HPE6-A82.VCEplus.premium.exam.60q

Number: HPE6-A82
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

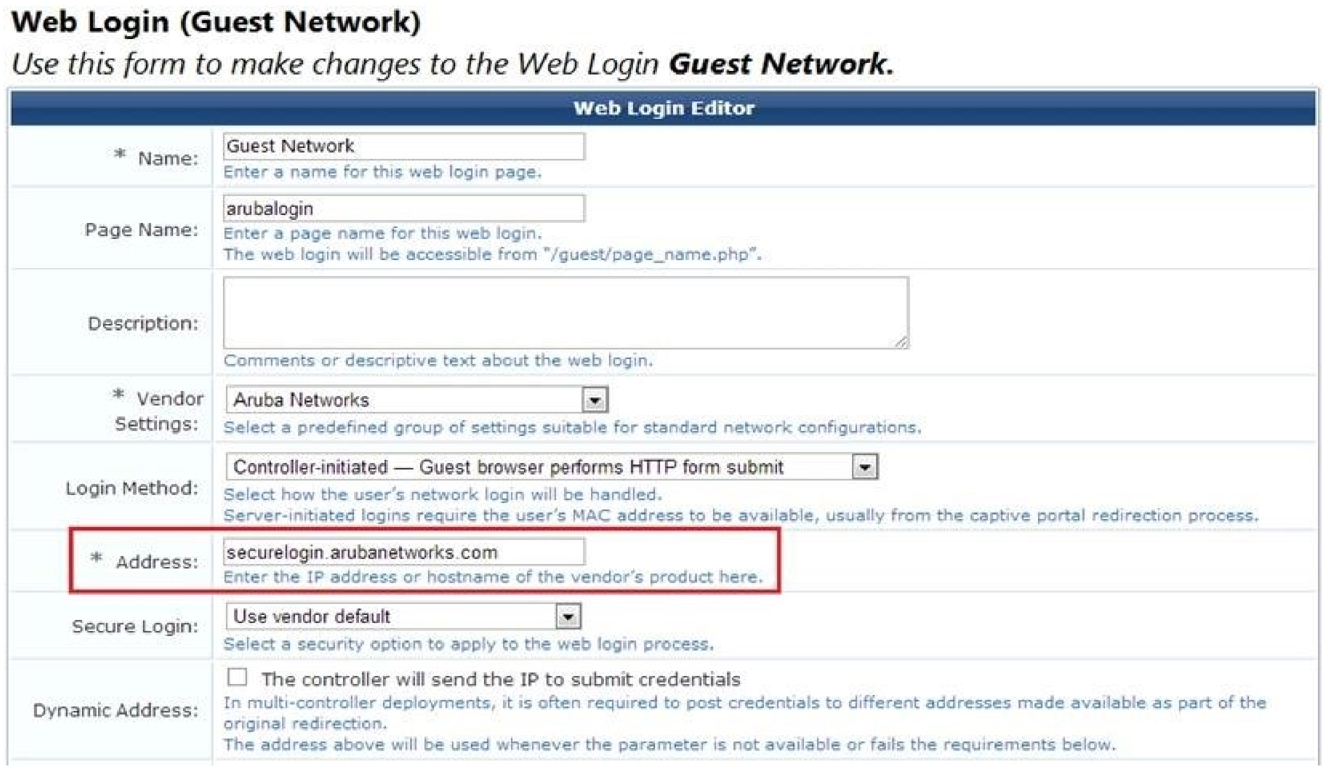
HPE6-A82

Aruba Certified ClearPass Associate

Version 1.0

Exam A

QUESTION 1
Refer to the exhibit.



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 above will be used whenever the parameter is not available or fails the requirements below.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 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? (Choose two.)

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 An organization has configured guest self-registration with internal sponsorship.

Which options can be configured to send guest users their credentials outside of the initial login web-page? (Choose two.)

A. Configure a Simple Mail Transport Protocol (SMTP) server in ClearPass Policy Manager administration.
B. Configure a Simple Mail Transport Protocol (SMTP) server in ClearPass Guest administration.
C. Configure a Short Message Service (SMS) Gateway in ClearPass Policy Manager administration.
D. Configure a Short Message Service (SMS) Gateway under ClearPass Guest configuration.
E. Configure the self-registration page for the guest to receive a Simple Mail Transport Protocol (SMTP) receipt.

Correct Answer: AE
Section: (none)
Explanation

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

QUESTION 4
DRAG DROP

Match the security description to the term that best fits. Options are used only once.

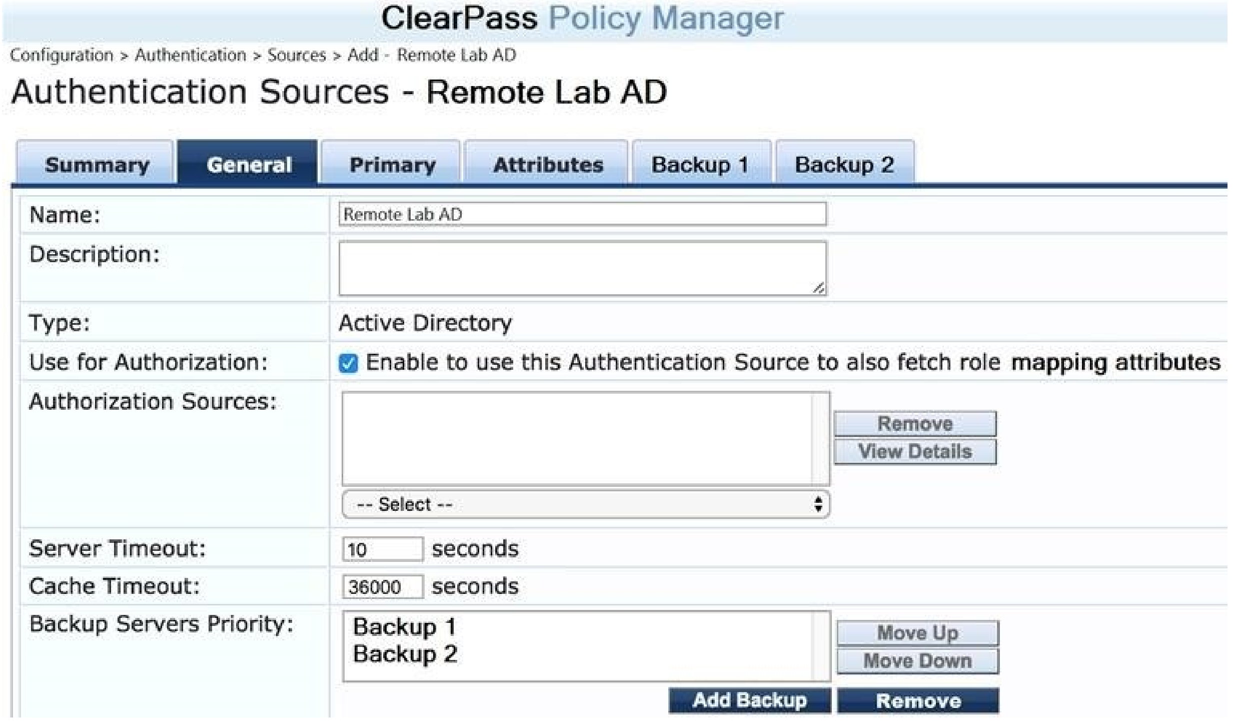
Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Refer to the exhibit.



ClearPass Policy Manager

Configuration > Authentication > Sources > Add - Remote Lab AD

Authentication Sources - Remote Lab AD

Name:	Remote Lab AD
Description:	
Type:	Active Directory
Use for Authorization:	☑ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	Backup 1 Backup 2

A client is attempting to authenticate using their Windows account with a bad password.

If the Remote Lab AD server is down for maintenance, what will be the expected result?

A. ClearPass receives a timeout attempt when trying the Remote Lab AD server first. It will then try the server Backup 1 and receive a result of **Active Directory Authentication failed**. No further processing will occur.
B. ClearPass try either server Backup 1 or Backup 2 depending on which has responded the fastest in prior attempts to authenticate ClearPass will then receive a result of **Active Directory Authentication failed**. No further processing will occur.
C. ClearPass receives a timeout attempt when trying the Remote Lab AD server first. It will then try the server Backup 1 and Backup 2; both will send a result authentication failed.
D. ClearPass receive a timeout attempt when trying the Remote Lab AD server first. No further processing will occur until the Remote Lab AD server is marked as "Down" by the Administrator.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
When ClearPass is communicating with external context servers, which connection protocol is typically used?

A. FTP over SSH
B. REST APIs over HTTPS
C. SOAP and XML
D. YAML

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
ClearPass receives fingerprinting profile data for a client device that is based on MAC OUI, NMAP, DHCP, and OnGuard.

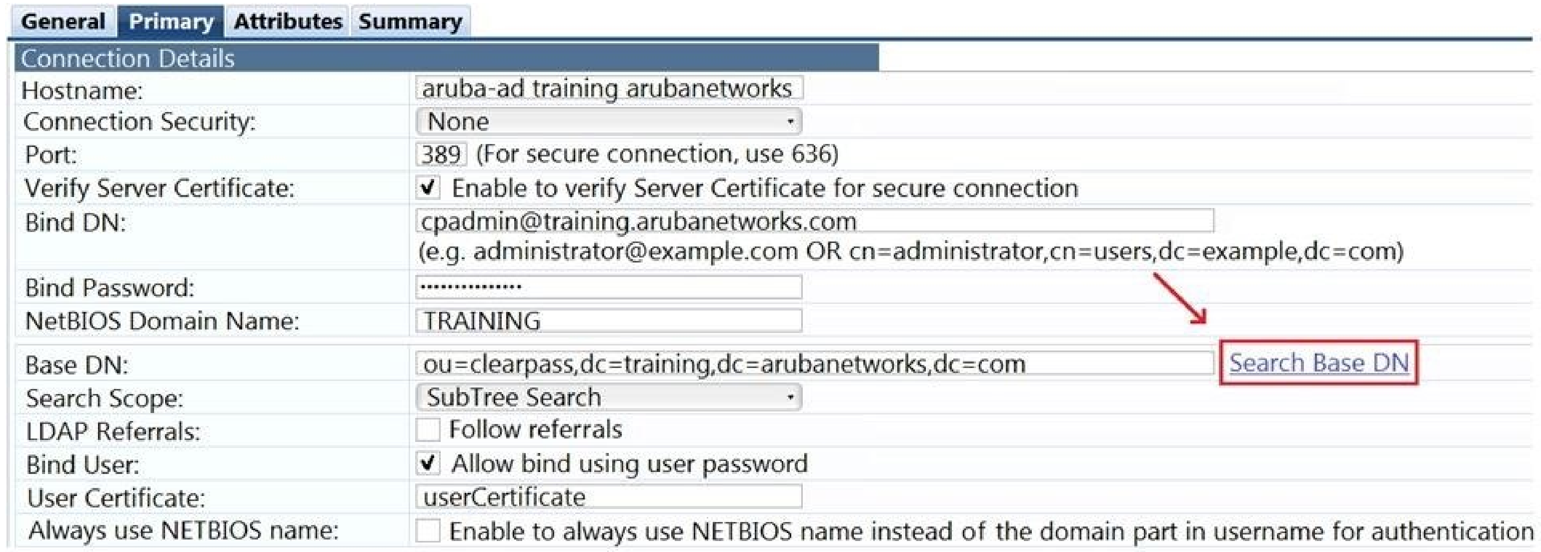
Which fingerprint or fingerprints are used?

A. NMAP because it is actively obtained
B. The last fingerprint gathered
C. OnGuard because it is application based
D. All fingerprints are applied

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.catelsys.eu/images/Catelsys/images/2017/04/0-Notices-ClearPass_Policy_Manager_User_Guide-1.pdf

QUESTION 8
Refer to the exhibit.



General | Primary | Attributes | Summary

Connection Details

Hostname:	aruba-ad training arubanetworks
Connection Security:	None
Port:	389 (For secure connection, use 636)
Verify Server Certificate:	☑ Enable to verify Server Certificate for secure connection
Bind DN:	cpadmin@training.arubanetworks.com (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	················
NetBIOS Domain Name:	TRAINING
Base DN:	ou=clearpass,dc=training,dc=arubanetworks,dc=com Search Base DN
Search Scope:	SubTree Search
LDAP Referrals:	□ Follow referrals
Bind User:	☑ Allow bind using user password
User Certificate:	userCertificate
Always use NETBIOS name:	□ Enable to always use NETBIOS name instead of the domain part in username for authentication

What does **Search Base Dn** do when joining an Active Directory domain? (Choose two.)

A. validates the connection details entered in the Connection Details
B. searches for the Base DN (Distinguished Name) based on what was typed in the field
C. sets the starting point in the directory tree for the Base DN (Distinguished Name) search
D. updates the Base DN (Distinguished Name) in Active Directory if no match is found
E. runs an Active Directory query that returns all results along with any matching the entered Base DN (Distinguished Name)

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.arubanetworks.com/techdocs/ClearPass/6.8/Aruba_DeployGd_HTML/Content/LDAP%20&%20SQL%20Auth%20Sources/LDAP_Auth_Source.htm

QUESTION 9 Which fingerprint collectors can help to distinguish between an iPhone and an iPad? (Choose two.)

A. SNMP
B. IF-MAP
C. MAC OUI
D. TCP header capture
E. HTTP

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
DRAG DROP

Match the correct Profiling Collector with the Collector Type. Collector Types may be used more than once.

Select and Place:

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
Sponsorship has been enabled on the guest network. A guest user connects and completes the self-registration form indicating a valid sponsor. The guest then clicks **submit**.

What is the current state of the guest account?

A. The guest account is created in an enabled state with the "Log In" button functional.
B. The guest account is created in disabled state, the "Log In" button will appear only after the sponsor approval process is completed.
C. The guest account is created in a disabled state with the "Log In" button grayed out.
D. The guest account is not yet created and remains in a disabled state. There is not "Log In" button yet displayed.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 What is the purpose of service rules in ClearPass?

A. selects the Enforcement Profiles used in a service
B. selects the Service to process a request
C. selects the Authentication Source for the client
D. selects the Posture Policy used with OnGuard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 What is a function of the posture token in ClearPass OnGuard? (Choose two.)

A. Identifies clients that are not security compliant.
B. Initiates the Auto-Remediation process.
C. Indicates the Health Status of the Client.
D. Denies access to unhealthy clients.
E. Controls access to network resources.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docplayer.net/18755148-Clearpass-onguard-configuration-guide.html (3)

QUESTION 14 Which ClearPass feature assesses endpoint context and client device type?

A. Profiling
B. Captive Portal
C. Onboard

D. Posture

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/About%20ClearPass/About_ClearPass.htm

QUESTION 15 When should a role mapping policy be used in an 802.1x service with Active Directory as the authentication source?

A. When you want to match Active Directory attributes directly to an enforcement policy.
B. When you want to match Active Directory attributes to an Aruba firewall role on an Aruba Network Access Device.
C. When you want to translate and combine Active Directory attributes into ClearPass roles.
D. When you want to enable attributes as roles directly without combining multiple attributes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 What is a good collector type used for ClearPass to discover devices with static IP addresses?

A. DHCP Collectors
B. ClearPass Air Monitors
C. Active Collectors
D. Network Functions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/PolicyProfile/Collectors.htm

QUESTION 17 When is it appropriate to use the built-in Local user database in ClearPass?

A. In a public-facing guest network environment where the guests are prompted to self-register.
B. In small-business environments where the user accounts rarely change and new accounts are uncommon.
C. In a hospitality deployment for guest accounts created and managed by staff.
D. In a large campus environment where Students and Contractors account for 35.000 entries that change weekly.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_CLI/local-userdb.htm

QUESTION 18
DRAG DROP

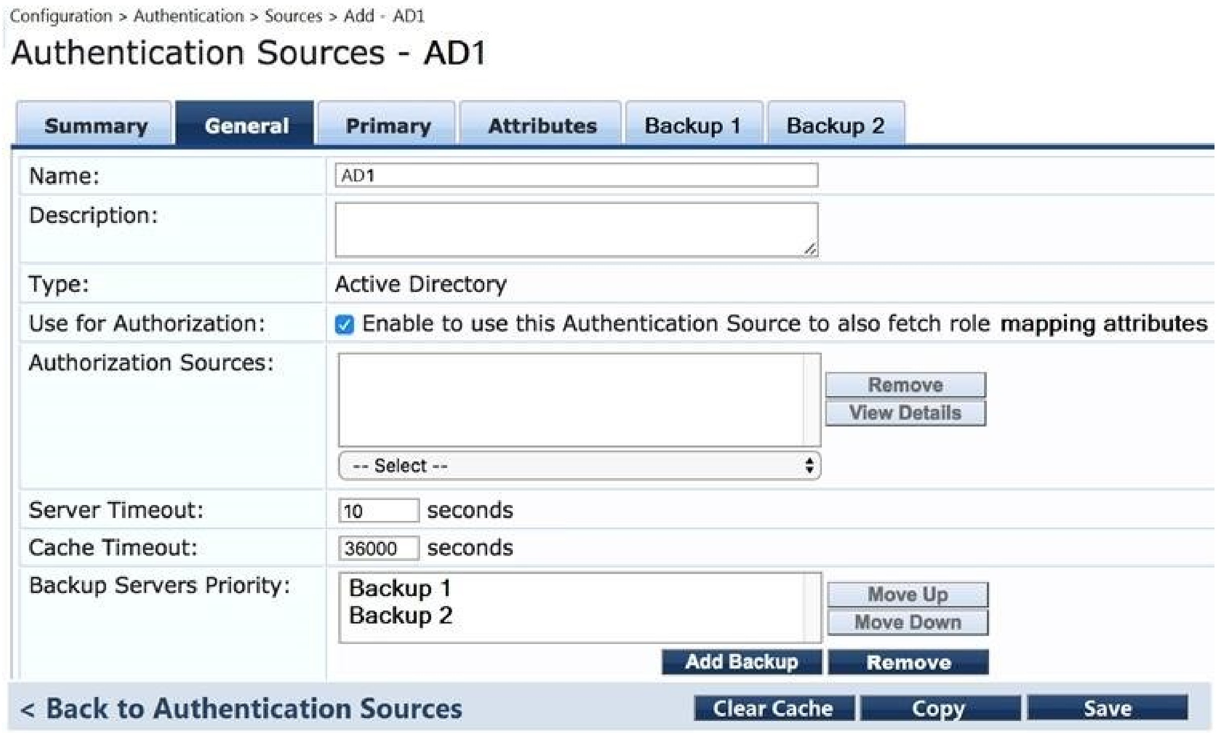
Match the ClearPass system description to the best term. Options are used only once.
Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Refer to the exhibit.



Configuration > Authentication > Sources > Add - AD1

Authentication Sources - AD1

Name:	AD1
Description:	
Type:	Active Directory
Use for Authorization:	☑ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	Backup 1 Backup 2

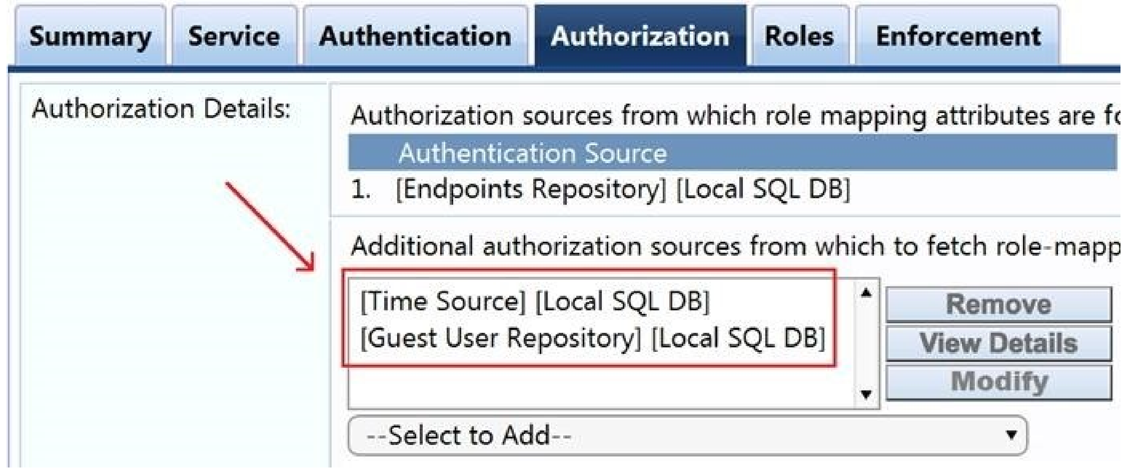
What are two consequences of the Cache Timeout being set to 36000 seconds? (Choose two.)

A. 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.
B. Less traffic is required between ClearPass and the AD server when re-authenticating within a 10 hour period.
C. 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.
D. A user changing departments may not see their Department attribute change in AD reflected while authenticating until the Cache Timeout period has ended.
E. On a failed authentication attempt, ClearPass will consider any subsequent attempts within 10 hours as total failed attempts before blacklisting the client.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Refer to the exhibit.



Authorization Details:

Authorization sources from which role mapping attributes are fe

Authentication Source

1. [Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapp

[Time Source] [Local SQL DB]
[Guest User Repository] [Local SQL DB]

When creating a new ClearPass Service, the **[Time Source]** has been added as an authorization source.

What time source is ClearPass referencing?

A. the ClearPass server where **Insight Master** has been enabled
B. the local clock of the ClearPass server doing the authentication
C. the local time setting found on the authenticating client machine
D. the NTP (Network Time Protocol) source indicated in the Cluster settings

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

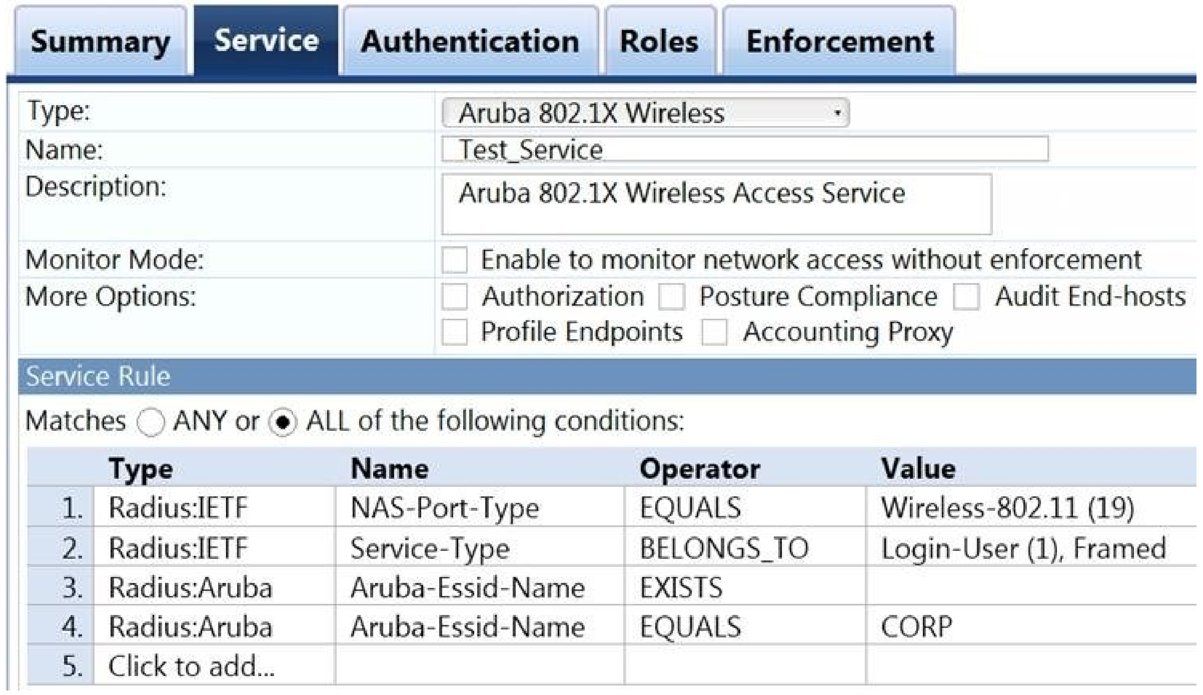
QUESTION 21 What is an effect of the Cache Timeout setting on the authentication source settings for Active Directory?

A. ClearPass will validate the user credentials, then, for the duration of the cache, ClearPass will just fetch account attributes.
B. The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the A/D server by caching the attributes.
C. ClearPass will validate the user credentials on the first attempt, then will always fetch the account attributes.
D. The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the A/D server by caching the credentials.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 22
Refer to the exhibit.



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 Endpoints □ Accounting Proxy

Service Rule

Matches ○ ANY or ● 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 user authentication request will match the service rules of the Policy Service shown?

A. a wireless user connection would fail because of miss-configured service rules
B. a wireless user connected to any SSID named "CORP"
C. a wireless user connecting to any SSID on an Aruba Controller
D. a wireless user connecting to an Aruba IAP on the SSID "CORP"

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 What is the significance of using the **[Allow ALL MAC AUTH]** as an Authentication Method for Guests?

A. Client attempts will fail without an additional Authentication method applied.
B. All clients with unknown endpoints will be granted guest access regardless of authorization.
C. All clients with known endpoints will be granted guest access regardless of authorization.
D. This removes the reliance on the known or unknown status for MAC authentication.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/Instant_UG/Authentication/AuthenticationMethods.htm

QUESTION 24 What is true regarding Posturing and Profiling?

A. Profiling describes categorizing the user based on their department while Posturing validates the user as authenticated.
B. Profiling is the act of identifying the endpoint type while Posturing is assigning a status as to the health of the endpoint.
C. Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.
D. Both Posturing and Profiling describe the same thing; what is the health of the client endpoint?

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

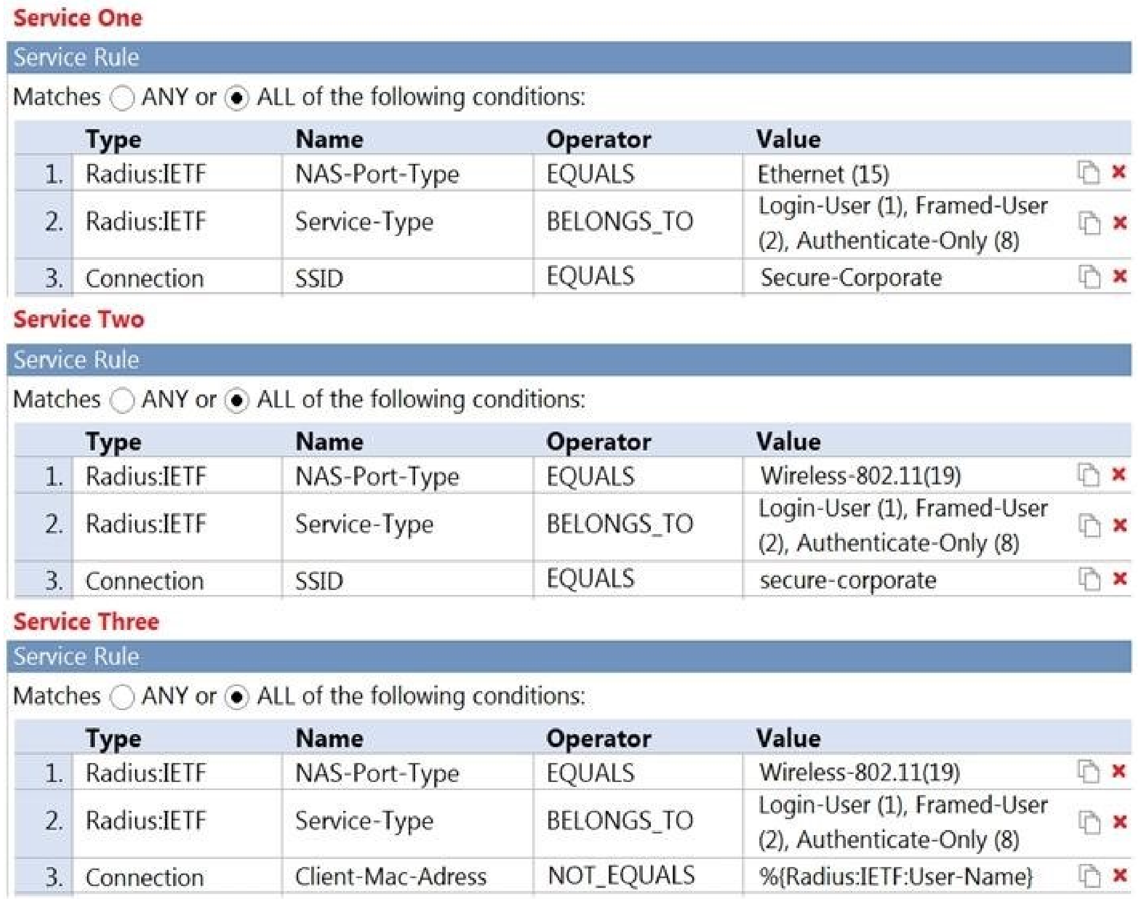
QUESTION 25 Which option supports DHCP profiling for
devices in a network?

A. DHCP profiling is enabled on ClearPass by default; configuration of DHCP relay on the Network Access Device (NAD) is not required.
B. Configuring DHCP relay on ClearPass in order to allow the client to receive DHCP after being profiled.
C. Enabling the DHCP server to profile endpoints and forward the meta-data to ClearPass.
D. Enabling DHCP relay on Network Access Devices (NADs) to forward DHCP requests to ClearPass.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Refer to the exhibit.



Service One

Service Rule

Matches ○ ANY or ● 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 ○ ANY or ● 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 ○ ANY or ● 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-Adress	NOT_EQUALS	%{Radius:IETF:User-Name}

A user connects to an Aruba Access Point wireless SSID named "Secure-Corporate" and performs an 802.1X authentication with ClearPass as the authentication server.

Based on this service configuration, which service will be triggered?
A. No service will be triggered
B. Service Three
C. Service TwoD. Service One

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27 Which two are required to add a Network Access Device (NAD) into ClearPass? (Choose two.)

A. HTTPS certificate
B. NAD IP address
C. ClearPass Admin login credentials
D. Shared Secret
E. SSH password

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 Which configuration options are necessary to add a Network Access Device into the ClearPass Policy Manager? (Choose two.)

A. HTTPS certificate
B. ClearPass Admin Password
C. CLI Console Password
D. NAD IP Address
E. Shared Secret

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 Which must be taken into account if a customer wants to use the DHCP collector with 802.1X authentication?

A. When a client sends an authentication request to ClearPass, the profiler will also gather DHCP information. B. Because DHCP fingerprinted is a Layer-3 function, it cannot be used with an 802.1X authentication service.
C. The client needs to connect to an open network first to be profiled, then shifted to the secure 802.1x network.
D. The client needs to be granted limited access before the enforcement policy can take into account the device type.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 30 Which statement is true about OnGuard? (Choose two.)

A. It is used to ensure that Antivirus/Antispyware programs are running
B. It supports both Windows and Mac OS X clients
C. It is used to identify and remove any malware/viruses

D. It only supports 802.1X authentication

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 Which are valid enforcement profile types? (Choose two.)

A. ClearPass Entity Update Enforcement
B. Aruba Script Enforcement
C. Policy Service Enforcement
D. RADIUS Change of Authorization (CoA)

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 What are "known" endpoints in ClearPass?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 Which option supports DHCP profiling for devices in a network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 34 What is RADIUS Change of Authorization (CoA)?

A. It is a mechanism that enables ClearPass to assigned a User-Based Tunnel (UBT) between a switch and controller for Dynamic Segmentation.
B. It allows clients to issue a privilege escalation request to ClearPass using RADIUS to switch to TACACS+.
C. It allows ClearPass to transmit messages to the Network Attached Device/Network Attached Server (NAD/NAS) to modify a user’s session status.
D. It forces the client to re-authenticate upon roaming to an access point controlled by a foreign mobility controller.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A customer with 677 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. The customer needs to add second guest service in the policy manager for the guest network.
B. The customer needs to add the AD server as an authentication source in a guest service.
C. Employees must be taken to a separate web login page on the guest network.
D. The customer needs to add the AD servers RADIUS certificate to the guest network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 What happens when a client successfully authenticates but does not match any Enforcement Policy rules?

A. A RADIUS reject is returned for the client.
B. A RADIUS Accept is returned with no Enforcement Profile applied.
C. A RADIUS Accept is returned, and the default Enforcement Profile is applied.
D. A RADIUS Accept is returned, and the default rule is applied to the device.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37 Your boss suggests configuring a guest self-registration page in ClearPass for an upcoming conference event.

What are the benefits of using guest self-registration? (Choose two.)

A. This will allow conference employees to pre-load additional device information as guests arrive and register.
B. This strategy effectively stops employees from putting their own corporate devices on the guest network.
C. This will enable additional information to be gathered about guests during the conference.
D. This allows guest users to create and manage their own login account.
E. This will allow employee personal devices to be Onboarded to the corporate network.
Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 Which Authorization Source supports device profile enforcement?

A. Local User Repository
B. OnGuard Repository
C. Endpoints Repository
D. Guest User Repository

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 Which items can be obtained from device profiling?
(Choose three.)

A. Device Category
B. Device Family
C. Device Health
D. Device Type
E. Device Location

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 Which is true regarding the Cisco Device Sensor feature in
ClearPass? (Choose two.)

A. Forwards DHCP and HTTP user-agent info to ClearPass using Control and Datagram Transport Layer Security (DTLS) encapsulation.
B. Requires the purchase of a supported Cisco Access Point licensed as an Aruba Monitor Mode AP, to then act as the sensor.
C. Forwards DHCP and HTTP user-agent info to ClearPass using RADIUS accounting packets.
D. Gathers raw endpoint data from Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).
E. Requires a Cisco Smart Net license to be installed on the Network Access Device (NAD) utilizing the feature.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 Which most accurately describes the "Select All Matches" rule evaluation algorithm in
Enforcement Policies?

A. Each rule is checked, and once a match is found, the Enforcement profile assigned to that rule is applied and the rule matching stops.
B. All rules are checked, and if there is no match, no Enforcement profile is applied.
C. All rules are checked for any matching rules and their respective Enforcement profiles are applied.
D. Each rule is checked, and once a match is found, the Enforcement profile assigned to that rule is applied, along with the default Enforcement profile.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

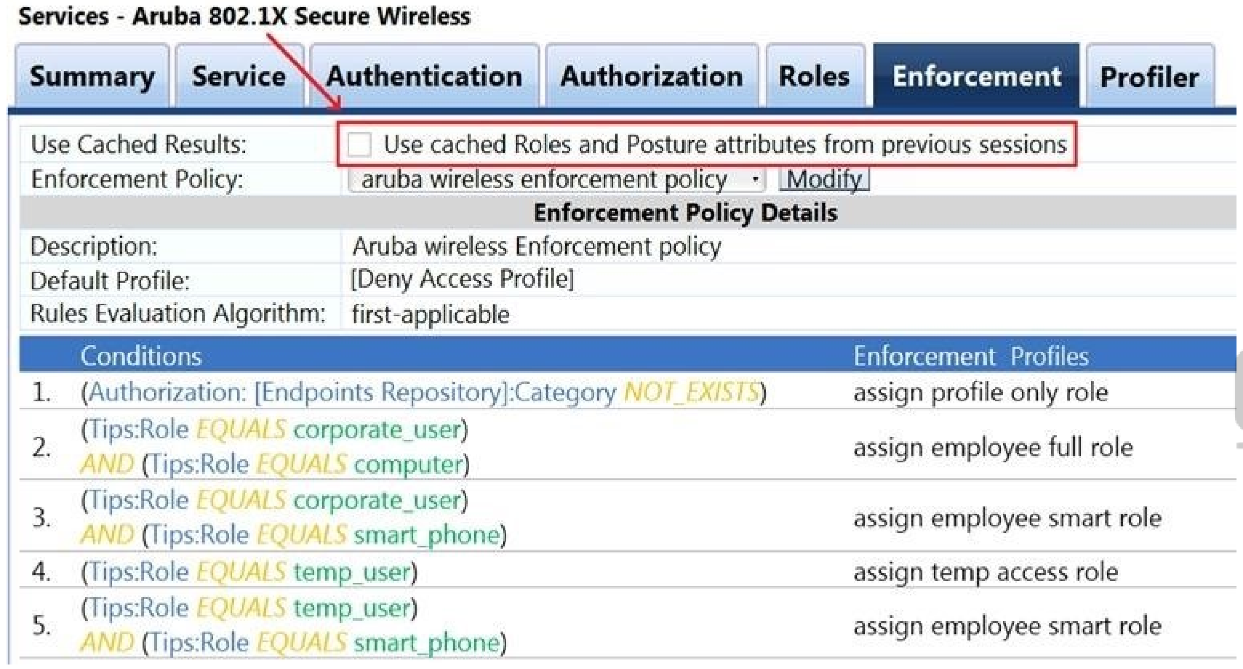
QUESTION 42 When using **Guest Authentication with MAC Caching** service template, which statements are true? (Choose two.)

A. The guest authentication is provided better security than without using MAC caching.
B. The endpoint status of the client will be treated as "known" the first time the client associates to the network.
C. Which wireless SSID and wireless controller must be indicated when configuring the template.
D. The client will be required to re-enter their credentials even if still within the MAC-Auth Expiry term.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Refer to the exhibit.



Services - Aruba 802.1X Secure Wireless

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	aruba wireless enforcement policy

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 NOT_EXISTS)	assign profile only role
2.	(Tips:Role EQUALS corporate_user) AND (Tips:Role EQUALS computer)	assign employee full role
3.	(Tips:Role EQUALS corporate_user) AND (Tips:Role EQUALS smart_phone)	assign employee smart role
4.	(Tips:Role EQUALS temp_user)	assign temp access role
5.	(Tips:Role EQUALS temp_user) AND (Tips:Role EQUALS smart_phone)	assign employee smart role

What is true regarding leaving the indicated option "Use cached Roles and Posture attributes from previous sessions" unchecked?

A. A posture change applied to an endpoint is going to be lost each time the client re-authenticates.
B. The service will make the enforcement decision based upon the updated Posture regardless of caching.
C. Posturing will no longer be evaluated in determining the enforcement policy for current or future sessions.
D. Cached posture results are no longer stored by ClearPass but instead are saved to the endpoint of the client.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 What are benefits of using Network Device Groups in ClearPass? (Choose two.)

A. Network Access Devices (NADs) only require Aruba factory installed certificates to join a Network Device Group.
B. Allows Service selection rules to match based upon which Network Device Group the Network Access Device (NAD) belongs to.
C. A Network Access Device is must be discovered by ClearPass prior to be added to a Network Device Group.

D. Another way to add a customizable "attribute" field to reference when processing authentication requests.
E. Can apply to both Network Access Devices (NADs) as well as client machines as a way to filter authentication requests.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 Which authentication method requires a client certificate?

A. EAP-TLS
B. Guest self-registration
C. PEAP
D. MAC Authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

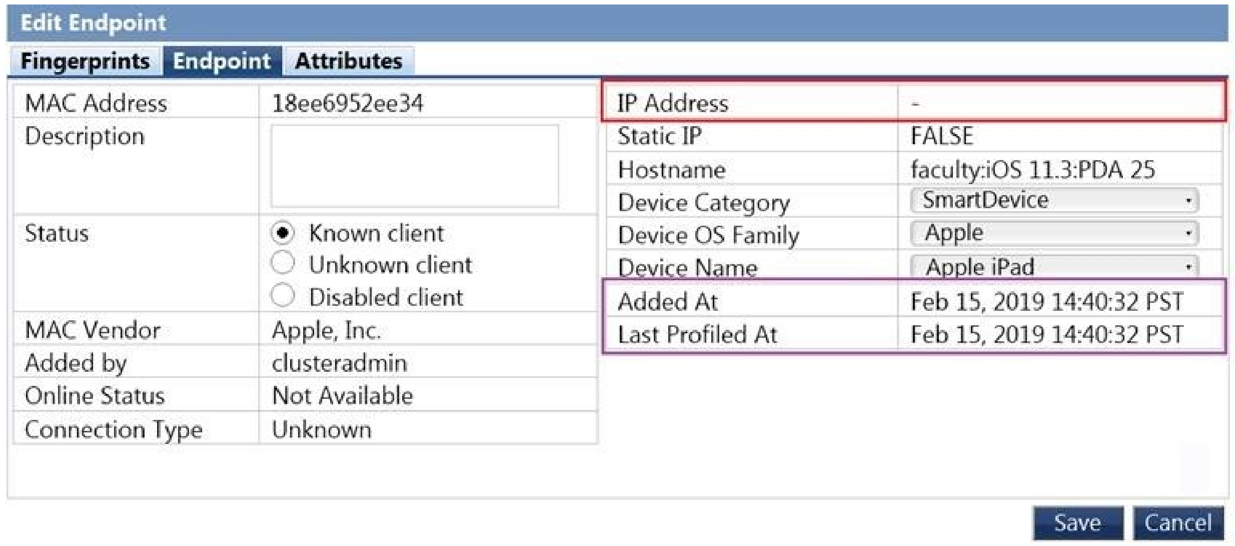
QUESTION 46 What needs to be configured for ClearPass use an enforcement rule base on client Data Cap?

A. Enable Logging of Accounting **Start-Stop** packets.
B. Interim Accounting on the Network Access Device (NAD).
C. Make sure the Endpoint Profiling is configured.
D. Enable Active Sessions in ClearPass Guest

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Refer to the Endpoint in the screenshot.



MAC Address	18ee6952ee34
Description	
Status	● Known client ○ Unknown client ○ Disabled client
MAC Vendor	Apple, Inc.
Added by	clusteradmin
Online Status	Not Available
Connection Type	Unknown

IP Address	-
Static IP	FALSE
Hostname	faculty:iOS 11.3:PDA 25
Device Category	SmartDevice
Device OS Family	Apple
Device Name	Apple iPad
Added At	Feb 15, 2019 14:40:32 PST
Last Profiled At	Feb 15, 2019 14:40:32 PST

What are possible ways that it was profiled? (Choose two.)

A. Exchange Plugging agent
B. NAD ARP listening handler
C. 3rd part MDM
D. DNS fingerprinting
E. Cisco Device Sensor

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48 Aruba self-registration with sponsorship is a solution best applied to which type of network?

A. a large corporate environment with hundreds of contractors requiring wireless access to printers and internet but no other guest access is allowed
B. a chain of auto part stores where employees are assigned mobile devices using a Mobile Device Manager (MDM) and public wireless is available for customers
C. a hotel where hundreds of guests are checked in and out of the building daily that may want access to wireless internet
D. a chain of coffee shops using in a public downtown area with a high amount of guest turnover needing access to public wireless

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

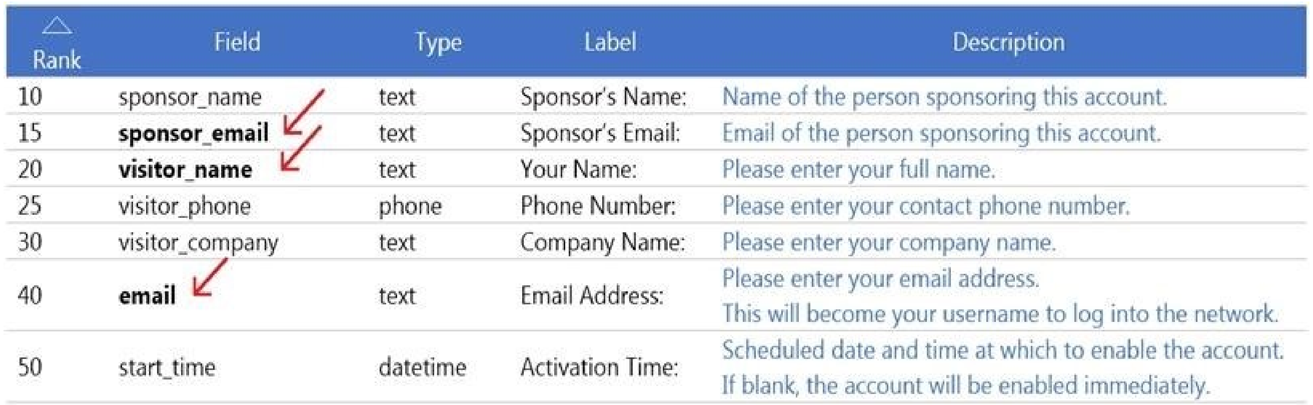
QUESTION 49 When joining ClearPass to an Active Directory (AD) domain, what information is required? (Choose two.)

A. Fully Qualified Domain Name (FQDN) of the AD Domain Controller.
B. ClearPass Policy Manager (CPPM) enterprise credentials.
C. Domain Administrator credentials with at least read access.
D. Cache Timeout value set to at least 10 hours.
E. Domain User credentials with read-write access.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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?

A. The field is a non-system field
B. The field is currently enabled
C. The field has been customized
D. The field is required

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
An organization with 347 employees wants to have the guest create their own accounts for access to the public WLAN, and when guests reconnect, they do not want the guest to have to log in again.

Which ClearPass features can be used to meet these requirements?

A. Guest access with MAC caching
B. Guest self-registration with sponsor approval
C. Enforcement based on endpoint profiling
D. ClearPass Onboard Portal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
What services are recommended to be allowed by the pre-authenticated role assigned to the Client during the Captive Portal process? (Choose three.)

A. DHCP options 43 and 150
B. RADIUS to ClearPass
C. HTTPS to ClearPass
D. HTTPS to the Internet
E. DHCP address assignment
F. DNS resolution

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

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?

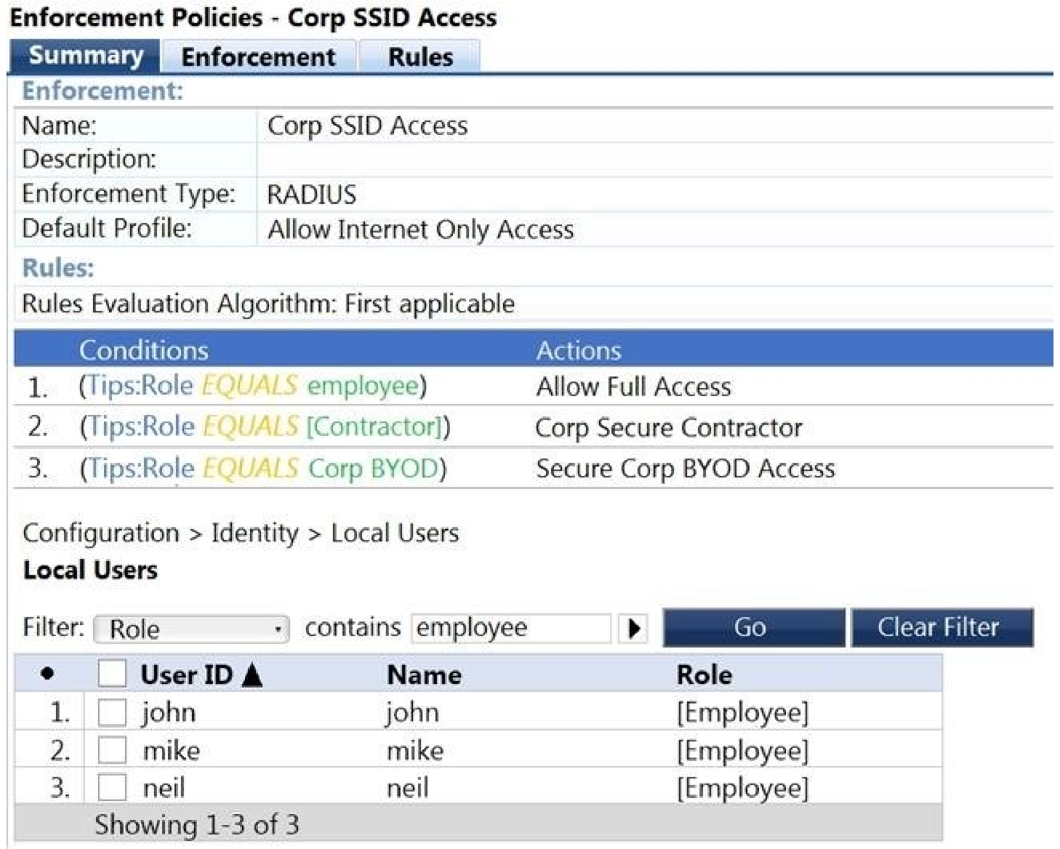
A. ClearPass Onboard Portal.
B. Guest access with Media Access Control (MAC) caching.
C. Enforcement based on endpoint profiling.
D. Guest self-registration with sponsor approval.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

Refer to the exhibit.



Enforcement Policies - Corp SSID Access

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

Configuration > Identity > Local Users

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

What will be the enforcement for the user "neil"?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55 Which actions are necessary to set up a ClearPass guest captive portal web login page to execute with no errors? (Choose two.)

A. Configure the vendor settings in the Web Login page to match the Network Access Device (NAD).
B. Install a publicly signed HTTPS certificate in ClearPass and the Network Access Device (NAD).
C. Install an enterprise Certificate Authority (CA) signed HTTPS certificate in the Network Access Device (NAD).
D. Install an enterprise Certificate Authority (CA) signed HTTPS certificate in ClearPass and the Network Access Device (NAD).
E. Configure the vendor settings in the Network Access Device (NAD) to match the web login page.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56 What is the benefit of installing a wild card certificate for captive portal authentication?

A. Wild card certificates provide greater security than normal certificates.
B. Allows different certificates for each controller for increased security.
C. Guests no longer are required to validate certificates during captive portal.
D. Allows the single wild card certificate to be installed on all controllers in the environment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57 What are two ways to add guest accounts to ClearPass? (Choose two.)

A. Importing accounts from Active Directory once ClearPass is added with Admin credentials.
B. Assigning the default role "Lobby Ambassador to a receptionist to then add the accounts.
C. Using the "Import Accounts" under ClearPass Guest.
D. Using the "Create Account" or "Create Multiple" options under ClearPass Guest.
E. Using the "Sync Accounts" under ClearPass Guest.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 58 Which ClearPass fingerprint collectors are valid for active profiling of endpoints? (Choose two.)

A. HTTP user agents
B. IF-MAP
C. DHCP fingerprinting
D. NMAPE. SNMP

Correct Answer: AE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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. Guest with self-registration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 Which Authorization Source support device profile enforcement?

A. OnGuard Repository
B. Local user Repository
C. Guest User Repository
D. Endpoint Repository

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: