HPE6-A79 Q&As

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/hpe6-a79.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

A network administrator has updated the ArubaOS code of a standalone Mobility Controller (MC) that is used for User-Based Tunneling (UBT) to a newer early release. Ever since the MC seems to reject PAPI sessions from the switch with the 10.1.10.10 IP address. Also the controller\\'s prompt is now followed by a star mark: "(MC_VA) [mynode] *#"

When opening a support ticket, an Aruba TAC engineer asks the administrator to gather the crash logs and if possible replicate UBT connection attempts from the switch while running packet captures of PAPI traffic on the controller and obtain the PCAP files. The administrator has a PC with Wireshark and TFTP server using the 10.0.20.20 IP address.

What commands must the administrator issue to accomplish these requests? (Choose two.)

A.
```
packet-capture destination ip-address 10.0.20.20
packet-capture datapath ipsec 10.1.10.10
```

B.
```
show tech-support logs.tar
copy flash: logs.tar tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

C.
```
tar logs
copy flash: logs.tar tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

D.
```
tar crash
copy flash: logs.tar tffp: 10.0.20.20 crash.tar
copy flash: logstarmd5sum.txt tffp: 10.0.20.20 crash.tarmd5sum.txt
```

E.
```
packet-capture destination ip-address 10.0.20.20
packet-capture controlpath udp all
```

A. Option A

B. Option B

C. Option C

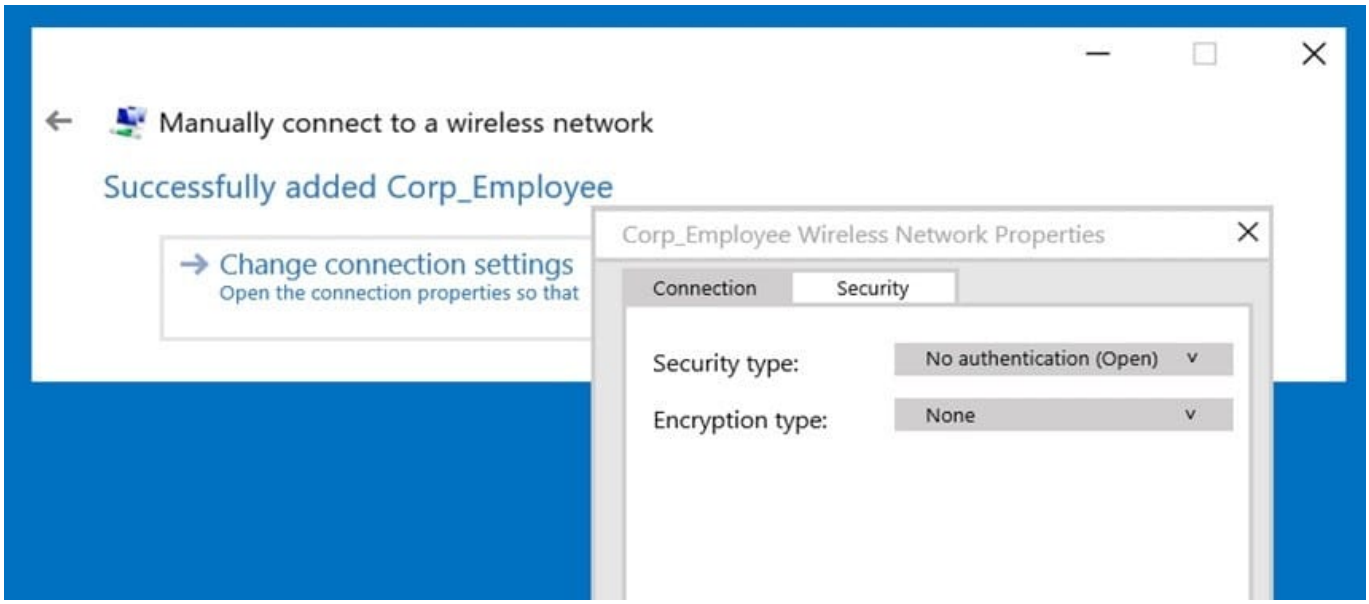
D. Option D

E. Option E

Correct Answer: BE

QUESTION 2

Refer to the exhibit.



A network administrator wants to configure an 802.1x supplicant for a wireless network that includes the following:

AES encryption EAP-MSCHAP v2-based user and machine authentication Validation of server certificate in Microsoft Windows 10

The network administrator creates a WLAN profile and selects the change connection settings option. Then the network administrator changes the security type to Microsoft: Protected EAP (PEAP), and enables user and machine authentication under Additional Settings.

What must the network administrator do next to accomplish the task?

A. Change default RC4 encryption for AES.

B. Enable user authentication under Settings

C. Change the security type to Microsoft: Smart Card or other certificate.

D. Enable server certificate validation under Settings.

Correct Answer: C

QUESTION 3

Users run encrypted Skype for Business traffic with no WMM support over an Aruba Mobility Master (MM) - Mobility Controller (MC) based network. When voice, video, and application sharing traffic arrive at the wired side of the network, all the flows look alike due to the lack of L2 and L3 markings

How can the network administrator identify these flows and mark QoS accordingly?

A. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and the firewall roles. Then enable WMM in a VAP profile.

B. Use a media firewall policy that match these three flows, and use permit and TOS actions with 56, 40, and 34 values for voice, video, and application sharing, respectively. Then enable the Skype4Business ALG in the UCC profiles.

C. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and the firewall roles. Then enable the Skype4Business ALG in the UCC profiles.

D. Confirm the MM is the Openflow controller of the MCs and Openflow is enabled in VAP and the firewall roles. Then integrate the MM with the Skype4Business SDN API, and enable the Skype4Business ALG in the UCC profiles.

Correct Answer: D

QUESTION 4

Refer to the exhibit.

```
(MC14-1) #show aaa authentication dot1x Corp-Network

802.1x Authentication Profile "Corp-Network"
-------------------------------------------
Parameter                                          Value
---------                                          -----
Max authentication failures                        0
Enforce Machine Authentication                     Enabled
Machine Authentication: Default Machine Role       guest
Machine Authentication Cache Timeout               24 hr(s)
Blacklist on Machine Authentication Failure        Disabled
Machine Authentication: Default User Role          guest
Interval between Identity Requests                 5 sec
Quiet Period after Failed Authentication           30 sec
Reauthentication Interval                          86400 sec
Use Server provided Reauthentication Interval      Disabled
Use the termination-action attribute from the Server  Disabled
Multicast Key Rotation Time Interval               1800 sec
Unicast Key Rotation Time Interval                 900 sec
Authentication Server Retry Interval               5 sec
Authentication Server Retry Count                  3
Framed MTU                                         1100 bytes
Max number of requests sent during an Auth attempt  5
Max Number of Reauthentication Attempts            3
Maximum number of times Held State can be bypassed  0
Dynamic WEP Key Message Retry Count                1
Dynamic WEP Key Size                               128 bits
Interval between WPA/WPA2 Key Messages             1000 msec
Delay between EAP-Success and WPA2 Unicast Key Exchange  0 msec
Delay between WPA/WPA2 Unicast Key and Group Key Exchange  0 msec
Time interval after which the PMKSA will be deleted  8 hr(s)
Delete Keycache upon user deletion                 Disabled
WPA/WPA2 Key Messages Retry Count                  3
Multicast Key Rotation                             Disabled
Unicast Key Rotation                               Disabled
Reauthentication                                   Disabled
Opportunistic Key Caching                          Enabled
```

The network administrator must ensure that the configuration will force users to authenticate periodically every eight hours. Which configuration is required to effect this change?

A. Set the reauth-period to 28800 enable reauthentication in the dot1x profile.

B. Set the reauth-period to 28800 enable reauthentication in the AAA profile.

C. Set the reauth-period to 28800 enable reauthentication in both dot1x and AAA profile.

D. Set the reauth-period to 28800 in the dot1x profile and enable reauthentication in the AAA profile.

Correct Answer: A

QUESTION 5

An Aruba Mobility Master (MM) - Mobility Controller (MC) solution is connected to a wired network that is ready to prioritize DSCP marked traffic. A group of WMM-enabled clients sends traffic marked at L2 only.

What must the network administrator do to map those markings to DSCP equivalent values when traffic is received by the APs?

A. Enable WMM in the SSID profile.

B. Enable WMM in the VAP profile.

C. Enable Skype4Business ALG Support.

D. Enable traffic to be marked with session ACLs.

Correct Answer: B