

DUMPSBOSS.

Aruba Certified Edge Professional Exam

HP HPE6-A75

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which statement is true about the Endpoint Profiler? (Select two.)

- A. The Endpoint Profiler uses DHCP fingerprinting for device categorization.
- B. Data obtained from the Endpoint Profiler can be used in Enforcement Policy.
- C. Endpoint Profiler requires a profiling license.
- D. The Endpoint Profiler requires the Onboard license to be enabled.
- E. The Endpoint Profiler can only categorize laptops and desktops.

ANSWER: A B

QUESTION NO: 2

Refer to the exhibit.

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

Exhibit: accp67-378

- A. mike
- B. We can't know this from the screenshot above.
- C. Employee
- D. john

ANSWER: B

QUESTION NO: 3

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:acop67-236

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: D E

QUESTION NO: 4

Refer to the exhibit.

Enforcement Policies - Enterprise Enforcement Policy

Summary		Enforcement	Rules
Enforcement:			
Name:	Enterprise Enforcement Policy		
Description:	Enforcement policies for local and remote employees		
Enforcement Type:	RADIUS		
Default Profile:	[Deny Access Profile]		
Rules:			
Rules Evaluation Algorithm: Evaluate all			
Conditions	Actions		
(Tips: Posture EQUALS HEALTHY (0))			
AND (Tips: Role MATCHES_ANY Remote Worker)			
1. Role Engineer	[RADIUS] EMPLOYEE_VLAN, [RADIUS] Remote Employee ACL		
(Tips: Role EQUALS Senior_Mgmt)			
AND (Date: Day-of-Week NOT_BELONGS_TO Saturday, Sunday)			
2. (Tips: Role EQUALS Senior_Mgmt)	[RADIUS] EMPLOYEE_VLAN		
AND (Date: Day-of-Week NOT_BELONGS_TO Saturday, Sunday)			
3. (Tips: Role EQUALS San Jose HR Local)	HR VLAN		
AND (Tips: Posture EQUALS HEALTHY (0))			
4. (Tips: Role EQUALS [Guest])	[RADIUS] WIRELESS_GUEST_NETWORK		
AND (Connection: SSID CONTAINS guest)			
5. (Tips: Role EQUALS Remote Worker)	RestrictedACL		
AND (Tips: Posture NOT_EQUALS HEALTHY (0))			

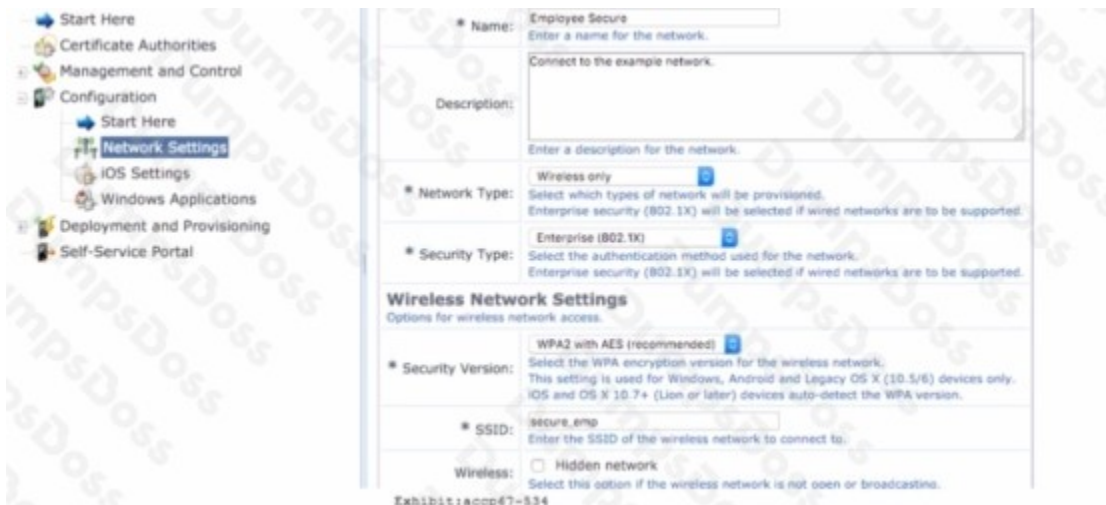
Based on the Enforcement Policy configuration, when a user with Role Engineer connects to the network and the posture token assigned is Unknown, which Enforcement Profile will be applied?

- A. EMPLOYEE_VLAN
- B. RestrictedACL
- C. Deny Access Profile
- D. HR VLAN
- E. Remote Employee ACL

ANSWER: C

QUESTION NO: 5

Refer to the exhibit.



Which statements accurately describe the status of the Onboarded devices in the configuration for the network settings shown? (Select two.)

- A. They will connect to Employee_Secure SSID after provisioning.
- B. They will connect to Employee_Secure SSID for provisioning their devices.
- C. They will use WPA2-PSK with AES when connecting to the SSID.
- D. They will connect to secure_emp SSID after provisioning.
- E. They will perform 802.1X authentication when connecting to the SSID.

ANSWER: D E

QUESTION NO: 6

Refer to the exhibit.

The screenshot shows the 'Identity' configuration page with the following settings:

* Certificate Authority:	Local Certificate Authority <small>Select the certificate authority that will be used to sign profiles and messages.</small>
* Signer:	Onboard Certificate Authority <small>Select the source that will be used to sign TLS client certificates.</small>
* Key Type:	1024-bit RSA – created by device <small>Select the type of private key to use for TLS certificates.</small>
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials <small>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.</small>

Exhibit: scop67-531

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 NO: 7

Refer to the exhibit.

```
Switch# ping 10.1.10.5
10.1.10.5 is alive, time = 3 ms

Switch# show radius authentication

Status and Counters - RADIUS Authentication Information

NAS Identifier      : Access-1
Invalid Server Addresses : 0
UDP
Server IP Addr  Port  Timeouts  Requests  Challenges  Accepts  Rejects
-----
10.1.10.5      1812  6         3         0           0        0
```

A network administrator sets up 802.1X authentication to a RADIUS server on an AOSSwitch. The RADIUS server and user devices are both set up to use REAP MSCHAPv2. The administrator tests the authentication and sees the output shown in the exhibit. Which issue could cause this output?

- A. The RADIUS shared secret does not match on the switch and the server.
- B. The administrator entered the wrong password for the test account.
- C. The switch does not have a certificate for port-access installed on the switch.
- D. The switch port is set for user mode 801. IX. but the RADIUS server is set for port mode.

ANSWER: A

QUESTION NO: 8

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 NO: 9

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

QUESTION NO: 10

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 802.1X to a RADIUS server at

10.254.378.521. The interface 802.1X settings are shown in the exhibit, and 802.1X is also enabled globally. The security team have added a requirement for port security on the interfaces as well. Before administrators enable port security, which additional step must they complete to prevent issues?

- A. Set an 802.1X 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