DUMPSBOSS.

Aruba Certified Mobility Professional Exam

HP HPE6-A71

Version Demo

Total Demo Questions: 22

Total Premium Questions: 224

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Fundamentals	2
Topic 2, WLAN Design	6
Topic 3, WLAN Implementation	78
Topic 4, WLAN Security	68
Topic 5, WLAN Operations	70
Total	224

QUESTION NO: 1

An administrator creates an AirGroup service rule to control access to shared AirPrint printers and Apple TV devices.

Which criteria can the administrator use to limit service visibility and access? (Choose two.)

A. User role

B. AP-based location

C. Controller serial number

D. RADIUS shared secret

E. AP radio transmit power

ANSWER: A B

Explanation:

AirGroup service rules can use **user-role-based criteria** to control which authenticated users are allowed to discover or use a service. This allows access to shared services to be determined by the policy assigned to a user rather than only by IP subnet membership.

AirGroup rules can also use **location-based criteria**. Location controls can limit service discovery and sharing to an appropriate physical scope, such as a particular AP group, AP name, or AP Fully Qualified Location Name. This helps prevent users in one building or floor from discovering services intended for another area.

Aruba documents service-rule controls in the ArubaOS AirGroup service rules documentation.

QUESTION NO: 2

Refer to the exhibit.

```
DR-mode) *#show switches
All Switches
-----------------
IP Address IPv6 Address    Name   Location  Type Model  Version  Status   Configuration State

---------                                    ----        ----     ---------

10.17.169.71  2001::1      A7030  Building1  MD  Aruba7030    8.0.1.0_57204  up

CONFIG DISASTER RECOVERY

Total Switches: 1
```

What is true about the operation of the Aruba Mobility Controller (MC) shown in the exhibit?

A. The Mobility master is in disaster recovery mode and will push changes to a Managed Controller.

B. The disaster recovery mode is enabled, and no changes will be forwarded to the Mobility Master.

C. The disaster recovery mode is disabled, and changes will be sent to the Mobility Master.

D. The disaster recovery mode is enabled, and changes will be sent to the Mobility Master.

ANSWER: D

Explanation:

The disaster recovery mode is enabled, and changes will be sent to the Mobility Master. In an ArubaOS 8 controller deployment, disaster recovery mode enables a managed device to retain and process configuration changes locally during a

Mobility Master connectivity failure. This provides operational continuity: administrators can make necessary changes on the managed controller even when the centralized management connection is unavailable. The managed controller records those changes in its local configuration database and, when communication with the Mobility Master is available, synchronizes the changes upstream so that the centralized configuration state is updated. The exhibit indicates that disaster recovery mode is enabled; therefore, the controller is operating with this local-change and synchronization capability. This behavior is particularly important for geographically distributed deployments, where temporary WAN or management-path failures should not prevent essential controller administration. Aruba's documentation describes disaster-recovery operation as allowing managed devices to continue configuration activity and synchronize the resulting configuration with the Mobility Master. See the ArubaOS Disaster Recovery documentation and the Aruba Mobility Master documentation.

QUESTION NO: 3

An AP connects to a controller. Then, the AP loses power and reboots.

Which parameters will the AP remember and use from its initial connection? (Select two.)

A. AP group

B. Server IP

C. AP IP address and subnet mask

D. Mobility Master IP

E. AirWave server name

ANSWER: B C

Explanation:

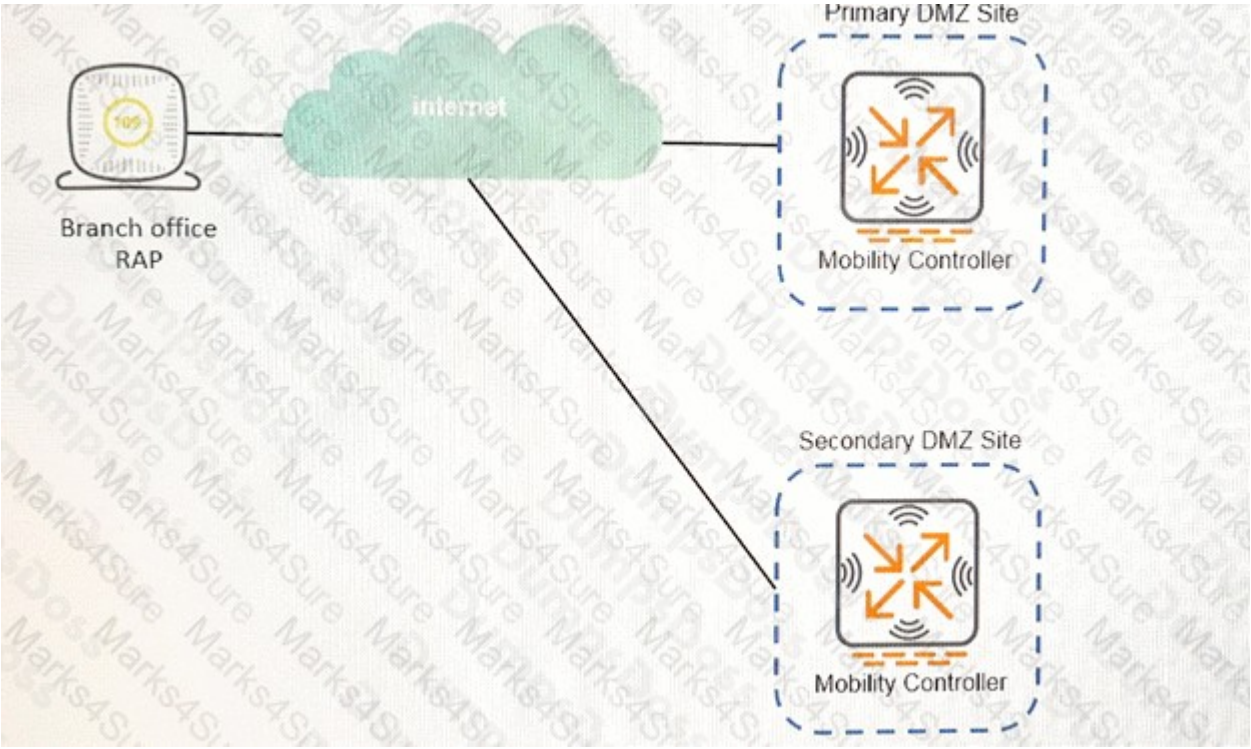
An Aruba campus AP retains information that helps it re-establish connectivity after a reboot rather than requiring a completely new discovery process every time. The **Server IP** is the address of the controller/managed device to which the AP previously established its secure control connection. The AP can use this stored address as a previously known controller target during subsequent startup and discovery processing.

The AP also retains its **AP IP address and subnet mask** as network bootstrap information. Retaining the prior network addressing information allows the AP to continue using its established management-network identity when applicable and supports recovery if it cannot immediately obtain fresh network parameters. This information is part of the AP's persistent provisioning/bootstrap state and is intended to make restart behavior more reliable.

Aruba's AP discovery documentation describes previously known controller information as one of the mechanisms available to an AP when reconnecting to the network. Aruba documentation also covers AP provisioning and the persistent network parameters used by APs during bootstrapping. See the ArubaOS AP Discovery documentation and the ArubaOS AP Provisioning documentation.

QUESTION NO: 4

Refer to the exhibit.



An administrator supports a RAP at a branch office shown in the exhibit. The company has one Mobility Controller (MC) at the Primary DMZ site and one at the Secondary DMZ site. The RAP is configured to connect to only the MC at the Primary DMZ site. A network outage with the ISP at the Primary DMZ site causes the RAP to reboot. Upon reboot, the RAP cannot build a tunnel to the Secondary DMZ site MC because the administrator forgot to add the Second LMS IP address to the AP Group configuration. Once the RAP can successfully connect, the administrator can add the Secondary DMZ MC as a backup LMS to fix the AP Group.

What should the administrator implement to allow the RAP to connect to the MC at the Secondary DMZ site while the outage at the primary site persists?

A. Dynamic discovery through DHCP Option 43

B. Static configuration from apboot mode

C. Dynamic discovery through DHCP Option 60

D. Dynamic discovery through multicast ADP

ANSWER: B

Explanation:

Static configuration from apboot mode is correct because it provides an immediate, out-of-band recovery method for directing the RAP to a reachable Mobility Controller when its normal controller discovery and AP-group configuration cannot be used. In this situation, the RAP has rebooted while the configured primary LMS is unavailable, and it cannot obtain the missing backup LMS setting because that configuration resides on the controller it cannot currently reach. Accessing the AP boot environment allows the administrator to statically set the controller/master information to the Secondary DMZ Mobility Controller. The RAP can then establish its secure tunnel to that reachable controller and receive its managed configuration. After connectivity is restored, the administrator can correct the AP system profile by configuring the secondary controller as the backup LMS, providing resilient controller failover for subsequent reboots or primary-site outages. Aruba documents that RAPs establish secure connections to managed devices and are centrally configured after connecting; boot-environment settings are useful when normal managed configuration cannot be reached. See the ArubaOS RAP documentation at ArubaOS Remote Access Points and the Aruba support documentation portal at Aruba Support Services.

QUESTION NO: 5

Refer to the exhibit.

Cluster Load Distribution for Aps

Type	IPV4 Address	Active Aps	Standby Aps
peer	10.1.10.101	131	176
peer	10.1.10.102	153	142
self	10.1.10.100	204	103
peer	10.1.10.103	112	179

Total: Active Aps 600 Standby Aps 600

An administrator sets up a cluster of Aruba Mobility Controllers (MCs). What can the administrator determine about the cluster from the command output shown in the exhibit?

A. AP load balancing is enabled.

B. User load balancing is enabled.

C. This is an L2-connected cluster.

D. This is an L3-connected cluster.

ANSWER: B

Explanation:

User load balancing is enabled. The displayed cluster status/configuration output indicates that client or user load balancing is active for the Mobility Controller cluster. In an ArubaOS controller cluster, user load balancing allows the cluster to distribute wireless client workload among cluster members rather than having a controller become disproportionately loaded. The controllers exchange cluster and client-load information so that an access point can be directed to establish a client's tunnel on a suitable cluster member. This supports more consistent controller resource utilization and helps the cluster scale as client demand changes.

Aruba distinguishes user load balancing from access-point load balancing because they control different allocation decisions. User load balancing concerns the controller selected to terminate or handle a wireless client session, and its enabled state is directly identified by the user/client load-balancing setting shown in the command output. ArubaOS cluster configuration and operational verification are documented in the ArubaOS cluster overview and the ArubaOS show lc-cluster CLI reference.

QUESTION NO: 6

A branch office location has two buildings: an office and a small warehouse that are within 20 meters of each other. A RAP at the branch office provides connectivity to the corporate office network. This RAP is also configured as a Remote Mesh Portal (RMP).

Which solution should the administrator implement to provide connectivity between the office and small warehouse buildings at the branch office location?

A. Deploy a Remote Mesh Portal in the warehouse building to connect to the Remote Mesh Portal in the office building.

B. Deploy a Remote Mesh Point AP in the warehouse building to connect to the Remote Mesh Portal in the office building.

C. Deploy an ArubaOS-Switch in the warehouse building with tunneled node to connect to the Remote Mesh Portal in the office building.

D. Deploy a Mesh Point AP in the warehouse building to connect to the Remote Mesh Portal in the office building.

ANSWER: B

Explanation:

Deploy a Remote Mesh Point AP in the warehouse building to connect to the Remote Mesh Portal in the office building. Aruba remote mesh extends connectivity at a remote site where installing a wired uplink between locations is impractical. In this design, the RAP in the office is configured as the Remote Mesh Portal and provides the upstream path through its established connection to the corporate network. A Remote Mesh Point in the warehouse establishes a wireless mesh backhaul to that portal, allowing clients and wired devices at the warehouse to reach the corporate network through the RAP tunnel.

The two buildings being only 20 meters apart makes a short-range outdoor or building-to-building wireless mesh link practical, subject to suitable radio placement, RF coverage, and line-of-sight considerations. The Remote Mesh Point role is specifically intended to join a Remote Mesh Portal; after joining, it can provide local access while forwarding traffic over the remote mesh link. Aruba documents the Remote Mesh Portal and Remote Mesh Point roles as the components used for remote mesh deployments in its ArubaOS Remote Mesh documentation.

QUESTION NO: 7

An administrator wants to implement 802.1X authentication on Ethernet ports on branch office controllers.

What must the administrator do to implement this policy?

A. Define the port as untrusted, and assign an AAA policy to the port.

B. Define the port as trusted, and assign an AAA policy to the port.

C. Define the port as untrusted, and assign an AAA policy to the VLAN.

D. Define the port as trusted, and assign an AAA policy to the VLAN.

ANSWER: A

Explanation:

Define the port as untrusted, and assign an AAA policy to the port. On an Aruba branch controller, wired client-facing interfaces must be configured as untrusted when the controller is expected to apply user authentication and access-control policy to devices connected through those interfaces. The AAA policy applied directly to the Ethernet port supplies the authentication behavior for that port, including the 802.1X method and the associated authentication-server and role-assignment processing. When a wired endpoint connects, the controller can therefore act as the authenticator, relay the client's credentials to the configured authentication service, and enforce the resulting user role after successful authentication.

This is a per-interface requirement because 802.1X port access control is evaluated at the physical access port where the supplicant connects. Configuring the access port as untrusted ensures that client traffic is handled under the controller's AAA controls rather than being treated as traffic arriving from an already trusted network device. Aruba's wired-access documentation describes assigning AAA profiles to Ethernet interfaces for wired authentication and using interface trust settings to control how connected devices are handled. See the ArubaOS wired AAA documentation and the ArubaOS AAA profile documentation.

QUESTION NO: 8

A company opens a new branch office and a RAP is used to connect to a corporate office Aruba Mobility Controller (MC). The company needs to provide connectivity to the office across the street. There is an AP across the street. However, there is no wired connectivity between the buildings.

Which actions can the administrator select to provide the required connectivity? (Choose two.)

A. Provision all Aps at the branch office as Mesh Points.

B. Provision all Aps at the branch offices as Mash Portals.

C. Implement one of the Aps as a Mesh Point.

D. Provision the RAP as a Mesh Portal.

E. Implement two mesh clusters.

ANSWER: C D

Explanation:

Provision the RAP as a Mesh Portal and implement one of the APs as a Mesh Point to extend connectivity across the street without installing a wired link between the buildings. In an Aruba mesh deployment, a mesh portal is the mesh AP with a wired network path and controller connectivity. Here, the RAP already provides the branch's connection through its WAN tunnel to the corporate Mobility Controller, so it can serve as the wired-side anchor for the mesh network. The AP in the other building can then be configured as a mesh point and establish a wireless mesh backhaul link to that portal. Client traffic at the remote AP is carried across the wireless mesh link to the RAP and then through the RAP tunnel toward corporate resources. This design uses the existing RAP connection while providing a practical building-to-building extension. Aruba's mesh documentation describes mesh portals as wired mesh APs and mesh points as APs that use wireless uplinks to reach a portal. For deployment concepts and mesh-role behavior, see the ArubaOS Mesh Overview and the ArubaOS Mesh Configuration documentation.

QUESTION NO: 9

An administrator configures RADIUS authentication for a wireless employee WLAN. The RADIUS server must assign authenticated users to VLAN 120.

Which RADIUS attribute should the server return to assign the VLAN?

A. Framed-IP-Address

B. Tunnel-Private-Group-ID

C. Aruba-User-Role

D. Class

ANSWER: B

Explanation:

Tunnel-Private-Group-ID is the RADIUS attribute used to communicate the VLAN identifier for an authenticated session. When the RADIUS server returns the appropriate tunnel attributes, including the VLAN ID in Tunnel-Private-Group-ID, the Mobility Controller can place the user session into VLAN 120.

The RADIUS response should also include the related tunnel attributes that indicate the VLAN assignment method, such as Tunnel-Type set to VLAN and Tunnel-Medium-Type set to IEEE-802. The controller applies the VLAN assignment after successful authentication and authorization.

ArubaOS RADIUS authorization behavior is documented in the ArubaOS RADIUS authentication documentation.

QUESTION NO: 10

An administrator enables Adaptive Radio Management (ARM) on Aruba APs in a campus WLAN.

Which functions can ARM perform? (Choose two.)

A. Select RF channels for AP radios

B. Adjust AP radio transmit power

C. Assign RADIUS-derived user roles

D. Authenticate 802.1X users

E. Create firewall policies for user roles

ANSWER: A B

Explanation:

ARM dynamically manages radio resources using information gathered from the wireless environment. It can **select RF channels** to reduce the effects of co-channel interference and neighboring WLAN activity. ARM can also **adjust transmit power** to help maintain appropriate coverage and reduce excessive cell overlap.

ARM does not authenticate users or assign user roles. Those functions are handled by the WLAN authentication and AAA configuration. ARM is also distinct from ClientMatch, which focuses on steering and optimizing client associations.

Aruba describes ARM radio-management functions in the ArubaOS ARM overview.

QUESTION NO: 11

An administrator implements a cluster of four Aruba Mobility Controllers (MCs) managed by a Mobility Master (MM). An AP Group is configured with two VAPs and deployed to an AP that will connect to the cluster. Each AP contains two radios.

How many GRE tunnels will be built from the AP to the Active AP Anchor Controller (A-AAC)?

A. 2

B. 4

C. 5

D. 8

ANSWER: C

Explanation:

5 is correct. In an ArubaOS clustered deployment, the AP selects an Active AP Anchor Controller as its anchor point and establishes the AP-to-controller tunnel relationships with that controller. The AP has one GRE tunnel used for AP control traffic, plus a GRE data tunnel for every Virtual AP instance. A VAP is instantiated independently on each radio to which it is applied. Therefore, two configured VAPs across two radios produce four VAP data-tunnel instances: two VAPs multiplied by two radios. Adding the single AP control GRE tunnel gives a total of five GRE tunnels from this AP to its Active AP Anchor Controller. The number of controllers in the cluster does not multiply this count; the question specifically asks for tunnels to the active anchor controller. This tunnel model lets the controller identify and apply the appropriate WLAN, security, and forwarding policies for traffic associated with each radio/VAP instance while maintaining AP control connectivity. Aruba's ArubaOS documentation provides the cluster and AP-anchor architecture context in the ArubaOS 8 Web Help; Aruba's documentation portal is also available at Aruba Networking TechDocs.

QUESTION NO: 12

An Administrator supports a group of employees that connect to the corporate office using the VIA client. An Aruba Mobility Controller (MC), behind a corporate firewall, terminates the user's VPN sessions. The VPN sessions fail to establish because of the existing firewall rules.

Which connections must the administrator allow on the firewall? (Choose three.)

A. UDP 8202

B. UDP 4500

C. UDP 8211

D. TCP 4443

E. TCP 443

F. UDP 500

ANSWER: B E F

Explanation:

Aruba VIA establishes remote-access VPN connectivity to a Mobility Controller using IPsec. The firewall must permit UDP 500 because it carries Internet Key Exchange (IKE) traffic, which negotiates the security associations and cryptographic parameters needed before the protected tunnel can be created. UDP 4500 must also be permitted because it supports IPsec NAT Traversal (NAT-T). NAT-T encapsulates IPsec traffic in UDP so that users behind home, hotel, or other address-translating devices can establish and maintain the VPN tunnel reliably. TCP 443 is required for VIA's HTTPS-based communication with the controller, including client connection and portal-related functions; it also provides an SSL/TLS transport path used by the VIA solution where applicable. These rules must be configured to allow inbound traffic from external VIA clients to the public-facing address that is translated or forwarded to the Mobility Controller. Aruba documents VIA as its remote-access VPN client solution and identifies the controller-side VPN services and required transport considerations in its ArubaOS documentation. See the ArubaOS VIA overview and the ArubaOS VIA client documentation.

QUESTION NO: 13

An administrator wants to implement a Live Upgrade (in-service upgrade) of a cluster in an Aruba wireless solution. Which ArubaOS feature does the Mobility Master (MM) use to ensure RF redundancy, so that when

one or more APs are rebooted there is no loss of wireless coverage for users?

A. AirMatch

B. Mobility Controller load balancing

C. AP image preload

D. AP image verification

ANSWER: A

Explanation:

AirMatch is correct because it provides the RF-aware planning required for an ArubaOS Live Upgrade. During an in-service upgrade, APs must reboot to install and activate the new software image. The Mobility Master uses AirMatch's knowledge of AP radio locations, channel and power plans, neighboring AP relationships, and coverage requirements to create an upgrade sequence that preserves RF redundancy. In practical terms, the system avoids rebooting APs that are important to the same coverage area at the same time. Remaining APs can continue serving clients while selected APs are upgraded and return to service, reducing the likelihood of a coverage hole or excessive co-channel disruption during the maintenance window. This is distinct from simply distributing an image: the key Live Upgrade requirement is a radio-aware, coverage-preserving AP reboot order. AirMatch continuously optimizes the WLAN radio environment and supplies the RF topology intelligence that allows the controller cluster to stage AP upgrades safely. Aruba's Live Upgrade documentation describes the use of AirMatch to determine AP upgrade ordering and maintain redundancy; see ArubaOS Live Upgrade documentation. Additional AirMatch design and operational details are available in the ArubaOS AirMatch documentation.

QUESTION NO: 14

A cluster has two Aruba 7240 Mobility Controllers (MCs) and two Aruba 7220 Mobility Controllers (MCs).

How is the cluster leader elected if all controllers have the default priority?

A. The 7240 controller with the highest MAC address is elected.

B. The controller with the highest IP address is elected.

C. The controller with the highest MAC address is elected.

D. The 7240 controller with the lowest IP address is elected.

ANSWER: A

Explanation:

The 7240 controller with the highest MAC address is elected. ArubaOS clustering accounts for controller platform capacity during leader selection when the controllers use their default cluster-priority settings. The 7240 platform has greater capacity than the 7220 platform, so a 7240 is selected ahead of either 7220 as the cluster leader. This helps ensure that the controller performing the cluster-leader role has the greater available platform capability for the control-plane responsibilities associated with maintaining cluster state and coordinating cluster operations.

Because there are two controllers of the preferred 7240 platform, ArubaOS uses the MAC-address tie-breaker between those equivalent candidates. The 7240 with the highest MAC address therefore becomes the cluster leader. This behavior is important in mixed-platform clusters: leaving the default priorities in place does not make the election a simple comparison across every controller's IP address or MAC address; platform capacity first determines the preferred controller class, and the MAC address resolves the tie among matching preferred controllers. Aruba's ArubaOS documentation provides cluster configuration and operational guidance at ArubaOS Cluster documentation and product technical documentation is available through Aruba Networking TechDocs.

QUESTION NO: 15

Where would an administrator define the split-tunneling mode for a RAP located at a branch office?

A. the Firewall policy on the RAP

B. the AAA policy on the controller

C. the Firewall policy on the controller

D. the VAP profile on the controller

ANSWER: D

Explanation:

The correct setting location is **the VAP profile on the controller**. In ArubaOS, a Remote Access Point applies the wireless configuration that it receives from the controller, including the Virtual AP profile assigned to the wireless network. The VAP profile contains the forwarding-mode setting that determines how client traffic is handled. When split-tunnel forwarding is selected, traffic intended for corporate resources is sent through the secure tunnel to the controller, while traffic destined for other networks, such as Internet-bound traffic, can be forwarded locally at the remote site. This provides centralized security and access to internal resources without unnecessarily backhauling all client traffic across the WAN link. The administrator therefore edits the relevant wireless network's VAP profile on the controller and sets its forwarding mode for split tunneling; the RAP downloads and enforces that configuration when it connects. Aruba documents split-tunnel operation for RAPs and identifies the Virtual AP configuration as the place where the forwarding behavior is configured. See the ArubaOS remote access point documentation at ArubaOS RAP split tunneling and the ArubaOS configuration documentation at Configuring Remote APs.

QUESTION NO: 16

Which methods can be used to configure RAP redundancy when connected to two redundant Aruba Mobility Controllers (MCs) in the DMZ? (Select two.)

A. Virtual IP address of the two controllers.

B. Active and Standby AAC.

C. Primary and backup LMS IP addresses.

D. IPSec High Availability (HA) between two cluster members.

E. AirWave direction to RAPs redundant Mobility Controllers.

ANSWER: C D

Explanation:

“Primary and backup LMS IP addresses.” is a supported controller-redundancy configuration for an Aruba AP, including a RAP. The primary LMS address identifies the normal Mobility Controller that terminates the AP connection, while the backup LMS address gives the RAP an alternate controller destination when the primary controller becomes unavailable. This configuration provides a direct, deterministic failover target and is configured through the AP system-profile/controller-assignment settings.

“IPSec High Availability (HA) between two cluster members.” is also appropriate for RAP deployments because a RAP uses an IPsec tunnel across the untrusted WAN or Internet to reach the Mobility Controller in the DMZ. IPsec HA allows the redundant controller pair to maintain RAP service availability by supporting tunnel termination and recovery on the peer controller when a controller failure occurs. This approach is designed specifically for resilient remote-access connectivity and should be used with controllers configured as the relevant HA or cluster peers. Aruba’s AP configuration guidance describes LMS and backup-LMS controller assignment, while the ArubaOS documentation covers clustered-controller and high-availability behavior. See ArubaOS 8.4 AP configuration documentation and ArubaOS 8.4 cluster overview.

QUESTION NO: 17

An administrator configures ClearPass enforcement profiles for an Aruba wireless deployment. The administrator wants ClearPass to return authorization information that changes both the user role and the VLAN assigned to an authenticated session.

Which attributes can ClearPass return? (Choose two.)

A. Aruba-User-Role

B. Tunnel-Private-Group-ID

C. AP-Group-Name

D. Mesh-Cluster-Name

E. AirMatch-Mode

ANSWER: A B

Explanation:

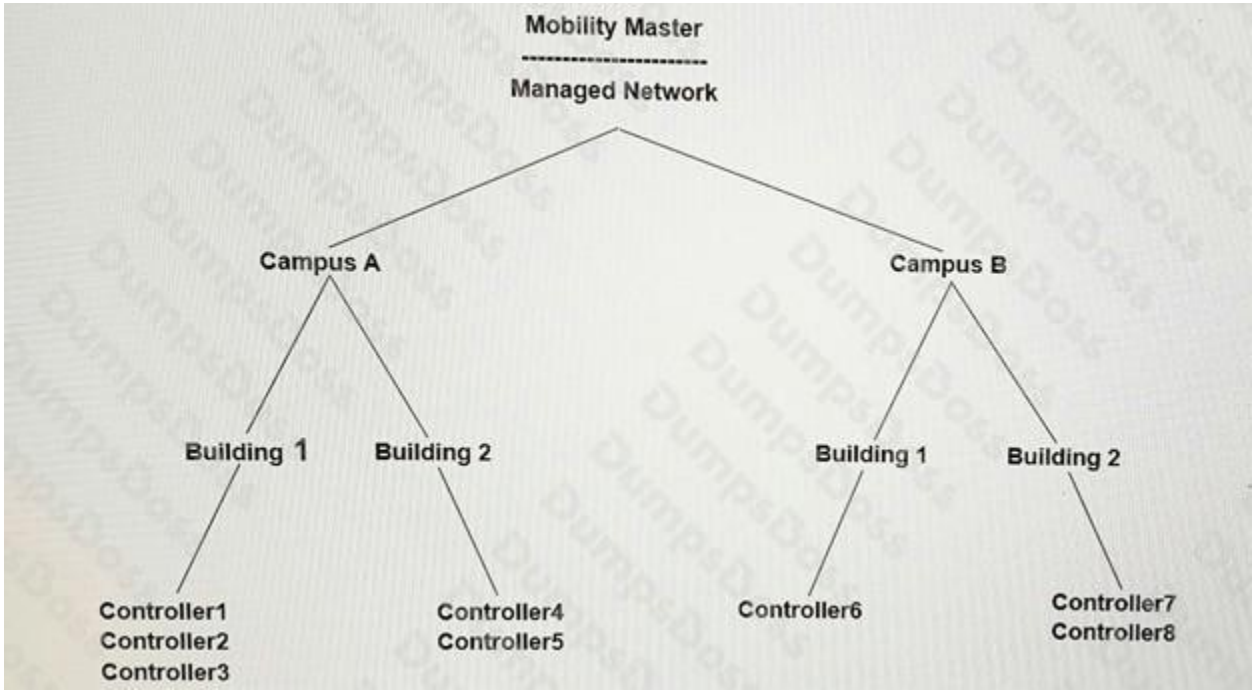
ClearPass can return the Aruba vendor-specific **Aruba-User-Role** attribute in a RADIUS Access-Accept message. The Mobility Controller uses this value to apply the named ArubaOS user role to the authenticated client session.

ClearPass can also return **Tunnel-Private-Group-ID** as part of a standard RADIUS VLAN assignment. When paired with the required tunnel type and tunnel medium attributes, the controller uses this attribute to assign the client to the specified VLAN.

ClearPass enforcement profiles support returning standard RADIUS attributes and Aruba vendor-specific attributes. Aruba role assignment is described in the ClearPass Aruba user-role documentation.

QUESTION NO: 18

Refer to the exhibit.



An administrator wants to centralize administrative access to the Aruba Mobility Controllers (MC) and Mobility Master (MM). ClearPass is set up and the preferred authentication protocols is TACACS+. Where should the administrator perform this configuration in the MM hierarchy shown in the exhibit?

A. At the Managed Network level

B. At the two campus levels

C. At both the Mobility Master and Managed Network levels

D. At the controller levels

ANSWER: C

Explanation:

At both the Mobility Master and Managed Network levels is correct because administrative-management authentication must be configured at a hierarchy level that covers each type of device being administered. The Mobility Master is the top-level management appliance and does not inherit configuration from a Managed Network node beneath it. Therefore, TACACS+ settings needed to authenticate administrators signing in to the Mobility Master must be configured at the Mobility Master level.

The Mobility Controllers are members of the Managed Network and inherit applicable configuration from that Managed Network level. Defining the TACACS+ server group and management-authentication settings there provides a centralized policy for the controllers in that managed network, including controllers organized into campus folders and device groups below it. Using ClearPass as the TACACS+ server also enables centralized administrator authentication and authorization, so privileges can be assigned through returned Aruba administrator roles rather than maintained independently on every controller.

This placement provides the intended scope: one configuration for Mobility Master administration and one inherited configuration for the managed controllers. ArubaOS documentation describes the configuration hierarchy and its inheritance model, as well as AAA and management-user authentication configuration, in the ArubaOS 8.10 User Guide and the ArubaOS AAA documentation.

QUESTION NO: 19

An administrator implements a ClearPass solution to authenticate Aruba wireless users. The Aruba wireless solution is an ArubaOS 8.x Mobility Master (MM) deployment. ClearPass sends an Aruba VSA role name for an authenticated user. However, the administrator notices that the role assigned to the user is different from the one assigned by the ClearPass server.

Which two items should the administrator verify that might be the cause of this problem? (Choose two.)

A. Enablement of user roles on the controller

B. Spelling of the role on the ClearPass server

C. Server-derived role assignment on the ClearPass server

D. Role existence on the Managed Network

E. Order assignment that the controller uses to select a user role

ANSWER: B D

Explanation:

The administrator should verify the **Spelling of the role on the ClearPass server** and **Role existence on the Managed Network**. In an ArubaOS 8.x deployment, ClearPass can return the Aruba-User-Role RADIUS vendor-specific attribute, containing the exact name of the user role that ArubaOS should assign. The role name is a literal value, so it must precisely match the name configured in ArubaOS, including capitalization, spaces, punctuation, and any other characters. A small mismatch prevents the intended role from being applied.

The specified role must also be present in the ArubaOS configuration available to the Managed Device that handles the client connection. In a Mobility Master architecture, role configuration is commonly defined in the applicable configuration hierarchy and then pushed to the managed devices. When the returned role is absent from that device's effective configuration, ArubaOS cannot apply the intended policy and can instead assign a fallback role, such as the initial role or another applicable role. Reviewing the Access Tracker RADIUS response in ClearPass and comparing its Aruba-User-Role value with the effective user-role configuration on the Managed Network is the appropriate validation workflow. Aruba documents RADIUS-assigned roles in the ArubaOS user-role assignment documentation and provides configuration guidance in the ClearPass Aruba user-role documentation.

QUESTION NO: 20

An administrator plans to add several Aruba Mobility Controllers (MCs) to an existing ArubaOS 8.x cluster.

Which conditions should the administrator verify before adding the new cluster members? (Choose two.)

A. Verify that all Mobility Controllers run the same ArubaOS software release.

B. Ensure that IP connectivity exists between all cluster members.

C. Configure all Mobility Controllers with the same management IP address.

D. Place all Mobility Controllers in the same AP group.

E. Configure a separate Mobility Master for each cluster member.

ANSWER: A B

Explanation:

The Mobility Controllers must run the same ArubaOS software release, and IP connectivity must exist between all cluster members. Cluster members exchange control and state information to coordinate AP and client services. Software-version consistency is required to ensure that all members support compatible clustering functions and state synchronization behavior.

Cluster members can operate across Layer 3 networks, but they require reliable IP reachability between their cluster addresses. The administrator should confirm routing, firewall policies, and latency requirements before adding remote controllers to the cluster.

QUESTION NO: 21

An administrator deploys Aruba mesh APs to provide wireless connectivity to an outdoor area where Ethernet cabling is not available.

Which statements describe the required mesh deployment configuration? (Choose three.)

A. A mesh portal requires a wired connection to the network.

B. Mesh APs in the same cluster must use matching cluster security settings.

C. A mesh point uses a wireless backhaul path to reach a mesh portal.

D. Each mesh point must use a unique mesh cluster name.

E. All mesh APs must be connected to the same controller VLAN.

ANSWER: A B C

Explanation:

A mesh portal requires a wired network connection and provides the upstream path for mesh traffic. Mesh points use a wireless backhaul connection to reach a mesh portal, either directly or through another mesh point. This allows client and wired-device traffic at remote locations to reach the wired network through the mesh infrastructure.

All APs participating in the same mesh cluster must use matching mesh-cluster settings, including the cluster name and shared WPA key or passphrase. These settings allow the mesh APs to authenticate each other and establish protected wireless backhaul links.

QUESTION NO: 22

An administrator implements AirGroup for an organization that has users and shared Apple TV devices on different VLANs.

Which benefits does AirGroup provide in this deployment? (Choose two.)

A. It provides controlled service discovery across VLANs.

B. It restricts service access according to policy.

C. It routes all multicast traffic between VLANs.

D. It assigns IP addresses to wireless clients.

E. It replaces DNS name resolution for network clients.

ANSWER: A B

Explanation:

AirGroup enables controlled discovery of supported services across Layer 3 boundaries and restricts access to discovered services according to policy. Standard Bonjour and mDNS advertisements are normally limited to the local subnet. AirGroup collects service advertisements and makes approved services available to authorized users on other VLANs or subnets.

AirGroup policies can limit service visibility and access based on identity and location information. For example, users can be permitted to discover an Apple TV in their assigned area while being prevented from discovering devices in another building or department.