Vendor: HP

Exam Code: HPE6-A79

Exam Name: Aruba Certified Mobility Expert Written Exam

Version: DEMO

QUESTION 1
Refer to the exhibit. A network administrator adds a Mobility Controller (MC) in the /mm level and notices that the device does not show up in the managed networks hierarchy. The network administrator accesses the CLI. executes the show switches command, and obtains the output shown in the exhibit.

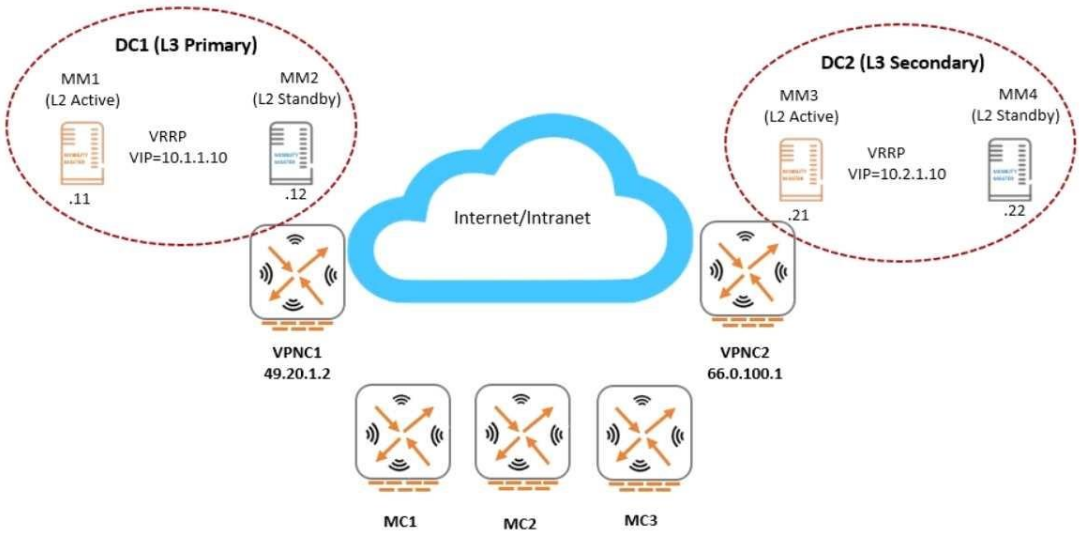
```
(MM1) [md] #show switches

All Switches
---------------
IP Address      IPv6  Address  Name  Location          Type     Model        Version      Status Configuration State      Config  Sync  Time (sec)  Confi
g ID
-------------   ------------ ---------  -------  --------------  -------  ---------  ---------  -------- ----------------------  ------  ----------  ---------
10.254.10.14    None         MM1   Building1.floor1  master   ArubaMM-VA  8.2.1.0_64044  up       UPDATE SUCCESSFUL       0                   415
10.254.10.114   None         MM2   Building1.floor1  standby  ArubaMM-VA  8.2.1.0_64044  up       UPDATE SUCCESSFUL       0                   415
10.1.140.100    None         MC1   Building1.floor1  MD       Aruba7030   8.2.1.0_64044  up       UNK(20:4c:03:06:e5:c0)  N/A                 N/A
Total Switches: 3
(MM1) [md] #
```

What is the reason that the MC does not appear as a managed device in the hierarchy?

A. The network administrator added the device using the wrong Pre-Shared Key (PSK).
B. The network administrator has not moved the device into a group yet.
C. The digital certificate of the MC is not trusted by the MM.
D. The IP address of the MC does not match the one that was defined in the MM.

Answer: B
Explanation:
UKN means unknown mac address. The MM doesn't know the mac address however the IP address is updated, so it form the IPSEC tunnel.
You need to create a group and provide the device, name, Model number and Mac address, to fix this issue.

QUESTION 2
Refer to the exhibit. An Aruba network is deployed with L2 and L3 Mobility Master (MM) redundancy across two datacenters, as shown in the exhibit. The network administrator confirms that all Mobility Controllers (MC) are currently communicating with MM1, which is the L2 Active and, L3 Primary.
Which MM IP will MCs communicate with if MM1 fails?



```
(MC2) #show running-config | include masterip
Building Configuration...
masterip 10.1.1.10 vpn-ip 19.20.1.2 ipsec aruba123 peer-id xx:xx:xx:xx:xx:xx
secondary masterip 10.2.1.10 vpn-ip 66.0.100.1 ipsec-factory-cert vpn-mac-1 xx:xx:xx:xx:yy:yy interface vlan 140
(MC2) #
```

A. 10.1.1.10
B. 10.1.1.12
C. 10.2.1.10
D. 10.2.1.21

Answer: A
Explanation:
MCs will continue using the VRRP/VIP address , thats why we use VRRP first place , the question clearly asks about which IP MCs use in their communication MCs communication goes to MM2 (after MM1 fail) but the used IP in communication is VIP IP 10.1.1.10.

QUESTION 3
A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.
B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.
C. Block all ports to the MMs except UDP 500 and 4500.
D. Install a PEFV license, and configure firewall policies that protect the MM.

Answer: C
Explanation:
Ports 4500 and 500 are essential for controller to controller communication , since other sites do not have static/available public IP , using VPN site to site by VPN concentrator is not an option here m question also states that both MMs are reachable on the internet already so blocking admin ports is essential.

QUESTION 4
A company has headquarters based in the US and rents internation office space in Mexico City so that 10 employees can work remotely. The company must implement a remote access technology so branch office employees can access all servers at the headquareters.

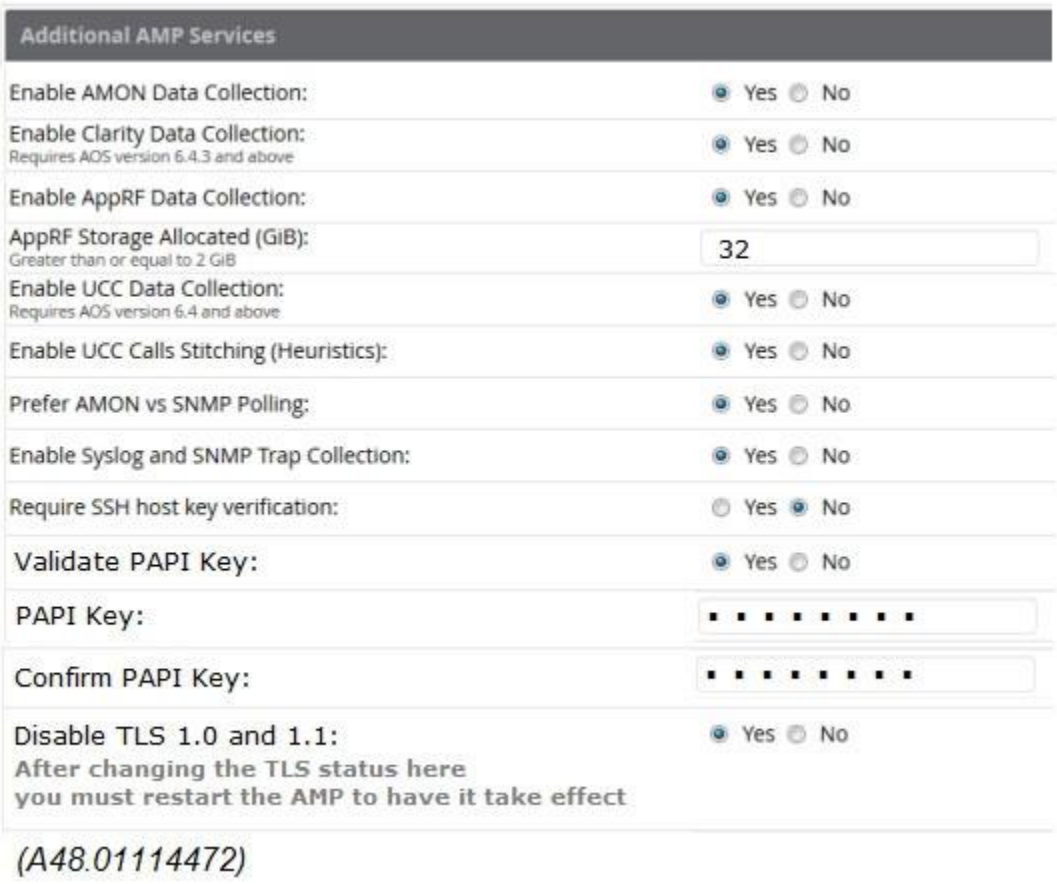
The office has both wired and wireless internet connectivity, with no restrictions on what device connects to the network. However, ports UDP 4500, 5060, and 5061 are blocked by the primeter firewall.

Which remote access technology is required to allow employees to access the servers at the headquarters?

A. BOC with CAPs
B. IAP VPN
C. RAP
D. VIA

Answer: A
Explanation:
Because VIA, RAP and IAP VPN use udp4500 for ipsec. But question says udp4500 blocked.

QUESTION 5
Refer to the exhibit. A network administrator configures a Mobility Master (MM)-Mobility Controller (MC) solution and integrates it with AirWave. The network administrator configures the SNMP and terminal credentials in the MM and MC, and then monitors the mobility devices from AirWave, including Clarity for user association and basic network services verification. However, AirWave does not display any UCC data that is available in the MM dashboard. Based on the information shown in the exhibit, which configuration step should the network administrator do next in the MM to complete the integration with AirWave?



A. Define AirWave as a management server in the MM.
B. Enable the inline network services statistics in the AMP profile.
C. Enable UCC monitoring in the AMP profile.
D. Verify the papi-security key in the AMP profile.

Answer: C
Explanation:
Default AMP mgmt profile has UCC monitoring disabled.

QUESTION 6
Refer to the exhibit. A network administrator configures an Instant AP (IAP) to establish an Aruba IPSec tunnel across the Internet, and configures two DHCP pools for wireless users. Based on the output shown in the exhibit, which device behaves as a DHCP server for the users?

```
(MC14-1) [MDC] #show iap table long

Trusted Branch Validation:     Enabled
IAP  Branch Table
-------------------------
Name VC  MAC Address  Status  Inner IP    Assigned Subnet  Assigned Vlan     Key                                                  Bid(Subnet Name)
                                                Tunnel End Points
-------- ---------------------- --------- -----------   ---------------------- ---------------------   ---------   ----------------------------
                                                -------------------------

IAP-1  a8:bd:27:c5:c3:3a UP     2.2.2.2          10.21.124.32/27     25     1f70772b01fdc02472357885f21393a9120e1823e154e98839  0(10.21.124.1-10.21.1
24.254,16), 0 (10.25.16.2-10.25.23.254,110:25)

Total No of UP Branches        :1
Total No of DOWN Branches      :0
Total No of Branches           :1
```

A. Mobility Master
B. Mobility Controller
C. External server
D. DSL modem
E. Virtual Controller

Answer: E
Explanation:
This process happens when you deploy distributed mode. In distributed mode DHCP should be virtual controller.

QUESTION 7
An airline wants to invest in an Aruba Mobility (MM)-Mobility Controller (MC) solution for the three hubs it has throughout the country. A single MM is located in the datacenter at one of the hubs. The MCs in the other two hubs reach the MM through a site-to-site IPSec VPN. The operations team does not want to lose monitoring and configuration control of the MCs if something happens to the datacenter where the MM resides. Which solution ensures that there is management access to the MCs in case of an MM failure due to a datacenter outage?

A. Deploy another MM in a different location, and enable L2 redundancy.
B. Install AirWave Management Platform, and enable Read and Write Management access on devices.
C. Deploy another MM in a different location, and enable L3 redundancy.
D. Deploy a local MM on each hub, and synchronize the configuration between all MMs.

Answer: C
Explanation:
L3 redundancy because of different physical location so IP communication is needed.

QUESTION 8

Refer to the exhibit. A network administrator deploys a new WLAN named Corp-Network. The security suite is WPA2 with 802.1X. A new ClearPass server is used as the authentication server. Connection attempts to this WLAN are rejected, and no trace of the attempt is seen in the ClearPass Policy Manager Access Tracker.
However, the network administrator is able to see the logs shown in the exhibit.
What must the network administrator do to solve the problem?

```
(MC14-1) #show log security 180

Jul 16 01:09:55    :124004:    <3573> <DBUG> |authmgr| Select server for method=802.1x,
user=host/wireless14.training.arubanetworks.com, essid=Corp-network, server-group=CAMPUS, last_srv <>
Jul 16 01:09:55    :124038:    <3573> <INFO> |authmgr| Reused server ClearPass for method=802.1x;
user=host/wireless14.training.arubanetworks.com, essid Corp-network, domain=<>, server-group=CAMPUS
Jul 16 01:09:55    :124004:    <3573> <DBUG> |authmgr| aal_auth_raw (1399) (INC) : os_auths 1, s ClearPass type 2 inservice 1
markedD 0 sg_name CAMPUS
Jul 16 01:09:55    :124004:    <3573> <DBUG> |authmgr| aal_auth_raw (1402) (INC) : os_reqs 1, s ClearPass type 2 inservice 1 markedD
0
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=18, server=ClearPass, IP=10.254.1.23,
server-group=CAMPUS, fd=87
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass: 10.254.1.23:1812
id:18, len:249
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name:
host/wireless14.training.arubanetworks.com
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.100
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 704D7B109EC6
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 204C0306E5C0
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\006
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-network
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP21
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2381] Aruba-Device-Type: (VSA with invalid
length – Don't send it)
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: phu\025\347\376\016\030
\253a-\014a\033\200\234
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_sequence.c:117] seq_num_timeout_handler: Freed 0
entries
Jul 16 01:10:00    :124004:    <3573> <WARN> |authmgr| |aaa| RADIUS server ClearPass server-group CAMPUS –
10.254.1.23-1812 timoeout for client=70:4d:7b:10:9e:c6 auth method 802.1x
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:1203] Sending radius request to ClearPass
server-group CAMPUS -10.254.1.23-1812 (retry1)
Jul 16 01:10:00    :124004:    <3573> <DBUG> |authmgr| APAE_Aborting_Tineout (5076) (DEC) : os_auths 0, s ClearPass
type 2 inservice 1 markedD 0 sg_name CAMPUS
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=18, server=(null), IP=
10.254.1.23, server-group=(null) fd=87
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server= (null), IP=
10.254.1.23, server-group=(null), fd=87
Jul 16 01:10:00    :121014:    <3573> <ERRS> |authmgr| |aaa| Received invalid reply digest from RADIUS server
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=18, server=ClearPass, IP=
10.254.1.23, server-group=CAMPUS fd=87
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc api.c:1228] Bad or unknown response from AAA server
```

A. Add the correct network device IP address in ClearPass.
B. Change the ClearPass server IP address in the MC.
C. Fix the RADIUS shared secret in the MC.
D. Disable machine authentication in the MC and client PC.

Answer: C
Explanation:
Logs show response is bad digest from RADIUS.

QUESTION 9
Refer to the exhibit. A network engineer configures some VAPs in customer groups and creates a pool of licenses with enough units for seven APs. The network engineer deploys the first two APs, looks at the ap database, and notices the APs are inactive and experience licensing-related issues. Based on the show command outputs shown in the exhibit, what must the engineer do to solve the problem?

```
(MC14-1) #show ap database | exclude =

AP Database
----------------
Name              Group     AP Type   IP Address        Status      Flags  Switch IP      Standby IP
---------         ---------  ---------  ----------------  ----------  ---------  ---------------  ----------------
70:3a:0e:cd:b0:a4 default     335       10.1.145.150      Up 3m:4s    IL     10.1.140.100   0.0.0.0
70:3a:0e:cd:b0:ac default     335       10.1.146.150      Up 3m:12s   IL     10.1.140.100   0.0.0.0

Total APs:2
(MC14-1) #
(MC14-1) #show license client-table

Built-in limit: 0
License Client Table
----------------------------
Service Type                                  System Limit  Server Lic.  Used Lic.  Remaining Lic.  FeatureBit
----------------                              ------------  -----------  ---------  --------------  ----------
Access Points                                 64            7            0          7               enabled
Next Generation Policy Enforcement Firewall Module  64      7            0          7               enabled
RF Protect                                    64            7            0          7               enabled
Advanced Cryptography                         4096          0            0          0               disabled
WebCC                                         64            0            0          0               disabled
MM-VA                                         65            0            1          0               enabled
MC-VA-RW                                      64            0            0          0               disabled
MC-VA-EG                                      64            0            0          0               disabled
MC-VA-IL                                      64            0            0          0               disabled
MC-VA-JP                                      64            0            0          0               disabled
MC-VA-US                                      64            0            0          0               disabled
VIA                                           4096          0            0          0               disabled
(MC14-1) #
(MC14-1) #show version | include Aruba

Aruba Operating System Software.
ArubaOS (MODEL: Aruba7030-US), Version 8.2.1.0
(MC14-1) #
```

A. Allocate two more MM-VA licenses to the pool.
B. Allocate two more MC-VA-US licenses to the pool.
C. Allocate seven more MM-VA licenses to the pool.
D. Allocate seven more MC-VA-US licenses to the pool.

Answer: C
Explanation:
As per the output total devices(controller+AP) = 8
This is a hardware controller model 7030, answer B & D only applicable for VMs.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**