Question: 1

An SNMP probe is sent from ClearPass to a network access device, but ClearPass is unable to obtain profiling information.
What are likely causes? (Select three.)

A. Only SNMP read has been configured but SNMP write is needed for profiling information.
B. An external firewall is blocking SNMP traffic.
C. SNMP is not enabled on the NAD.
D. SNMP community string in the ClearPass and NAD configuration is mismatched.
E. SNMP probing is not supported between ClearPass and NADs.

Answer: B,C,D

Verify firewall port 162 (default) is open between AMP and the controller.
SNMP must be enabled on the NAD.
The community string that ClearPass is using to access the NAD might be wrong.
References: https://community.arubanetworks.com/t5/Monitoring-Management-Location/SNMP-Get-Failed-quot-error-message/ta-p/169774

Question: 2

Which database in the Policy Manager contains the device attributes derived by profiling?

A. Endpoints Repository
B. Client Repository
C. Local Users Repository
D. Onboard Devices Repository
E. Guest User Repository

Answer: A

Configure [Endpoints Repository] as Authorization Source. Endpoint profile attributes
derived by Profile are available through the '[Endpoint Repository]' authorization source.
These attributes can be used in role-mapping or enforcement policies to control network
access. Available attributes are:
Authorization:[Endpoints Repository]:MAC Vendor
Authorization:[Endpoints Repository]:Category
Authorization:[Endpoints Repository]:OS Family
Authorization:[Endpoints Repository]:Name
References: ClearPass Profiling TechNote (2014), page 29
https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf

Question: 3

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
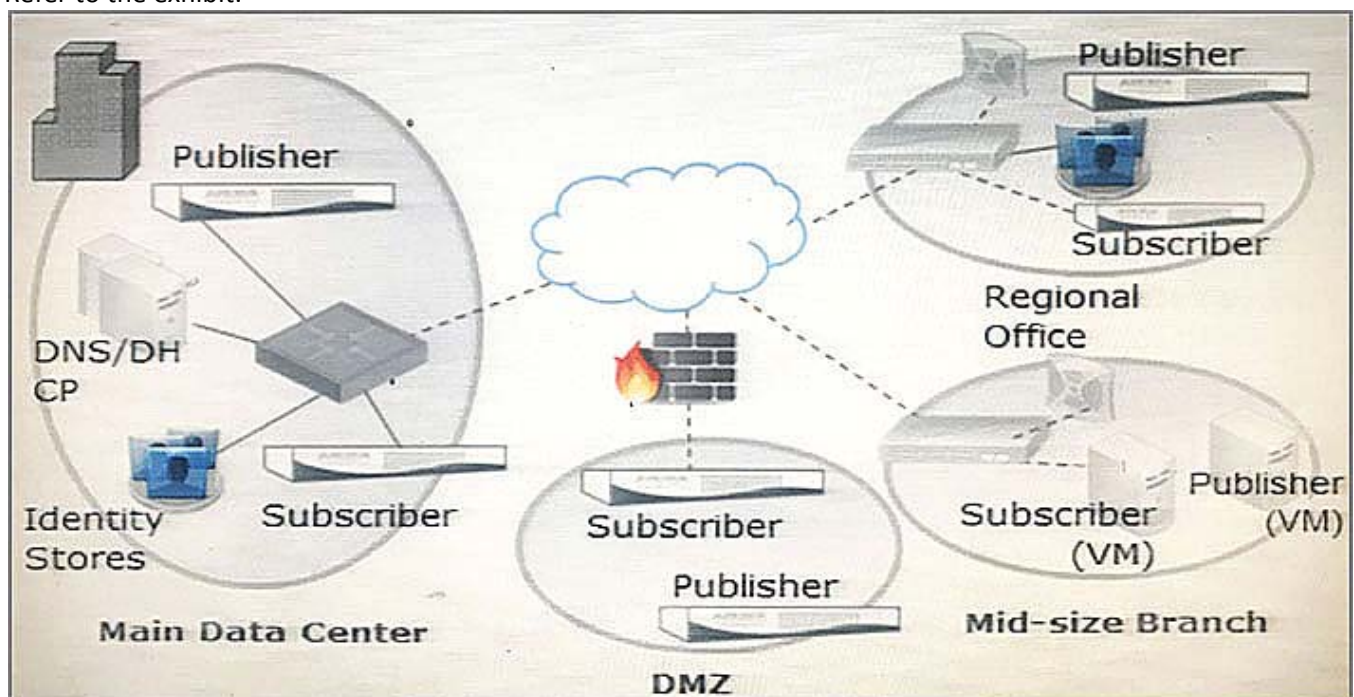E. Local User repository

Answer: A

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 send 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%20 Profiling%20TechNote.pdf

Question: 4

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

References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deployment/Design_guidelines.htm

Question: 5

Refer to the exhibit.

Administration » Server Manager » Server Configuration

Server Configuration

Cluster-Wide Parameters			⊗

General	Cleanup Intervals	Notifications	**Standby Publisher**	Virtual IP Configuration

Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	TRUE ▼	FALSE
Designated Standby Publisher	cp82.clearpass ▼	0
Failover Wait Time	10 ▼ minutes	10

Restore Defaults   Save   Cancel

Which statements accurately describe the cp82 ClearPass node? (Select two.)

A. It becomes the Publisher when the primary Publisher fails.
B. It operates as a Publisher in the same cluster as the primary Publisher when the primary is active.
C. It operates as a Publisher in a separate cluster when the Publisher is active.
D. It operates as a Subscriber when the Publisher is active.
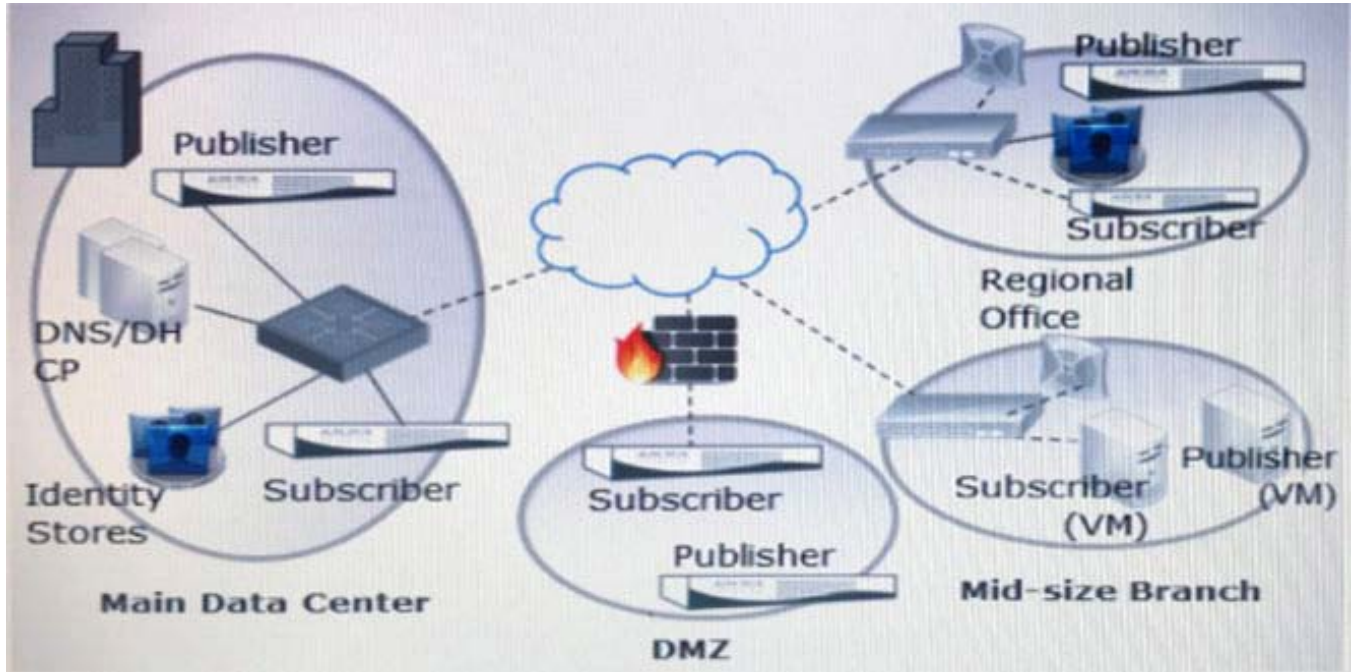E. It stays as a Subscriber when the Publisher fails.

Answer: A,D

ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.
When a Publisher failure is detected, the designated subscriber node is promoted to active Publisher status.

References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deployment/Standby_publisher.htm

Question: 6

Refer to the exhibit.

A customer wants to enable Publisher redundancy.
Based on the network topology diagram shown, which node should the network administrator configure as the standby Publisher for the Publisher in the main data center?

A. Subscriber in the main data center
B. Publisher in the regional office
C. Any of the other three Publishers
D. Publisher in the mid-size branch
E. Publisher in the DMZ

Answer: A

ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.
References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deployment/Standby_publisher.htm

Question: 7

A customer wants to implement Virtual IP redundancy, such that in case of a ClearPass server outage, 802.1x authentications will not be interrupted. The administrator has enabled a single Virtual IP address on two ClearPass servers.
Which statements accurately describe next steps? (Select two.)

A. The NAD should be configured with the primary node IP address for RADIUS authentication on the 802.1x network.
B. A new Virtual IP address should be created for each NAD.
C. Both the primary and secondary nodes will respond to authentication requests sent to the Virtual IP address when the primary node is active.
D. The primary node will respond to authentication requests sent to the Virtual IP address when the primary node is active.
E. The NAD should be configured with the Virtual IP address for RADIUS authentications on the 802.1x network.

Answer: D,E

In an Aruba network, APs are controlled by a controller. The APs tunnel all data to the controller for processing, including encryption/decryption and bridging/forwarding data. Local controller redundancy provides APs with failover to a backup controller if a controller becomes unavailable. Local controller redundancy is provided by running VRRP between a pair of controllers. The APs are then configured to connect to the "virtual-IP" configured for the VRRP instance.
References: http://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VRRP/Redundancy_Parameters.htm

Question: 8

ClearPass and a wired switch are configured for 802.1x authentication with RADIUS CoA (RFC 3576) on UDP port 3799. This port has been blocked by a firewall between the wired switch and ClearPass.
What will be the outcome of this state?

A. RADIUS Authentications will fail because the wired switch will not be able to reach the ClearPass server.
B. During RADIUS Authentication, certificate exchange between the wired switch and ClearPass will fail.
C. RADIUS Authentications will timeout because the wired switch will not be able to reach the ClearPass server.
D. RADIUS Authentication will succeed, but Post-Authentication Disconnect-Requests from ClearPass to the wired switch will not be delivered.
E. RADIUS Authentication will succeed, but RADIUS Access-Accept messages from ClearPass to the wired switch for Change of Role will not be delivered.

Answer: D

Question: 9

Which statement accurately describes configuration of Data and Management ports on the ClearPass appliance? (Select two.)

A. Static IP addresses are only allowed on the management port.
B. Configuration of the data port is mandatory.
C. Configuration on the management port is mandatory.
D. Configuration of the data port if optional.
E. Configuration of the management port is optional.

Answer: C,D

The Management port (ethernet 0) provides access for cluster administration and appliance maintenance using the WebUI, CLI, or internal cluster communication. This configuration is mandatory.
The configuration of the data port is optional. If this port is not configured, requests are redirected to the Management port.
References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/1%20About%20ClearPass/Hardware_Appliance.htm

Question: 10

Which licenses are included in the built-in Starter kit for ClearPass?

A. 10 ClearPass Guest licenses, 10 ClearPass Onguard licenses and 10 ClearPass Onboard licenses
B. 25 ClearPass Profiler licenses
C. 25 ClearPass Enterprise licenses
D. 10 ClearPass Enterprise licenses
E. 25 ClearPass Redundancy licenses

Answer: C

All CPPM's comes bundled with 25 Enterprise application licenses so you can test the functionality of the Applications as this license can be used for any of them.
References: http://community.arubanetworks.com/t5/Security/ClearPass-licensing-explained-August-MHC/td-p/195719

Question: 11

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: 12

A customer would like to deploy ClearPass with these requirements:
every day, 100 employees need to authenticate with their corporate laptops using EAP-TLS
every Friday, a meeting with business partners takes place and an additional 50 devices need to authenticate using Web Login Guest Authentication
What should the customer do regarding licenses? (Select two.)

A. When counting policy manager licenses, include the additional 50 business partner devices.
B. When counting policy manager licenses, exclude the additional 50 business partner devices.
C. Purchase Onboard licenses.
D. Purchase guest licenses.
E. Purchase Onguard licenses.

Answer: A,C