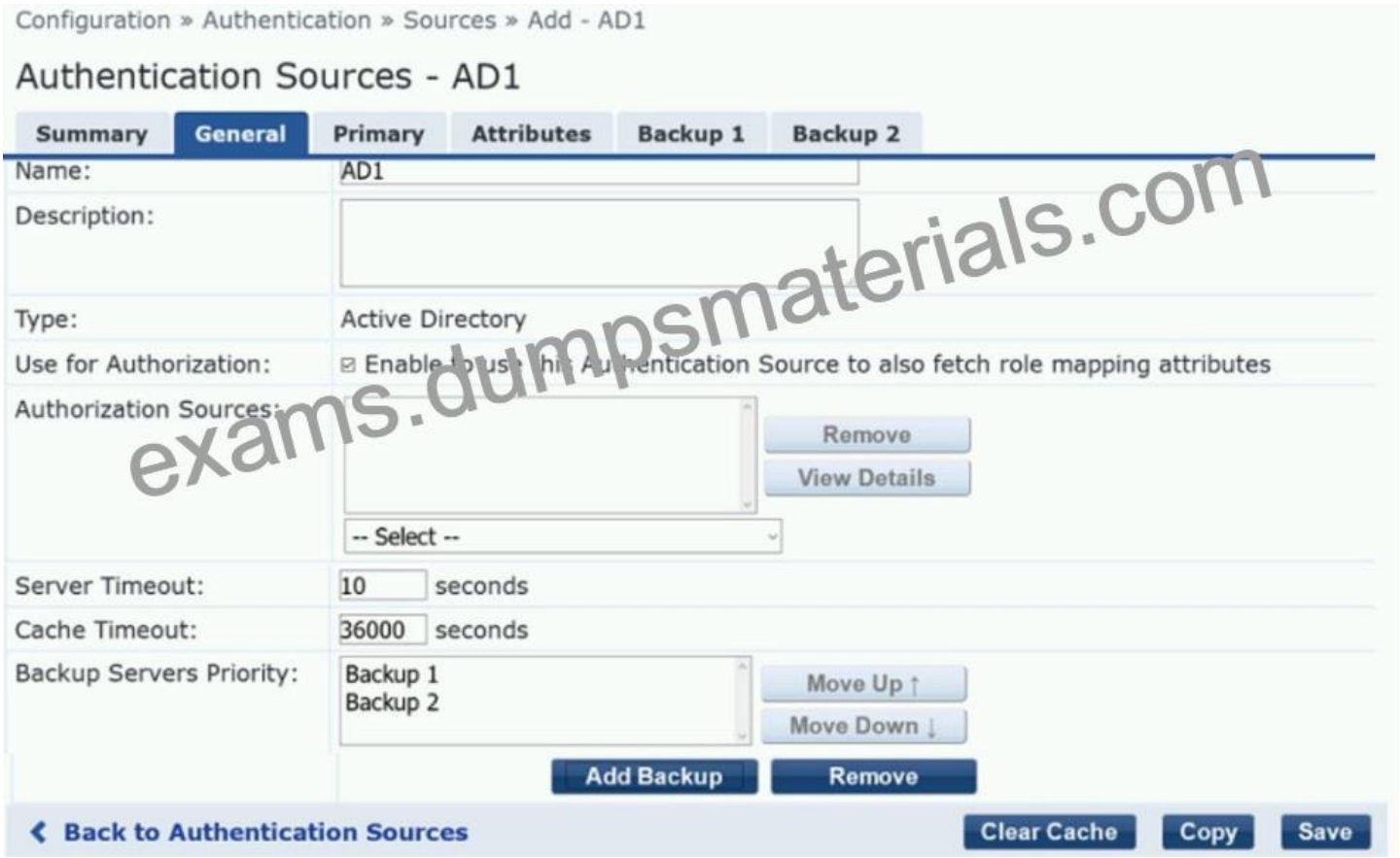
NO.48 What are benefits of using Network Device Groups in ClearPass? (Select two.)
* Allows Service selection rules to match based upon which Network Device Group the Network Access Device (NAD) belongs to
* Network Access Devices (NADs) only require Aruba factory installed certificates to join a Network Device Group
* A Network Access Device is must be discovered by ClearPass prior to be added to a Network Device Group
* Another way to add a customizable “attribute” field to reference when processing authentication requests
* Can apply to both Network Access Devices (NADs) as wen as client machines as a way to filter authentication requests

NO.49 What is RADIUS Change of Authorization (CoA)?
* It allows ClearPass to transmit messages to the Network Attached Device/Network Attached Server (NAD/NAS) to modify a user’s session status
* It allows clients to issue a privilege escalation request to ClearPass using RADIUS to switch to TACACS+
* It is a mechanism that enables ClearPass to assigned a User-Based Tunnel (UBT) between a switch and controller for Dynamic Segmentation
* It forces the client to re-authenticate upon roaming to an access point controlled by a foreign mobility controller.

Explanation

Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGu

NO.50 Refer to the exhibit.



What are two consequences of the Cache Timeout being set to 36000 seconds? (Select two.)
* ClearPass will cache all user and machine attributes from AD every 10 hours in anticipation of one of those users or machines attempting to authenticate.
* Less traffic is required between ClearPass and the AD server when re-authenticating within a 10 hour period.
* The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the AD server by caching user credentials for a 10 hour period.
* A user changing departments may not see their Department attribute change in AD reflected while authenticating until the Cache Timeout period has ended.
* On a failed authentication attempt, ClearPass will consider any subsequent attempts within 10 hours as total failed attempts before blacklisting the client.

NO.51 What needs to be configured for ClearPass use an enforcement rule base on client Data Cap?
* Interim Accounting on the Network Access Device (NAD).
* Enable Active Sessions in ClearPass Guest
* Enable Logging of Accounting Start-Stop packets.
* Make sure the Endpoint Profiling is configured

HP HPE6-A82 Exam Syllabus Topics:

TopicDetailsTopic 1- Configure ClearPass as an authentication server for both corporate users and guestsTopic 2- Device profiling and posture checks- Endpoint Analysis and PostureTopic 3- Overview and Active Directory- Guest and OnboardTopic 4- ClearPass Policy Manager and ClearPass Guest

HPE6-A82 Dumps Updated Practice Test and 61 unique questions:
https://www.dumpsmaterials.com/HPE6-A82-real-torrent.html]