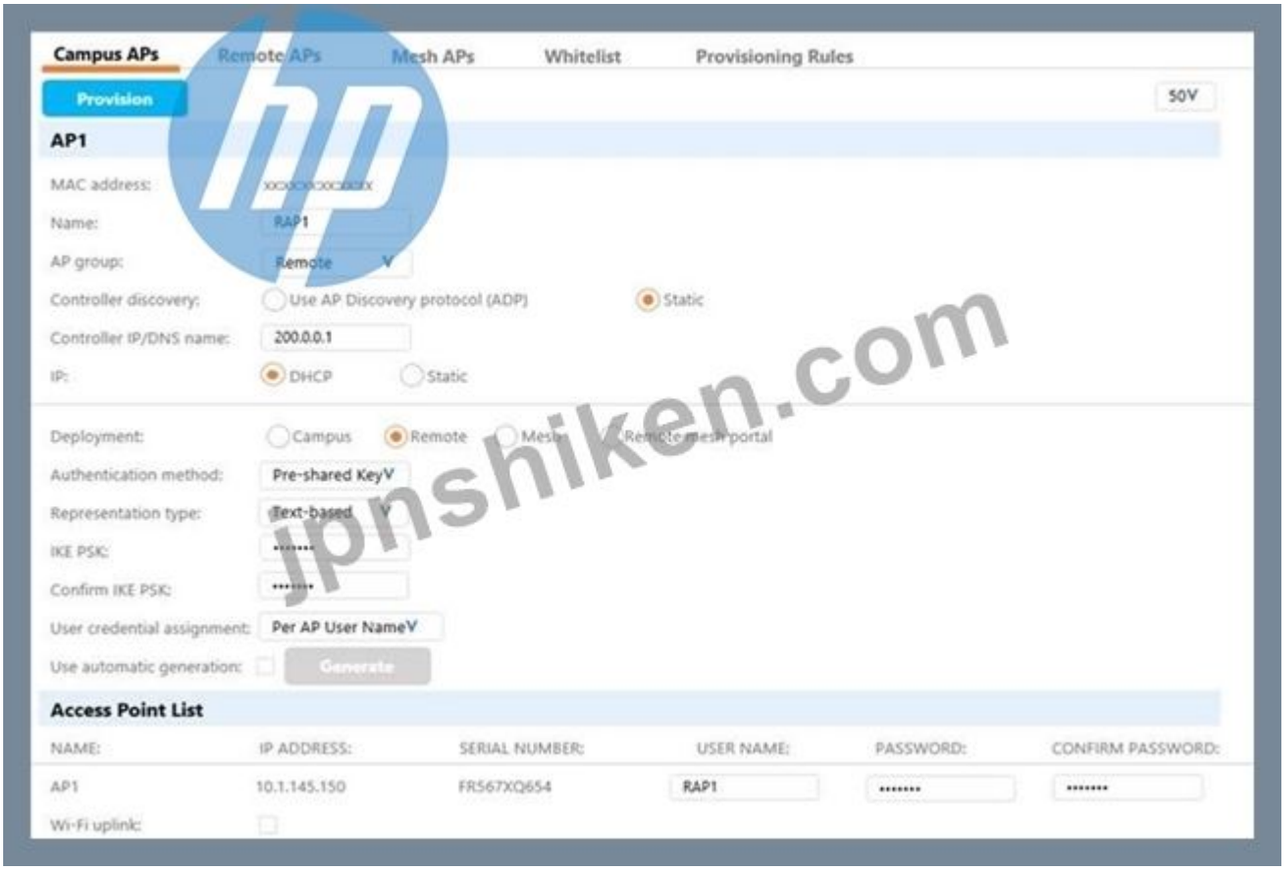
HP.HPE6-A79.v2023-04-03.q18

試験コード：	HPE6-A79
試験名称：	Aruba Certified Mobility Expert Written Exam
認証ベンダー：	HP
無料問題の数：	18
バージョン：	v2023-04-03
ページの閲覧量：	327
問題集の閲覧量：	1217

https://www.jpnshiken.com/shiken/HP.HPE6-A79.v2023-04-03.q18.html

質問: **1**

展示を参照してください。



ネットワーク管理者は、モビリティ マスター (MM) モビリティ コントローラー (MC) アーキテクチャと、RAP を終端するための DMZ 内の MC を備えています。ネットワーク ファイアウォールは、UDP 500 と 4500 の両方について、DMZ 内の MC へのアクセスを許可するようにプロビジョニングされています。次に、図に示されているように AP のプロビジョニングに進みます。

RAP が MC に正常に接続できるようにするために、管理者が必要とする追加の構成手順はどれですか? (2つ選んでください。)

A. /mm/mynode レベルで IP ローカル プールと PSK を作成します。

B. MM の InternalDB に RAP1 アカウントを作成します。

C. MC の InternalDB に RAP1 アカウントを作成します。

D. MM レベルで CPsec ホワイトリストに RAP1 エントリを追加します。
E. デバイス ノード レベルで IP ローカル プールと PSK を作成します。
正解: **(**正解を表示します**)**

質問: **2**
展示を参照してください。

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


Name: contractor14, IP:10.1.141.150, MAC: xx:xx:xx:xx:xx:xx, Age: 00:00:00
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 128/0
Authentication: Yes, status: successful, method: 802.1x, 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_VSA
```

ネットワーク管理者は、展開を評価して、ユーザーに適切な役割が割り当てられていることを検証し、展示の出力を確認しています。ロールはどのようにユーザーに割り当てられますか?
A. MC は、サーバーの派生ルールに基づいてロールを割り当てました。
B. MC は、認証方法に基づいてデフォルトの役割を割り当てました。
C. MC は、マシン認証のデフォルト ユーザー ロールを割り当てました。
D. MC は、Aruba VSA に基づいて役割を割り当てました。
正解: **(**正解を表示します**)**

質問: **3**
組織は、次のクライアント カテゴリへの接続を提供する WLAN インフラストラクチャを導入したいと考えています。
* 従業員
* 請負業者
※ゲストユーザー
* 認証や暗号化をサポートしない企業の IoT レガシー デバイス 従業員と請負業者は、企業の資格情報で認証し、AD グループのメンバーシップに基づいてネットワーク アクセスを取得する必要があります。ゲスト ユーザーは、事前定義された資格情報を使用してキャプティブ ポータルで認証する必要があります。従業員のみが L2 暗号化を実行します。
チャネルの使用を最大化しながら要件を満たす実装計画はどれですか?
A. WPA2-AES および 802.1x 認証を実行する単一の VAP を作成します。MAC 認証 L2 フェールスルー、キャプティブ ポータル、および VIA のサポート。
B. WPA2-AES および 802.1x 認証を実行する VAP1 を作成します。VAP2 は MAC 認証でオープンシステム暗号化を実行し、VAP3 はキャプティブ ポータルと L2 フェールスルーでオープンシステムを実行します。
C. WPA2-AES と 802.1x 認証を実行する VAP1 と、MAC 認証とキャプティブ ポータルを使用したオープン システム暗号化を実行する VAP2 を作成します。

D. WPA2-AES および 802.1x 認証を実行する VAP1 を作成します。VAP2 は MAC 認証でオープンシステム暗号化を実行し、VAP3 はキャプティブ ポータルでオープンシステムを実行します。
正解: **C** (コメントを発表する)

質問: **4**
2 つの企業間のジョイント ベンチャーにより、完全に機能する WLAN Aruba ソリューションが実現します。ネットワーク管理者は、次のスクリプトを使用して、WLAN ソリューションを 2 つの RADIUS サーバー、radius1 および radius2 と統合します。

```
aaa authentication-server radius radius1
   host 10.254.1.1
   key key111
!
aaa authentication-server radius radius2
   host 10.20.2.2
   key key222
!
aaa server-group group-corp
auth-server radius1

aaa profile aaa-corp
authentication-dot1x authenticated
dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
essid corp
opmode wpa2-aes
!
wlan virtual-ap vap-corp
aaa-profile aaa-corp
ssid-profile ssid-corp
!
ap-group building1
virtual-ap vap-corp
```


すべてのユーザーは username@domainname.com タイプの資格情報で認証されますが、radius1 にはドメイン名部分を持つユーザー アカウントがあります。
corp1.com ユーザーを radius1 で認証し、corp2 ユーザーを radius2 で認証するには、どの追加構成が必要ですか?

```
aaa authentication-server radius radius1
trim-fqdn
!
aaa server-group-corp
 auth-server radius1 match-domain corp1.com
 auth-server radius1 match-domain corp2.com


aaa authentication-server radius radius1
 trim-fqdn
!
aaa server-group-corp
 auth-server radius1 match-authstring corp1.com
 auth-server radius1 match-authstring corp2.com


aaa authentication-server radius radius1
!
aaa server-group-corp
 auth-server radius1 match-string corp1.com trim-fqdn
 auth-server radius1 match-string corp2.com


aaa server-group-corp
 auth-server radius1 match-fqdn corp1.com
 auth-server radius1 trim-fqdn
 auth-server radius2 match-fqdn corp2.com
```

A. オプション C
B. オプション D
C. オプション A
D. オプション B
正解: **(**正解を表示します**)**

質問: **5**
展示を参照してください。

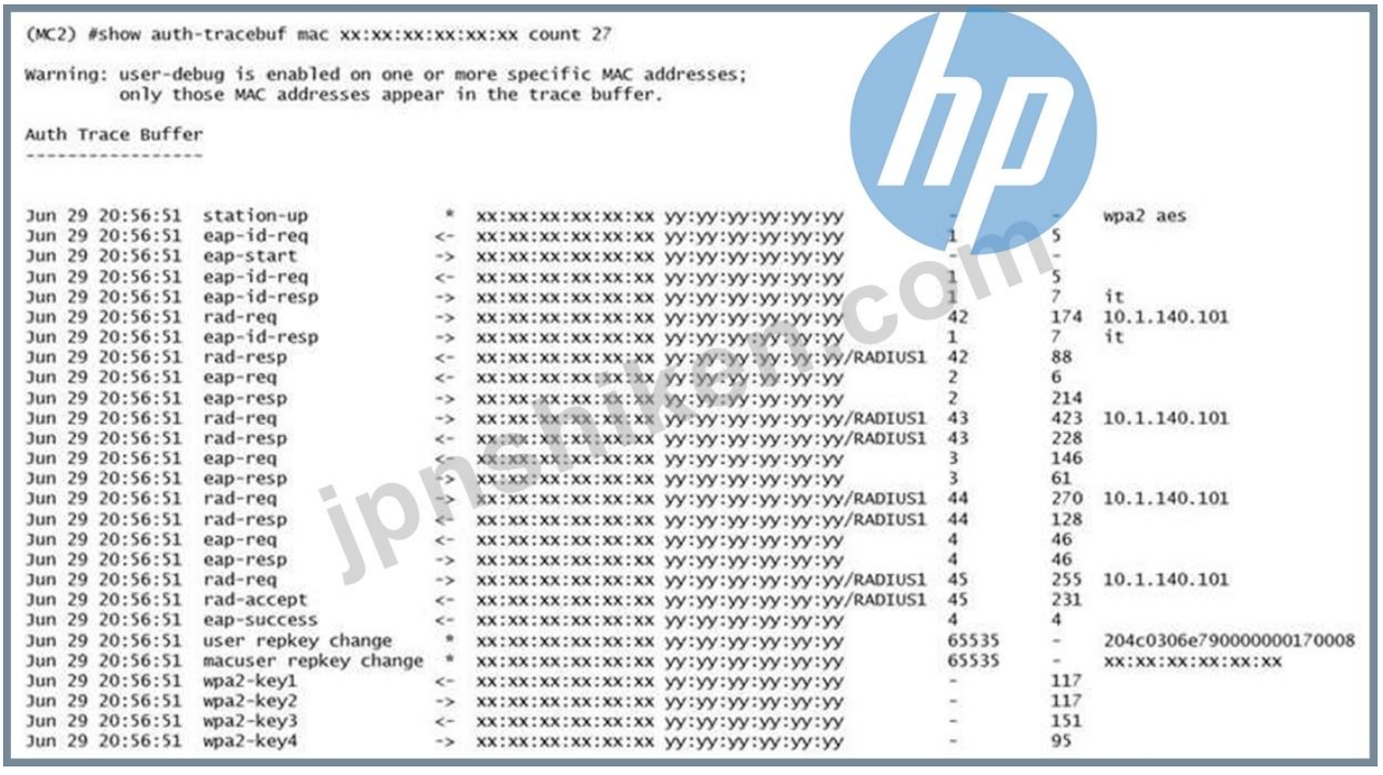
```
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=Employee,
 fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass:10.254.1.23:1812 id:45, len:260
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Identifier: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Calling-Station-Id: 608E9A910FT8
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Called-Station-Id: 446468O7DE4G
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Service-Type: Framed User
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Framed MTU: 1100
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  EAP-Message: \002\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  State: AGcATgBnAKj9IQQAkgYQj1ulavmnP5/OVnaOPQ==
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Essid-Name: EmployeesNet
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP22
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-AP-Group: CAMPUS
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2381]  Aruba-Device-Type: (VSA with invalid length - Don't send it)
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Message-Auth: \487e\326\445\540\318/f\789\416\110\874\4482\612
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:95]  Find Request: id=45, server=(null), IP=10.254.1.23, server-group=(null) fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:48]  Del Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=Employee,
fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1228] Authentication Successful
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Recv-Key: \640\510\973>J\644\238n\421\789\252iP\612\439|K
\0551\898h\354\519\733Fe0\450\739(\456\152-"c\217bR\794\777\649\147\682\400\118\493y\452\731(
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Send-Key: \641\486\489\011\60S\784\064h\027\3824\677\723\
884 \375o\446 \398\453
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  EAP-Message: \003\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Message-Auth: z\498XS\330\480\512\383\498\711
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Class: \202\00S\456)\123\789C\056\2578#\876\041\579"\656\741\081
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_ID: -
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Rad-Length: 250
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_CODE: \002
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RAD_AUTHENTICATOR: PN\495\591\685$\211\481\982G\363RD\261\696\025
Jun 23 21:28:17 :124003:  <5533> <INFO> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass, user=xx:xx:xx:
xx:xx:xx
```

ネットワーク管理者は、請負業者が EmployeesNet という名前の WLAN にアクセスできるようにしたいと考えています。ネットワーク アクセスを制限するために、ネットワーク管理者は、このカテゴリのユーザを請負業者ユーザ ロールに割り当てたいと考えています。これを行うには、ネッ

トワーク管理者は、ClearPass が契約者の値で Aruba-User-Role を返すように ClearPass を構成します。
ソリューションをテストするとき、ネットワーク管理者は間違った役割を受け取ります。
ネットワーク管理者は、他の役割の割り当てに影響を与えずに請負業者の役割を請負業者のユーザーに割り当てるにはどうすればよいですか?
A. M で請負業者のファイアウォール ロールを作成します。
B. AAA プロファイルで契約者をデフォルトの役割として設定します。
C. サーバーグループにサーバー逸脱ルールを作成します。
D. AAA プロファイルの CPPM オプションからのダウンロード ロールを確認します。
正解: **D** (コメントを発表する)

質問: **6**
ネットワーク管理者は、モビリティ マスター (MM) - モビリティ コントローラー (MC) ベースのネットワーク セキュリティを担当します。最近、エア モニタがネットワーク内の不正 AP を検出したため、管理者は 『tarpit」ベースのワイヤレス封じ込めを有効にしたいと考えています。
管理者は、どのプロファイルで 『tarpit」ワイヤレス封じ込めを有効にする必要がありますか?
A. IDS プロファイル
B. IDS DOS プロファイル
C. IDS 一般プロファイル
D. IDS Unauthorized デバイス プロファイル
正解: (正解を表示します)

質問: **7**
展示を参照してください。



```
(MC2) #show auth-tracebuf mac xx:xx:xx:xx:xx:xx count 27

Warning: user-debug is enabled on one or more specific MAC addresses;
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------


Jun 29 20:56:51  station-up            *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                -    -    wpa2 aes
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                1    5
Jun 29 20:56:51  eap-start             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                -    -
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                1    5
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                1    7    it
Jun 29 20:56:51  rad-req                ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                42   174  10.1.140.101
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                1    7    it
Jun 29 20:56:51  rad-resp               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        42   88
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                2    6
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                2    214
Jun 29 20:56:51  rad-req                ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        43   423  10.1.140.101
Jun 29 20:56:51  rad-resp               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        43   228
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                3    146
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                3    61
Jun 29 20:56:51  rad-req                ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        44   270  10.1.140.101
Jun 29 20:56:51  rad-resp               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        44   128
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                4    46
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                4    46
Jun 29 20:56:51  rad-req                ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        45   255  10.1.140.101
Jun 29 20:56:51  rad-accept            <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1        45   231
Jun 29 20:56:51  eap-success           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                4    4
Jun 29 20:56:51  user repkey change     *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                65535  -    204c0306e790000000170008
Jun 29 20:56:51  macuser repkey change  *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                65535  -    xx:xx:xx:xx:xx:xx
Jun 29 20:56:51  wpa2-key1             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                -    117
Jun 29 20:56:51  wpa2-key2             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                -    117
Jun 29 20:56:51  wpa2-key3             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                -    151
Jun 29 20:56:51  wpa2-key4             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy                -    95
```

ネットワーク管理者は、クライアントの接続を検証しており、資料に示されている show コマンドを実行しています。ワイヤレス ステーションで使用された認証方法はどれですか?

A. 802.1X マシン認証
B. 802.1X ユーザー認証
C. MAC 認証
D. EAP 認証

正解: **B** (コメントを発表する)

質問: **8**

展示を参照してください。

```
Access-1# show ubt state

Local Master Server (LMS) State:

LMS Type      IP Address     State
-------------------------------------------------------
Primary     : 10.1.224.100   ready_for_bootstrap
Secondary   : 10.1.140.100   ready_for_bootstrap

Switch Anchor Controller (SAC) State:

              IP Address          MAC Address          State
-------------------------------------------------------------------
Active      : 10.1.224.100        xx:xx:xx:xx:xx:xx   Registered


User Anchor Controller(UAC): 10.1.224.100

User               Port    State                              Bucket ID   Gre Key
-------------------------------------------------------------------------------
xx:xx:xx:xx:yy:yy   1/1/20 registered                         255         20
Access-1#
```


展示に示されている出力に基づいて、Access-1 がトンネルを確立した Aruba デバイスはどれですか?

A. L3 クラスタ内の MC のペア
B. スタンドアロン MC のペア
C. 単一のスタンドアロン MC
D. VXLAN を実行するスイッチのペア

正解: **A** (コメントを発表する)

質問: **9**

1 つの国に 50 の小さなコーヒー ショップを持つ企業は、本社と支社の両方の場所での接続ニーズを解決する単一のモビリティ ソリューションを必要としています。コーヒー ショップには、顧客用のローカル WiFi インターネット アクセスをプロビジョニングする必要があります。
また、ショップには、売上をアップロードし、コンピュータ システムを介して物資を要求し、必要に応じて電話をかけるために本社のリソースと通信できるプライベート WLAN が必要です。ネッ

トワーク運用を簡素化するには、コーヒー ショップのネットワーク デバイスをクラウドで管理する必要があります。
最小のコストで企業のニーズを最もよく満たすのはどのテクノロジですか?
A. CAP付きBOC
B. SD ブランチ
C. RAPで発動
D. IAPVPN
正解: **(**正解を表示します**)**

質問: **10**
ネットワーク管理者は、ユーザーベースのトンネリング (UBT) に使用されるスタンドアロン モビリティ コントローラー (MC) の ArubaOS コードを新しい早期リリースに更新しました。MC が 10.1.10.10 の IP アドレスを持つスイッチからの PAPI セッションを拒否しているように見えて以来。また、コントローラーのプロンプトの後に星印が表示されるようになりました: (MC_VA) [mynode] *#」コントローラで PAPI トラフィックのパケット キャプチャを実行し、PCAP ファイルを取得します。管理者は、10.0.20.20 IP アドレスを使用する Wireshark と TFTP サーバーを備えた PC を持っています。
これらの要求を達成するために管理者が発行する必要があるコマンドは何ですか? 2つ選んでください。)

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

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

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

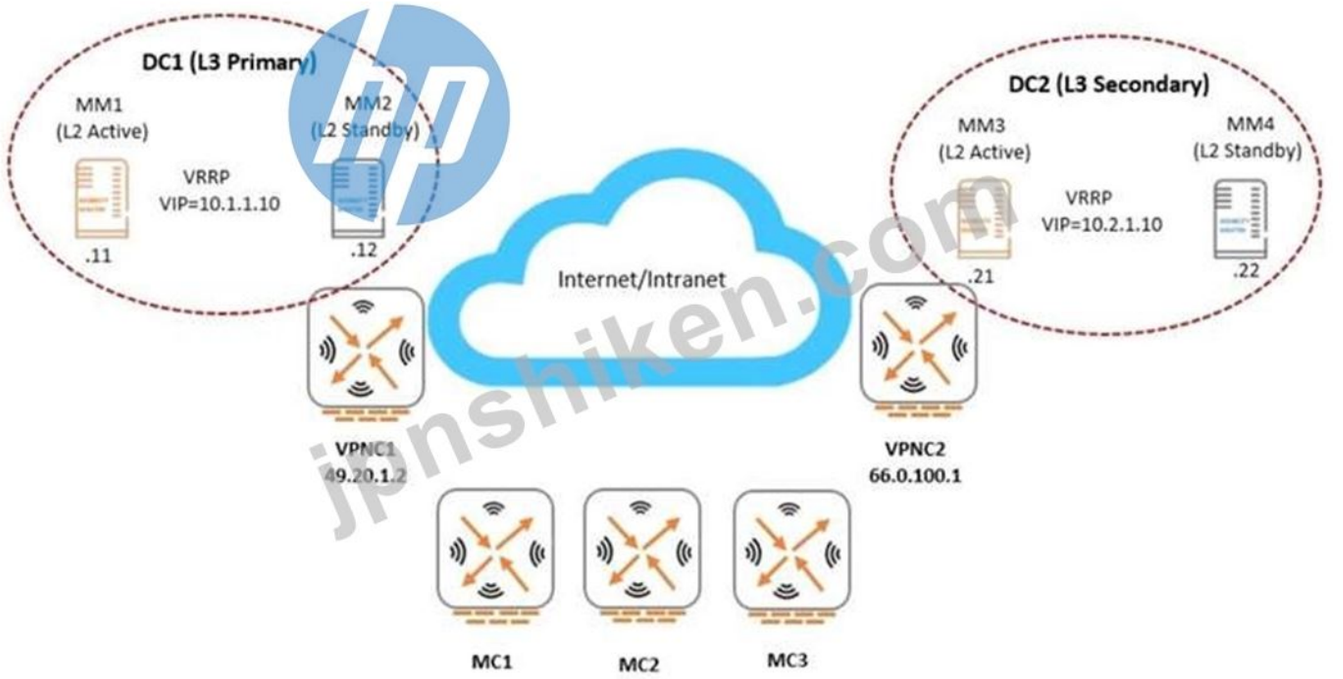
D.
```
tar crash
copy flash: logs.tar tffp: 10.0.20.20 crash.tar
copy flash: logstarmd5sum.txt tffp: 10.0.20.20 crash.tarmd5sum.txt
```

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

A. オプション B
B. オプション C
C. オプション E
D. オプション D

E. オプション A
正解: **(**正解を表示します**)**

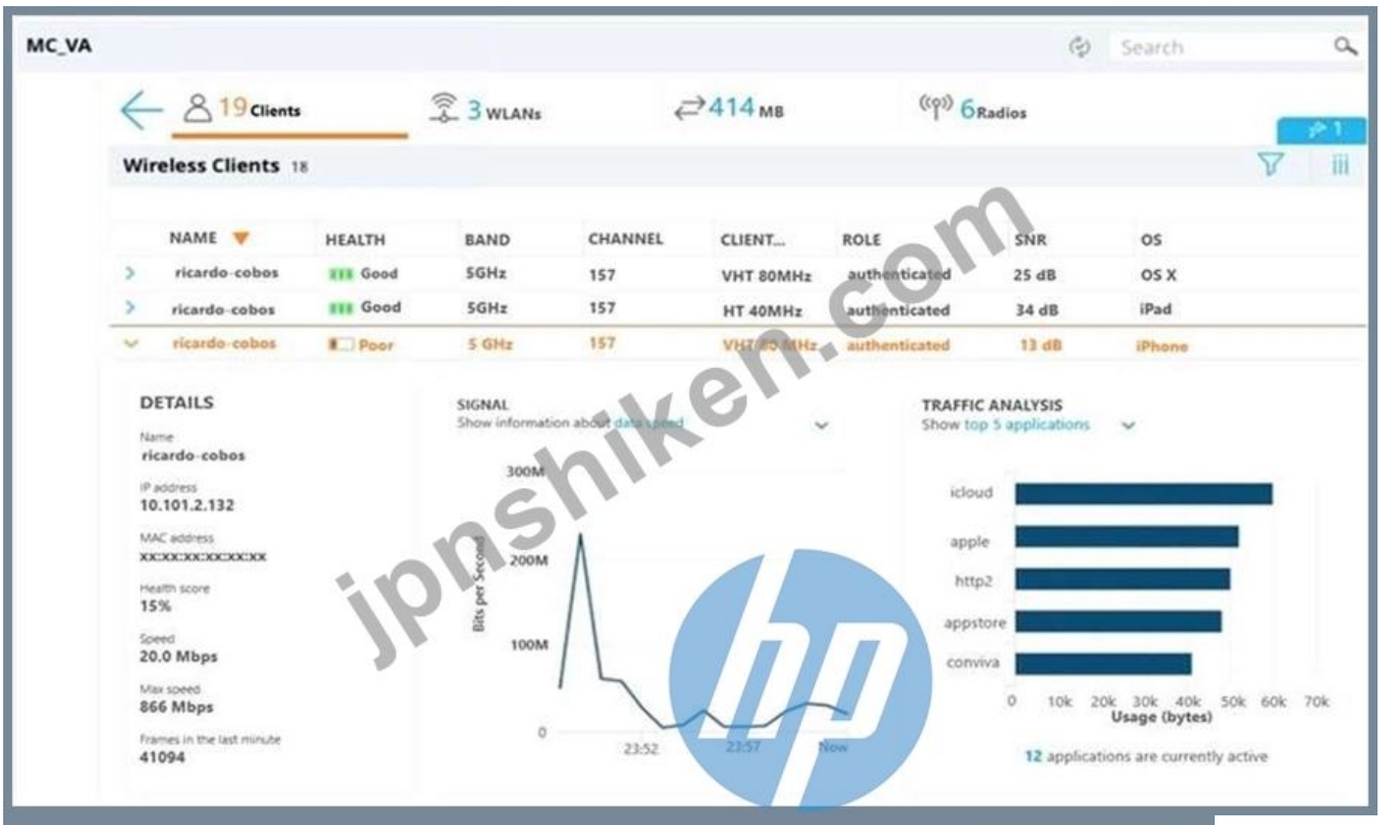
質問: **11**
展示を参照してください。

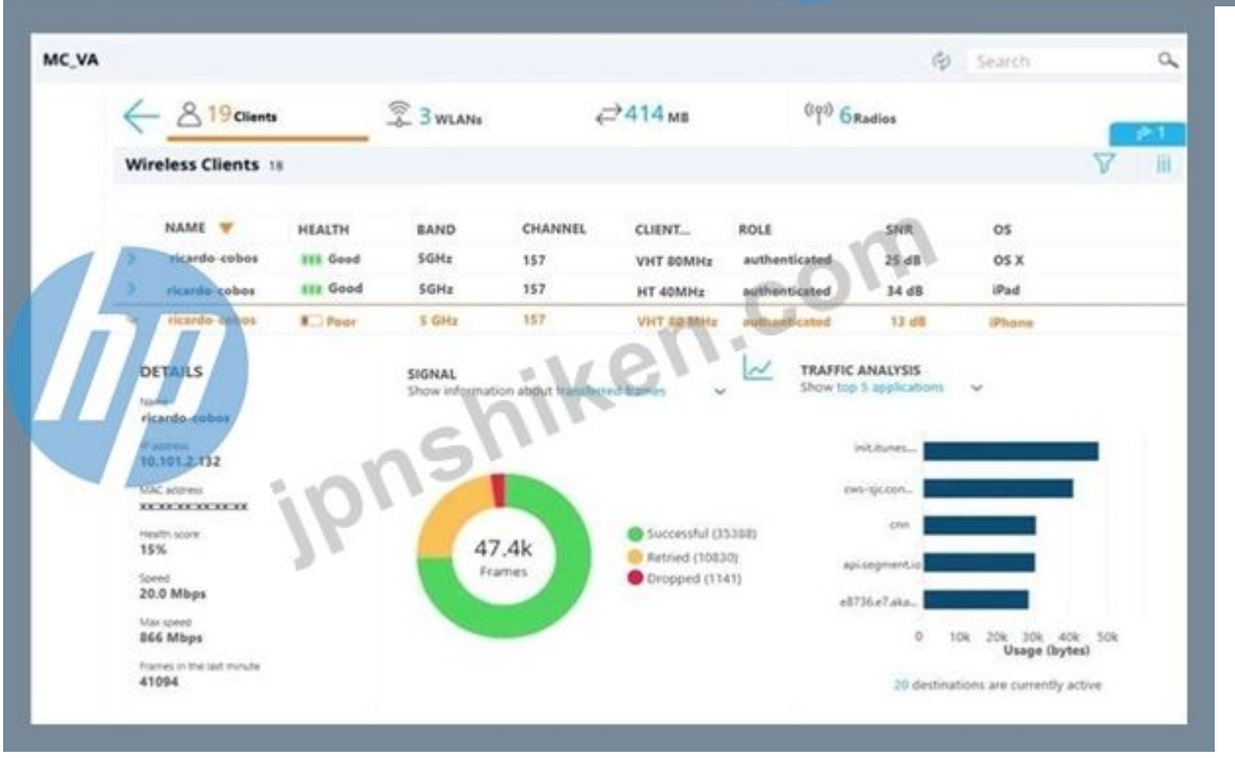



```
(MC2) #show running-config | include masterip
Building Configuration...
masterip 10.1.1.10 vpn-ip 19.20.1.2 ipsec aruba123 peer-id xx:xx:xx:xx:xx:xx
secondary masterip 10.2.1.10 vpn-ip 66.0.100.1 ipsec-factory-cert vpn-mac-1 xx:xx:xx:xx:yy:yy interface vlan 140
(MC2) #
```

図に示されているように、Aruba ネットワークは、2 つのデータセンター間で L2 および L3 モビリティ マスター (MM) の冗長性を備えて展開されています。ネットワーク管理者は、すべてのモビリティ コントローラ (MC) が現在、L2 アクティブで L3 プライマリである MM1 と通信していることを確認します。
MM1 に障害が発生した場合、MC はどの MM IP と通信しますか?
A. 10.1.1.12
B. 10.2.1.21
C. 10.2.1.10
D. 10.1.1.10
正解: **(**正解を表示します**)**

質問: **12**
展示品を参照してください。





ユーザーが応答時間が遅いことをネットワーク管理者に報告し、WLAN に問題がある可能性を示唆します。ユーザーの電話は、5 GHz 帯域の 802.11ac をサポートしています。ネットワーク管理者は、Mobility Master (MM) でユーザーを見つけ、資料に示されている出力を確認します。

データを分析した後、ネットワーク管理者は何を結論付けることができますか?

A. SNR が良好であるため、再送信率が高いのは、隠れノード シナリオまたは高い干渉が原因であるに違いありません。

B. クライアントの状態は良くありませんが、SNR は中程度です。クライアントと AP の両方で TX 電力を増やす必要があります。
C. 成功したフレーム数が多く、最高速度が高い場合は、クライアントが正常であることを示しています。接続はいつでも改善されます。
D. 低 SNR により、クライアントは低 MC に後退することになります。したがって、速度は遅く、再送信は高くなります。
正解: **(**正解を表示します**)**

質問: **13**
535 人のユーザーを抱える企業は、1000 を超える Aruba AP、2 台の 7220 モビリティ コントローラー、および 1 台のモビリティ マスター (MM) 仮想アプライアンスをキャンパス サーバー ファームに配置した Aruba ソリューションを導入しています。MC は HA Fast フェイルオーバー グループをデュアル モードで実行し、50% の AP キャパシティで動作します。
MM または MC に障害が発生した場合、ネットワーク管理者は、ネットワークが完全に管理可能であり、MC 負荷が 80% を超えないようにする必要があります。
これらの要件を満たすためにネットワーク管理者は何ができますか?
A. HA グループでオーバーサブスクリプションを有効にします。
B. AP を 2 つの異なる AP グループに配置します。
C. MM を追加し、DC の冗長性を有効にします。
D. AP 負荷分散を使用してクラスターを作成します。
E. AP を同じ階層レベルに配置します。
F. サーバー ファームに MC と MM を追加します。
正解: **(**正解を表示します**)**

質問: **14**
展示品を参照してください。
資料1

資料 2

```
(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
```

資料3

```
(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
```

資料 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
```

キャプティブ ポータル ベースのソリューションは、モビリティ マスター (MM) - モビリティ コントローラー (MC) ネットワークに展開されます。ワイヤレス ステーションがネットワークに接続し、認証プロセスを試みます。アウトプットは展示品に示されています。

認証およびキャプティブ ポータル サーバーに関連する名前はどれですか?

A. MC2 の内部データベースが認証サーバーで、cp.mycompany.com がキャプティブ ポータル サーバーです。

B. cp.mycompany.com は認証サーバーで、ClearPass.23 はキャプティブ ポータル サーバーです。

C. ClearPass.23 は認証サーバーで、cp.mycompany.com はキャプティブ ポータル サーバーです。

D. ClearPass.23 は認証サーバー、MC2 はキャプティブ ポータル サーバーです。

正解: **C** (コメントを発表する)

質問: **15**

ある企業が、1610 室のホテル、カジノ、コンベンション センターを備えたリゾートの建設を計画しています。同社は、スケーラビリティとサービスベースのアプローチを提供するモビリティ ソリューションに関心を持っています。このソリューションでは、コンベンション センターの WLAN インフラストラクチャを、リゾートでイベントを主催する任意の顧客 (テナント) にレンタルできます。
ソリューションは以下を提供する必要があります。
* ユーザーがホテルからカジノまたはコンベンション センターに移動するときのシームレスなローミング
* コンベンション センターでのリゾートおよび顧客所有の SSID の同時伝搬
* 顧客 (テナント) へのリゾート ネットワーク インフラストラクチャへの管理アクセスなし
* お客様 (テナント) へのレンタル SSID の設定および監視権限 どの展開が要件を満たしていますか?
A. マルチゾーン AP を備えた MM-MC インフラストラクチャをデプロイし、テナント SSID 用に 1 つのゾーンを配置します。
B. MM-MC インフラストラクチャを展開し、MC と AP に異なる階層グループを作成します。
C. AirWave と共に IAP を展開します。役割ベースの管理アクセス制御を展開します。
D. IAP を展開します。異なる中央アカウントでそれらを管理します。
E. ゾーン ベースの SSID を使用して IAP を展開し、異なる中央アカウントで管理します。
正解: **D (**コメントを発表する**)**

質問: **16**
ネットワーク管理者は、Airwave Management Platform (AMP) サーバーを展開し、それを Mobility Master (MM) - Mobility Controller (MC) ベースの WLAN と統合しました。AMP サーバーには、アクセス ポイント (AP) を含むすべての Aruba Mobility デバイスが「UP」デバイス リストに既に含まれています。
管理者が「Airwave>Devices>Monitor」の下で AP に対して実行できる 2 つのアクションは何ですか? (2つ選んでください。)
A. そのアクセス ポイントに対して MC の show コマンドを呼び出します。
B. AP の無線モードを無効にして変更します。
C. スペクトラム解析をローカルで実行します。
D. AP が終端する MC の WebUI を開きます。
E. アクセス ポイントを再プロビジョニングします。
正解: **(**正解を表示します**)**

質問: **17**
サッカー スタジアム向けの Aruba WiFi ソリューションには、2500 の AP、2 つのモビリティ マスター (MM)、および 8 つのモビリティ コントローラー (MC) が含まれます。主な要件は、シームレスなローミングと、MC の障害時でも AP とクライアントの均一な配布です。
シームレスなローミングを提供し、MC 障害の前後にすべての MC 間で AP クライアントの分散を提供する MC の展開オプションはどれですか?
A. デュアル モードの 8 メンバー HA グループ
B. デュアル モードの 2 メンバー HA グループ
C. 2 つの 4 メンバー L2 接続クラスター
D. 8 メンバーの L2 接続クラスター
正解: **(**正解を表示します**)**

質問: **18**
展示を参照してください。

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

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

ネットワーク管理者は、ユーザーが 8 時間ごとに定期的に認証されるように構成されていることを確認する必要があります。この変更を有効にするには、どの構成が必要ですか?

A. reauth-period を 28800 に設定して、dotlx と AAA プロファイルの両方で再認証を有効にします。

B. reauth-period を 28800 に設定して、AAA プロファイルで再認証を有効にします。

C. dotlx プロファイルで reauth-period を 28800 に設定し、AAA プロファイルで再認証を有効にします。

D. reauth-period を 28800 に設定し、dotlx プロファイルで再認証を有効にします。

正解: **D** (コメントを発表する)