Q&A

Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

HPE6-A75 Dumps
HPE6-A75 Braindumps
HPE6-A75 Real Questions
HPE6-A75 Practice Test
HPE6-A75 Actual Questions

PASS

killexams.com

HP

HPE6-A75

Aruba Certified Edge Professional (ACEP)

ORDER FULL VERSION

Question: 150

Which technologies can prevent split brain in a VSF fabric that includes Aruba 2930F switches?

A. ARP MAD or OOBM MAD
B. VLAN MAD or ARP MAD
C. OOBM MAD or LLDP MAD
D. LLDP MAD or VLAN MAD

Answer: D

Question: 151

Refer to the exhibit.

Configuration » Services » Edit - CompanyX Onboard Authorization

Services - CompanyX Onboard Authorization

Summary	Service	Authentication	Roles	**Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy: CompanyX Onboard Authorization Policy ▾ **Modify**   Add new En

Enforcement Policy Details

Description: Sample policy controlling authorization during Onboard provisioning
Default Profile: [Deny Access Profile]
Rules Evaluation Algorithm: evaluate-all

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	[Allow Access Profile], [Aruba Terminate Session]

Exhibit:accp67-543

Based on the configuration of the Enforcement Profiles In the Onboard Authorization service shown, which Onboarding action will occur?

A. The device will be disconnected from the network after Onboarding so that an EAP-TLS authentication is not performed.
B. The device will be disconnected from and reconnected to the network after Onboarding is completed.
C. The deviceâs onboard authorization request will be denied.
D. The device will be disconnected after post-Onboarding EAP-TLS authentication, so a second EAP-TLS authentication is performed.
E. After logging in on the Onboard web login page, the device will be disconnected form and reconnected to the network before Onboard begins.

Answer: B

Question: 152

Refer to the exhibit.

Configuration » Authentication » Sources » Add - remotelab AD

Authentication Sources - remotelab AD

| Summary | General | Primary | **Attributes** |

Specify filter queries used to fetch authentication and authorization attributes

Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	Role, Attribute
	title	Title	Attribute
	company	company	-
	memberOf	memberOf	Role, Attribute
	telephoneNumber	Phone	Attribute
	mail	Email	Attribute

Exhibit:accp67-312

Based on the Attribute configuration shown, which statement accurately describes the status of attribute values?

A. Only the attribute values of department and memberOf can be used in role mapping policies.
B. The attribute values of department, title, memberOf, telephoneNumber, and mail are directly applied as ClearPass.
C. Only the attribute value of company can be used in role mapping policies, not the other attributes.
D. The attribute values of department and memberOf are directly applied as ClearPass roles.
E. Only the attribute values of title, telephoneNumber, and mail can be used in role mapping policies.

Answer: D

Question: 4

An administrator wants to use Airwave to manually add devices on the network.

Where should the administrator perform this action?

A. in Device Setup
B. in Groups
C. in AMP Setup
D. in Devices

Answer: A

Question: 153

Refer to the exhibit.

```
Switch-1# show link-keepalive

 Status and Configuration - UniDirectional Link Detection (UDLD)

   Keepalive Retries  : 4
   Keepalive Interval : 5000 ms
   Keepalive Mode     : forward-then-verify

                 Physical           Keepalive Adjacent            UDLD
   Port  Enabled Status             Status    Switch              VLAN
   ----- ------- ------------------ --------- ------------------- ----------
   A23   Yes     up                 failure   00fd45-653ae9       untagged
```

Switch-1 and Switch-2 connect on interface A23. The switches experience a connectivity issue. The network administrator sees that both switches show this interface as up. The administrator sees the output shown in the exhibit on Switch-1.

What is a typical issue that could cause this output?

A. a hardware issue, such as a broken cable
B. asymmetric routing introduced by a routing configuration error
C. an issue with queuing, caused by mismatched QoS settings
D. mismatched IP addresses on the VLAN for the link

Answer: A

Question: 154

An administrator supports a RAP to a branch office. Employees at the branch office connect to an employee SSID that allows for split tunneling of the employee traffic. The RAP initially connects to the corporate office controller, but later loses connectivity to it.

Which operating mode should the administrator configure for a secondary SSID to be advertised during the loss of connectivity?

A. Standard
B. Persistent
C. Always
D. Backup

Answer: B

Question: 155

Refer to the exhibit.

Identity

These options control the generation of device credentials

* Certificate Authority:	Local Certificate Authority ▾	Select the certificate authority that will be used to sign profiles and messages.
* Signer:	Onboard Certificate Authority ▾	Select the source that will be used to sign TLS client certificates.
* Key Type:	1024-bit RSA – created by device ▾	Select the type of private key to use for TLS certificates.
* Unique Device Credentials:	☑ Include the username in unique device credentials	When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.

Exhibit:accp67-531

Based on the configuration for the client's certificate private key as shown, which statements accurately describe the settings? (Select two.)

A. More bits in the private key will increase security.
B. The private key for TLS client certificates is not created.
C. The private key is stored in the ClearPass server.
D. More bits in the private key will reduce security.
E. The private key is stored in the user device.

Answer: A,E

Question: 156

Refer to the exhibit.

Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Summary	Enforcement	Rules

Enforcement:

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

Rules:

Rules Evaluation Algorithm: First applicable

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

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

A. Deny Access

B. Employee VLAN
C. Internet VLAN
D. Full Access VLAN

Answer: B

Question: 157

An administrator creates service-based policies for AirGroup on the Mobility Master (MM).

The administrator can define location-based policy limits based on which information?

A. AP names, AP groups, controller names, and controller groups
B. AP Fully Qualified Location Names (FQLNs) and controller Fully Qualified Domain Names (FQDNs)
C. AP names, AP groups, and AP Fully Qualified Location Names (FQLNs)
D. Controller names, controller groups, and controller Fully Qualified Domain Names (FQDNs)

Answer: C

Question: 158

A network administrator can set the OSPF metric-type on an AOS-Switch to Type 1 or Type 2.

What is the difference?

A. A Type 2 metric marks external routes that can be advertised in NSSAs, while a Type 1 metric marks external routes that can only be advertised in normal areas.
B. A Type 2 metric assigns cost 1 to a 100 Gbps link, while a Type 1 metric assigns cost 1 to all links of 100 Mbps or higher.
C. A Type 2 metric is assigned to multiple external routes that are aggregated together, while a Type 1 metric does not permit external route aggregation.
D. A Type 2 metric stays the same as the external route is advertised, while a Type 1 metric increments with internal OSPF link costs.

Answer: D

Question: 159

Which protocol do Mobility Controllers (MCs) use to detect a failed Mobility Master (MM)?

A. VRRP
B. SNMP
C. PAPI
D. IPSec

Answer: B

Question: 160

A company requires AOS-Switches at the campus core. The switches:

â Will act as the default gateways for several campus VLANs

â Must provide redundancy for their services and tolerate the loss of a link or an entire switch

â Must recover from the failure of one of the switches within a second or less

VRRP and MSTP are proposed to meet these requirements.

What is an issue with this proposal?

A. VRRP provides redundancy against lost links but not a failed switch.
B. VRRP provides routing redundancy but not default gateway redundancy.
C. VRRP does not interoperate with MST
D. VRRP takes longer than a second to fail over.

Answer: B

Question: 161

Refer to the exhibit.
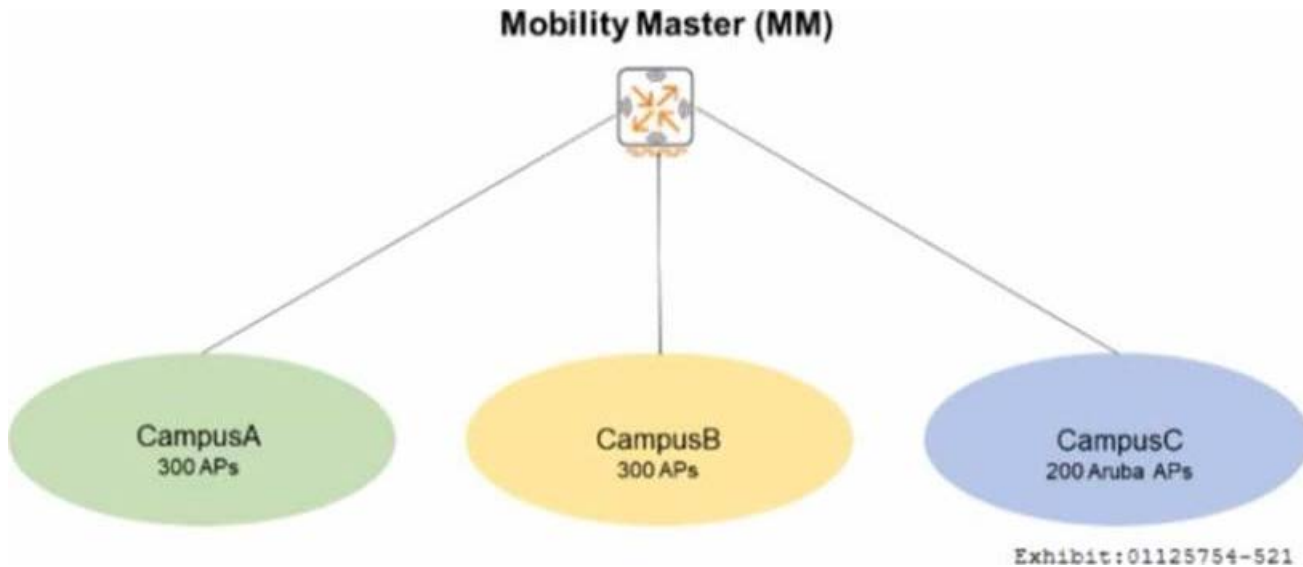
An administrator implements AP licensing on a Mobility Master (MM).

â¢ Each campus is responsible to purchase its own AP licenses.

â¢ There are 900 AP licenses deployed in the global pool

â¢ There are three dedicated pools.

â¢ From the global pool, 300 AP licenses are assigned to each dedicated pool.

Network engineers at CampusA want to deploy an additional 100 APs. Currently all of the AP licenses in CampusA and CampusB are allocated, but only 200 of the AP licenses m CampusC are allocated.

What can the administrator do to add capacity for CampusA in alignment with campus policies?

A. Allow CampusA to share from the CampusC pool.

B. Add 100 more AP licenses and assign them to the CampusA pool.
C. Move 100 licenses from the CampusC pool to the global pool.
D. Add 100 more AP licenses to the global pool.

Answer: B

Question: 162

What must an OSPF router do when it receives a link state update?

A. It must participate in a new election for the Designated Router and Backup D
B. It must initiate a graceful restart timer.
C. It must re-establish adjacency with its Designated Router and Backup D
D. It must run the shortest path first algorithm.

Answer: C

Question: 163

Refer to the exhibit.

Exhibit 1
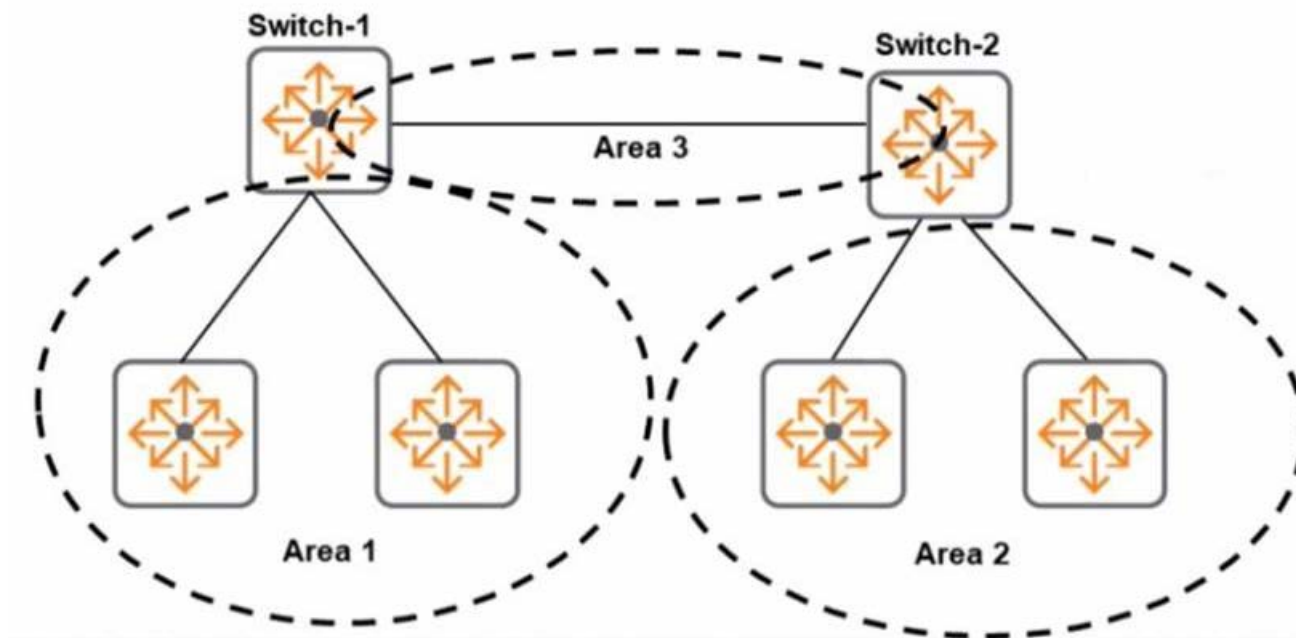
A company has attempted to implement OSPF without success. The devices in Area I need to be able to reach Area 2.
Routes should be aggregated for advertisement in other areas.

What must be changed to meet these requirements?

A. Change Area 3 to Area 0; remove Area 1 from Switch-2 and Area 2 from Switch-1.
B. Add the 10.2.0.0/16 range on Swttch-1 and the 10.1.0.0/16 range on Switch-2.
C. Add Area 1 and Area 2 on VIAN 100 on both Switch-1 and Switch-2. Remove Area 3.
D. Move the 10.1.0.0/16 range to Area 2 on Switch-1 and the 10.2.0.0/16rangetoArea 1 onSwitch-2.

Answer: A

Question: 164

Refer to the exhibit.

```
Switch-1(config)# show running-config interface 1-20
Running configuration:

interface 1
    untagged vlan 20
    aaa port-access authenticator
    exit
#output the same for interfaces 2-20
```

Several interfaces on an AOS-Switch enforce 802. IX to a RADIUS server at 10.254.378.521. The interface 802. IX settings are shown in the exhibit, and 802. IX is also enabled globally. The security team have added a requirement tor port security on the interfaces as well.

Before administrators enable port security, which additional step must they complete to prevent issues?

A. Set an 802. l X client limit on the interfaces.
B. Manually add legitimate MAC addresses to the switch authorized MAC list.
C. Enable eavesdropping protection on the interfaces.
D. Enable DHCP snooping on VLAN 20.

Answer: D

Question: 165

in a VPN that uses certificate-based authentication, which component must be configured on the Mobility Master (MM) to allow a RAP to successfully connect to a Mobility Controller (MC)

A. RAP VPN username and password
B. WLAN and new RAP group
C. RAP IPSec pre-shared key
D. RAP whitelist

Answer: D

Question: 166

An administrator implements the MultiZone feature and uses two clusters that utilize CPSec. A primary and a data zone are created. MultiZone APs successfully build sessions to the primary cluster but fail to establish sessions to the data zone cluster.

What must the administrator do to solve this problem?

A. Enable CPSec in the MultiZone profile for both the primary and data zone.
B. Enable MultiZone booting in the MultiZone AP apboot configuration mode.
C. Add the MultiZone APs to the data zoneâs CPSec whitelist.
D. Use different AP Group names for the two zones.

Answer: D

Question: 167

CORRECT TEXT

Which is a valid policy simulation types in ClearPass? (Select three.)

A. Enforcement Policy
B. Posture token derivation
C. Role Mapping
D. Endpoint Profiler
E. Chained simulation

Answer: A,C,E

Question: 168

Refer to the exhibit.

	Conditions	Role Name
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive
2.	(Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor
3.	(Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device
4.	(Authorization:remotelab AD:UserDN EXISTS)	[Employee]
5.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	HR Local
6.	(Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User
7.	(Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee

Exhibit:accp67-236

An AD user's department attribute is configured as *HR". The user connects on Monday using their Windows Laptop to a switch that belongs to the Device Group HQ.

Which role is assigned to the user in ClearPass?

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

Answer: A,D,E

SAMPLE QUESTIONS