# HPE6-A48$^{Q\&As}$

## Aruba Certified Mobility Expert 8 Written Exam

## Pass HP HPE6-A48 Exam with 100% Guarantee

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

https://www.leads4pass.com/hpe6-a48.html

### 100% Passing Guarantee
### 100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

**QUESTION 1**

Refer to the exhibit.



**New WLAN**

General — VLANs — Security — Access

More Secure
  Enterprise
  Personal
  Open
Less Secure

| | |
|---|---|
| Key management: | WPA-2 Personal |
| Passphrase: | •••••••••• |
| Retype: | •••••••••• |
| MAC authentication: | Enabled |
| Blacklisting: | Disabled |

General — VLANs — Security — Access

Default role: logon

Mac authentication role: scanners

Show roles

(A48.01114361)

A company acquires ten barcode scanners to run inventory tasks. These Wifi devices support WPA2-PSK security only. The network administrator deploys a WLAN named scanners using the configuration shown in the exhibit.

What must the network administrator do next to ensure that the scanner devices successfully connect to their SSID?

A. Add scanner MAC addresses in user derivation rules.

B. Add scanner MAC addresses in the internal database.

C. Set internal as the MAC authentication server group.

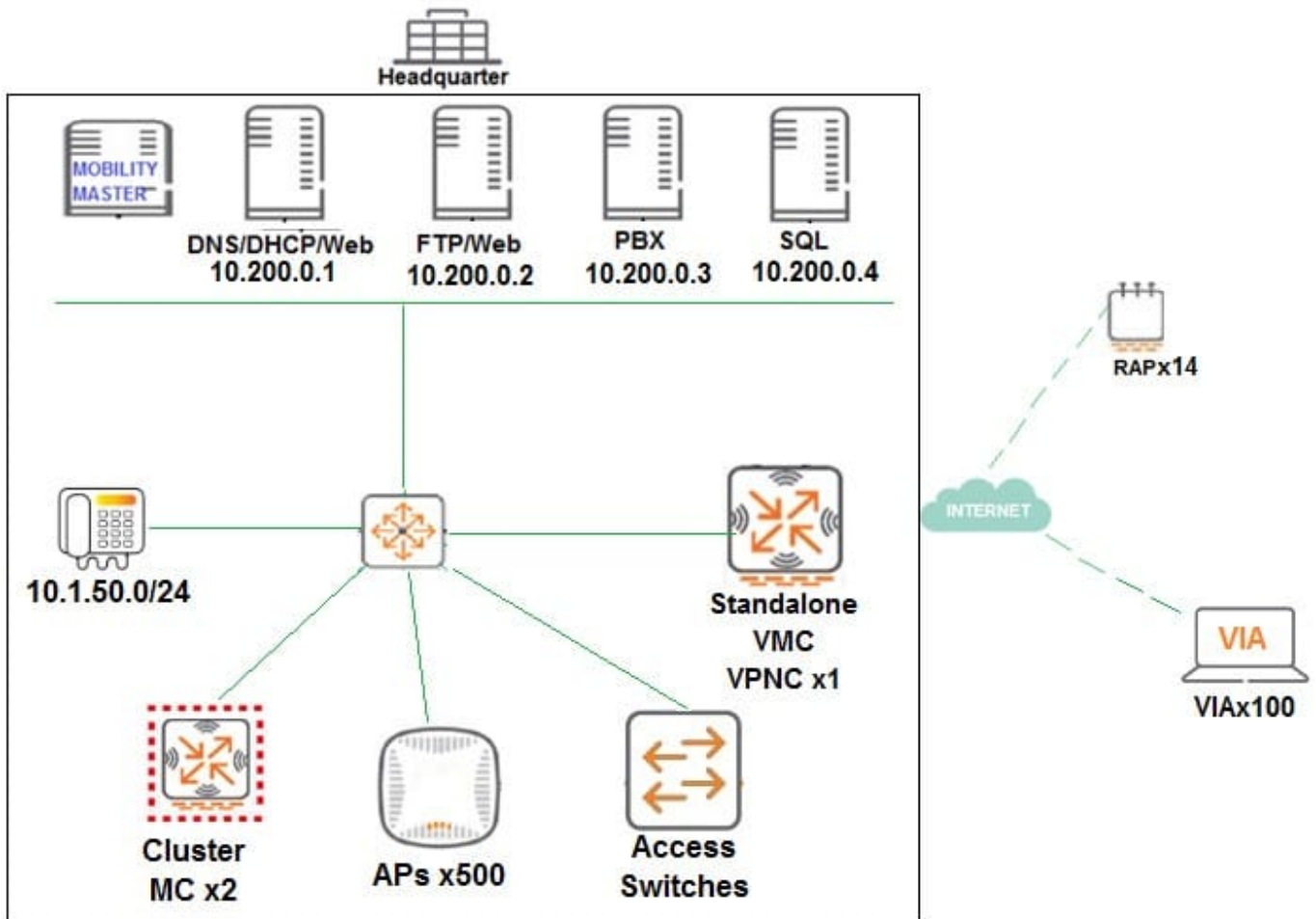D. Enable L2 Authentication Fail Through.

Correct Answer: C

**QUESTION 2**

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.

| Cluster | Redundancy | **VPN** | Firewall | IP Mobility | External Services | Guest Provisioning | DHCP Server | WAN |
|---|---|---|---|---|---|---|---|---|

> IKEv1

> IKEv2

⌄ **General VPN**

**Address Pools**

| POOL NAME | START ADDRESS | END ADDRESS |
|---|---|---|
| raps | 172.16.0.0 | 172.16.0.254 |

**+**

NAT-T:

Source-nat:

Aggressive group name: | changeme | (Only needed for XAUTH)

Server-certificate for VPN clients: | -None-

PRIMARY DNS SERVER:

SECONDARY DNS SERVER:

PRIMARY WINS SERVER:

SECONDARY WINS SERVER:

> Dialer
> Shared Secrets
> Certificates for VPN Clients

The standalone VMC will act as a VPN Concentrator of the RAPs. The network administrator configures the Standalone VMC with a pool of addresses and the SOHOs AP Group from the MM.

Which additional steps must the network administrator perform to allow the RAPs to terminate their IPSec tunnels and associate to the Standalone VMC?

A. Add RAP MAC addresses into the RAP whitelist, and associate them with the SOHOs AP-Group.

B. Add RAP MAC addresses into the CPSec whitelist, and associate them with the SOHOs AP-Group.

C. Configure the same IP Pool at the MM group level, then create user accounts for the RAPs in the internal database.

D. Create user accounts with the sys-ap-role, and define shared secrets to associate to RAP IP addresses at the MM group level.

Correct Answer: D

**QUESTION 3**

Refer to the exhibit.
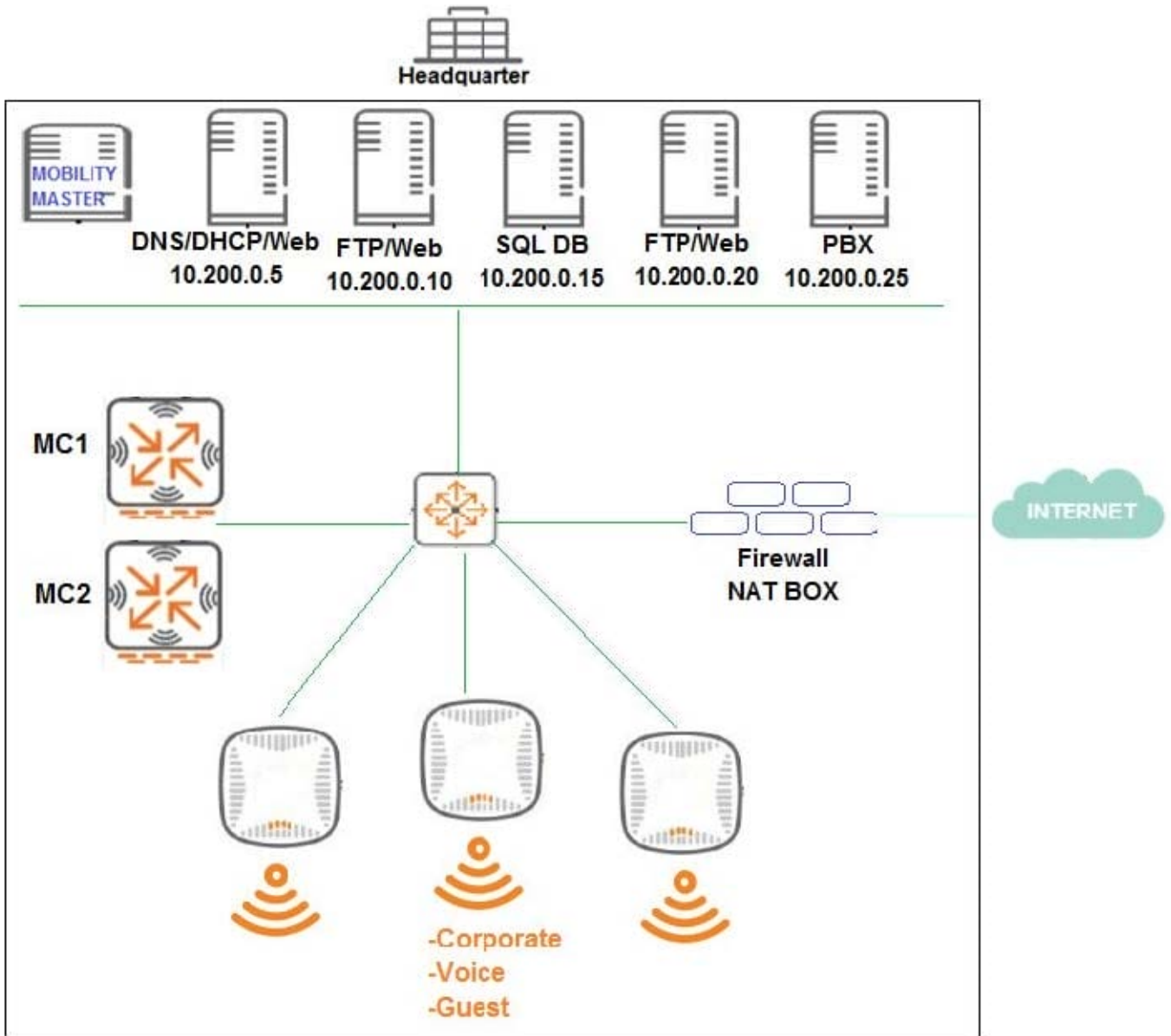


An organization provides WiFi access through a corporate SSID with an Aruba Mobility Master (MM)Mobility Controller (MC) network that includes PEF functions. The organization wants to have a single firewall policy configured and applied to the employee role.

This policy must allow users to reach Web, FTP, and DNS services, as shown in the exhibit. Other services should be exclusive to other roles. The client NICs should receive IP settings dynamically.

Which policy design meets the organization\'s requirements while minimizing the number of policy rules?

A. netdestination alias1 host 10.200.0.10 host 10.200.0.20 ip access-list session policy1 user host 10.200.0.5 svc-dns permit user host 10.200.0.5 svc-http permit

user alias alias1 svc-http permit user alias alias1 svc-ftp permit

B. netdestination alias1 host 10.200.0.5 host 10.200.0.10 host 10.200.0.20 netdestination alias2 host 10.200.0.10 host

10.200.0.20 ip access-list session policy1 any any svc-dhcp permit user host 10.200.0.5 svc-dns permit user alias alias1 svc-http permit user alias alias2 svc-ftp permit

C. netdestination alias1 host 10.200.0.10 host 10.200.0.20 ip access-list session policy1 any any svc-dhcp permit user host 10.200.0.5 svc-dns permit user host 10.200.0.5 svc-http permit user alias alias1 svc-http permit user alias alias1 svc-ftp permit

D. netdestination alias1 host 10.200.0.5 host 10.200.0.10 host 10.200.0.20 netdestination alias2
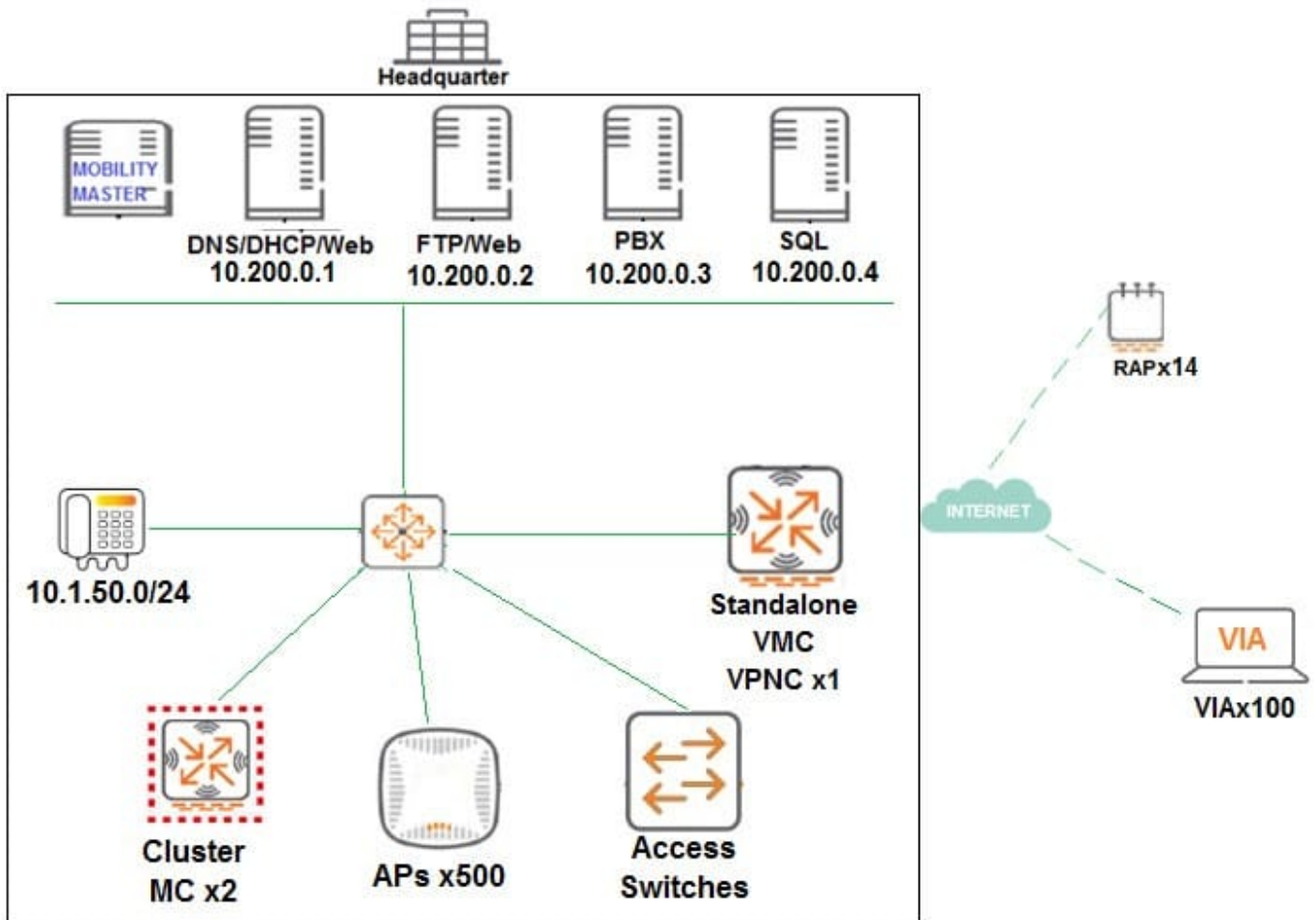
Correct Answer: C

---

**QUESTION 4**

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.

Refer to the scenario and the exhibit.

What is the minimal license capacity in use to support this proposal?

A. License     Number

| License | Number |
| --- | --- |
| MM-VA | 502 |
| Access Points | 514 |
| PEF | 514 |
| RF Protect | 514 |
| VIA | 100 |

B. License     Number

| License | Number |
| --- | --- |
| MM-VA | 503 |
| MC-VA | 14 |
| Access Points | 514 |
| PEF | 514 |
| VIA | 100 |

C. License     Number

| License | Number |
| --- | --- |
| MM-VA | 517 |
| MC-VA | 114 |
| Access Points | 514 |
| PEF | 514 |
| VIA | 100 |

D. License     Number

| License | Number |
| --- | --- |
| MM-VA | 502 |
| MC-VA | 14 |
| Access Points | 514 |
| PEF | 514 |
| RF Protect | 500 |
| VIA | 100 |

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

**QUESTION 5**

Refer to the exhibit.

```
Access-1 (config) # show tunneled-node-server state

Local Master Server (LMS) State

LMS Type       IP Address      State       Capability   Role
Primary    :   10.1.140.100    Complete    Per User     Operational Primary
Secondary  :   10.1.140.101    Complete    Per User     Operational Secondary

Switch Anchor Controller (SAC) State
                  IP Address    Mac Address          State
SAC           :   10.1.140.100  204c03-06e5c0        Registered
Standby-SAC   :   10.1.140.101  204c03-06e790        Registered

User Anchor Controller (UAC)  :  10.1.140.100
User                Port      VLAN       State        Bucket ID
005056-a5510b       20        143        Registered   255

User Anchor Controller (UAC) : 10.1.140.101
User                Port      VLAN       State        Backet ID
```

Based on the output shown in the exhibitm with which Aruba devices has Access-1 established tunnels?

A. a pair of MCs within a cluster

B. a single standalone MC

C. a pair of MCs with APFF enabled

D. a pair of switches

Correct Answer: B

**QUESTION 6**

Refer to the exhibit.

(A48.0.11i4234)

A network administrator wants to configure an 802.1x supplicamt 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 Additonal Settings.

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

A. Enable user authentication under Settings.

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

C. Enable server certificate validation under Settings.

D. Enable computer autentication under Settings.

Correct Answer: B

**QUESTION 7**

Refer to the exhibit.

(MM1) [mynode] #show airmatch debug history ap-name AP20

2 GHz radio mac 70:3a:0e:5b:0a:c0    ap name   AP20

| Time of Change | Chan | Bandwidth | EIRP(dBm) | Mode | Source |
|---|---|---|---|---|---|
| 2018-07-16 05:01:56 | 11->11 | 20-> 20 | 8.0-> 23.0 | AP->AP | Solver |
| 2018-07-16 05:01:48 | 6 ->11 | 20-> 20 | 8.0-> 8.0 | AP ->AP | Solver |
| 2018-07-15 13:26:13 | 11 -> 7 | 20-> 40 | 8.0-> 6.0 | AP ->AP | Min Channel Bandwidth Change |
| 2018-07-15 12:21:39 | 1 ->11 | 40-> 20 | 8.0-> 6.0 | AP ->AP | Max Channel Bandwidth Change |
| 2018-07-15 12:20:08 | 11 -> 1 | 20-> 40 | 8.0-> 6.0 | AP ->AP | Min Channel Bandwidth Change |
| 2018-07-15 12:18:47 | 7 ->11 | 40-> 20 | 8.0-> 6.0 | AP ->AP | Max Channel Bandwidth Change |
| 2018-07-15 11:47:26 | 11-> 7 | 20-> 40 | 8.0-> 6.0 | AP ->AP | Min Channel Bandwidth Change |

Help desk staff receive reports from users that there is inefficient wireless service in a location serviced by AP20, AP21, and AP22, and open a ticket. A few hours later, the users report that there is a drastic improvement in service. The staff still wants to determine the cause of the problem so the next day thay start monitoring the tasks.

They access the Mobility Master (MM), and obtain the output shown in the exhibit.

What could be the cause of the problem that the users reported?

A. AirMatch was running an initial incremental optimization.

B. An operator used AirMatch to manually freeze AP channel and power.

C. An operator manually assigned settings in the radio profile.

D. AirMatch was running a full on-demand optimization.

Correct Answer: B

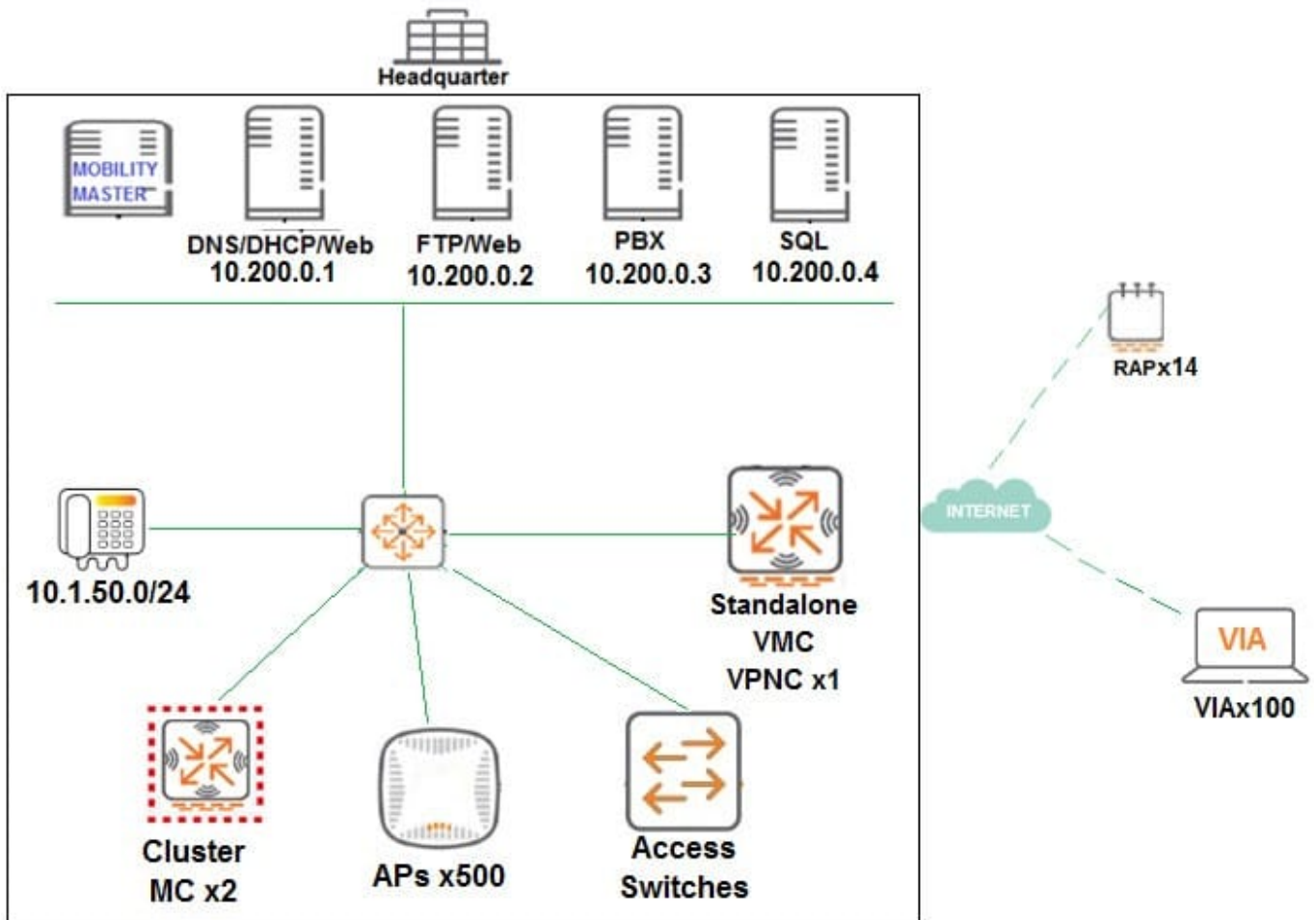**QUESTION 8**

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.

Refer to the scenario and the exhibit.

(MC2) [MDC] #show ip access-list split-tunneling

ip access-list session split-tunneling
split-tunnelimg
-----------------------

| Priority | Source | Destination | Service | Application | Action | TimeRange |
|----------|--------|-------------|---------|-------------|--------|-----------|
| 1 | any | any | svc-dhcp | | permit | |

| Log | Expired | Queue | TOS | 8021P | Blacklist | Mirror DisScan | IPv4/6 | | |
|-----|---------|-------|-----|-------|-----------|----------------|--------|--|--|
| 2 | | Low user | 10.200.0.0.255.255.255.252 any | | | | 4 | permit | |
| 3 | 10.200.0.0 255.255.255.252 user | Low | | any | | | 4 | permit | |
| 4 | user | Low | 10.1.50.0 255.255.255.0 | svc-rtsp | | | 4 | permit | |
| 5 | user | Low | 10.1.50.0 255.255.255.0 | svc-sip-udp | | | 4 | permit | |
| 6 | 10.1.50.0 255.255.255.0 user | Low | | svc-rtsp | | | 4 | permit | |
| 7 | 10.1.50.0 255.255.255.0 user | Low | | svc-sip-udp | | | 4 | permit | |
| | | Low | | | | | 4 | | |

Which command must the network administrator add in the split-tunneling policy to meet the requirements for the RAP employee SSID?

A. user any svc-http permit

B. user any any src-nat pool dynamic-srcnat

C. any user any src-nat pool dynamic-srcnat

D. user any any dst-nat

Correct Answer: B

**QUESTION 9**

A network administrator implements a SIP-based IP telephone solution. The objective is to ensure that APs use 100% of

their airtime for network access whenever a voice call is taking place, to minimize communication delays. The network administrator also wants to ensure that a log entry is generated when voice calls occur.

Which setup accomplishes these tasks?

A. ip access-list session voice user any svc-rtsp permit log queue high user any svc-sip-udp permit log queue high

B. ip access-list session voice user any-svc-rtsp permit disable-scanning log user any svc-sip-udp permit disable-scanning log

C. ip access-list session voice user any svc-rtsp permit log dot1p-priority 7 user any svc-sip-udp permit log dot1p-priority 7

D. ip access-list session voice user any svc-rtsp permit log tos 56 user any svc-sip-udp permit log tos 56

Correct Answer: C

---

**QUESTION 10**

Refer to the exhibit.

```
a8:bd:27:c5:c3:3a# sh dhcp subnets
```

**DHCP Subnet Table**
--------------------------------

| VLAN | Type | Subnet | Mask | Gateway | Mode | Rolemap |
|------|------|--------|------|---------|------|---------|
| 124 | l3 | 10.21.124.32 | 255.255.255.224 | 10.21.124.33 | local,split-tunnel | |
| 81 | l2 | 0.0.0.0 | 255.255.255.255 | 0.0.0.0 | remote,full-tunnel | |

A network engineer deploys two different DHCP pools in an Instant AP (IAP) cluster for WLANs that will have connectivity to a remote site using Aruba IPSec.

Based on the output shown in the exhibit, which IAP-VPN DHCP modes are being used?

A. distributed L3 and centralized L3

B. distributed L3 and local L3

C. distributed L3 and centralized L2

D. local L3 and centralized L2

Correct Answer: C

---

**QUESTION 11**

Refer to the exhibits.
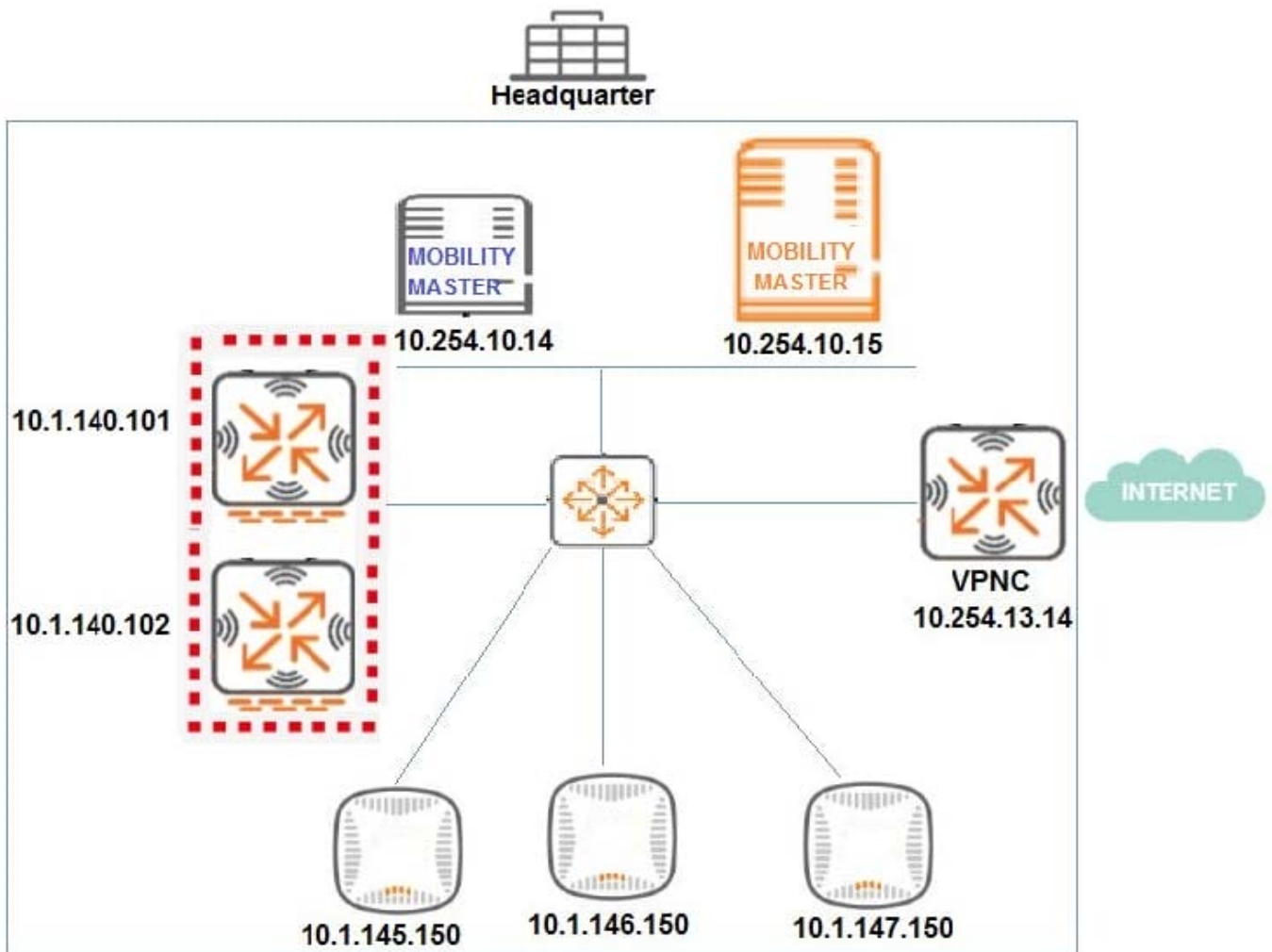
Exhibit 1

Exhibit 2

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

AP Database
-------------------

Name        Group       AP Type      IP Address      Status  Flags  Switch IP  Standby IP
--------    --------    ----------    ---------------  --------  -------  -------------  ---------------

Total APs:0
(MC14-1) #ping 10.1.145.150

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 10.1.145.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.206/0.2402/0.356 ms
```

Exhibit 3

```
[      11.611533] bonding: bond0: link status definitely down for interface eth1, disabling it
Starting watchdog process...
Getting an IP address...
[      12.689236] device eth0 entered promiscuous mode
10.1.145.150 255.255.255.0 10.1.145.1
Running ADP...Done.Master is 10.1.140.100
[      22.039696] ath_hal: 0.9.17.1 (AR5416, AR9380, REGOPS_FUNC, WRITE_EEPROM, 11D)
[      22.131095] ath_rate_atheros: Copyright (c) 2001-2005 Atheros Communications, Inc, All Rights Reserved

[      37.552112] pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
[      37.638632] pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
AP rebooted due to loss power
shutting down watchdog process (nanny will restart it)...
         <<<<<       Welcome to the Access Point       >>>>>
– # ping 10.1.140.100
PING 10.1.140.100 (10.1.140.100): 56 data bytes
^C
--- 10.1.140.100 ping statistics ---
40 packets transmitted, 0 packets received, 100% packet loss
– # ping 10.1.140.1
PING 10.1.140.1 (10.1.140.1) : 56 data bytes
64 bytes from 10.1.140.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 10.1.140.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.1.140.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 10.1.140.1: icmp_seq=3 ttl=255 time=0.3 ms
64 bytes from 10.1.140.1: icmp_seq=4 ttl=255 time=0.3 ms
^C
--- 10.1.140.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
– #
```

A network engineer deploys a Master Controller (MC) cluster at Headquarter to offer high levels of redundancy, and prepares the wired side of the network. This preparation includes the VLAN, DHCP Settings, and unicast routing services that APs require to reach the cluster.

The network engineer waits for 20 minutes after connecting the APs and sees that no SSIDs are advertised. The network engineer logs into one of the MCs and one of the AP\\'s consoles to obtain the outputs shown in the exhibits.
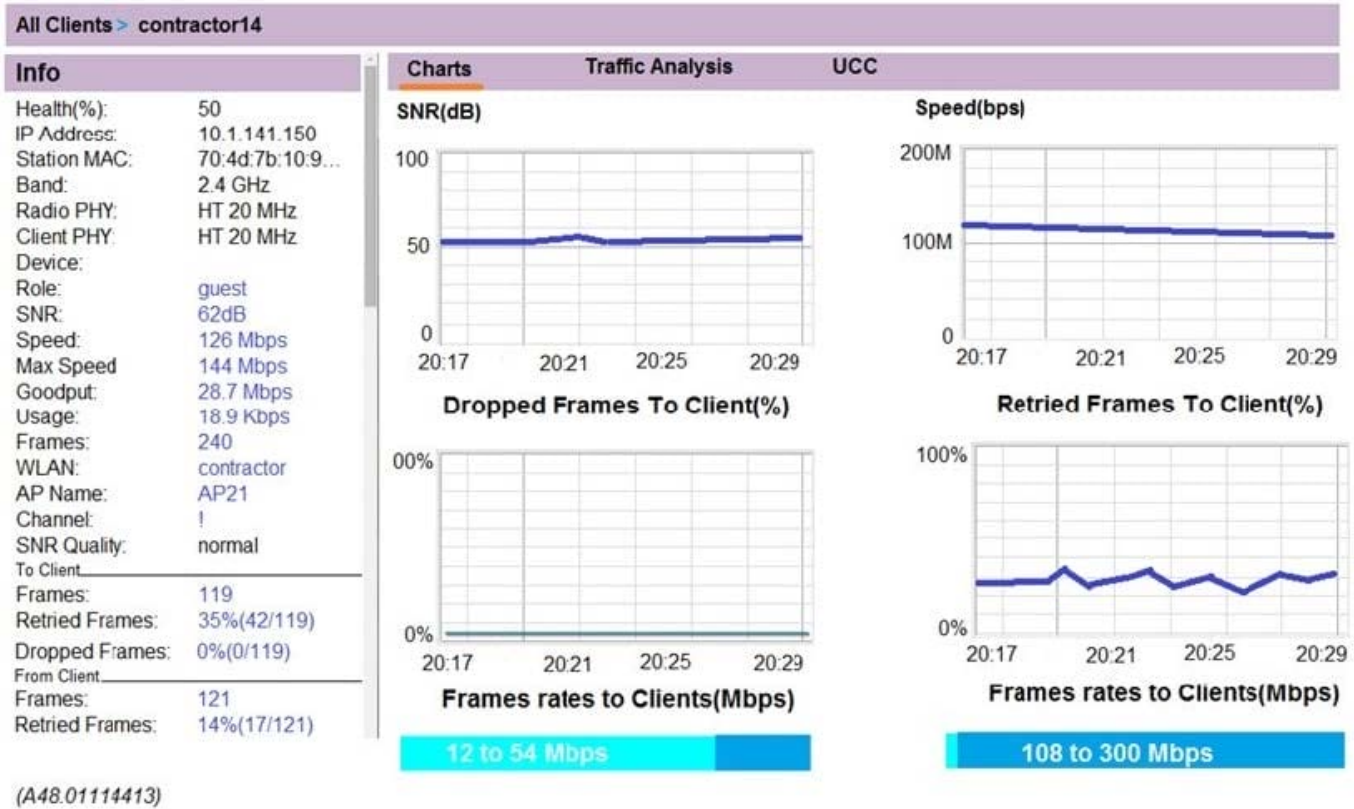
What can the network engineer do to fix the APs discovery process, to ensure the best scalability even if one MC fails?

A. Reprovision the APs with a different Master IP.

B. Modify the IP address in one of the MCs.

C. Modify option 43 in the DHCP pool.

D. Create a VRRP instance in the MCs.

Correct Answer: C

**QUESTION 12**

Refer to the exhibit.



**All Clients > contractor14**

| Info | |
|---|---|
| Health(%): | 50 |
| IP Address: | 10.1.141.150 |
| Station MAC: | 70:4d:7b:10:9... |
| Band: | 2.4 GHz |
| Radio PHY: | HT 20 MHz |
| Client PHY: | HT 20 MHz |
| Device: | |
| Role: | guest |
| SNR: | 62dB |
| Speed: | 126 Mbps |
| Max Speed | 144 Mbps |
| Goodput: | 28.7 Mbps |
| Usage: | 18.9 Kbps |
| Frames: | 240 |
| WLAN: | contractor |
| AP Name: | AP21 |
| Channel: | ! |
| SNR Quality: | normal |
| To Client | |
| Frames: | 119 |
| Retried Frames: | 35%(42/119) |
| Dropped Frames: | 0%(0/119) |
| From Client | |
| Frames: | 121 |
| Retried Frames: | 14%(17/121) |

(A48.01114413)

A user reports show response time to a network administrator and suggests that there might be a problem with the WLAN. The user\\'s laptop supports 802.11n in the 2.4 GHz band only. The network administrator finds the user on the Mobility Master (MM) and reviews the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

A. Client health is low, and retried frames are high. It is possible there is high channel utilization.

B. Client health is low, but SNR is high. It is possible data in the dashboard is not accurate and needs to be updated.

C. The speed is good. Client health seems to be related to a problem with the client NIC.

D. The network is low because of low SNR. TX power must be increased in both the client and the AP.

Correct Answer: B

---

**QUESTION 13**

Refer to the exhibit.

```
(MC1) [MDC] #show ip access-list no-webapps

ip access-list session no-webapps
no-webapps
--------------------
```

| Priority | Source | Destination | Service | Application | Action | TimeRange | Log | Expired | Queue | TOS | 8021P | Blacklist | Mirror | DisScan | IPv4/6 | Contract |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | user | any | | app facebook | deny send-deny-response | | | | | Low | | | | | | 4 |
| 2 | user | any | | app youtube | deny send-deny-response | | | | | Low | | | | | | 4 |
| 1 | user | any | | app netflix | deny send-deny-response | | | | | Low | | | | | | 4 |

A network administrator completes the initial configuration dialog of the Mobility Controllers (MCs) and they join the Mobility Master (MM) for the first time. After the MM-MC association process, the network administrator only creates AP groups, VAPs, and roles. Next, the network administrator proceeds with the configuration of the policies and creates the policy shown in the exhibit.

Which additional steps must be done to make sure this configuration takes effecr over the contractor users?

A. Apply the policy in the contractors user role. Enable deep packet inspection.

B. Apply the policy in the contractors user role. Enable deep packet inspection. Reload the MCs.

C. Enable the firewall visibility. Enable web-content classification Reload the MCs.

D. Enable firewall visibility Enable web-content classification Reload the MMs.

Correct Answer: A

---

**QUESTION 14**

Refer to the exhibits.

Exhibit 1

**CONTROLLERS** | **ACCESS POINTS** | **CLIENTS** | **ALERTS**
✓ 1  ( ! ) 1  |  ✓ 2  ( ! ) 0  |  📶 1  🕸 0  |  ⚠ 0

> **MC14-1**

| | |
|---|---|
| Name: | MC14-1 |
| Reachability: | Unreachable |
| Health: | Good |
| Uptime: | - |
| Model: | Aruba7030-US |
| Serial Number: | CRDD12919 |
| Country: | - |
| Group: | md > Westcoast > SantaClara > Building1 |
| Configuration State: | - |
| Configuration Version: | - |

(A48.01114452)

Exhibit 2 A network administrator adds a new Mobility Controller (MC) to the production Mobility Master (MM) and deploys APs that start broadcasting the employees SSID in the West wing of the building. Suddenly, the employed report client disconnects. When accessing the MM the network administrator notices that the MC is unreachable, then proceeds to access the MC\\'s console and obtains the outputs shown in the exhibits.

```
top2 – 22:23:48 up 6:11, 0 users, load average: 0.11, 0.10, 0.08
Tasks: 202 total, 2 running, 198 sleeping, 0 stopped, 2 zombie
Cpu(s): 1.2%us, 2.9%sy, 0.2%ni, 95.6%id, 0.1wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3085600k total, 1831312k used, 1254288k free, 19488k      buffers
Swap: 1048544k total,      0k useed, 1048544k free, 889680k      cached
```

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 3556 | root | 20 | 0 | 147m | 79m | 15m | R | 85 | 2.7 | 0:39.54 | profmgr |
| 3017 | root | 20 | 0 | 9472 | 3952 | 2656 | S | 23 | 0.1 | 1:30.44 | syslogd |
| 3565 | root | 10 | -10 | 132m | 36m | 13m | S | 15 | 1.2 | 0:37.09 | auth |
| 4007 | root | 20 | 0 | 68208 | 8896 | 5920 | S | 10 | 0.3 | 0:23.41 | ofa |
| 3497 | root | 20 | 0 | 334m | 137m | 10m | S | 6 | 4.6 | 11:31.80 | fpapps |
| 3894 | root | 20 | 0 | 124m | 23m | 5472 | S | 6 | 0.8 | 0:10.00 | dds |
| 4125 | root | 20 | 0 | 52640 | 6496 | 3296 | S | 6 | 0.2 | 0:28.97 | vrrp |
| 13 | root | 20 | 0 | 0 | 0 | 0 | S | 4 | 0.0 | 0:02.05 | everts/1 |
| 3583 | root | 20 | 0 | 173m | 25m | 9696 | S | 4 | 0.8 | 1:47.79 | stm |
| 12505 | root | 20 | 0 | 3104 | 1680 | 1248 | R | 4 | 0.1 | 0:00.03 | top2 |
| 3511 | root | 20 | 0 | 51088 | 6288 | 3712 | S | 2 | 0.2 | 0:04.90 | pim |
| 3807 | root | 20 | 0 | 220m | 71m | 5568 | S | 2 | 2.4 | 0:18.20 | fw_visibility |
| 1 | root | 20 | 0 | 4160 | 1104 | 912 | S | 0 | 0.0 | 0:03.13 | init |
| 2 | root | 20 | 0 | 0 | 0 | 0 | S | 0 | 0.0 | 0:00.00 | kthreadd |

What should the network administrator do next to solve the current problem?

A. Decommission the MC from the MM, and add it again.

B. Open a TAC case, and send the output of tar crash.

C. Verify the license pools in the MM.

D. Kill two zombie processes, then reboot the MC.

Correct Answer: D

**QUESTION 15**

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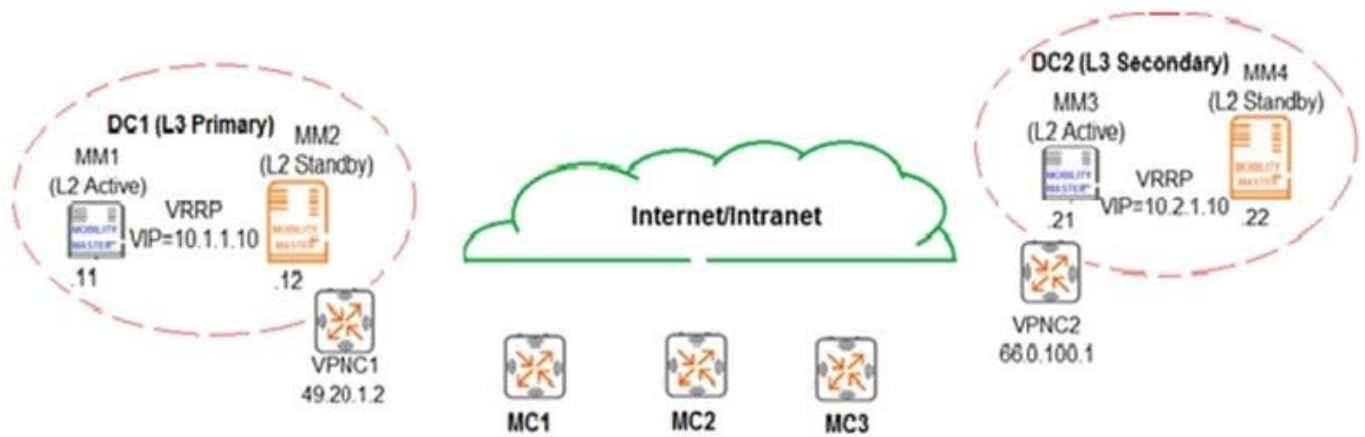
An Aruba network is deployed with L2 and L3 Mobility Master (MM) redundancy across two datacenters, as shown in the exhibit. The network administrator confirms that all Mobility Controllers (MC) are currently communicating with MM1, which is the L2 Active, and L3 Primary. Which MM IP will MCs communicate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

A. 10.1.1.10

B. 10.1.1.12

C. 10.2.1.10

D. 10.2.1.21

Correct Answer: B

[HPE6-A48 PDF Dumps](#)          [HPE6-A48 VCE Dumps](#)          [HPE6-A48 Practice Test](#)