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

Refer to the exhibits.

```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(MM1) [md] (config) #user-role corp-employee
(MM1) ^[md] (config-submode)#access-list session allowall
(MM1) ^[md] (config-submode)#exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #aaa profile corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-default-role corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-server-group Radius
(MM1) ^[md] (AAA Profile "corp-employee") #exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #write memory

Saving Configuration...

Configuration Saved.
```

```
(MM1) [md] (config) #cd MC1
(MM1) [20:4c:03:06:e5:c0] (config) #mdc
```

```
Redirecting to Managed Device Shell

(MC1)  [MDC] #show switches

All Switches
------------
IP Address     IPv6 Address  Name  Location          Type  Model      Version        Status  Configuration State  Config Sy
----------     ------------  ----  --------          ----  -----      -------        ------  -------------------  ---------
10.1.140.100   None          MC1   Building1.floor1  MD    Aruba7030  8.6.0.2_73853  up      UPDATE SUCCESSFUL    11

Total Switches:1
(MC1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP             MAC             Name           Role    Age(d:h:m)  Auth     VPN link  AP name  Roaming   Essid/Bssid/Ph
----------     ------------        ------         ----    ----------  ----     --------  -------  -------
10.1.141.150   yy:yy:yy:yy:yy:yy   hector.barbosa guest   00:00:23    802.1x             AP22     Wireless  corp-employee/

User Entries: 1/1
 Curr/Cum Alloc:3/18 Free:0/15 Dyn:3 AllocErr:0 FreeErr:0
(MC1) [MD] #show aaa profile corp-employee


AAA Profile "corp-employee"
---------------------------
Parameter                                          Value
---------                                          -----
Initial role                                       guest
MAC Authentication Profile                         N/A
MAC Authentication Server Group                    default
802.1X Authentication Profile                      corp-employee_dot1_aut
802.1X Authentication Server Group                 Radius
Download Role from CPPM                            Disabled
Set username from dhcp option 12                   Disabled
L2 Authentication Fail Through                     Disabled
Multiple Server Accounting                         Disabled
User idle timeout                                  N/A
Max IPv4 for wireless user                         2
RADIUS Accounting Server Group                     N/A
RADIUS Roaming Accounting                          Disabled
RADIUS Interim Accounting                          Disabled
RADIUS Acct-Session-Id In Access-Request           Disabled
RFC 3576 server                                    N/A
User derivation rules                              N/A
Wired to Wireless Roaming                          Enabled
Reauthenticate wired user on VLAN change           Disabled
Device Type Classification                         Enabled
Enforce DHCP                                       Disabled
PAN Firewall Integration                           Disabled
Open SSID radius accounting                        Disabled
Apply ageout mechanism on bridge mode wireless clients  Disabled
(MC1) [MDC] #
```

A network administrator has fully deployed a WPA3 based WLAN with 802.1X authentication. Later he defined corp-employee as the default user-role for the 802.1X authentication method in the aaa profile. When testing the setup he realizes the client gets the "guest" role.

What is the reason "corp-employee" user role was not assigned?

A. The administrator forgot to map a dot1x profile to the corp-employee aaa profile.

B. The administrator forgot to enable PEFNG feature set on the Mobility Master.

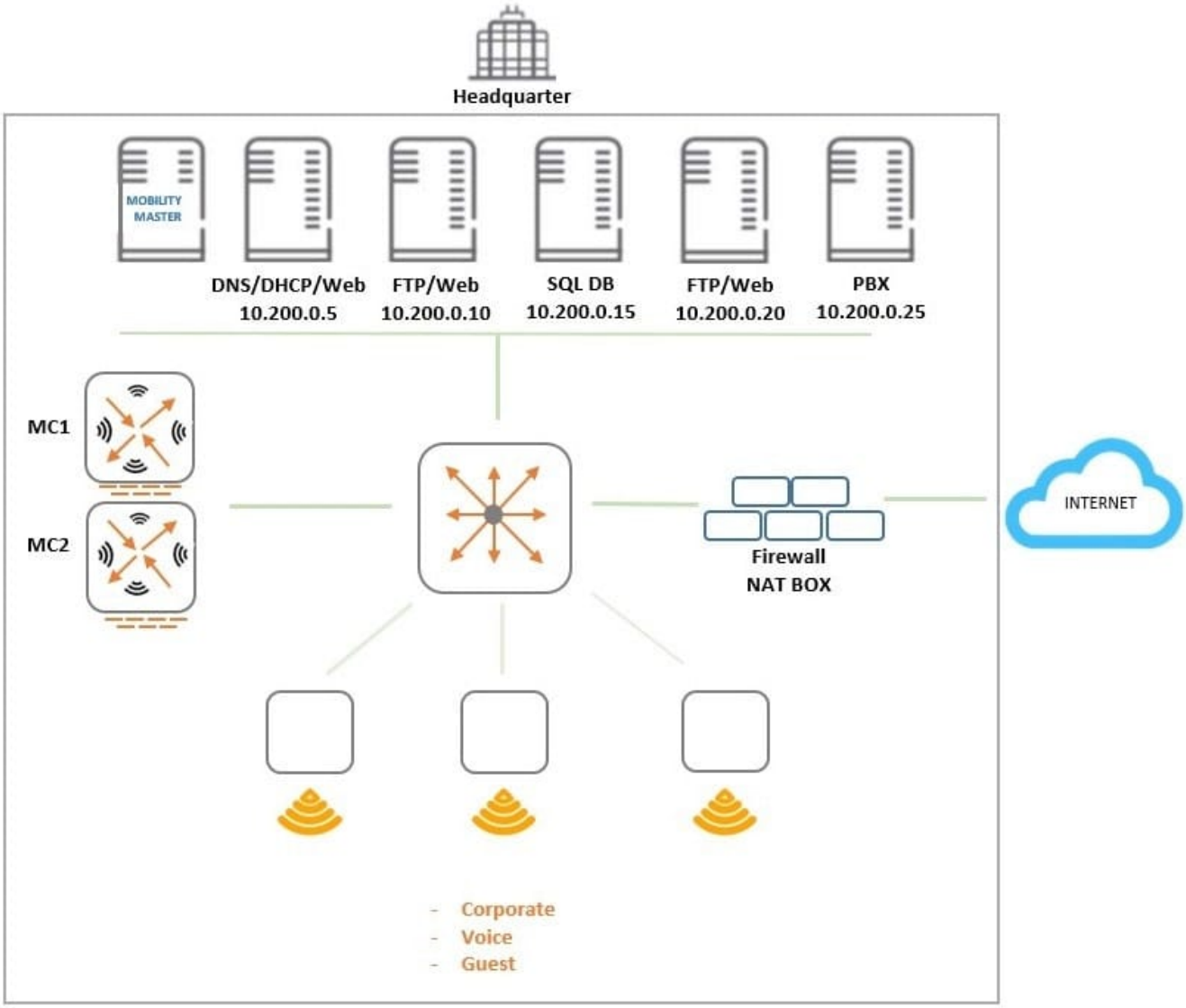
C. MC 1 has not received the configuration from the mobility master yet.

D. The Mobility Master lacks MM-VA licenses; therefore, it shares partial configuration only.

Correct Answer: C

QUESTION 2

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 10.200.0.5
   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
   user host 10.200.0.5 svc-dns permit
   user alias alias1 svc-http permit
   user alias alias2 svc-ftp permit
```

B.

```
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
```

C.

```
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
```

D.

```
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
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 3

Refer to the exhibits. Exhibit 1

```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
     IP              MAC             Name    Role                  Age(d:h:m)  Auth    VPN link  AP name  Roaming  Essid/Bssid/Phy
      Profile   Forward mode Type     Host Name   User Type
---------    ----------          -----   ----                   ---------- ----   -------- --------- -------- ---------------
      -------      -------------      ----- ---------   --------
192.168.14.101  xx:xx:xx:xx:xx:xx           guest-guest-logon     00:00:32                  AP1       Wireless  Guest/yy:yy:yy:yy:yy:yy/a-
VHT  Guest    tunnel         Win 10             WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:2/5 Free:0/3 DVN:2 AllocErr:0 FreeErr:0
```

Exhibit 2 Exhibit 3

```
(MC2) [MDC] #show rights guest-guest-logon

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'guest-guest-logon'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 2
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 98/0
  Openflow: Enabled
  MaxSessions = 65535

  Check CP Profile for Accounting = TRUE
  Captive Portal profile = default
```

```
(MC2) [MDC] #show aaa authentication captive-portal Guest

Captive Portal Authentication Profile "Guest"
---------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
Redirect Pause                              10 sec
User Login                                  Enabled
Guest Login                                 Disabled
Logout popup window                         Enabled
Use HTTP for authentication                 Disabled
Logon wait minimum wait                     5 sec
Logon wait maximum wait                     10 sec
Logon wait CPU utilization threshold        60%
Max Authentication failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  https://cp.mycompany.com/guest/web_login.php
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
```

Exhibit 4

```
(MC2) [MDC] #show aaa authentication captive-portal default

Captive Portal Authentication Profile "default"
-----------------------------------------------
Parameter                                       Value
---------                                       -----
Default Role                                    guest
Default Guest Role                              guest
Server Group                                    Guest
Redirect Pause                                  10 sec
User Login                                      Enabled
Guest Login                                     Disabled
Logout popup window                             Enabled
Use HTTP for authentication                     Disabled
Logon wait minimum wait                         5 sec
Logon wait maximum wait                         10 sec
Logon wait CPU utilization threshold            60%
Max Authentication failures                     0
Show FQDN                                       Disabled
Authentication Protocol                         PAP
Login page                                      /auth/index.html
Welcome page                                    /auth/welcome.html
Show Welcome Page                               Yes
Add switch IP addresses in the redirection URL  Disabled

(MC2) [MDC] #show aaa server-group default

Fail Through: No
Load Balance: No

Auth Servers
------------
Name        Server-Type    trim-FQDN   Match-Type  Match-Op  Match-Str
----        -----------    ---------   ----------  --------  ---------
Internal    Internal       No

Role/VLAN derivation rules
--------------------------
Priority   Attribute   Operation   Operand   Type    Action    Value   Validated
--------   ---------   ---------   -------   ----    ------    -----   ---------
1          role        value-of              String  set role          No
```

A captive portal-based solution is deployed in a Mobility Master (MM) - Mobility Controller (MC) network. A wireless station connects to the network and attempts the authentication process. The outputs are shown in the exhibits. Which names correlate with the authentication and captive portal servers?

A. ClearPass.23 is the authentication server, and cp.mycompany.com is the captive portal server.

B. ClearPass.23 is the authentication server, and MC2 is the captive portal server.

C. Internal database in MC2 is the authentication server, and cp.mycompany.com is the captive portal server.

D. cp.mycompany.com is the authentication server, and ClearPass.23 is the captive portal server.

Correct Answer: A

QUESTION 4

Refer to the exhibit.

```
(MC_VA) [mynode] #show aaa debug role user mac xx:xx:xx:xx:xx:xx

Role Derivation History
=======================
    0: l2 role->logon, mac user created
    1: l2 role->authenticated, station Authenticated with auth type: 802.1x
    2: l2 role->corp, RFC 3576 l3 role change COA
(MC_VA) [mynode] #
```

A network administrator has Mobility Master (MM) - Mobility Controller (MC) based network and has fully integrated the MCs with ClearPass for RADIUS-based AAA services. The administrator is testing different ways to run user role derivation.

Based on the show command output, what method has the administrator use for assigning the "corp" role to client with MAC xx:xx:xx:xx:xx:xx?

A. Dynamic Authorization using VSA attributes.

B. Dynamic Authorization using IETF attributes.

C. Server Derivation Rules using IETF attributes.

D. User Derivation Rules using the client\\'s MAC.

Correct Answer: A

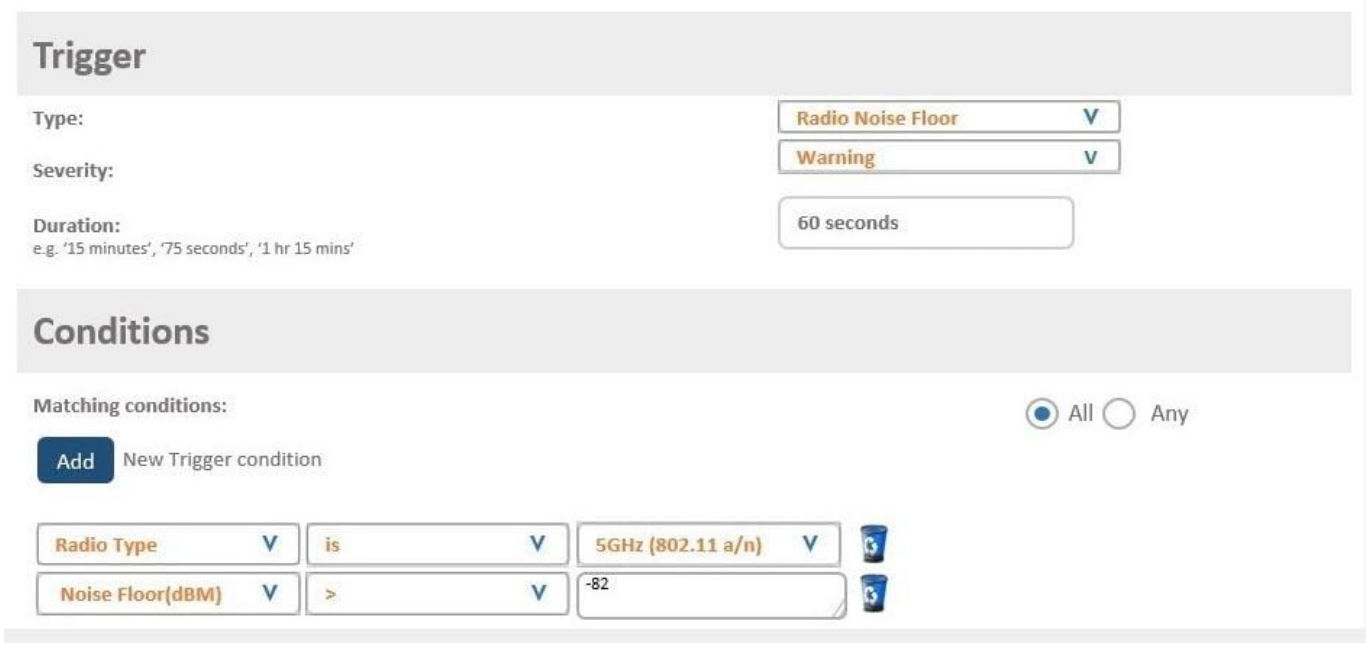
QUESTION 5

HOTSPOT

A network administrator wants to receive a warning level alarm every time the noise floor rises above -82 dBm on any of the AP radios.

Which alarm definition must the network administrator create to accomplish this?

Hot Area:



Correct Answer: