Aruba Certified Mobility Expert Written Exam

Exam description

This exam tests your technical expert skills with WLAN design, implementation, and configuration in complex multisite highly available network environments using the Aruba Controller, Access Point, and AirWave product lines. It also tests your ability to design, implement, monitor, troubleshoot, and maintain end-to-end WLAN campus and branch solutions, and resolve issues in an existing customer infrastructure.

Exam ID	HPE6-A79
Exam type	Proctored
Exam duration	2 hours
Exam length	60 questions
Passing score	65%
Delivery languages	English

Register for this Exam
You need an HPE Learner ID and a Pearson VUE login and password.

Passing the HPE6-A79 Aruba Certified Mobility Expert Written Exam is required before registering for the practical exam.

No reference material is allowed at the testing site. This exam may contain beta test items for experimental purposes.

During the exam, you can make comments about the exam items. We welcome these comments as part of our continuous improvement process.

Ideal candidate for this exam

Typical candidate is recognized as an expert-level resource, advisor, and mentor to networking professionals. Candidate has extensive hands on Aruba WLAN configuration, administration, and troubleshooting experience. Candidate have more than 4 years of experience implementing complex, highly available, multisite Aruba WLANs, and a minimum of one year experience using AirWave to manage and monitor Aruba WLAN deployments. Candidate also has a minimum of 3 years of switching and routing experience.

Exam contents

This exam has 60 questions.

Advice to help you take this exam

- Complete the training and review all course materials and documents before you take the exam.
- Exam items are based on expected knowledge acquired from job experience, an expected level of industry standard knowledge, or other prerequisites (events, supplemental materials, etc.).
- Successful completion of the course alone does not ensure you will pass the exam.
- Read this HPE Exam Preparation Guide and follow its recommendations.
- Visit HPE Press for additional reference materials, study guides, practice tests, and HPE books.

Objectives

This exam validates that you can:

Percentage of Exam	Sections/Objectives
24%	Analyze functional requirements to create a solution design and implementation plan. • Analyze a complex multisite highly available network to determine the physical infrastructure connectivity requirements. • Analyze an entire WLAN infrastructure to determine the licensing requirements. • Analyze an entire WLAN infrastructure to determine the architectural requirements. • Analyze a complex highly available multi-controller environment to determine redundancy requirements. • Analyze a complex highly available multi-controller environment to determine mobility requirements. • Analyze a scenario to determine remote access requirements. • Analyze a scenario to determine AirWave scalability requirements. • Analyze customer requirements to determine the need for QoS. • Analyze customer requirements to determine roles, firewall policies, and rule requirements. • Analyze customer requirements to determine the need for a multizone deployment.
21%	Configure and validate Aruba WLAN solutions. • Configure and validate a WLAN to support voice and video optimization. • Configure a secure WLAN and integrate it with an existing infrastructure. • Validate client connectivity to a secure WLAN. • Configure and validate a complex multisite high availability mobility environment. • Configure a guest WLAN and validate client connectivity. • Configure and validate remote connectivity using RAP or a branch office solution.
20%	Implement advanced services and security solutions. • Configure role derivation and integrate with an existing AAA server. • Configure and verify tunneled node. • Configure and validate IAP-VPN to a controller for remote access. • Configure advanced firewall policies. • Configure a WLAN with WPA2/PSK Mac authentication for role derivation. • Implement RFProtect. • Configure and validate a multizone solution.
17%	Manage and monitor Aruba solutions. • Use AirWave and a Mobility Master to gather information about client health. • Create triggers and custom reports in AirWave. • Monitor the Spectrum Analyzer dashboard on the Mobility Controller. • Monitor and analyze controller health. • Monitor and optimize the RF environment. • Integrate and monitor devices with AirWave.
18%	Perform advanced troubleshooting. • Troubleshoot controller licensing. • Troubleshoot controller and AP communication in a Mobility Master-Mobility Controller-Virtual Mobility Controller environment. • Troubleshoot client connectivity and network access. • Troubleshoot UCC issues. • Troubleshoot multizone.

Sample questions

Sample questions are provided only as examples of question style, format and complexity/difficulty. They do not represent all question types and do not reflect all topic areas. These sample questions do not represent a practice test.

1. Refer to the exhibit.

```
(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  Ty
    Host Name  User Type
----------    ------------       ------    ----      ----------  ----        --------  -------  -------   ---------------                        -------       ------------  --
    ---------  ---------
10.1.141.150  70:4d:7b:10:9e:c6  it        guest     00:00:00    8021x-User            AP22     Wireless  Corp-employee/70:3a:0e:5b:0a:d2/a-VHT  Corp-Network  tunnel        Wi
10             WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:3/42 Free:0/39 Dyn:3 AllocErr:0 FreeErr:0
(MC2) [MDC] #show user mac 70:4d:7b:10:9e:c6
This operation can take a while depending on number of users. Please be patient ....


Name: it, IP: 10.1.141.150, MAC: 70:4d:7b:10:9e:c6, Age: 00:00:00
Role: guest (how: ROLE_DERIVATION_DOT1X), ACL: 7/0
Authentication: Yes, status: successful, method: 8021x-User, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE DERIVATION DOT1X


(MC2) [MDC] #show log security 55


Aug 27 09:18:28 :124003:  <3562> <INFO> |authmgr|  Authentication result=Authentication Successful(0), method=802.1x, server=ClearPass.23, use
r=70:4d:7b:10:9e:c6
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  server_cbh (257)(DEC) : os_reqs 0, s ClearPass.23 type 2 inservice 1 markedD 0
Aug 27 09:18:28 :124607:  <3562> <DBUG> |authmgr|  server_cbh(): response=0 from Auth server 'ClearPass.23 for client:4 proto:0 eap-type:25'.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  server_cbh (638)(DEC) : os_auths 0, s ClearPass.23 type 2 inservice 1 markedD 0 sg_name Cor
p-Network
Aug 27 09:18:28 :124612:  <3562> <DBUG> |authmgr|  AuthSurv_onAuthSucc(authsurv:0): Entered, proto:0 eap-type:0x19 for username:'it' auth-serv
er:'ClearPass.23' server-group:'Corp-Network' AnyRadLdapInOOS:'DontCare'.
Aug 27 09:18:28 :124097:  <3562> <DBUG> |authmgr|  Setting authserver 'ClearPass.23' for user 0.0.0.0, client 802.1x.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  rx_dot1x_radius: EAP packet code 3
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  decode_vendor_attribs: vendor_id 311
Aug 27 09:18:28 :124184:  <3562> <DBUG> |authmgr|  {L2} Authenticating Server is ClearPass.23.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|   logging role event for 0x224b04c: 0x216fe0c,0x80b07, index 5
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  user_download: User N/A  Router Acl(0)
Aug 27 09:18:28 :124234:  <3562> <DBUG> |authmgr|  Tx message to Sibyte, blocking with ack, Opcode = 164, msglen = 352 1 user messages bundled
, actions = 17
Aug 27 09:18:28 :124105:  <3562> <DBUG> |authmgr|  MM: mac=70:4d:7b:10:9e:c6, state=6, name=it, role=guest, dev_type=, ip=0.0.0.0, new_rec=0.
Aug 27 09:18:28 :124105:  <3562> <DBUG> |authmgr|  MM: mac=70:4d:7b:10:9e:c6, state=3, name=it, role=guest, dev_type=, ip=10.1.141.150, new_re
c=1.
Aug 27 09:18:28 :124105:  <3562> <DBUG> |authmgr|  MM: mac=70:4d:7b:10:9e:c6, state=6, name=it, role=guest, dev_type=, ip=0.0.0.0, new_rec=1.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  AUTH GSM repkey: repkey 0 (mac 70:4d:7b:10:9e:c6)
Aug 27 09:18:28 :124230:  <3562> <DBUG> |authmgr|  Rx message 21/23, length 351 from 10.254.10.214:8344
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  Local DB auth failed for user 70:4d:7b:10:9e:c6, error (User not found in UserDB)
Aug 27 09:18:28 :132219:  <3562> <INFO> |authmgr|  MAC=70:4d:7b:10:9e:c6 Local User DB lookup result for Machine auth=FAILURE
Aug 27 09:18:28 :132020:  <3562> <INFO> |authmgr|  Station it 70:4d:7b:10:9e:c6 failed Machine authentication update role guest
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|   logging role event for 0x224b04c: 0x216fe0c,0x80b07, index 6
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  user_download: User N/A  Router Acl(0)
```

A network administrator evaluates a deployment to validate that users are assigned to the proper roles. Based on the output shown in the exhibit, what can the network administrator conclude?

a. The MC assigned the role based on server derivation rules.
b. The MC assigned the machine authentication default user role.
c. The MC assigned the role based on user derivation rules.
d. The MC assigned the default role based on the authentication method.

2. A company offers guest access with an open SSID and an internal Mobility Controller (MC) captive portal. The network administrator needs to integrate a more scalable solution with a remote RADIUS and captive portal server.
The network administrator fully deploys a guest solution with self–registration in ClearPass, and defines the MC as a RADIUS client. Next, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

Which two configuration components must the network administrator modify in the MC to complete the deployment? (Select two.)

a. AAA server profile
b. Initial role firewall policies
c. VAP profile
d. Authentication server group
e. Captive portal profile

3. Refer to the exibit.

```
(MC11) [mynode] #show ap database

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  Down       2      10.254.13.14  0.0.0.0
a8:bd:27:c5:c3:3a  default  335      10.1.147.2    Down       2      10.254.13.14  0.0.0.0
AP11               CAMPUS   335      10.1.146.150  Up 6m:35s  2z     10.254.13.14  0.0.0.0

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE version 2
       B = Built-in AP; C = Cellular RAP; D = Dirty or no config
       E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
       G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
       M = Mesh node
       N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
       S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
       Y = Mesh Recovery
       c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
       i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP

Total APs:3
(MC11) [mynode] #show ap bss-table

fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-standard, p-persistent, b-backup, a-always), n-anyspot

cluster (cluster role): U-UAC, A-AAC, sU-Standby UAC, sA-Standby AAC

Aruba AP BSS Table
------------------
bss                ess            port  ip            phy    type  ch/EIRP/max-EIRP  cur-cl  ap name  in-t(s)  tot-t   mtu   acl-state  acl  fm  cluster  datazone
---                ---            ----  --            ---    ----  ----------------  ------  -------  -------  -----   ---   ---------  ---  --  -------  --------
70:3a:0e:5b:0a:c4  Company_Guest  N/A   10.1.146.150  g-HT   ap    6/8.0/25.6        0       AP11     0        3m:40s  1500  -          79   T           yes
70:3a:0e:5b:0a:d4  Company_Guest  N/A   10.1.146.150  a-VHT  ap    153E/9.0/28.5     0       AP11     0        3m:40s  1500  -          79   T           yes

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2
Num Associations:0
```

Based on the output shown in the exhibit, what is the current relationship between AP11 and MC11?

a. AP11 is a multizone AP, and MC11 is its datazone.
b. AP11 is a multizone AP, and MC11 is its primary zone.
c. AP11 is a CAP, and MC11 terminates its active tunnels.
d. AP11 is a CAP, and MC11 terminates its standby tunnels.

4. Refer to the exhibit.

```
(MC1) [MDC] #show aaa authentication dot1x DOT1X-EMP

802.1X Authentication Profile "DOT1X-EMP"
-----------------------------------------
Parameter                                                 Value
---------                                                 -----
WPA/WPA2 Key Message Retry Count                          3
Multicast Key Rotation                                    Disabled
Unicast Key Rotation                                      Disabled
Reauthentication                                          Enabled
Opportunistic Key Caching                                 Enabled
Validate PMKID                                            Enabled
Use Session Key                                           Disabled
Use Static Key                                            Disabled
xSec MTU                                                  1300 bytes
Termination                                               Disabled
Termination EAP-Type                                      N/A
Termination Inner EAP-Type                                N/A
Enforce Suite-B 128 bit or more security level Authentication  Disabled
Enforce Suite-B 192 bit security level Authentication     Disabled
Token Caching                                             Disabled
Token Caching Period                                      24 hr(s)
CA-Certificate                                            N/A
Server-Certificate                                        default
TLS Guest Access                                          Disabled
TLS Guest Role                                            guest
Ignore EAPOL-START after authentication                   Disabled
Handle EAPOL-Logoff                                       Disabled
Ignore EAP ID during negotiation.                         Disabled
WPA-Fast-Handover                                         Disabled
Check certificate common name against AAA server          Enabled
```

Based on the output shown in the exhibit, which configuration change is required to validate user credentials in a server group that includes LDAP and the internal database?

a. aaa authentication dot1x DOT1X-EMP
   termination eap-type eap-peap
   termination inner-eap-type eap-mschapv2
b. aaa authentication dot1x DOT1X-EMP
   termination eap-type eap-tls
   ca-cert AD.mycompany.com
   server-cert AD-signed.mycompany
c. aaa authentication dot1x DOT1X-EMP
   ca-cert AD.mycompany.com
   server-cert AD-signed.mycompany.com
   server server-retry 5
d. aaa authentication dot1x DOT1X-EMP
   termination enable
   termination eap-type eap-peap
   termination inner-eap-type eap-mschapv2

5. Refer to the exhibit.

```
(MC1) #show log security 56

Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=63, server=ClearPass.23, IP=10.254.1.23, server-group=SG-
ClearPass.23, fd=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass.23:10.254.1.23:1812 id:63,len:263
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  User-Name: employee33
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.10.214
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Identifier: 10.1.140.100
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Calling-Station-Id: 704D7B109EC6
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Called-Station-Id: 204C0306E5C0
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Service-Type: Framed-User
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Framed-MTU: 1100
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  EAP-Message: \002\004
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  State: ADQAxwA/AOB0ygEAaXRZwzRK4ays3Cn40Y9hNA==
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Essid-Name: Employee
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP2
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-AP-Group: MainCampus-SC-B1
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2381]  Aruba-Device-Type: (VSA with invaild length - Don't send it)
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Message-Auth: 4x\227;\310\356\205>\020\014WP\353Ss=
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=63, server=(null), IP=10.254.1.23, server-group=(null) f
d=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null), fd=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=63, server=ClearPass.23, IP=10.254.1.23, server-group=SG-
ClearPass.23 fd=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1228] Authentication Successful
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  {Microsoft} MS-MPPE-Recv-Key: \262\250\331*T\270\333[\305@V\205^W\334\361\
225\337\017y(\253E\3022\376\241\360K\031\030h'\277\270\333\366[j\226\201:\351a\011\334\010\020\271\222
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  {Microsoft} MS-MPPE-Send-Key: \273\362!\274\271QV\353\344#\001\246\355\360
<V\025v^z\275y\031\237/\343\263H\003\264\230[WP\265\331\311g\333\371\344\1773\216|\005F\271cO
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  EAP-Message: \003\004
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  Message-Auth: \330\252F\223\007R\037G\343\304\352$K[?\375
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  User-Name: employee33
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  {Aruba} Aruba-User-Role: profiling
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  Class: \202\005\250)\210\215C\344\2536#\356\200\243"\006\271\013
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  PW_RADIUS_ID: 7
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  Rad-Length: 248
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  PW_RADIUS_CODE: \002
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  PW_RAD_AUTHENTICATOR: Y\341\326J}\244\306\213\360\020\217\217\177{\341\262


Jun 26 15:27:46 :124003:  <3575> <INFO> |authmgr|  Authentication result=Authentication Successful(0), method=802.1x, server=ClearPass.23, user=70:
4d:7b:10:9e:c6
```

A network administrator deploys an employee WLAN and uses ClearPass as the authentication and policy server. Change of Authorization (CoA) is used to disconnect users once the client has been profiled. This permits a more granular control over connections prior to assigning the ultimate user role.

When users connect, the network administrator notices they always remain in the profiling firewall role and the CoA action does not occur. It has been confirmed that the ClearPass server configuration is correct. The network administrator debugs an authentication attempt and sees the output shown in the exhibits.

What must the network administrator do to successfully deploy this solution?

a. Change the RADIUS NAS–ID of the authentication server at the Managed Device group level.
b. Use an IP address for the calling station ID in the authentication server configuration at the MC device level.
c. Change the RADIUS Client NAS IPv4 address at the MC device level.
d. Enable interim accounting in the Managed Device group level.

Answers

This section provides answers to and references for the sample questions.

1. Refer to the exhibit.

```
(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  Ty
    Host Name  User Type
----------    ------------       ------    ----      ----------  ----        --------  -------  -------   --------------                         -------       ------------  --
    ---------  ---------
10.1.141.150  70:4d:7b:10:9e:c6  it        guest     00:00:00    8021x-User            AP22     Wireless  Corp-employee/70:3a:0e:5b:0a:d2/a-VHT  Corp-Network  tunnel        Wi
10             WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:3/42 Free:0/39 Dyn:3 AllocErr:0 FreeErr:0
(MC2) [MDC] #show user mac 70:4d:7b:10:9e:c6
This operation can take a while depending on number of users. Please be patient ....


Name: it, IP: 10.1.141.150, MAC: 70:4d:7b:10:9e:c6, Age: 00:00:00
Role: guest (how: ROLE_DERIVATION_DOT1X), ACL: 7/0
Authentication: Yes, status: successful, method: 8021x-User, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE DERIVATION DOT1X
```

```
(MC2) [MDC] #show log security 55

Aug 27 09:18:28 :124003:  <3562> <INFO> |authmgr|  Authentication result=Authentication Successful(0), method=802.1x, server=ClearPass.23, use
r=70:4d:7b:10:9e:c6
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  server_cbh (257)(DEC) : os_reqs 0, s ClearPass.23 type 2 inservice 1 markedD 0
Aug 27 09:18:28 :124607:  <3562> <DBUG> |authmgr|  server_cbh(): response=0 from Auth server 'ClearPass.23 for client:4 proto:0 eap-type:25'.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  server_cbh (638)(DEC) : os_auths 0, s ClearPass.23 type 2 inservice 1 markedD 0 sg_name Cor
p-Network
Aug 27 09:18:28 :124612:  <3562> <DBUG> |authmgr|  AuthSurv_onAuthSucc(authsurv:0): Entered, proto:0 eap-type:0x19 for username:'it' auth-serv
er:'ClearPass.23' server-group:'Corp-Network' AnyRadLdapInOOS:'DontCare'.
Aug 27 09:18:28 :124097:  <3562> <DBUG> |authmgr|  Setting authserver 'ClearPass.23' for user 0.0.0.0, client 802.1x.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  rx_dot1x_radius: EAP packet code 3
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  decode_vendor_attribs: vendor_id 311
Aug 27 09:18:28 :124184:  <3562> <DBUG> |authmgr|  {L2} Authenticating Server is ClearPass.23.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|   logging role event for 0x224b04c: 0x216fe0c,0x80b07, index 5
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  user_download: User N/A  Router Acl(0)
Aug 27 09:18:28 :124234:  <3562> <DBUG> |authmgr|  Tx message to Sibyte, blocking with ack, Opcode = 164, msglen = 352 1 user messages bundled
, actions = 17
Aug 27 09:18:28 :124105:  <3562> <DBUG> |authmgr|  MM: mac=70:4d:7b:10:9e:c6, state=6, name=it, role=guest, dev_type=, ip=0.0.0.0, new_rec=0.
Aug 27 09:18:28 :124105:  <3562> <DBUG> |authmgr|  MM: mac=70:4d:7b:10:9e:c6, state=3, name=it, role=guest, dev_type=, ip=10.1.141.150, new_re
c=1.
Aug 27 09:18:28 :124105:  <3562> <DBUG> |authmgr|  MM: mac=70:4d:7b:10:9e:c6, state=6, name=it, role=guest, dev_type=, ip=0.0.0.0, new_rec=1.
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  AUTH GSM repkey: repkey 0 (mac 70:4d:7b:10:9e:c6)
Aug 27 09:18:28 :124230:  <3562> <DBUG> |authmgr|  Rx message 21/23, length 351 from 10.254.10.214:8344
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  Local DB auth failed for user 70:4d:7b:10:9e:c6, error (User not found in UserDB)
Aug 27 09:18:28 :132219:  <3562> <INFO> |authmgr|  MAC=70:4d:7b:10:9e:c6 Local User DB lookup result for Machine auth=FAILURE
Aug 27 09:18:28 :132020:  <3562> <INFO> |authmgr|  Station it 70:4d:7b:10:9e:c6 failed Machine authentication update role guest
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|   logging role event for 0x224b04c: 0x216fe0c,0x80b07, index 6
Aug 27 09:18:28 :124004:  <3562> <DBUG> |authmgr|  user_download: User N/A  Router Acl(0)
```

A network administrator evaluates a deployment to validate that users are assigned to the proper roles. Based on the output shown in the exhibit, what can the network administrator conclude?

a. The MC assigned the role based on server derivation rules.

b. The MC assigned the machine authentication default user role.

c. The MC assigned the role based on user derivation rules.

d. The MC assigned the default role based on the authentication method.

2. A company offers guest access with an open SSID and an internal Mobility Controller (MC) captive portal. The network administrator needs to integrate a more scalable solution with a remote RADIUS and captive portal server.
The network administrator fully deploys a guest solution with self-registration in ClearPass, and defines the MC as a RADIUS client. Next, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

   Which two configuration components must the network administrator modify in the MC to complete the deployment? (Select two.)

   a. AAA server profile

   b. Initial role firewall policies

   c. VAP profile

   d. Authentication server group

   e. Captive portal profile

3. Refer to the exibit.

```
(MC11) [mynode] #show ap database

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  Down       2      10.254.13.14  0.0.0.0
a8:bd:27:c5:c3:3a  default  335      10.1.147.2    Down       2      10.254.13.14  0.0.0.0
AP11               CAMPUS   335      10.1.146.150  Up 6m:35s  2z     10.254.13.14  0.0.0.0

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE version 2
       B = Built-in AP; C = Cellular RAP; D = Dirty or no config
       E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
       G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
       M = Mesh node
       N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
       S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
       Y = Mesh Recovery
       c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
       i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP

Total APs:3
(MC11) [mynode] #show ap bss-table

fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-standard, p-persistent, b-backup, a-always), n-anyspot

cluster (cluster role): U-UAC, A-AAC, sU-Standby UAC, sA-Standby AAC

Aruba AP BSS Table
------------------
bss                ess            port  ip            phy    type  ch/EIRP/max-EIRP  cur-cl  ap name  in-t(s)  tot-t   mtu   acl-state  acl  fm  cluster  datazone
---                ---            ----  --            ---    ----  ----------------  ------  -------  -------  -----   ---   ---------  ---  --  -------  --------
70:3a:0e:5b:0a:c4  Company_Guest  N/A   10.1.146.150  g-HT   ap    6/8.0/25.6        0       AP11     0        3m:40s  1500  -          79   T           yes
70:3a:0e:5b:0a:d4  Company_Guest  N/A   10.1.146.150  a-VHT  ap    153E/9.0/28.5     0       AP11     0        3m:40s  1500  -          79   T           yes

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2
Num Associations:0
```

Based on the output shown in the exhibit, what is the current relationship between AP11 and MC11?

a. AP11 is a multizone AP, and MC11 is its datazone.

b. AP11 is a multizone AP, and MC11 is its primary zone.

c. AP11 is a CAP, and MC11 terminates its active tunnels.

d. AP11 is a CAP, and MC11 terminates its standby tunnels.

4. Refer to the exhibit.

```
(MC1) [MDC] #show aaa authentication dot1x DOT1X-EMP

802.1X Authentication Profile "DOT1X-EMP"
-----------------------------------------
Parameter                                                  Value
---------                                                  -----
WPA/WPA2 Key Message Retry Count                           3
Multicast Key Rotation                                     Disabled
Unicast Key Rotation                                       Disabled
Reauthentication                                           Enabled
Opportunistic Key Caching                                  Enabled
Validate PMKID                                             Enabled
Use Session Key                                            Disabled
Use Static Key                                             Disabled
xSec MTU                                                   1300 bytes
Termination                                                Disabled
Termination EAP-Type                                       N/A
Termination Inner EAP-Type                                 N/A
Enforce Suite-B 128 bit or more security level Authentication  Disabled
Enforce Suite-B 192 bit security level Authentication      Disabled
Token Caching                                              Disabled
Token Caching Period                                       24 hr(s)
CA-Certificate                                             N/A
Server-Certificate                                         default
TLS Guest Access                                           Disabled
TLS Guest Role                                             guest
Ignore EAPOL-START after authentication                    Disabled
Handle EAPOL-Logoff                                        Disabled
Ignore EAP ID during negotiation.                          Disabled
WPA-Fast-Handover                                          Disabled
Check certificate common name against AAA server           Enabled
```

Based on the output shown in the exhibit, which configuration change is required to validate user credentials in a server group that includes LDAP and the internal database?

a. aaa authentication dot1x DOT1X-EMP
   termination eap-type eap-peap
   termination inner-eap-type eap-mschapv2

b. aaa authentication dot1x DOT1X-EMP
   termination eap-type eap-tls
   ca-cert AD.mycompany.com
   server-cert AD-signed.mycompany

c. aaa authentication dot1x DOT1X-EMP
   ca-cert AD.mycompany.com
   server-cert AD-signed.mycompany.com
   server server-retry 5

d. aaa authentication dot1x DOT1X-EMP
   termination enable
   termination eap-type eap-peap
   termination inner-eap-type eap-mschapv2

5. Refer to the exhibit.

```
(MC1) #show log security 56


Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=63, server=ClearPass.23, IP=10.254.1.23, server-group=SG-
ClearPass.23, fd=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass.23:10.254.1.23:1812 id:63,len:263
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  User-Name: employee33
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.10.214
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Identifier: 10.1.140.100
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Calling-Station-Id: 704D7B109EC6
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Called-Station-Id: 204C0306E5C0
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Service-Type: Framed-User
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Framed-MTU: 1100
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  EAP-Message: \002\004
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  State: ADQAxwA/AOB0ygEAaXRZwzRK4ays3Cn40Y9hNA==
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Essid-Name: Employee
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP2
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-AP-Group: MainCampus-SC-B1
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2381]  Aruba-Device-Type: (VSA with invaild length - Don't send it)
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Message-Auth: 4x\227;\310\356\205>\020\014WP\353Ss=
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=63, server=(null), IP=10.254.1.23, server-group=(null) f
d=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null), fd=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=63, server=ClearPass.23, IP=10.254.1.23, server-group=SG-
ClearPass.23 fd=64
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1228] Authentication Successful
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  {Microsoft} MS-MPPE-Recv-Key: \262\250\331*T\270\333[\305@V\205^W\334\361\
225\337\017y(\253E\3022\376\241\360K\031\030h'\277\270\333\366[j\226\201:\351a\011\334\010\020\271\222
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  {Microsoft} MS-MPPE-Send-Key: \273\362!\274\271QV\353\344#\001\246\355\360
<V\025v^z\275y\031\237/\343\263H\003\264\230[WP\265\331\311g\333\371\344\1773\216|\005F\271cO
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  EAP-Message: \003\004
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  Message-Auth: \330\252F\223\007R\037G\343\304\352$K[?\375
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  User-Name: employee33
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  {Aruba} Aruba-User-Role: profiling
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  Class: \202\005\250)\210\215C\344\2536#\356\200\243"\006\271\013
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  PW_RADIUS_ID: ?
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  Rad-Length: 248
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  PW_RADIUS_CODE: \002
Jun 26 15:27:46 :121031:  <3575> <DBUG> |authmgr| |aaa| [rc_api.c:1245]  PW_RAD_AUTHENTICATOR: Y\341\326J}\244\306\213\360\020\217\217\177{\341\262

Jun 26 15:27:46 :124003:  <3575> <INFO> |authmgr|  Authentication result=Authentication Successful(0), method=802.1x, server=ClearPass.23, user=70:
4d:7b:10:9e:c6
```

A network administrator deploys an employee WLAN and uses ClearPass as the authentication and policy server. Change of Authorization (CoA) is used to disconnect users once the client has been profiled. This permits a more granular control over connections prior to assigning the ultimate user role.

When users connect, the network administrator notices they always remain in the profiling firewall role and the CoA action does not occur. It has been confirmed that the ClearPass server configuration is correct. The network administrator debugs an authentication attempt and sees the output shown in the exhibits.

What must the network administrator do to successfully deploy this solution?

a. Change the RADIUS NAS-ID of the authentication server at the Managed Device group level.

b. Use an IP address for the calling station ID in the authentication server configuration at the MC device level.

c. Change the RADIUS Client NAS IPv4 address at the MC device level.

d. Enable interim accounting in the Managed Device group level.

For more information

Contact our program

Information is as of February 2024, Revision 5