Cisco.300-430J.v2026-02-19.q120

試験コード： 300-430J
試験名称： Implementing Cisco Enterprise Wireless Networks (300-430日本語版)
認証ベンダー： Cisco
無料問題の数： 120
バージョン： v2026-02-19
ページの閲覧量： 111
問題集の閲覧量： 1478
https://www.jpnshiken.com/shiken/Cisco.300-430J.v2026-02-19.q120.html

質問: **1**
エンジニアが、Cisco Catalyst 9800シリーズ ワイヤレス コントローラに登録されているAPに対して、ローカルMAC認証リストを実装しようとしています。APのMACアドレスリストは追加されましたが、コントローラはAPのMAC認証を強制していません。MACに対するAP認証はどこで有効になっていますか？
A. Configuration > Security > AAA > AAA Advanced > AP Policy
B. Configuration > Wireless > AP Global Config
C. Configuration > Tags & Profiles > AP Join > default-ap-profile
D. Configuration > Security > AAA > Authentication > AAA Method List
正解: **(**正解を表示します**)**

質問: **2**
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで Cisco OEAP が有効になっている場所は?
A. RF プロファイル
B. フレックス プロファイル
C. ポリシー プロファイル
D. AP 参加プロファイル
正解: **(**正解を表示します**)**
The Cisco OfficeExtend Access Point (OEAP) feature is enabled on a Cisco Catalyst 9800 Series Wireless Controller through the Flex Profile. The Flex Profile allows for the configuration of various settings specific to FlexConnect deployments, including OEAP settings, which enable remote workers to connect to the corporate network securely.
References :=
* CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide
* Cisco documentation on Catalyst 9800 Series Wireless Controllers

質問: **3**

エンジニアが高可用性ワイヤレス ネットワークを設計しています。高可用性のためにどのメカニズムに焦点を当てる必要がありますか?

A. SNR

B. チャネルの再利用

C. RSSI

D. セルの重なり

正解: **(正解を表示します)**

When designing a high availability wireless network, the focus should be on cell overlap. Adequate cell overlap ensures that if one access point fails, another can provide coverage without service interruption, thus maintaining network resilience and availability. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **4**

エンジニアは、Cisco ISE で新しい一意の NAD をセットアップしています。

構成する必要がある 2 つのパラメーターはどれですか? 2つ選んでください。)

A. デバイスのホスト名

B. デバイスのパスワード

C. RADIUS フォールバック

D. デバイスの IP アドレス

E. RADIUS 共有シークレット

正解: **(正解を表示します)**

When setting up a new Network Access Device (NAD) on Cisco ISE, it is essential to configure the device's IP address and the RADIUS shared secret. The device IP address is used to identify the NAD within the network, and the RADIUS shared secret is a password used between the ISE and the NAD to ensure secure communication.

質問: **5**

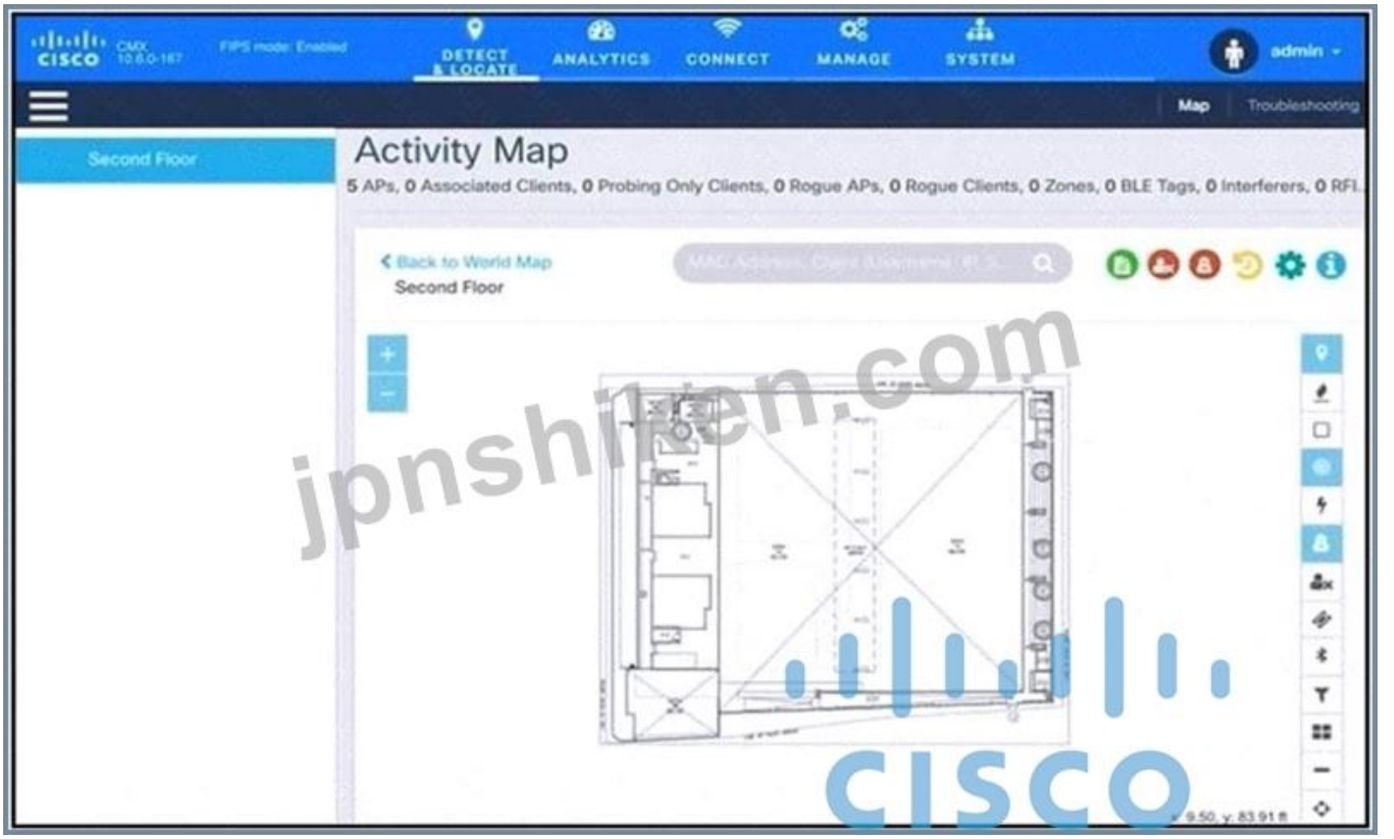
別紙を参照してください。

音声トラフィックがネットワークを通過する際に正しくタグ付けされるようにするには、どのCOS-DSCPマップを変更する必要がありますか?

A. COS of 6 to DSCP 46
B. COS of 3 to DSCP 26
C. COS of 7 to DSCP 48
D. COS of 5 to DSCP 46
正解: **(**正解を表示します**)**
In Quality of Service (QoS) for networking, Class of Service (COS) and Differentiated Services Code Point (DSCP) are used for traffic classification and prioritization. Voice traffic is generally given high priority due to its sensitivity to delay and requires proper tagging to maintain quality over the network.
The correct mapping for voice traffic, according to best practices, is a COS value of 5 mapped to a DSCP value of 46. This is because DSCP 46 corresponds to Expedited Forwarding (EF), which is typically used for voice traffic prioritization in IP networks.
The exhibit shows the output from a command on a network device that displays the current mappings between COS values and DSCP values. The mapping that needs modification for correct voice traffic tagging can be identified by looking at the standard practice for voice QoS, which uses a COS value of 5 mapped to a DSCP value of 46.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **6**
ある企業はシスコのワイヤレスソリューションを導入しており、Cisco ISEを使用して802.11aを使用して企業ユーザーを認証しています
X. ユーザはエンドポイントごとにグループ化し、ポリシープロファイルを追加してIDグループに割り当てる必要があります。Cisco ISEユーザインターフェイスでの設定パスは何ですか？
A. ポリシー > プロファイリング > プロファイリングポリシー > 追加
B. ポリシー > ポスチャ > ポスチャプロファイル > 追加
C. ポリシー > ポリシー要素 > プロファイリング > 追加
D. ポリシー > クライアントプロビジョニング > クライアントプロビジョニングポリシー > 追加
正解: **(**正解を表示します**)**

質問: **7**
別紙を参照してください。



エンジニアは、毎日オフィスを訪れるユーザー数を追跡・検出するためにCisco CMXソリューションを導入しました。CMXダッシュボードにデータが表示されません。この問題を解決するにはどうすればよいですか？

A. シングル サインオン認証を構成します。

B. WLC を CMX に追加します。

C. SCP を使用して、エクスポートされたマップを CMX サーバーから PI にコピーします。

D. CMX サーバに評価ライセンスをインストールします。

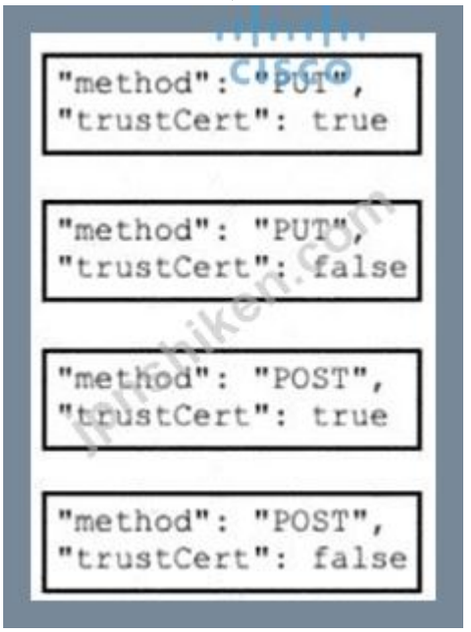
正解: **(**正解を表示します**)**

The issue with the Cisco CMX dashboard not showing any data can be resolved by integrating the Wireless LAN Controllers (WLCs) with the CMX system. The CMX solution relies on data from the WLCs to track and detect users' presence in the office area. Without the WLCs being added to CMX, the system cannot collect the necessary analytics and location data for its operations.

質問: **8**

別紙を参照してください。ネットワーク管理者は、Cisco Catalyst Center v2.3.7のレポート通知機能を使用して、セキュリティアドバイザリデータレポートの通知を自動化する必要があります。UI/CLIよりもプログラム可能なアプローチを優先し、管理者はCisco DNA Center APIを介してWebhookを作成し、外部アプリケーションにリアルタイムのHTTP通知を送信することにしました。Webhook URLは https://example.com/webhook は自己署名証明書を使用したHTTPSを使用しています。Webhookが正しく機能するには、ペイロードに特定の設定が必要です。自己署名証明書を使用してセキュ

リティアドバイザリデータレポートを抽出するようにWebhookを設定するPythonスクリプトを完成させるには、コードのボックスにどのコードスニペットを配置する必要がありますか？



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

質問: **9**
アクセス ポイントの名前を変更し、ワイヤレス コントローラの正しい AP グループに追加するには、エンジニアが読み取り/書き込みアクセス権を必要とします。Cisco ISE TACACS を使用する場合、最低限必要なカスタム属性はどれですか?
A. role1=WLAN
B. role1=WLAN role2=SECURITY
C. role1=WLAN role2=WIRELESS
D. role1=WIRELESS
正解: **D (**コメントを発表する**)**
To rename access points and add them to the correct AP groups on a wireless controller, the minimum custom attributes required using Cisco ISE TACACS is role1=WIRELESS. This role provides the necessary permissions for read/write access to wireless-related configurations. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **10**
Cisco ISEを使用した中央Web認証でSSIDが設定されています。新しいSSIDは、外部コントローラからアンカーコントローラへのゲストトンネリングを使用します。Web認証方式のRADIUS認証要求を実行するデバイスとして、ISEにどのデバイスを設定する必要がありますか？

A. 認証サーバー
B. アンカーコントローラー
C. 外部コントローラ
D. AP
正解: **B (**コメントを発表する**)**

質問: **11**
ワイヤレス エンジニアは、大企業向けの社内ワイヤレス ネットワークを可能な限り効率的な方法で実装する必要があります。ワイヤレス ネットワークは、さまざまな部門の 300 人の従業員に対して 32 の VLAN をサポートする必要があります。エンジニアはどのソリューションを選択する必要がありますか?
A. 展開内の AP の半分をサポートするように 2 番目の WLC を構成します。
B. 単一の SSID を設定し、さまざまなユーザ ロールに従って VLAN 割り当て用に Cisco ISE を実装します。
C. 異なる AP グループを構成して異なる VLAN をサポートし、すべての WLAN を両方の無線でブロードキャストできるようにします。
D. 16 個の WLAN を 2.4 GHz 帯域でブロードキャストするように構成し、16 個の WLAN を 5.0 GHz 帯域でブロードキャストするように構成します。
正解: **B (**コメントを発表する**)**
For a large company requiring support for 32 VLANs for different departments, the most efficient solution is to configure one single SSID and use Cisco ISE for dynamic VLAN assignment based on user roles. Cisco ISE can classify users into different groups and assign them to the appropriate VLANs. This approach reduces the complexity of managing multiple SSIDs and simplifies the user experience while maintaining a high level of security and network segmentation. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **12**
エンジニアは、IEEE 802.1X ワイヤレス ネットワークで、クライアントが中央リポジトリと Cisco WLC のローカル クレデンシャルを使用して認証されるようにしています。WLAN で完了する必要がある 2 つの構成要素はどれですか? （2つ選んでください。）
A. TACACS+
B. MAC認証
C. ローカル EAP が有効
D. Web 認証
E. LDAP サーバー
正解: **(**正解を表示します**)**
On a WLAN that uses IEEE 802.1X for wireless network authentication, enabling local EAP allows clients to authenticate using locally stored credentials on the Cisco Wireless LAN Controller (WLC), which is useful in scenarios where the external RADIUS server is unavailable.

The LDAP server option is used to authenticate clients against a central repository, such as an LDAP directory. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **13**
エンジニアは、管理者ユーザが認証された後、RBAC を気にすることなく、Active Directory を使用して WLC への管理アクセスを制御する必要があります。このタスクを達成するためにエンジニアが構成する 2 つの機能はどれですか? (2つ選んでください。)
A. デバイス管理ポリシー セット
B. ユーザー アクセス モード: ReadWrite
C. ACL
D. RADIUS サーバー
E. TACACS サーバー
正解: **(正解を表示します)**
To control administrative access to the WLC using Active Directory without concern for RBAC post- authentication, the engineer would configure a RADIUS server (option D) and a TACACS server (option E).
These servers can integrate with Active Directory to authenticate users, and once authenticated, the admin user's access level can be determined without the need for additional role-based access control configurations within the WLC. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, focusing on the integration of WLC with RADIUS and TACACS servers for administrative access control.

質問: **14**
エンジニアは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで証明書をプロビジョニングする必要があります。顧客はサードパーティの CA サーバを使用しています。証明書を要求してインストールするには、コントローラと CA サーバ間でどのプロトコルを使用する必要がありますか?
A. SCEP
B. TLS
C. LDAP
D. SSL
正解: **(正解を表示します)**
The Simple Certificate Enrollment Protocol (SCEP) is used to securely issue certificates to network devices in a scalable manner. When provisioning certificates on a Cisco Catalyst 9800 Series Wireless Controller using a third-party CA server, SCEP is the protocol that facilitates this process. It allows the controller to request and install certificates automatically, which is essential for establishing secure communications within the network. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI
300-430 Official Cert Guide)

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/trustpoints/b- configuring-trustpoints-on-cisco-catalyst-9800- series-controllers/c-workflow-to-configure-a-trustpoint-for-a- third-party-certificate-on-catalyst-9800.html

質問: **15**
Cisco CMXのポータルを使用して、ゲストアクセス用にWLANを設定しています。どのレイヤ3セキュリティ設定を選択する必要がありますか？
A. Webポリシースプラッシュページリダイレクト
B. Webポリシー条件付きリダイレクト
C. Webポリシー認証
D. ウェブポリシーパススルー
正解: **(**正解を表示します**)**

質問: **16**
ネットワークエンジニアは、500台のAPを備えたコントローラでマルチキャストを有効にした後、コントローラのCPUオーバーヘッドとネットワーク全体の使用率が急上昇することに気づきました。この問題を修正する機能はどれですか？
A. コントローラのIGMPスヌーピング
B. マルチキャストAP マルチキャストモード
C. ブロードキャスト転送
D. ユニキャストAPマルチキャストモード
正解: **D (**コメントを発表する**)**
Enabling unicast AP multicast mode can correct the issue of increased controller CPU overhead and overall network utilization after multicast is enabled. This mode allows the controller to send multicast traffic to the APs as unicast, which is more efficient for the wireless medium and reduces the load on the controller's CPU.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

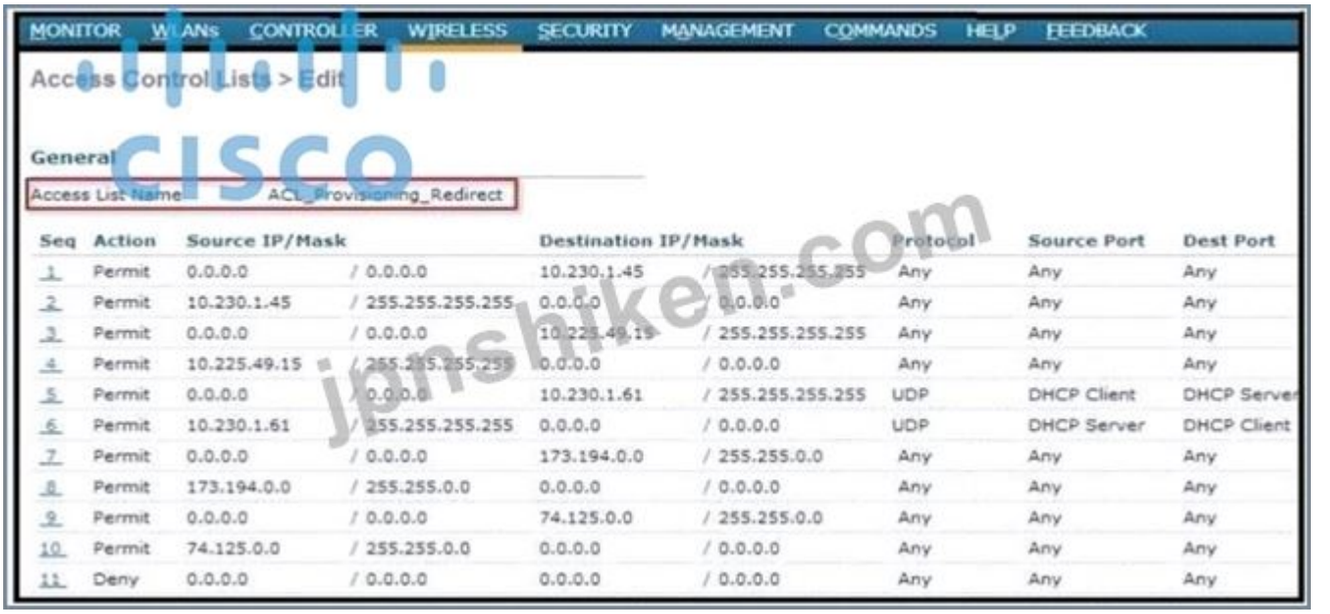
質問: **17**
ある企業では、WLCに2つのWLANが設定されています。APをFlexConnectモードに変換すると、WLAN Aは動作しますが、WLAN Bは動作しないという報告があります。APをローカルモード

に変換すると、WLAN Bは動作しますが、WLAN Aは動作しません。この設定を完了するには、どのような操作が必要ですか？
A. WLAN-VLAN マッピングを使用して Cisco FlexConnect グループを作成します。
B. WLAN 上のローカル スイッチングを無効にします。
C. AP グループを WLAN インターフェイスにマッピングします。
D. AP を Cisco FlexConnect グループに参加させます。
正解: **(**正解を表示します**)**
FlexConnect is a wireless solution for branch office and remote office deployments. It allows APs to switch client data traffic locally and perform client authentication locally when they are disconnected from the WLC.
For WLAN A to work in FlexConnect mode and WLAN B to work in local mode, the APs need to be part of a FlexConnect group with proper WLAN-VLAN mappings. This ensures that the correct VLAN is used for each WLAN, which is essential when the APs are operating in FlexConnect mode. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **18**
ネットワーク エンジニアは、ゲスト アクセスに使用される新しいワイヤレス ネットワークを作成しました。企業ネットワークはすべてのレートを使用する必要があります。ゲスト ネットワークは、802.11n データ レートではなく、より低いレートのみを使用する必要があります。このタスクを実行するには、WLAN の WMM ポリシーを何に設定する必要がありますか?
A. 必須
B. 許可
C. 無効
D. 必須
正解: **(**正解を表示します**)**
To ensure that the guest network uses only lower rates instead of 802.11n data rates, the WMM (Wi-Fi Multimedia) policy of the WLAN should be set to disabled . This will prevent the use of 802.11n data rates, which require WMM to be enabled. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **19**
小売企業のマーケティング部門は、新支店（hp-GA4B6C828354AB）の開店プロモーションビデオを制作しました。ビデオは、無線マルチキャスト経由で、関心のある人だけが受信する必要があります。この機能を可能にするのは何ですか？
A. WMF
B. DCA
C. TPC
D. WMM
正解: **(**正解を表示します**)**

質問: **20**
別紙を参照してください。



BYODクライアントのアクセスを制限するためのACLが設定されています。ACLはデバイスをゲストポータルにリダイレクトする必要があります。
ACL は、DHCP サーバー以外のローカル ネットワーク上のどの 2 つのデバイスへのアクセスを許可する必要がありますか? (2 つ選択してください。)

A. RADIUS server
B. DNS server
C. Cisco ISE
D. SNMP server
E. WLC

正解: **A,C (**コメントを発表する**)**

An ACL configured for BYOD clients to redirect to a guest portal must allow access to the RADIUS server and Cisco ISE. The RADIUS server is crucial for authentication services, a core component of network access control for BYOD. Cisco ISE integrates with the network infrastructure to provide comprehensive security, including guest access management, thus its accessibility is essential for the redirection process to function correctly. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **21**
ある大学は、学生から報告されたWi-Fiの問題をネットワーク管理者が解決できるように、Cisco Catalyst Center（旧DNA Center）ソリューションを導入しました。キャプチャされたデータパケットの表示、監視、トラブルシューティングには、クライアントダッシュボードを使用する必要があります。どの機能を使用する必要がありますか？

A. Intelligent Capture

B. Packet Capture
C. Packet Sniffer
D. Cisco CleanAir
正解: **B (**コメントを発表する**)**

質問: **22**
ネットワーク管理者は、Cisco CMX の基本的な実装を完了したばかりで、ロケーション トラッキングの実装を試みています。管理者は、NMSP を介して WLC の 1 つ間の接続を確立する際に問題を抱えています。この接続を確立するには、何を構成する必要がありますか? (2つ選んでください。)
A. Cisco CMX サーバに永久ライセンスを追加します。
B. Cisco CMX と WLC の間のファイアウォール ポート 16113 で許可します。
C. WLC で NMSP を有効にします。
D. 初めて WLC を追加した後、Cisco CMX を再起動します。
E. Cisco CMX サーバの MAC アドレスと SSC キーを WLC に追加します。
正解: **(**正解を表示します**)**
To establish connectivity between a Wireless LAN Controller (WLC) and Cisco's Connected Mobile Experiences (CMX) through Network Mobility Services Protocol (NMSP), it is essential to enable NMSP on the WLC, which facilitates communication with location-based services like CMX. Additionally, for secure communication, it is necessary to add the MAC address of the Cisco CMX server to the WLC along with its SSC (Self-Signed Certificate) key, ensuring that both devices can authenticate each other and establish a trusted connection. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **23**
エンジニアが Cisco ISE を使用してワイヤレス インフラストラクチャへの管理アクセスを設定し、WLC syslog 設定の設定を許可する役割はどれですか?
A. 管理
B. セキュリティ
C. コントローラー
D. ワイヤレス
正解: **(**正解を表示します**)**
The MANAGEMENT role should be configured for administrative access to the wireless infrastructure using Cisco ISE. This role allows the configuration of WLC syslog settings, among other management tasks, ensuring proper logging and monitoring of the wireless network. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **24**

顧客は、従業員が個人のデバイスをワイヤレス ネットワークに簡単にオンボーディングできるようにしたいと考えています。また、訪問者は、受付デスクの誰かとやり取りする必要なく、同じネットワークに接続できる必要があります。この要件をサポートするには、Cisco ISE でどのプロセスを設定する必要がありますか?

A. MAC 認証バイパス

B. ネイティブ サプリカント プロビジョニング

C. ローカル Web 認証

D. 自己登録ゲスト ポータル

正解: **D** (コメントを発表する)

To meet the requirement of allowing employees to easily onboard their personal devices and visitors to connect without reception desk intervention, configuring a self-registration guest portal on Cisco ISE is the appropriate solution. This feature enables guests to create their own accounts and gain network access, streamlining the process for both employees' personal devices and visitors. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **25**

図を参照してください。イベント会社は、クライアントにWi-Fiへの無料ゲストアクセスを提供するイベントで、無線クライアントの位置追跡詳細を収集する必要があります。ネットワークエンジニアは、Cisco WLCとCisco CMXサーバを統合する必要があります。どのコマンドを実行する必要がありますか？

```
Please enter controller type [WLC / NGWC] [WLC]: WLC
Please enter controller ip: 0.0.0.0
Please enter the controller version [Optional]:
Please enter controller SNMP version [v1 / v2c / v3] [v2c]: v2c
Please enter controller SNMP write community [private]:
```

```
[cmxadmin@cmx]# cmxctl config controllers floors wlc-ip-address
```

```
[cmxadmin@cmx]# cmxctl config controllers add
```

```
[cmxadmin@cmx]# cmxctl config controllers import
```

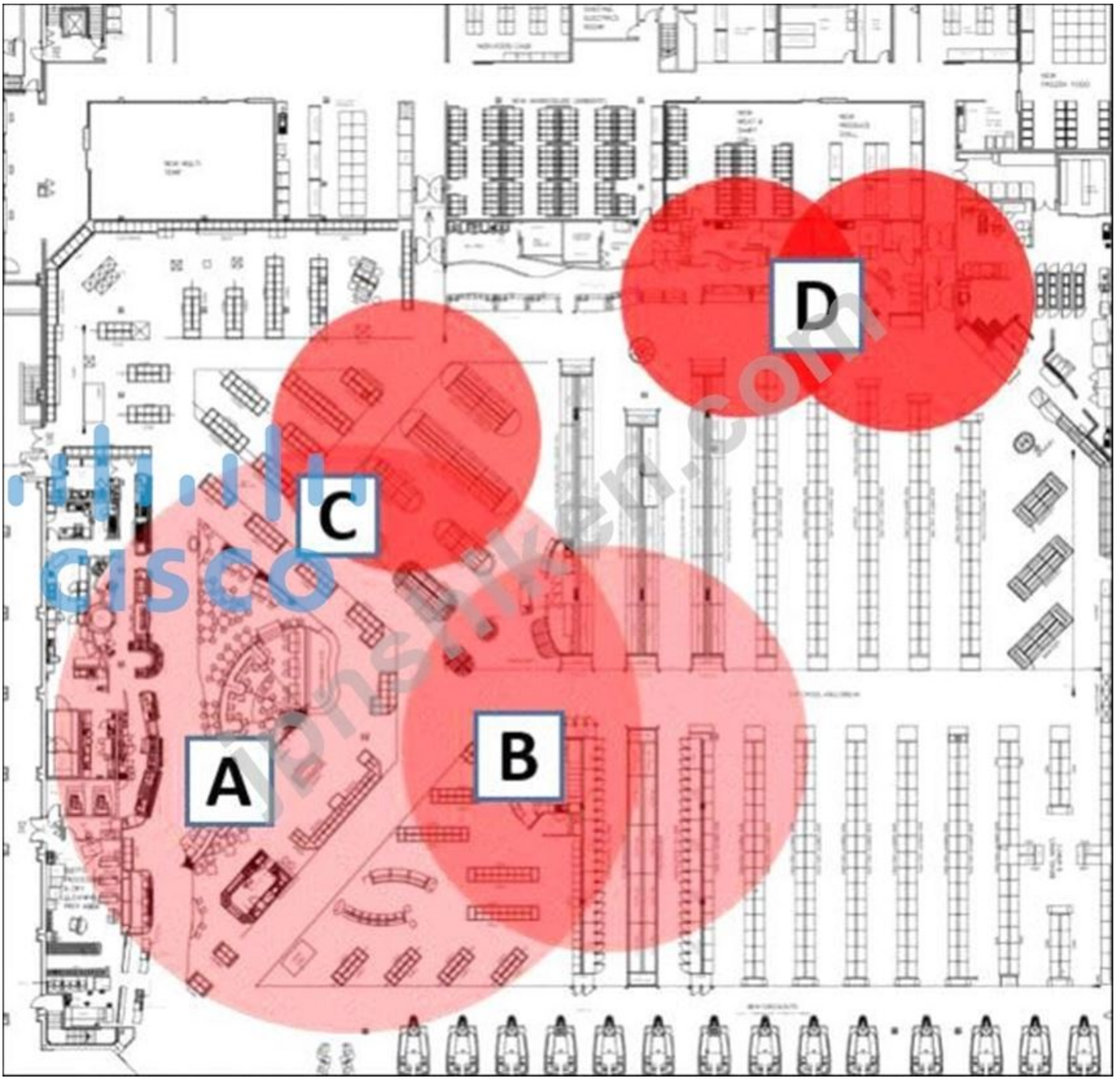
```
[cmxadmin@cmx]# cmxctl config controllers activeap
```

A. オプションD

B. オプションB

C. オプションA
D. オプションC
正解: (正解を表示します)

質問: **26**
別紙を参照してください。



Cisco CleanAirの干渉源の影響ゾーンマップを見ると、ワイヤレスネットワークに最も大きな影響を与えるのはどのエリアですか？
A. A
B. B
C. C
D. D

正解: (正解を表示します)
The exhibit provided appears to be a floor map overlay with Cisco CleanAir Zone of Impact for interferers, which shows different areas affected by interference on a wireless network. The area labeled 'A' indicates the greatest impact on the wireless network due to its larger size compared with other zones, suggesting more significant interference or a stronger source of interference within this zone. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide) Reference: https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112139-cleanair-uwn-guide-00.html

質問: **27**
Cisco WLC がネットワークに追加され、ネットワーク デバイスとして Cisco ISE が追加されましたが、認証に失敗しています。ネットワーク デバイス構成内のどの構成を確認する必要がありますか?
A. SNMP RO コミュニティ
B. デバイス インターフェイスの資格情報
C. デバイス ID
D. 共有秘密
正解: (正解を表示します)
When a Cisco Wireless LAN Controller (WLC) is added to Cisco ISE as a network device for authentication purposes, it is crucial to verify the shared secret configured within the network device settings. The shared secret is used to secure communication between the WLC and ISE, ensuring that the authentication messages are encrypted and authenticated. If the shared secret does not match on both the WLC and ISE, the authentication will fail. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **28**
無線ネットワークが実装され、マルチキャストビデオを無線リンク経由で無線ユーザーに確実にストリーミング配信できるようになりました。クライアントからビデオをストリーミングできないという報告があった後、管理者はクライアントが12 Mbpsのデータレートで接続しており、ネットワーク上の有効なマルチキャストアドレスにストリーミングしようとしていると判断しました。この場合、適用する必要がある2つのアクションはどれですか？ 2つ選択してください。）
A. コントローラ上で設定されているすべての WLAN の IGMP スヌーピングをオフにします。
B. コントローラ上のマルチキャストビデオ用のビデオストリームを実装します。
C. マルチキャスト ダイレクトが正しく動作し、マルチキャスト ダイレクトがグローバルに有効になるようにします。
D. マルチキャストを有効にする WLAN の WLAN QoS 値を Bronze に変更します。
E. ワイヤレス マルチキャストが確認応答を使用しないため、RTSP がビデオをストリーミングできるようにします。

正解: (正解を表示します)
To ensure reliable streaming of multicast video over a wireless link, it's essential to optimize the multicast settings on the controller. Option B, implementing video-stream for the multicast video on the controller, is a feature that optimizes the delivery of multicast streams by converting them into unicast streams for specific clients, thus improving reliability. Option C, allowing multicast-direct to work correctly, involves enabling multicast-direct globally, which allows multicast packets to be sent directly to clients without the need for them to subscribe to a specific multicast group, enhancing efficiency and reliability. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **29**
Cisco Context Aware Services で追跡できるデバイスはどれですか?
A. 有線および無線デバイス
B. ワイヤレス デバイス
C. 有線デバイス
D. シスコ認定ワイヤレス デバイス
正解: (正解を表示します)
Cisco Context Aware Services provide real-time tracking of mobile assets and users by gathering contextual information from networked devices. This service is not limited to wireless devices; it can track both wired and wireless devices within the network. The technology utilizes elements like Received Signal Strength Indicator (RSSI) and Time Difference of Arrival (TDoA) for location tracking and telemetry. References:
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, and Cisco Context Aware Software FAQ.
Reference: https://www.cisco.com/c/en/us/support/docs/wireless/context-aware-software/110836-cas-faq.html

質問: **30**
エンジニアは、Cisco Prime Infrastructure に表示される不正なアクセス ポイントをトラブルシューティングしています。
WLC で識別された不正なアクセス ポイントを封じ込めるためにエンジニアが使用できる APS の最大数はいくつですか?
A. 3
B. 4
C. 6
D. 5
正解: (正解を表示します)
In Cisco Prime Infrastructure, the maximum number of APs that can be used to contain an identified rogue access point in the WLC is four (4). This containment process involves using nearby APs to disrupt the rogue AP's signals, thereby preventing it from effectively communicating with client devices. References: CCNP Enterprise Wireless Design ENWLSD

300-425 and Implementation ENWLSI 300-430 Official Cert Guide, which includes information on rogue AP detection and containment strategies within the WLC and Cisco Prime Infrastructure.

質問: **31**
エンジニアが仮想 MSE を展開しています。ネットワークには 3000 の AP があり、7000 の IPS ライセンスが必要です。
エンジニアはどのサイズのサーバーにスケーリングしますか?
A. 仮想
B. 標準
C. ハイエンド
D. ローエンド
正解: **(**正解を表示します**)**
For a network with 3000 APs and 7000 IPS licenses, scaling to a high-end server is appropriate. This will provide the necessary resources and capabilities to support the large number of APs and the extensive licensing requirements for the Intrusion Prevention System.

質問: **32**
mDNS の構成に関して適用されている 2 つの制限はどれですか? (2つ選んでください。)
A. mDNS は宛先ポートとして UDP ポート 5436 のみを使用します。
B. mDNS は UDP ポート 5353 を宛先ポートとして使用できません。
C. mDNS は、ローカルでスイッチされる WLAN を使用する FlexConnect AP ではサポートされていません。
D. コントローラー ソフトウェアは 7.0.6+ よりも新しい必要があります。
E. mDNS は IPv6 ではサポートされていません。
正解: **(**正解を表示します**)**
mDNS has specific restrictions regarding its configuration. Option C is correct because mDNS is not supported on FlexConnect APs with a locally switched WLAN, which limits its deployment in certain network designs. Option D is also correct; the controller software must be newer than version 7.0.6 to support mDNS features, which means that older controller software versions do not have the necessary capabilities to handle mDNS. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **33**
ワイヤレスエンジニアがISEを使用してLWAを設定しています。顧客はスタートアップ企業で、ワイヤレスユーザーにディレクトリ認証を要求しましたが、LDAPが利用できません。同等のセキュリティとユーザーエクスペリエンスを実現するには、どのようなソリューションを提案すべきでしょうか？
A. SAMLを使用します。
B. RADIUSサーバーの内部データベースを使用します
C. 企業の WLAN で事前共有キーを使用します。
D. Novell eDirectory を使用します。
正解: **(正解を表示します)**
For a startup company without LDAP, using the internal database of the RADIUS server is a viable solution to authenticate wireless users. This approach allows the company to maintain a directory of users within the RADIUS server itself, providing similar security and user experience as LDAP would. Users can be authenticated against this internal database, ensuring secure access to the wireless network. References:
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **34**
エンジニアは、単一のソースから単一のドメイン内で EIGRP と BGP を使用して、ネットワーク上で全社ビデオ会議用にワイヤレスのマルチキャストを構成しています。どのタイプのマルチキャスト ルーティングを実装する必要がありますか?
A. プロトコルに依存しないマルチキャスト デンス モード
B. ソース固有のマルチキャスト
C. マルチキャスト ソース検出プロトコル
D. プロトコルに依存しないマルチキャスト スパース モード
正解: **(正解を表示します)**
For a network using EIGRP and BGP within a single domain from a single source, Protocol Independent Multicast Sparse Mode (PIM-SM) is the most suitable multicast routing to be implemented. PIM-SM is efficient for networks with a large number of networks and few receivers, which seems to be the case for an all-company video meeting.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **35**
ある企業には、Cisco ISE を備えた Cisco ワイヤレス ネットワークがあります。会社は、従業員が個人のモバイル デバイスをワイヤレス ネットワーク上で使用できるようにしたいと考えています。会社は、デバイスが特定の基準を満たしている場合にのみネットワークへのアクセスを許可したいと考えています。この要件を満たすために、同社はネットワーク エンジニアにネイティブ

サプリカント プロファイルの作成を依頼しました。プロファイルの作成時に構成する必要がある2 つのフィールドはどれですか? (2つお選びください。)
A. WLC 名
B. 許可されたプロトコル (LEAP/EAP-TTLS)
C. 許可されたプロトコル (PEAP/TLS)
D. 許可されたプロトコル (Ms-CHAPv2/EAP-FAST)
E. SSID 名
正解: **(**正解を表示します**)**

質問: **36**
エンジニアは、HRユーザーとVIPユーザーに異なるルールを持つ新しいCisco AVCプロファイルを定義しています。両方のユーザータイプは単一のSSIDに接続し、Cisco ISEを介してActive Directoryの認証情報を使用して認証します。エンジニアは、AVCプロファイルをユーザータイプに動的に適用したいと考えています。Cisco ISEに適用する必要があるCisco AVペア属性はどれですか？
A. avc-protile-name
B. policy-avc-role
C. role-name-avc
D. policy-role-avc
正解: **A (**コメントを発表する**)**

質問: **37**
ワイヤレスコントローラにはRADIUSサーバがグローバルに設定されています。このコントローラでは、WLAN Aに別のRADIUSサーバがマッピングされています。コントローラはWLAN Aからのクライアントの認証にどのRADIUSサーバを使用しますか？
A. 最初にグローバルに設定されているRADIUSサーバを使用し、認証に失敗した場合はWLAN Aにマッピングされ ているRADIUSサーバに戻ります。
B. 最初にWLAN Aにマッピングされ ているRADIUSサーバ、認証に失敗した場合はグローバルに設定されているRADIUSサーバに戻ります。
C. WLAN Aにマッピングされ ているRADIUSサーバー
D. グローバルに設定されたRADIUSサーバー
正解: **C (**コメントを発表する**)**

質問: **38**
エンジニアは、以下をサポートするように展開を構成します。
Cisco CMX
少なくとも 3000 AP のライセンス
6000 wIPS ライセンス
Cisco vMSE アプライアンスは、この導入に合わせたサイズにする必要があります。エンジニアはどの Cisco vMSE リリース 8 オプションを導入する必要がありますか?

A. 大規模な vMSE
B. ローエンド vMSE
C. 標準 vMSE
D. ハイエンド vMSE
正解**: (**正解を表示します**)**
For a deployment that supports Cisco Connected Mobile Experiences (CMX), licenses for at least 3000 Access Points (APs), and wIPS licenses for 6000 sensors, a High-End vMSE is required. This version of MSE is designed to handle large-scale deployments with high license and sensor requirements, ensuring that the system can manage the data and analytics for such a substantial wireless environment. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問**: 39**
エンジニアは、Mobility Express AP がインストールされ、Apple エンドユーザー デバイスを使用して、ワイヤレス ネットワークに Fastiane を実装しようとしています。セキュリティ上の懸念により、IT 部門はすべての iPad をバージョン 14.5.423551943 に更新しました。エンジニアがユーザー WLAN で構成する必要がある QoS プロファイルはどれですか?
A. プラチナ
B. ベスト エフォート
C. ブロンズ
D. シルバー
正解**: (**正解を表示します**)**
Fastlane is a feature developed by Apple and Cisco that provides a higher-quality user experience for critical business applications. To implement Fastlane, the WLAN must use the Platinum QoS profile, which is designed to prioritize business-critical traffic and applications. Since the IT department has updated the iPads to a specific version, it is important to ensure that the QoS settings align with the requirements of Fastlane to maintain application performance and security.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問**: 40**
別紙を参照してください。

Event	5405 RADIUS Request dropped
Failure Reason	11036 The Message-Authenticator RADIUS attribute is invalid

無線エンジニアが無線ネットワークをRADIUSサーバーと統合しました。RADIUSサーバーの設定は正しいものの、ユーザーから接続できないという報告を受けています。トラブルシューティング中に、エンジニアは認証リクエストがドロップされていることに気付きました。この問題を解決するにはどうすればよいですか？

A. ワイヤレス コントローラから RADIUS サーバーの IP への接続を許可します。
B. RADIUS サーバーで設定されている有効なクライアント ユーザー名を指定します。
C. コントローラと RADIUS サーバで共有秘密キーを設定します。
D. RADIUS サーバーに設定されているのと同じ EAP タイプを使用してクライアントを認証します。
正解**: (**正解を表示します**)**
The issue described indicates that authentication requests from the wireless network to the RADIUS server are being dropped. This problem is often due to a mismatch in shared-secret keys between the wireless controller and the RADIUS server. The shared secret is a password-like value that must be configured on both sides to ensure secure communication. By configuring both sides with matching shared-secret keys, it ensures that authentication messages are properly encrypted and decrypted by each party, allowing for successful user connection.
References: (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問**: 41**
ある企業がオンプレミスイベントの要件を収集しています。イベント中、専用WLANに接続されたワイヤレスクライアントは、正常に動作するために平均391595179ビット/秒の帯域幅を必要とするビデオアプリケーションを実行します。このWLANに適用する必要があるQoSマーキングは何ですか？
A. プラチナ
B. ゴールド
C. シルバー
D. ブロンズ
正解**: (**正解を表示します**)**
The Platinum QoS marking is typically used for the highest-priority traffic, such as voice and video. Given the requirement for a high average bitrate for the video application, Platinum would be the appropriate QoS marking to ensure the necessary bandwidth and priority on the WLAN.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問**: 42**
ある病院は、既存の無線インフラを利用して、病室への屋内経路案内を提供したいと考えています。無線ネットワークは位置情報サービス仕様を使用しています。この要件をサポートするには、どの2つのコンポーネントをインストールする必要がありますか？ 2つ選択してください。）
A. WIPS
B. Cisco MSE
C. Cisco CMX ビジターコネクト
D. Cisco CMX AppEngage
E. Cisco CMX アナリティクス

正解: **B,C (**コメントを発表する**)**
To offer indoor directions to patient rooms using the existing wireless infrastructure, the hospital would need to install Cisco MSE (B) and Cisco CMX Visitor Connect . Cisco Mobility Services Engine (MSE) provides advanced location services, including tracking for Wi-Fi clients, which is essential for indoor navigation.
Cisco CMX Visitor Connect, part of the Cisco Connected Mobile Experiences (CMX) solutions, allows for the customization of visitor experiences, such as indoor navigation. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **43**
エンジニアは、企業のワイヤレス ネットワークを担当しています。企業は世界中にオフィスを分散させており、すべての AP は FlexConnect モードで設定されています。ネットワークは、802.11r および CCKM をサポートするように構成する必要があります。この目標を達成するために何を実装する必要がありますか?
A. VLAN ベースの中央スイッチングを有効にします。
B. FlexConnect ローカル認証を有効にします。
C. FlexConnect ローカル スイッチングを有効にします。
D. FlexConnect グループを作成します。
正解: **(**正解を表示します**)**
For an enterprise wireless network with distributed offices globally and APs configured in FlexConnect mode, enabling FlexConnect local authentication is essential to support 802.11r and CCKM. This configuration allows for fast roaming and maintains a secure connection by locally authenticating the clients without having to go back to the central site, thus providing a seamless and efficient roaming experience for the users.

質問: **44**
エンジニアはショッピングセンターの無線ネットワークを管理しています。ネットワークには、Cisco WLC、Cisco MSE、Cisco Prime Infrastructureが含まれています。Cisco CMXロケーションアナリティクスを使用するには何が必要ですか？
A. Cisco MSE で追跡パラメータを有効にします。
B. Context Aware と CMX Browser Engage を有効にします。
C. フロア マップを使用して Cisco Prime Infrastructure をインストールします。
D. Cisco MSE で履歴パラメータを設定します。
正解: **(**正解を表示します**)**
Cisco Connected Mobile Experiences (CMX) Location Analytics requires accurate tracking of devices within the wireless network's coverage area. To utilize CMX Location Analytics effectively, it is essential to enable tracking parameters in Cisco Mobility Services Engine (MSE). This allows MSE to collect data on device locations and movements within the environment, which can then be analyzed by CMX for insights into customer behavior, asset tracking, or other

analytical purposes. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **45**
エンジニアは、192.168.1.10 の WLC 管理 IP アドレスと 192.168.2.0/24 の AP サブネットを持つネットワークに管理制御を制限するために RADIUS を実装しています。エンジニアが RADIUS サーバーで定義するエントリはどれですか?
A. WLC およびネットワーク範囲 192.168.2.0/255.255.254.0 で定義された管理アクセス
B. 仮想インターフェースのNASエントリとネットワーク範囲 192.168.2.0/255.255.255.0
C. WLC およびネットワーク範囲 192.168.1.0/255.255.254.0 で定義された共有秘密
D. コマンドの WLC ロールとネットワーク範囲 192.168.1.0/255.255.255.0
正解: **(**正解を表示します**)**
For RADIUS to restrict administrative control effectively, the engineer needs to define a Network Access Server (NAS) entry that corresponds to the WLC's management IP address and the AP subnet. The correct entry would be the NAS IP of the virtual interface (typically used for RADIUS communications) and the specific network range of the AP subnet, which is 192.168.2.0 with a subnet mask of
255.255.255.0. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **46**
エンジニアがゲストアクセス用の新しいワイヤレスネットワークを設定しています。ゲストユーザーがネットワークにアクセスする前に、会社のFacebookページを閲覧できるようにする必要があります。ワイヤレスコンポーネントとしてCisco MSEを使用しています。設定において、外部リダイレクトURLとしてどのURLを使用する必要がありますか？
A. http://<MSE>:8083/visitor/login.do
B. http://<MSE>:8083/fbwifi/forward
C. http://<MSE>:8084/visitor/login.do
D. http://<MSE>:8084/fbwifi/forward
正解: **B (**コメントを発表する**)**
The correct URL to be used in the configuration as the external redirection URL for guests to view the company's Facebook page before accessing the network is http://<MSE>:8083/fbwifi/forward (B). This URL is associated with the Cisco MSE's Facebook Wi-Fi feature, which facilitates the redirection process. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI
300-430 Official Cert Guide.

質問: **47**
PIM スパース モードと PIM デンス モードの違いは何ですか?
A. スパース モードは 1 つのスイッチのみをサポートします。高密度モードは、マルチスイッチ ネットワークをサポートします。
B. スパース モード フラッド。密モードは配布ツリーを使用します。
C. スパース モードは配布ツリーを使用します。密モードフラッド。
D. スパース モードはマルチスイッチ ネットワークをサポートします。デンス モードは、1 つのスイッチのみをサポートします。
正解: **(**正解を表示します**)**
Protocol Independent Multicast (PIM) sparse mode and dense mode are two different multicast routing mechanisms. Sparse mode uses distribution trees and is designed for networks where multicast groups are sparsely distributed across the network, minimizing unnecessary traffic. In contrast, dense mode floods the network with multicast traffic and then prunes back the branches where there are no interested receivers, which can lead to inefficient use of bandwidth.
References := CCNP Enterprise Wireless Design ENWLSD
300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **48**
顧客の倉庫施設には、自律モードのCisco 3700シリーズAPが10台設置されています。Cisco WLAN電話機をサポートするために、新しいVoWLANサービスを導入しています。すべての有線QoSは設定済みです。顧客は、すべてのVoWLANシグナリングとRTPトラフィックを有線ネットワークと無線ネットワーク間で優先させる必要があります。必要な設定は何ですか？
A. すべての AP で Fastlane をオンにします。
B. 音声とビデオを最適化するには、すべての AP で EDCA を設定します。
C. すべての AP の RTP およびシグナリングに Cisco AVC プロファイルを適用します。
D. すべてのAPでAWID優先度マッピングを有効にする
正解: **(**正解を表示します**)**

質問: **49**
BYOD 用にデュアル SSID 設計を実装する際の重要な考慮事項は何ですか?
A. プロビジョニング SSID を使用した後、クライアントに SSID を切り替えるために使用された ACL により、ユーザーは関連付けを行い、MAC フィルタリングによってネットワークを横断するように強制されます。
B. 複数の WLC を使用する場合、クライアントがプロビジョニングされ、ネットワークを正しく通過するには、WLAN ID が正確である必要があります。

C. このセットアップの SSID は、クライアントが Cisco ISE で認証されるように NAC State-RADIUS NAC で設定するか、Cisco ISE がクライアントを関連付けるために NAC State-ISE NAC で設定する必要があります。
D. 1 つの SSID はプロビジョニング用で、もう 1 つの SSID はネットワークへのアクセス用です。プロビジョニング後にクライアントを REAL SSID に接続させるために、ACL の使用を強制しないでください。
正解: **D** (コメントを発表する)
In a dual SSID design for BYOD, one SSID is used for provisioning devices, and the other is for network access. It's important not to enforce an ACL to switch SSIDs after provisioning because this could disrupt the user experience. Instead, the process should be seamless, with the device automatically connecting to the access SSID after provisioning is complete. References := (CCNP Enterprise Wireless Design ENWLSD 300-
425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **50**
FlexConnect リモート オフィスの導入では、屋内で 5 つの 2702i AP を使用し、屋外で 2 つの 1532i AP を使用しています。コード アップグレードが実行され、FlexConnect スマート AP イメージ アップグレードが利用されているが、FlexConnect マスター AP が設定されていない場合、WLC と AP の間で何回のイメージ転送が発生しますか?
A. 1
B. 2
C. 5
D. 7
正解: **B** (コメントを発表する)
When using FlexConnect Smart AP Image Upgrade without a configured FlexConnect Master AP, the WLC will transfer the image to one indoor AP and one outdoor AP separately. Each AP model needs a different firmware image due to hardware differences. Therefore, there will be two image transfers from the WLC: one for the 2702i APs and another for the 1532i APs.
References :=
* CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide
* Cisco documentation on FlexConnect Smart AP Image Upgrade

質問: **51**
ワイヤレス クライアントのクライアント プロファイリングに使用される 3 つのプロパティはどれですか? (3つ選んでください。)
A. HTTP ユーザー エージェント
B. DHCP
C. MAC OUI
D. ホスト名

E. OS バージョン
F. IPアドレス
正解: **(**正解を表示します**)**
Client profiling involves using various properties to identify and classify wireless clients. The HTTP user agent can provide information about the client's device type and browser, DHCP can reveal details about the client's network configuration and requests, and the MAC OUI (Organizationally Unique Identifier) can be used to determine the manufacturer of the device. These properties are crucial for profiling because they offer insights into the device's capabilities and identity. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **52**
ある医療機関は、多数の不正APに気づき、ハニーポット攻撃を懸念しています。これらの攻撃を検知時に最も効率的に防ぐために、ワイヤレスネットワークエンジニアはCisco Prime Infrastructureでどのような設定を行う必要がありますか？
A. 自動封じ込めレベルを 0 に設定し、[SSID を使用する] 封じ込めオプションを選択します。
B. 手動封じ込めレベルを 4 に設定し、アドホック不正 AP 封じ込めオプションを選択します。
C. 自動封じ込めレベルを 0 に設定し、アドホック不正 AP 封じ込めオプションを選択します。
D. 自動封じ込めレベルを 4 に設定し、[SSID を使用する] 封じ込めオプションを選択します。
正解: **(**正解を表示します**)**
To prevent honeypot attacks most efficiently, the wireless network engineer should set the auto containment level to 4 and select the Using Our SSID containment option (D). This configuration allows the system to automatically contain rogue APs that are spoofing the organization's SSID, which is a common tactic in honeypot attacks. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **53**
エンジニアは、WLANインフラストラクチャを使用してゲストのトラフィックフローを追跡する必要があります。この追跡を実現するには、どのCisco CMX機能を設定して使用する必要がありますか？
A. 検出して位置を特定する
B. 分析
C. つながりとエンゲージメント
D. プレゼンス
正解: **A (**コメントを発表する**)**
To track guest traffic flow using the WLAN infrastructure, the 'detect and locate' feature of Cisco CMX must be configured and used. This feature allows the engineer to monitor the location and movement of guests within the WLAN coverage area.
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **54**
Cisco MSE と Cisco Prime Infrastructure ネットワーク管理ソフトウェア間の通信に使用される 2 つのプロトコルはどれですか? (2つ選んでください。)
A. HTTPS
B. Telnet
C. 石鹸
D. SSH
E. NMSP
正解: **A,E (コメントを発表する)**
The two protocols used to communicate between the Cisco Mobility Services Engine (MSE) and the Cisco Prime Infrastructure network management software are HTTPS and NMSP (Network Mobility Services Protocol). HTTPS is used for secure web-based communications, while NMSP is a Cisco proprietary protocol used specifically for efficient, real-time communication between MSE and network management software like Cisco Prime Infrastructure. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **55**
顧客は、ワイヤレス ネットワークが、ワイヤレス インフラストラクチャで使用されていないチャネルから偽の脅威を検出していることを懸念しています。導入する必要があるテクノロジーを 2 つ選択してください。(2つ選んでください。)
A. FlexConnect モード
B. モニターモード
C. サブモードなしのスニファ モード
D. WIPS サブモードを使用したローカル モード
E. 不正検出モード
正解: **B,D (コメントを発表する)**
To address concerns about detecting spurious threats from channels not used by the wireless infrastructure, deploying APs in monitor mode (B) and local mode with WIPS submode (D) would be beneficial. Monitor mode allows APs to listen to the wireless spectrum and identify potential threats, while WIPS (Wireless Intrusion Prevention System) submode enhances the ability to detect and mitigate wireless threats. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-
430 Official Cert Guide

質問: **56**
APが802.1xを使用して有線インフラストラクチャに認証するには、WLCのグローバル設定ページで何を設定する必要がありますか?
A. ローカル アクセス ポイントの資格情報

B. RADIUS共有秘密
C. TACACSサーバーのIPアドレス
D. サプリカントの認証情報
正解: **B (**コメントを発表する**)**
On the Global Configuration page of a Wireless LAN Controller (WLC), for an Access Point (AP) to use IEEE 802.1X for authenticating to the wired infrastructure, it is necessary to configure a RADIUS shared secret. This secret will be used by the AP as part of its credentials when communicating with a RADIUS server during the authentication process. References: (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

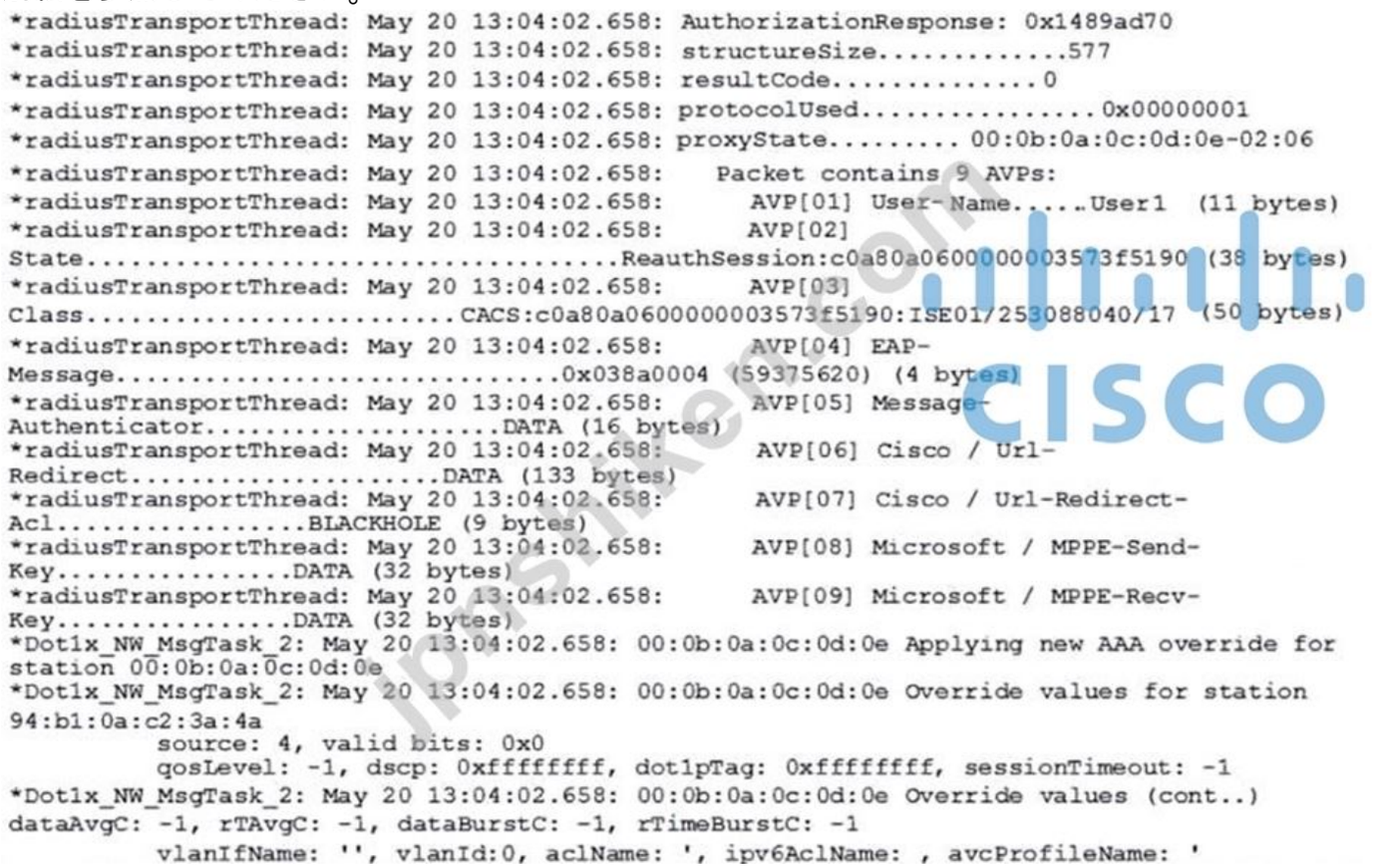
質問: **57**
エンジニアは、3 人の幹部用に Cisco OEAP を設定する必要があります。管理インターフェイスで NAT アドレスが設定されるとすぐに、内部 IP 管理アドレスに関連付けようとしている AP に対して WLC が応答していないことがわかります。これを調整するには、どのコマンドを使用する必要がありますか?
A. config flexconnect office-extend nat-ip-only 無効
B. config network ap-discovery nap-ip-only enable
C. config flexconnect office-extend nat-ip-only enable
D. config network ap-discovery nat-ip-only disable
正解: **(**正解を表示します**)**
When configuring Cisco OfficeExtend Access Points (OEAPs), enabling NAT IP only for office-extend is necessary if the APs are behind a NAT device and need to communicate with the Wireless LAN Controller (WLC) using the internal IP management address. The command config flexconnect office-extend nat-ip-only enable allows the APs to discover and associate with the WLC when the management interface is configured with a NAT address.

質問: **58**
エンジニアは、ソーシャルメディア認証を使用してゲストにアクセスを提供するようにMSEを設定する必要があります。ゲストがFacebookの認証情報を使用して認証できるように、エンジニアはどのサービスを設定しますか？
A. ソーシャルコネクト
B. クライアントコネクト
C. ビジターコネクト
D. ゲスト接続
正解: **(**正解を表示します**)**
To provide guests access using social media authentication, the engineer must configure the "Social Connect" service. This service allows guests to use their Facebook credentials, among other social media platforms, to authenticate and gain network access. It simplifies the guest access process by leveraging existing social media accounts for authentication. References :=

(CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **59**

別紙を参照してください。



エンジニアがクライアント接続の問題のトラブルシューティングを行っています。クライアントはRUN状態ですが、Cisco ISEによる認証後もトラフィックが通過しません。この問題を解決するには、どのような操作が必要ですか？

A. 認証後に別のクライアント VLAN を設定します。

B. トラフィックの許可を妨げる ACL を無効にします。

C. より低い WMM QoS を適用します。

D. クライアントへのレート制限を有効にします。

正解: **(**正解を表示します**)**

When a client is authenticated but cannot pass traffic in the RUN state, it indicates that an ACL may be blocking the traffic post-authentication. Disabling or modifying this ACL to allow traffic can resolve the connectivity issue, ensuring that the client's traffic flows correctly after authentication with Cisco ISE.

質問: **60**

シングルSSIDを使用する場合、ISEバージョン2.1 BYODで何を設定する必要がありますか？

A. オープン認証

B. 802.1x

C. 認証なし
D. WPA2
正解**: (**正解を表示します**)**
In Cisco ISE version 2.1 for BYOD with a Single SSID setup, 802.1x must be configured to provide the necessary layer of security and to facilitate the device registration process. 802.1x authentication allows for the use of EAP (Extensible Authentication Protocol) to authenticate users before they can access the network.
This ensures that only authorized devices can join the BYOD network, providing a secure method for device onboarding and access control. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問**: 61**
お客様は、WLC がデータ センターに配置されている分散型ワイヤレス導入モデルを使用しています。ファイル サーバーはデータ センターにあるため、企業 WLAN "Corp-401266017" からのトラフィックはコントローラーを通過する必要があり、ゲスト WLAN "Guest-19283746" トラフィックは各オフィスに設置されたローカル インターネット回線を使用する必要があります。このタスクを達成するのはどの構成ですか?
A. 企業およびゲスト WLAN のローカル スイッチングを無効にします。
B. 企業 WLAN のローカル スイッチングを無効にし、ゲスト WLAN に対して有効にします。
C. 企業およびゲスト WLAN のローカル スイッチングを有効にします。
D. 企業 WLAN のローカル スイッチングを有効にし、ゲスト WLAN のローカル スイッチングを無効にします。
正解**: (**正解を表示します**)**
In a distributed wireless deployment model, the traffic can either be switched locally or sent back to the controller. For the corporate WLAN "Corp-401266017", it is essential that the traffic goes through the controllers in the data center to access the file servers securely. Therefore, local switching should be disabled for this WLAN. Conversely, for the guest WLAN "Guest-19283746", the requirement is to use the local Internet line. Enabling local switching for this WLAN allows the traffic to bypass the controller and use the local internet, reducing latency and potentially providing a better user experience for guests. References:
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, specifically the sections discussing WLAN traffic forwarding and local switching options.

質問: 62
企業のネットワーク管理者は、Cisco Catalyst Center（旧DNA Center）を利用したキャプティブポータルリダイレクト用のゲストSSIDを作成する必要があります。ネットワークには、Cisco Catalyst 9800-80 WLC、Cisco
9130AXI AP、およびコネクタを使用したCisco Spaces（旧Cisco DNA Spaces）です。ゲストクライアントのキャプティブポータルリダイレクトをサポートするには、管理者はセキュリティACLとインターセプトACLを作成する必要があります。ACLの要件は次のとおりです。
ACL WA-v4-int34.235.248.212 は、クライアントからのトラフィックに最初に適用され、Cisco DNA Spaces ポータル IP アドレス 34.235.248.212 への HTTP(s) トラフィックはデータプレーン上に保持されます。ドロップや転送は行わず、トラフィックをデータプレーンに引き渡します。その後、仮想 IP トラフィックを除き、CPU にリダイレクトのために送信します。仮想 IP トラフィックは、すべての HTTP(s) トラフィックに対して Web サーバによって処理されます。その他の種類のトラフィックはデータプレーンに渡されます。
ACL WA-sec-34.235.248.212は、Cisco SpacesポータルIPへのHTTPおよびHTTPSトラフィックを許可する必要があります。
管理者がWeb認証パラメータマップで設定した34.235.248.212です。DNSとDHCPトラフィックは許可する必要がありますが、それ以外のトラフィックはドロップする必要があります。HTTPトラフィックはこのACLに到達する前に傍受されるため、このACLでカバーする必要はありません。
どの構成が ACL 要件を実装しますか?

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

質問: **63**
無線ネットワークには、Cisco WLCが参加している2つのRFグループがあります。APはラウンドロビン方式を使用して異なるコントローラに関連付けられています。すべてのコントローラに対して不正アクセスの抑制を展開する必要がありますが、ネットワークは友好的なAPから送信されるRRMネイバーパケットの影響を受けてはなりません。どのAP認証保護タイプを有効にする必要がありますか？
A. APセキュリティ
B. APアクセス制御
C. AP認証
D. AP無線保護ルール
正解: **(**正解を表示します**)**

質問: **64**
エンジニアが、Cisco ISEでAPのMACアドレスをローカルユーザとして利用し、Cisco ISEでAP認証を実装しました。最近まで正常に動作していましたが、再起動したAPが一時的にネットワークから切断され、コントローラに再接続できないことが判明しました。実装を完了するには、どのアクションを実行すればよいでしょうか？
A. AP の Cisco ISE に有効な EAP 証明書をインストールします。
B. 認証に失敗したため、除外リストから AP を削除します。
C. バグのため、Cisco ISE を新しいバージョンにアップグレードします。
D. パスワードが変更されていないアカウントを無効にする Cisco ISE パスワード ポリシーを無効にします。
正解: **(**正解を表示します**)**

質問: **65**
エンジニアは、優先順位を調整し、WLAN の QoS プロファイルを上書きするように WebEx を構成したいと考えています。このタスクを完了するには、どの構成が必要ですか?
A. WebEx の WLAN 予約帯域幅を変更します
B. WebEx 用の AVC プロファイルを作成する
C. WebEx の ACL を作成する
D. AVC アプリケーション WebEx-app-sharing をマークに変更します。
正解: **B (**コメントを発表する**)**
To adjust the precedence and override the QoS profile on the WLAN for WebEx, an Application Visibility and Control (AVC) profile needs to be created for WebEx. AVC profiles allow for the identification and prioritization of specific applications over the wireless network, ensuring that critical applications like WebEx receive the necessary bandwidth and QoS treatment.
References := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **66**
マルチキャストを有効にし、マルチキャスト ストリームのサブスクリプションを確認し、コンテンツをサブスクライブしたクライアントだけにストリーミングするために、WLC に適用される 2 つの設定はどれですか? (2つ選んでください)
A. IGMP スヌーピングを有効にする
B. IGMP タイムアウトを 180 秒に設定します。
C. ブロードキャスト転送を有効にする
D. 802.3x フロー制御モードを有効にします。
E. AP マルチキャストを 238.255.255.255 に設定します。
正解: **(**正解を表示します**)**
IGMP snooping is a feature that allows a network switch to listen to the Internet Group Management Protocol (IGMP) network traffic. This feature enables the switch to identify the multicast streams to which hosts are interested and to forward multicast traffic intelligently. By enabling IGMP snooping on the Wireless LAN Controller (WLC), it ensures that multicast streams are only forwarded to the access points (APs) where clients are subscribed to them. Setting the AP multicast mode to a specific multicast address, such as 238.255.255.255, allows the WLC to send multicast traffic to APs using this address, which helps in efficient distribution of the multicast stream.

質問: **67**
エンジニアは、自律型APを802.1x認証用に設定する必要があります。最高のセキュリティを実現するために、ユーザー認証には認証サーバーが使用されます。テスト中に、APがユーザー認証要求を認証サーバーに渡すことができませんでした。サーバーとAP間の通信を可能にするために、AP側で設定する必要がある2つの項目はどれですか？ 2つ選択してください。）
A. ユーザー名とパスワード

B. PAC暗号化キー
C. RADIUS IPアドレス
D. 共有秘密
E. グループ名
正解**: (**正解を表示します**)**
When configuring an autonomous Access Point (AP) for 802.1x authentication using an external authentication server like RADIUS, it's essential that AP knows where to send authentication requests and has a secure method of communicating with it. The RADIUS server's IP address must be configured on AP so it knows where to forward user credentials for verification. Additionally, a shared secret must be set up between AP and RADIUS server as part of their secure communication protocol; without this shared secret, they cannot trust each other's communications. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問**: 68**
別紙を参照してください。ネットワーク管理者は、Cisco DNA Catalyst CenterのWebhook機能を使用して、AP - 使用状況とクライアントの内訳レポートに関連する複数のイベントの通知を受信する必要があります。これらの通知を処理する外部サービスは、コールバックURL
https://example にあります
com/webhook にあり、要件は次のとおりです。
•An API key is passed in the X-API-Key header with the value xyz789.
•The payload must be in JSON format, specified in the Content-Type header.
•The callback URL must include a query parameter event_type to indicate the type of notification.
•A custom header X-Source with the value CiscoDNAC to identify the notification source.
Webhookを設定するPythonスクリプトを完成させるには、コード内のボックスにどのコードスニペットを配置する必要がありますか？

A. オプションC
B. オプションD
C. オプションB
D. オプションA
正解: **D** (コメントを発表する)

質問: **69**
ネットワーク エンジニアは、ネットワークでマルチキャストを構成する必要があります。実装では、複数のマルチキャスト グループと PIM ルーターを使用します。各マルチキャスト グループに最適な RP の自動検出を提供するアドレスはどれですか?
A. 224.0.0.13
B. 224.0.0.14
C. 224.0.1.39
D. 224.0.1.40
正解: (正解を表示します)
In a multicast implementation using multiple multicast groups and PIM routers, the address that provides automatic discovery of the best RP (Rendezvous Point) for each multicast group is 224.0.1.39. This address is used by the Auto-RP feature, which allows for dynamic RP discovery and simplifies the management of multicast groups across the network. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **70**
Cisco Hyperlocationの検出しきい値は現在-50dBmに設定されています。無線ユーザの位置を確認したところ、不一致が見つかりました。Cisco Hyperlocationの精度を向上させるため、エンジニアは検出しきい値を-100dBmに変更しようとしました。しかし、Cisco Catalyst 9800シリーズ ワイヤレスコントローラでは、この変更を適用できません。この問題を解決するには、どのような対策を講じるべきでしょうか？
A. Cisco Hyperlocation を無効にし、Cisco Hyperlocation 検出しきい値を変更してから有効にします。
B. 新しい Cisco Hyperlocation 検出範囲を使用して Cisco CMX に新しいプロファイルを作成し、WLAN に適用します。
C. AP を監視モードに設定し、無線をシャットダウンしてから、Cisco Hyperlocation 検出しきい値を変更します。
D. コントローラ上のすべての無線をシャットダウンし、Cisco Hyperlocation の検出範囲を変更して、無線を再度有効にします。
正解: **(**正解を表示します**)**
To resolve the issue of changing the Cisco Hyperlocation detection threshold, the engineer should shut down all radios on the controller, change the Cisco Hyperlocation detection range, and then enable the radios again.
This process ensures that the new threshold settings are applied correctly across the network.

質問: **71**
ワイヤレス エンジニアは、クライアント トラッキングを実装する必要があります。無線デバイスの位置を特定するために、到来角が使用する方法はどれですか?
A. 受信信号強度
B. 三角測量
C. 到達距離
D. 入射角
正解: **(**正解を表示します**)**
The angle of arrival (AoA) method for client tracking determines the location of a wireless device using triangulation. This technique involves measuring the angle at which the signal arrives at different receivers (access points) and using this information to pinpoint the device's location within the network. References:
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich2.html

質問: **72**
エンジニアは、Cisco Spaces（旧Cisco DNA Spaces）で不正AP追跡を設定する必要があります。エンジニアは、最新のサンプルに関係なく、RSSI測定値を古いものと見なし、位置計算に使用し

ないようにするまでの時間を設定する必要があります。この要件を満たすには、何を設定する必要がありますか？

A. 相対破棄RSSI時間

B. 位置破棄RSSI時間

C. 不正破棄RSSI時間

D. 絶対破棄RSSI時間

正解: **(**正解を表示します**)**

質問: **73**

別紙を参照してください。

エンジニアはCisco PI 3.0を使用してフロアマップ上に不正APの位置を示す必要がありますが、左側のナビゲーションメニューの 『マップ』に不正APのオプションが表示されません。この表示が表示されない理由は何ですか？

A. 保証ライセンスがインストールされていません。

B. コントローラーの動作ステータスのバックグラウンド タスクが無効になっています。

C. AP オプションの検出された干渉源の表示機能が無効になっています。

D. Cisco MSE は Cisco PI に追加されていません。

正解: **D (**コメントを発表する**)**

The absence of rogue AP options in the navigation menu under Maps in Cisco Prime Infrastructure (PI) version 3.0 indicates that there is an issue with integrating location services, which are provided by Mobility Services Engine (MSE). Without adding MSE to PI, location-based services such as tracking rogue access points cannot be utilized or displayed within PI's interface. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **74**
ネットワーク エンジニアは、ワイヤレス クライアントが接続された 8865 IP 電話を導入しています。適切な QoS を適用するには、IP 音声トラフィックをクライアント データ トラフィックから区別する必要があります。
どのスイッチ構成機能を有効にする必要がありますか?
A. WME
B. QBSS
C. 音声 VLAN
D. QoS ルーティング
正解: **(**正解を表示します**)**
The Voice VLAN feature on switches allows the network to distinguish between voice traffic and data traffic from wireless clients connected to IP phones. This is crucial for applying the appropriate QoS to ensure that voice traffic is prioritized over client data traffic. References: CCNP Enterprise Wireless Design ENWLSD
300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **75**
クライアント トラフィックが AP スイッチ ポートでネットワークに入るように Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するコマンド セットはどれですか?
.
.
.
.

```
config terminal
wireless profile policy [policy name]
local switching
end
```

```
config terminal
wireless flexconnect policy [policy name]
local switching
end
```

```
config terminal
wireless flexconnect policy [policy name]
no central switching
end
```

```
config terminal
wireless profile policy [policy name]
no central switching
end
```

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

正解: **C** (コメントを発表する)

The correct command set for configuring a Cisco Catalyst 9800 Series Wireless Controller so that the client traffic enters the network at the AP switch port is Option C:

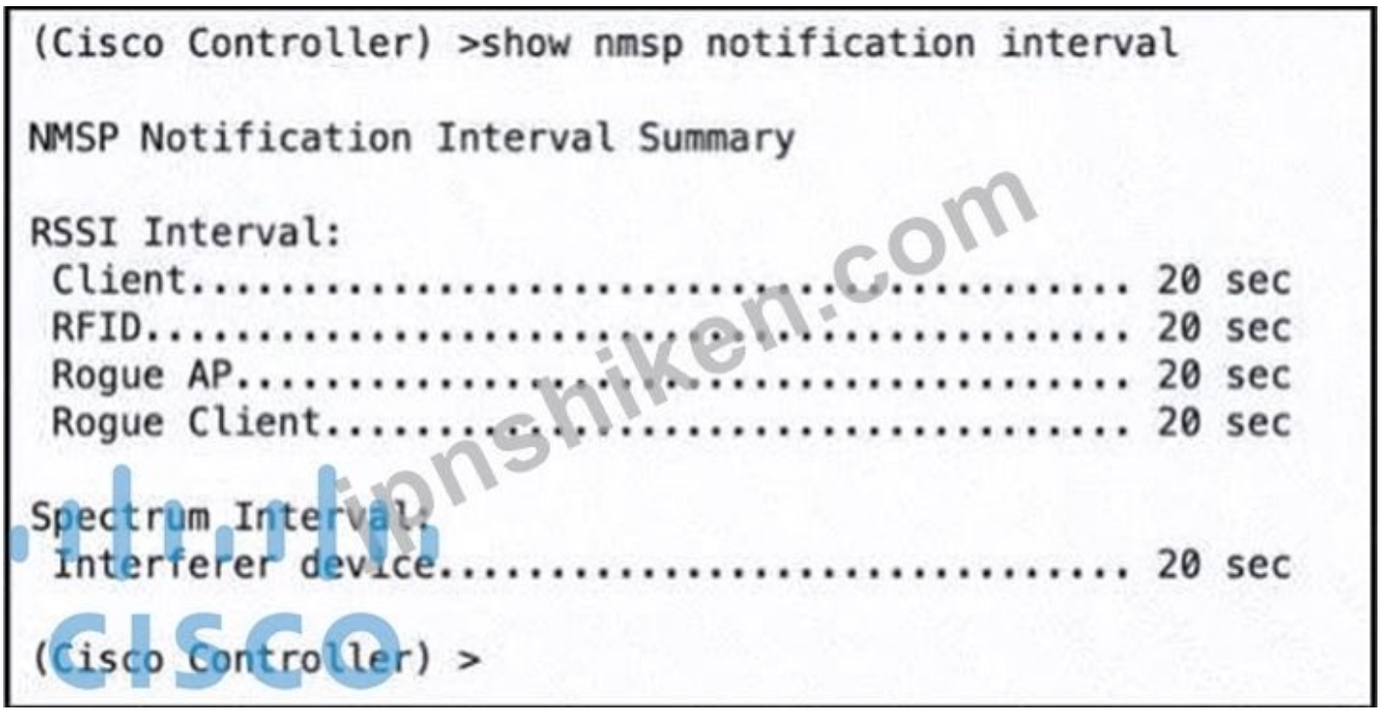
config terminal
wireless profile policy [policy name]
no central switching
end

This configuration disables central switching, which means that client traffic will be locally switched at the access point level rather than being sent through the controller. This is useful in scenarios where local switching is preferred due to reasons such as reducing latency or conserving bandwidth on WAN links.

References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **76**
ワイヤレス管理者はこの情報を受け取り、バージョン 10.6 を使用して分析を収集することにより、ハイ アベイラビリティでの CMX 展開を完了します。
プライマリ サーバーの IP アドレス
セカンダリ サーバーの IP アドレス
自動として設定されるフェールオーバー モード
セカンダリ サーバーのルート パスワード
NOC 通知の電子メール ID
これらのパラメータを使用すると、高可用性を有効にできません。問題を解決するアクションはどれですか?
A. セカンダリ サーバーの cmxadmin パスワードを挿入します。
B. コントローラが CMX サーバーに到達するには、IP プロトコル 4242 を使用します。
C. プライマリ サーバーとセカンダリ サーバーを異なるサブネットに配置します。
D. プライマリ サーバーの仮想 IP アドレスを有効にします。
正解: **(**正解を表示します**)**
For CMX high availability deployment, enabling the virtual IP address of the primary server is critical. This virtual IP facilitates seamless failover to the secondary server without requiring DNS updates or manual intervention, ensuring uninterrupted service during primary server outages.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)
https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/managing_cisco_cmx_system_settings.html#task_35253AFE18234DDA8C6E04C297D725F5:~:text=Primary%20and%20Secondary.-,Enabling%20High%20Availability%20for%20Cisco%20CMX%
20Using%20the%20Web%20UI,-Procedure

質問: **77**
別紙を参照してください。



管理者は、コントローラからCisco CMXへの位置情報更新の速度が遅いことに気づきました。不正アクセスポイントの位置情報更新を5秒ごとに取得するには、どのコマンドを設定する必要がありますか？

A. 設定位置通知間隔 RSSI 不正 5

B. config nmsp 通知間隔 rssi 不正 5

C. config サブスクリプション通知間隔 RSSI 不正 5

D. config cmx 通知間隔 RSSI 不正 5

正解: **B (**コメントを発表する**)**

The correct command to configure the controller to update Cisco CMX every 5 seconds for rogue devices is

"config nmsp notification interval rssi rogues 5". NMSP (Network Mobility Services Protocol) is used by Cisco wireless controllers to manage and communicate with connected services such as Cisco CMX. The command structure "config nmsp notification interval" followed by the specific type of device or metric, in this case, 'rssi rogues', and the desired interval time '5' seconds, sets the frequency of NMSP notifications for RSSI updates related to rogue devices.

References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **78**

ネットワークエンジニアは、無線クライアントが接続された8865台のIP電話を導入しています。適切なQoSを適用するには、IP音声トラフィックとクライアントデータトラフィックを区別する必要があります。どのスイッチ設定機能を有効にする必要がありますか？

A. 音声VLAN

B. QBSS

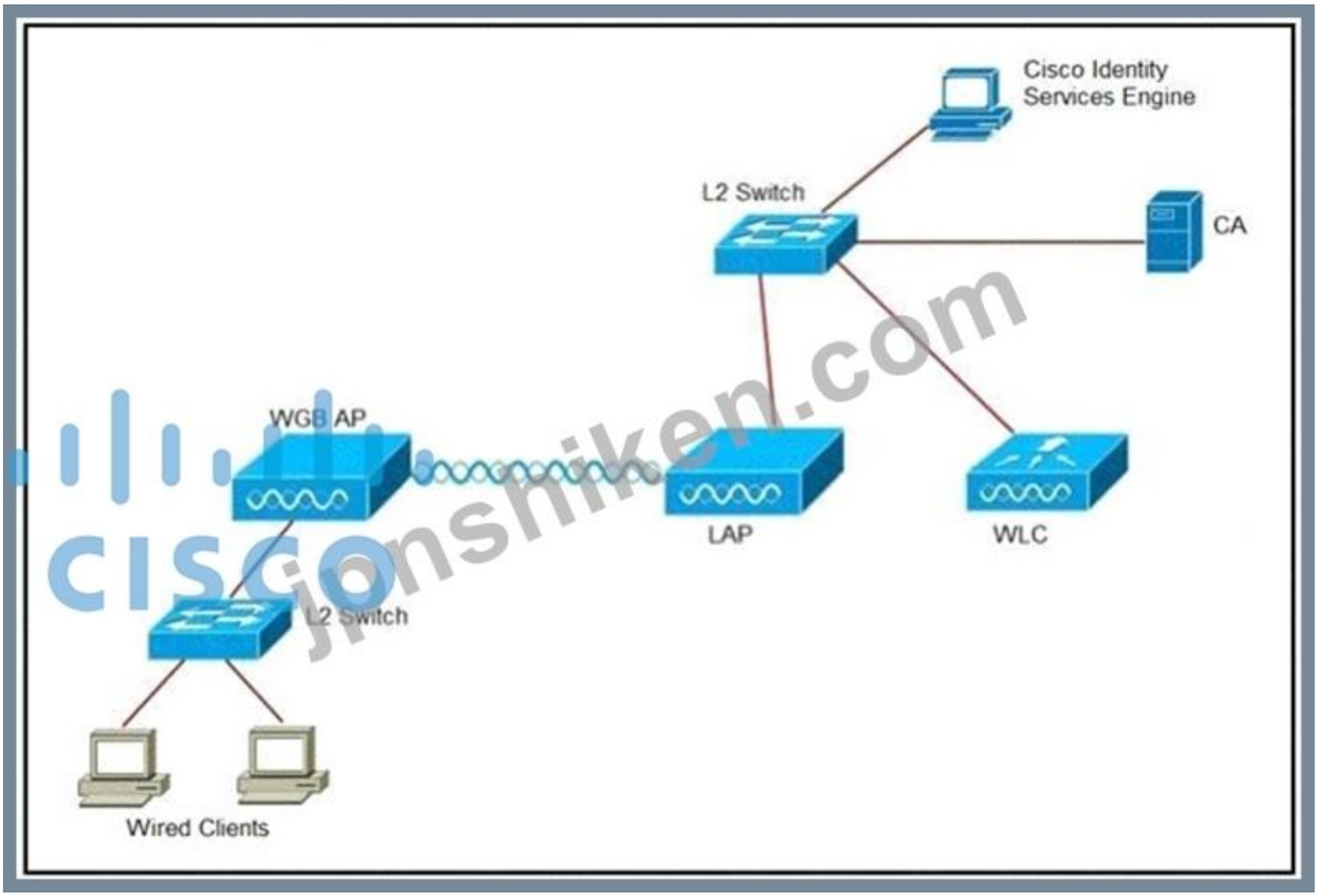
C. WME

D. QoSルーティング

正解: (正解を表示します)
The Voice VLAN feature on switches allows the network to distinguish between voice traffic and data traffic from wireless clients connected to IP phones. This is crucial for applying the appropriate QoS to ensure that voice traffic is prioritized over client data traffic. References: CCNP Enterprise Wireless Design ENWLSD
300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **79**
エンジニアは、ブランチオフィスをサポートするためにシスコのワイヤレスネットワークを導入しています。すべてのAPはFlexConnectモードであり、SSIDはトラフィックをローカルにスイッチングします。顧客は、VoWLANサービスのすべてのQoSがレイヤ2マーキングに基づくことを要求しています。APに接続するスイッチポートにはどのような設定が必要ですか？
A. MLS Trust COS
B. MLSAWID1P
C. MLS Trust DSCP
D. MLSAWID UP
正解: (正解を表示します)

質問: **80**
別紙を参照してください。



エンジニアは、フォークリフトをWGB経由で無線ネットワークに接続し、RADIUSサーバーに対してWGB証明書を認証する必要があります。この設定に必要な3つの手順はどれですか？ 3つ選択してください。）
A. WGB で証明書、WLAN、および無線インターフェイスを設定します。
B. WLC で証明書を設定します。
C. ISE を使用して認証するように WLAN を設定します。
D. ISE からのルート証明書を使用してアクセス ポイントを設定します。
E. ISE で WGB をネットワーク デバイスとして設定します。
F. 証明書を検証するデバイスが接続できるように ISE でポリシーを設定します。
正解**: (**正解を表示します**)**
To connect a Workgroup Bridge (WGB) to a wireless network and authenticate its certificate against a RADIUS server like ISE, the following steps are necessary:
* A. Configure the certificate, WLAN, and radio interface on WGB: This is essential because the WGB needs to have the correct certificate to present to the RADIUS server for authentication. Additionally, the WLAN and radio interface must be configured to ensure proper communication with the wireless network.
* E. Configure WGB as a network device in ISE: By configuring the WGB as a network device within ISE, it becomes a recognized entity that can be authenticated and authorized accordingly.
* F. Configure a policy on ISE to allow devices to connect that validate the certificate: This step ensures that only devices with a validated certificate, such as the WGB, can connect to the network, enhancing security.

質問**: 81**
Cisco ISO XEを実行するCisco Catalyst 3850シリーズスイッチでコマンドを入力します。コマンドは何を実行しますか？
A. RADIUS サーバーによって検証されるユーザー ID またはデバイス ID を定義します。
B. 承認されたセッションの長さとクライアントの帯域幅使用量に関する情報を取得します。
C. どのセッションがまだアクティブであるかを追跡するために使用される RADIUS サーバーを定義します。
D. ユーザーまたはデバイスのアクセス レベルを定義します。
正解**: (**正解を表示します**)**
The command in question is typically used to configure the switch to interact with a RADIUS server for session tracking purposes. The RADIUS server keeps track of authenticated sessions, ensuring that they are still active and monitoring for any changes in status. This is crucial for maintaining network security and ensuring that only authorized users have access to network resources.

質問**: 82**
セキュリティ学習は、Cisco WLC を含むすべてのネットワーク デバイスへのアクセスに関係しています。管理サブネットのみに管理へのアクセスを許可するには、CPU ACL を作成して適用しま

す。ただし、ゲスト ユーザーは Web ポータルにアクセスできません。管理者のみがアクセスできるようにするには、何を構成する必要がありますか?

A. ゲスト ポータルは、Cisco WLC の CPU ACL で設定する必要があります。

B. 事前認証 ACL で Cisco ISE へのアクセスを許可する必要があります。

C. ゲスト ネットワークからの管理トラフィックは、ACL ルールで構成する必要があります。

D. 仮想インターフェイスへのトラフィックを許可する必要があります。

正解: **(**正解を表示します**)**

To ensure that only admins have access to network device management while allowing guest users to reach the web portal, access to Cisco ISE must be permitted on the pre-authentication ACL. This configuration allows guests to interact with the portal without granting them broader network access.

質問: **83**

```
policy-map BW_Limit
 class BW_Limit1_AVC_UI_CLASS
  police cir 8000
   conform-action drop
   exceed-action drop
 class BW_Limit1_ADV_UI_CLASS
  set dscp af41
 class BW_Limit2_ADV_UI_CLASS
  police cir 50000
   conform-action transmit
   exceed-action drop
 class class-default
  police cir 100000
   conform-action transmit
   exceed-action drop
```

図を参照してください。大学のネットワーク管理者は、図書館において無線ゲストユーザーが大量のアップリンクインターネット帯域幅を消費し、職員用SSIDでスループットの問題を引き起こしていることに気づきました。この帯域幅消費を抑制するため、管理者はゲスト向けに以下のQoSポリシーを設定する予定です。

- remarks DSCP 46 to 34
- drops Netflix and YouTube traffic
- rate limits a host specified in an ACL to 50 Kbps
- rate limits all other traffic to 100 Kbps

管理者はどのクラスマップ設定を実装する必要がありますか？

```
class-map match-all BW_Limit1_AVC_UI_CLASS
  match protocol youtube
  match protocol netflix
class-map match-any BW_Limit1_ADV_UI_CLASS
  match dscp af41
class-map match-all BW_Limit1_ADV_UI_CLASS
  match access-group name specifichostACL

class-map match-all BW_Limit1_AVC_UI_CLASS
  match protocol youtube
  match protocol netflix
class-map match-any BW_Limit1_ADV_UI_CLASS
  match dscp af41
class-map match-all BW_Limit2_ADV_UI_CLASS
  match access-group name specifichostACL

class-map match-all BW_Limit1_AVC_UI_CLASS
  match protocol youtube
  match protocol netflix
class-map match-any BW_Limit1_ADV_UI_CLASS
  match dscp af34
class-map match-all BW_Limit2_ADV_UI_CLASS
  match access-group name specifichostACL

class-map match-all BW_Limit1_AVC_UI_CLASS
  match protocol youtube
  match protocol netflix
class-map match-any BW_Limit1_ADV_UI_CLASS
  match dscp ef
class-map match-all BW_Limit2_ADV_UI_CLASS
  match access-group name specifichostACL
```

A. オプションD

B. オプションC

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: **84**
ワイヤレス管理者は、外部サーバを使用せずに、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続されているさまざまなクライアント タイプを評価する必要があります。この評価を達成するには、どの構成をコントローラーに追加する必要がありますか?
A. ネイティブ プロファイル
B. MAC 分類
C. ローカル プロファイル
D. デバイス分類
正解: **(**正解を表示します**)**
To assess different client types connected to a Cisco Catalyst 9800 Series Wireless Controller without using external servers, the device classification feature (D) can be used. This feature allows the controller to classify devices based on their MAC addresses and other characteristics. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **85**
別紙を参照してください。

あるお客様は、世界各地の異なるWLANにCisco FlexConnectを導入しており、別の場所に新しいブランチオフィスを開設する予定です。エンジニアの任務は、すべての無線設定を実行し、新しいAP用のスイッチポートの設定方法を提案することです。スイッチングチームは、スイッチポートにどのような設定を行う必要がありますか？

A. トランクモード

B. アクセスモード

C. 単一VLAN

D. 複数のVLAN

正解: **(**正解を表示します**)**

For new Access Points (APs) in a Cisco FlexConnect deployment, switch ports should be configured in trunk mode. This allows the APs to handle traffic for multiple WLANs or SSIDs, each associated with different VLANs. Trunk mode enables the AP to tag traffic with the correct VLAN

IDs as per its configuration. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **86**
ある大学のキャンパスでは、Cisco Catalyst CenterとCisco Spacesを使用し、大学のモバイルアプリを活用して学生や来客に屋内案内を提供しています。IT管理者は、高層ビル、特に階段やエレベーターの近くでは、位置追跡が不正確であることに気づきました。調査の結果、異なる階にあるAPからの信号が重複しているため、三角測量誤差が発生していることがわかりました。ITチームは既に、APが互いの真上または真下に配置されていないことを確認しました。しかし、問題は解決せず、垂直構造物の近くでは位置精度が依然として信頼できません。ITチームはこの問題を解決するためにどのような措置を講じる必要がありますか？
A. トラフィック量の多いエリアでの信号の重複を補うために、AP あたりの最大許容クライアント接続数を増やします。
B. APの送信電力と方向を調整して、フロア間の垂直信号伝播を最小限に抑え、水平三角測量のカバレッジを最適化します。
C. カバレッジ ホールの検出と軽減を有効にして、階段やエレベーターの近くで信号強度が不安定な領域に対処します。
D. 建物内のすべての AP が同じチャネルを使用するように設定し、フロア間で一貫した信号カバレッジを提供します。
正解: **(**正解を表示します**)**

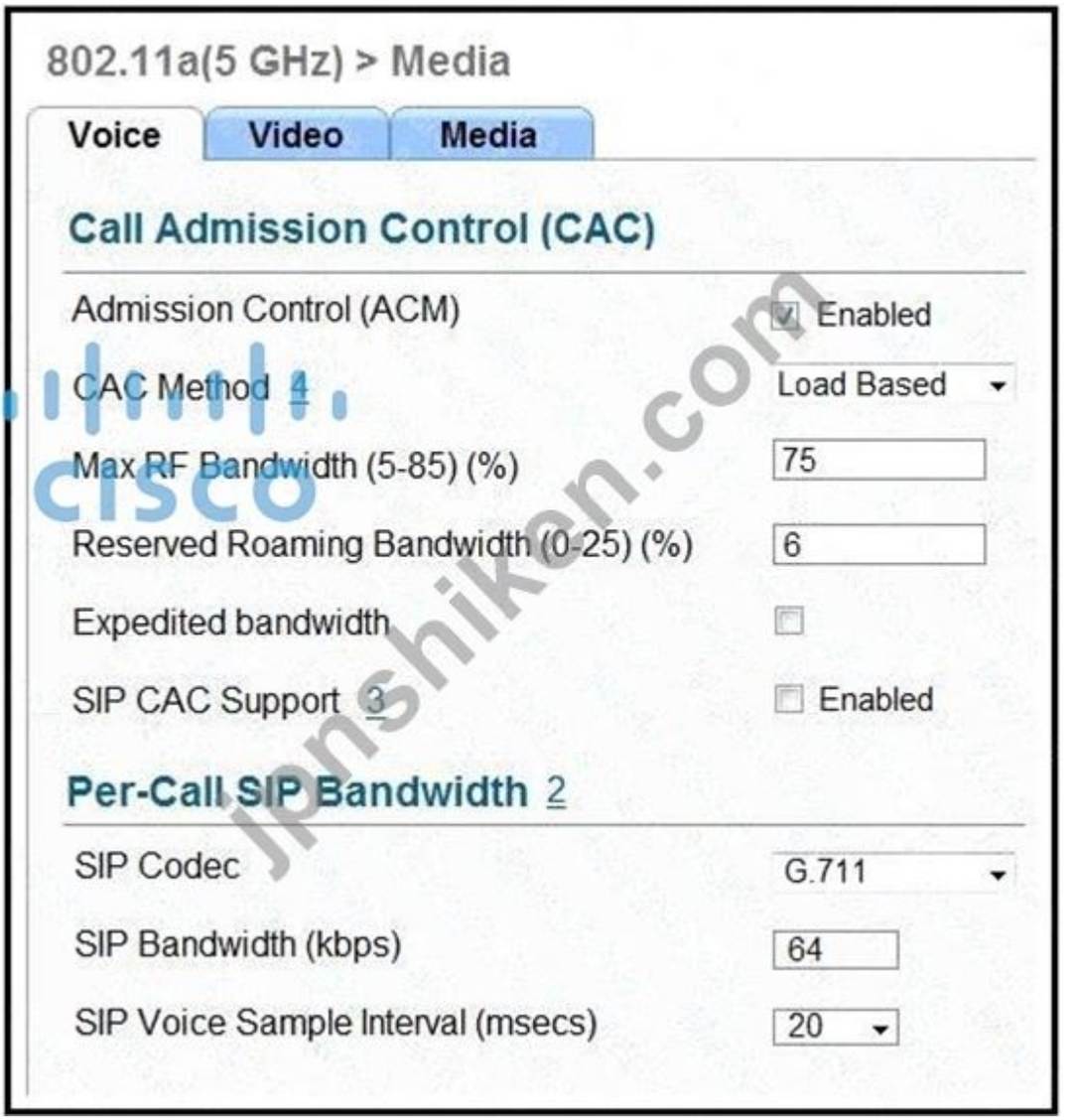
質問: **87**
ゲストネットワークのソーシャルログインを設定しています。Cisco CMX Visitor Connectで設定可能なソーシャルコネクタのオプションは3つありますか？ （3つ選択してください）
A. LinkedIn
B. Pinterest
C. Medium
D. Google+
E. Facebook
F. Myspace
正解: **(**正解を表示します**)**
Cisco CMX Visitor Connect supports various social connectors for guest network login. The configurable social connectors include LinkedIn, Google+, and Facebook, but not Pinterest, Medium, or Myspace. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI
300-430 Official Cert Guide

質問: **88**
Cisco WLCを設定する際に、BranchA-FCGという名前のFlexConnectグループにVLAN ID 30のVLANを追加するCLIコマンドはどれですか？

A. config flexconnect BranchA-FCG VLAN 30 を追加
B. config flexconnect BranchA-FCG VLAN に 30 を追加します
C. config flexconnect グループ BranchA-FCG VLAN 30 を追加
D. config flexconnect グループ BranchA-FCG VLAN に 30 を追加します
正解**: (**正解を表示します**)**
The correct command to add a VLAN with a specific ID to a FlexConnect group in a Cisco Wireless LAN Controller (WLC) is 'config flexconnect group BranchA-FCG vlan 30 add'. This command specifies the FlexConnect group name 'BranchA-FCG' and the VLAN ID '30', followed by the action 'add', which is consistent with Cisco's CLI syntax for WLC configuration.
References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問**: 89**
ゲスト/BYOD デバイスの自己登録を実装する場合、従業員が同時に 4 つのデバイスをネットワークに接続しようとするとどうなりますか?
A. 最後のデバイスが削除され、新しく追加されたデバイスがアクティブなデバイスとして更新されます。
B. 登録は許可されていますが、常に 1 つのデバイスしか接続されていません。
C. すべてのデバイスがネットワーク上で同時に許可されます。
D. パージ時間は、デバイスがポータルに登録されている期間を決定します。
正解**: B (**コメントを発表する**)**
In a self-registration setup for guest/BYOD devices, when an employee tries to connect multiple devices simultaneously, the system allows the registration of all devices. However, it restricts the active connection to only one device at a time. This ensures that network resources are not overburdened by a single user connecting multiple devices. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問**: 90**
別紙を参照してください。



この WLAN 構成を最大限に活用するには、VoWLAN 電話機でどの 2 つの項目をサポートする必要がありますか? (2 つ選択してください。)

A. TSPEC

B. SIFS

C. 802.11e

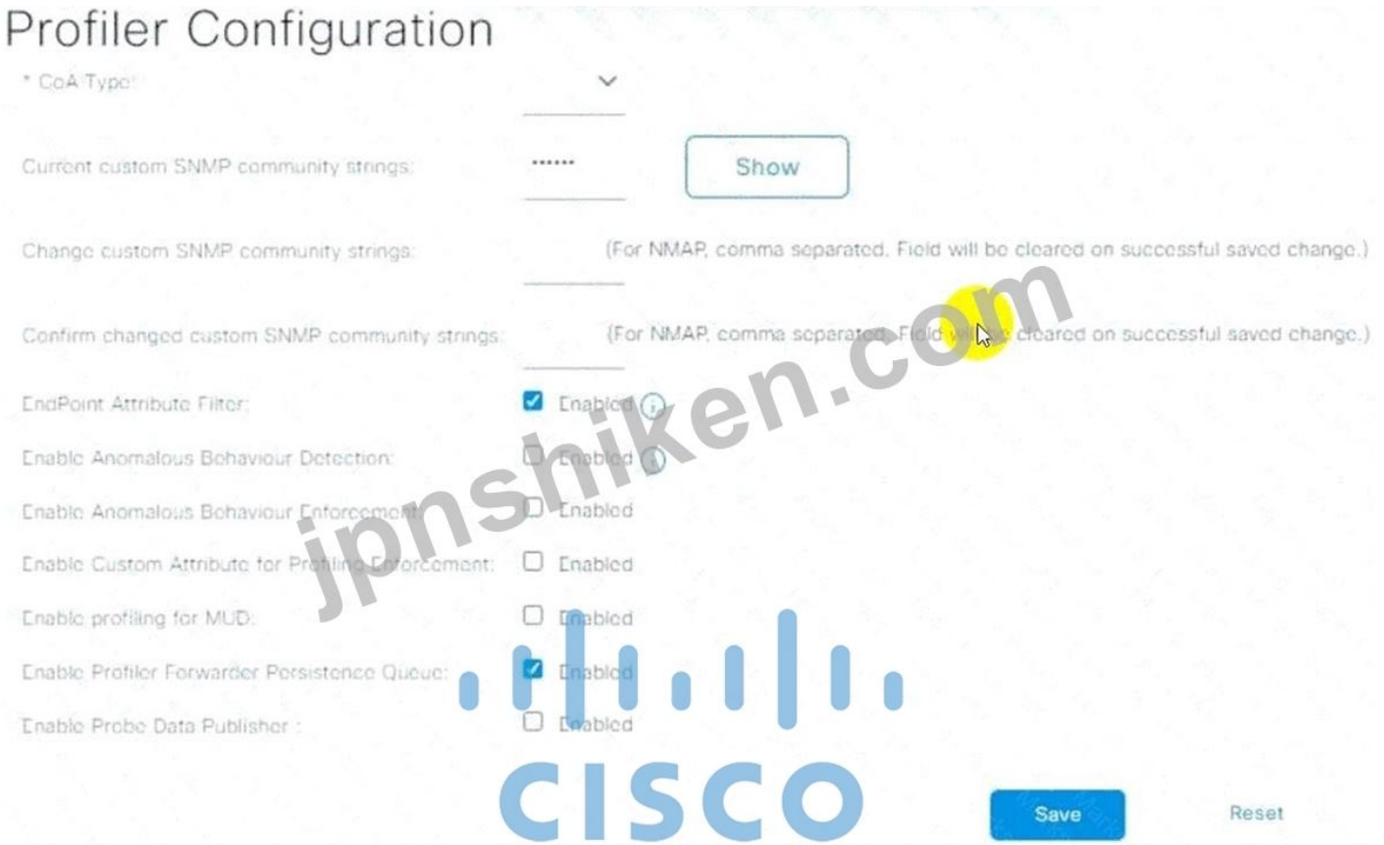
D. WMM

E. APSD

正解: **(**正解を表示します**)**

To take full advantage of the WLAN configuration, VoWLAN phones must support 802.11e, which is a standard for wireless QoS, and Wi-Fi Multimedia (WMM), which is a subset of 802.11e that provides prioritized media delivery. These standards ensure that voice traffic is prioritized appropriately in the wireless network. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI
300-430 Official Cert Guide)

質問: **91**



図を参照してください。ネットワーク管理者は、Cisco Catalyst 9800 WLCを、Cisco ISEを介してローカルクライアントプロファイリングからRADIUSプロファイリングに移行する必要があります。エンジニアは、クライアントタイプがWindowsであることを検出してRADIUS CoAを有効にし、プロファイル検出に基づいてアクセスポリシーを即座に更新する必要があります。エンジニアはCisco ISEでどのCoAタイプの設定を適用する必要がありますか？

A. CoAなし
B. 再認証
C. バウンス
D. 事前認証
E. ポート

正解: **(**正解を表示します**)**

質問: **92**

ある医療機関では、Cisco Spacesと統合されたCisco Catalyst Centerを使用して、医療機器の動きをリアルタイムで追跡しています。ITチームは、医療用トロリーが頻繁に移動するエリアで位置精

度が著しく低下していることに気付きました。現場調査の結果、トロリーが設置された環境では、クライアントデバイスを検出できるAPの数が不足していることが判明しました。APは、天井設置の標準ガイドラインに従って設置されています。ITチームは既にWi-Fi以外のデバイスからの干渉を排除し、適切なRFプロファイルを設定しています。この問題を解決するために、ITチームはどのような対策を講じるべきでしょうか？
A. 障害物を減らし、正確な三角測量のために信号経路を改善するために、影響を受けるエリアのAPを下げます。
B. スペクトル分析を有効にして、Wi-Fi 以外のデバイスの干渉を検出し、AP チャネルを自動的に調整します。
C. 信号干渉を補正するために、病院内のすべての AP の送信電力を上げます。
D. 信号の三角測量が不要になるように、Cisco Spaces に位置ベースの FastLocate 機能を実装します。
正解: **A (**コメントを発表する**)**

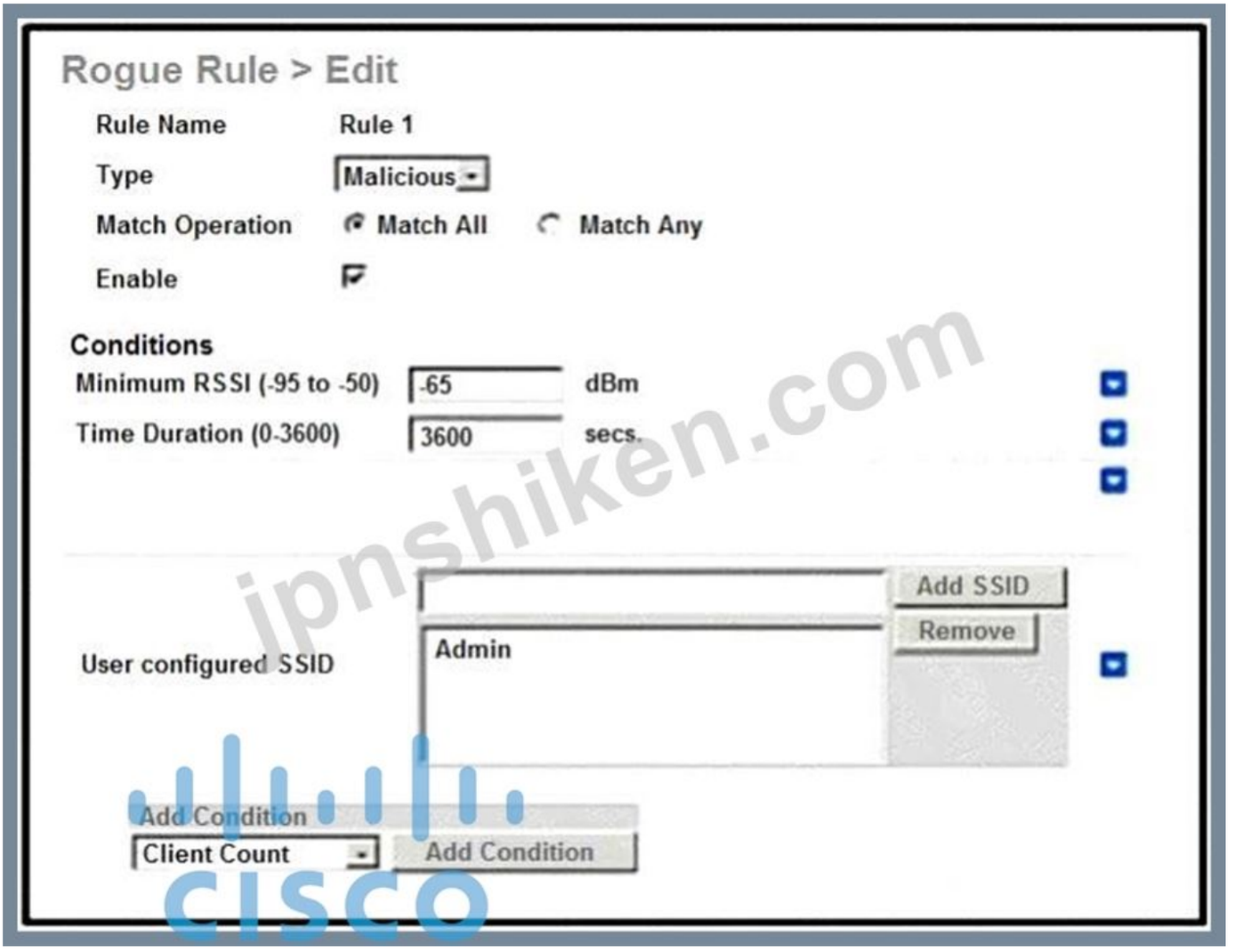
質問: **93**
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのデフォルトの IEEE 802.1x AP 認証設定は何ですか?
A. 802.1x ポート認証を使用する EAP-PEAP
B. 802.1x ポート認証を使用した EAP-TLS
C. CAPWAP DTLS + ポート認証による EAP-FAST
D. CAPWAP DTLS を使用した EAP-FAST
正解: **(**正解を表示します**)**
The default IEEE 802.1x AP authentication configuration on a Cisco Catalyst 9800 Series Wireless Controller is EAP-FAST with CAPWAP DTLS (Option D). This method uses EAP-FAST for authentication within a secure tunnel established by Datagram Transport Layer Security (DTLS) over CAPWAP, which provides both security for authentication credentials and encryption for wireless management frames. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **94**
ログを確認した後、エンジニアはRRMがIEEE 802.11以外の干渉源のチャネルを変更し続けていることに気づきました。エリアを調査した後、RRMはチャネルを変更しないことが決定されました。802.11以外の干渉を無視するには、どの機能を有効にする必要がありますか？
A. Cisco AP の負荷を回避する
B. 802.11以外のノイズを避ける
C. 持続的な非WiFi干渉を回避する
D. 外部APの干渉を回避する
正解: **(**正解を表示します**)**
The feature that must be enabled to ignore non-802.11 interference is "Avoid Persistent Non-WiFi Interference." This setting allows the Radio Resource Management (RRM) to not react to

non-802.11 noise and interference, which can be crucial in environments where such interference is common but does not significantly impact wireless performance. By enabling this feature, RRM will not change the channel in response to non-IEEE 802.11 interferers, thus maintaining a stable channel plan. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **95**
マルチキャスト トラフィックを必要とする AP だけではなく、すべての AP がマルチキャスト トラフィックを受信しています。この問題の原因は何ですか?
A. マルチキャスト グループにはすべての AP が含まれます
B. 間違ったマルチキャスト アドレスが使用されました
C. マルチキャスト グループに間違った VLAN が割り当てられています
D. マルチキャスト IGMP スヌーピングが有効になっていません
正解: **(**正解を表示します**)**
If all APs are receiving multicast traffic instead of only those that need it, it indicates that Multicast Internet Group Management Protocol (IGMP) snooping is not enabled. IGMP snooping is a feature that allows a network switch to listen to IGMP network traffic and ensure that multicast packets are only sent to the ports associated with interested receivers, thus preventing unnecessary traffic on the network. References := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **96**
別紙を参照してください。



エンジニアがCisco WLC上の不正アクセスポイントを管理しようとしています。設定に基づいて、コントローラによって悪意のあるアクセスポイントとしてマークされるのはどのAPですか？

A. SSID が admin の不正 AP が 4000 秒間検出され、-70 dBm で受信されました

B. SSID admin を持つ不正 AP が 3000 秒間検出され、-60dBm で受信されました

C. SSID admin を持つ不正 AP が 4000 秒間検出され、-60dBm で受信されました

D. SSID admin を持つ不正 AP が 3000 秒間検出され、-70 dBm で受信されました

正解**: (**正解を表示します**)**

The configuration for the Rogue Rule named "Rule 1" is set to classify an access point (AP) as malicious if it meets certain conditions. The rule specifies that the AP must have a Minimum RSSI (Received Signal Strength Indicator) of less than or equal to -65 dBm and must have been seen for a Time Duration greater than or equal to 3600 seconds. Among the options provided, both A and C have been seen for more than 3600 seconds, which satisfies the Time Duration condition. However, for the RSSI condition, only option C with an RSSI of -60 dBm meets the criteria of being less than or equal to -65 dBm. Therefore, option C is the correct answer, as it fulfills both conditions set by the Rogue Rule.

質問**: 97**

大規模で高可用性のワイヤレス ネットワークを構成する場合、コントローラの負荷を軽減し、同じモビリティ メッセージを維持するモビリティ グループへの変更はどれですか?

A. モビリティ グループのマルチキャスト メッセージングを構成します。

B. 不要なコントローラーをモビリティ グループから削除します。

C. コントローラーをモビリティ グループとは別の RF グループに構成します。

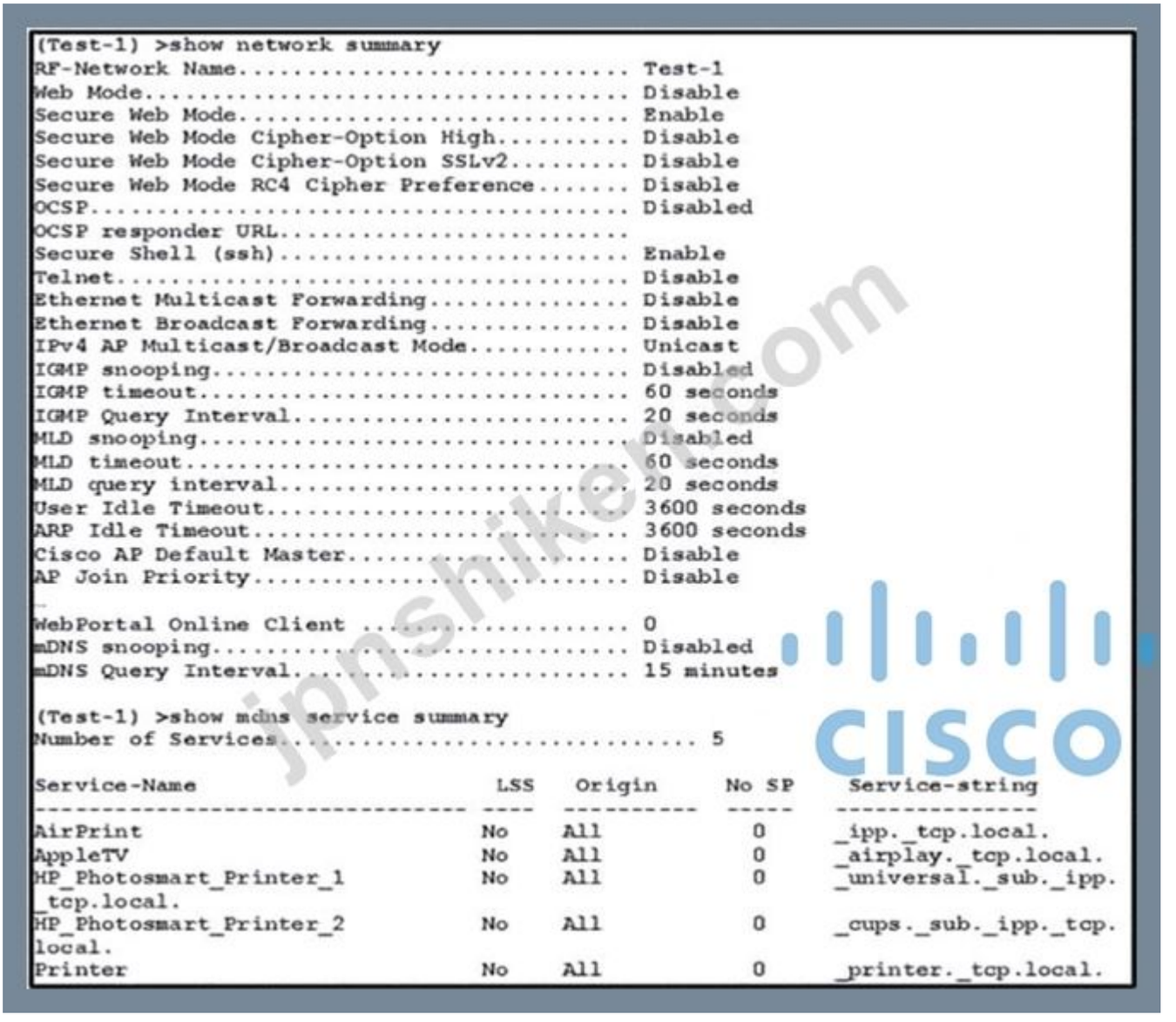
D. コントローラーをコントローラーごとに異なるモビリティ グループに分けます。

正解: **(**正解を表示します**)**

Removing unnecessary controllers from the mobility group (B) would create less load on the controllers while maintaining the same mobility messages. This is because each controller in a mobility group shares its client database with other controllers, which can lead to increased overhead. By minimizing the number of controllers in the group, the load is reduced. References: CCNP Enterprise Wireless Design ENWLSD 300-
425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **98**

別紙を参照してください。



```
(Test-1) >show network summary
RF-Network Name.............................. Test-1
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High........... Disable
Secure Web Mode Cipher-Option SSLv2.......... Disable
Secure Web Mode RC4 Cipher Preference........ Disable
OCSP......................................... Disabled
OCSP responder URL...........................
Secure Shell (ssh)........................... Enable
Telnet....................................... Disable
Ethernet Multicast Forwarding................ Disable
Ethernet Broadcast Forwarding................ Disable
IPv4 AP Multicast/Broadcast Mode............. Unicast
IGMP snooping................................ Disabled
IGMP timeout................................. 60 seconds
IGMP Query Interval.......................... 20 seconds
MLD snooping................................. Disabled
MLD timeout.................................. 60 seconds
MLD query interval........................... 20 seconds
User Idle Timeout............................ 3600 seconds
ARP Idle Timeout............................. 3600 seconds
Cisco AP Default Master...................... Disable
AP Join Priority............................. Disable

WebPortal Online Client ..................... 0
mDNS snooping................................ Disabled
mDNS Query Interval.......................... 15 minutes

(Test-1) >show mdns service summary
Number of Services........................... 5

Service-Name                    LSS   Origin     No SP   Service-string
------------------------------- ----  ---------  -----   --------------
AirPrint                        No    All          0     _ipp._tcp.local.
AppleTV                         No    All          0     _airplay._tcp.local.
HP_Photosmart_Printer_1         No    All          0     _universal._sub._ipp.
_tcp.local.
HP_Photosmart_Printer_2         No    All          0     _cups._sub._ipp._tcp.
local.
Printer                         No    All          0     _printer._tcp.local.
```

エンジニアは、Bonjour サービスを使用して WLAN 上で印刷できるようにする BYOD ポリシーを構成しました。
しかし、エンジニアは印刷がうまくいかないようです。WLCファームウェアは8.xです。コントローラーに何を実装する必要がありますか？
A. mDNS と IGMP スヌーピングを有効にします。
B. 場所固有のサービスを有効にします。
C. セキュア Web モードの暗号オプション SSLv2 を設定します。
D. IGMPクエリ間隔の値を増やす
正解: **(**正解を表示します**)**
For printing services using Bonjour in a WLAN environment where mDNS services are utilized, especially with WLC firmware version 8.x, it's essential that:
* Enable mDNS and IGMP snooping (Option A): Multicast DNS or mDNS needs to be enabled for Bonjour services to function correctly as they rely on this protocol for service discovery within local networks. IGMP snooping improves network efficiency by ensuring multicast traffic is only forwarded to nodes that have explicitly requested it.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **99**
エンジニアはCisco Prime Infrastructureレポートを使用して、WLANのセキュリティ状態を監視しています
Adaptive wIPS Top 10 AP レポートを実行すると、どのような出力が生成されますか?
A. モニターモードAPからの最後の10個のwIPSイベント
B. wIPSイベントが最も多かったスニファーモードAPの最後の10個
C. wIPSイベントが最も多かった10個の監視モードAPのうち最後の10個
D. スニファーモードAPからの最後の10個のwIPSイベント
正解: **A (**コメントを発表する**)**

質問: **100**
コントローラ間でローミングする際に、マルチキャストデータをクライアントにシームレスに転送しながら、ネットワークのレイヤ2マルチキャストフレームのフラッディングを防ぐために適用される設定はどれですか？
A. 中央のレイヤ 3 スイッチで IGMPv3 を有効にします。
B. WLC で IGMP スヌーピングを有効にします。
C. WLC でマルチキャスト モードを有効にします。
D. 中央のレイヤ 3 スイッチにマルチキャスト グループを作成します。
正解: **B (**コメントを発表する**)**
To prevent the network from a Layer 2 flooding of multicast frames and ensure a seamless transfer of multicast data to the client when roaming, IGMP snooping should be enabled on the

WLC. This feature allows the WLC to monitor and control multicast traffic at Layer 2, preventing unnecessary multicast forwarding.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **101**
コントローラは、環境内の AP が干渉を検出していることを示していますが、Cisco DNA Center の AP ヘルス スコアは影響を受けていません。Cisco DNA Center が干渉を無視している 2 つの理由は何ですか? (2つ選んでください。)
A. 干渉は 2.4 GHz 無線で 30% 以下です。
B. 干渉は 2.4 GHz 無線で 50% 以下です。
C. Cisco DNA Center には、AP ヘルス スコアに Cisco CleanAir 干渉のみが含まれます。
D. 干渉は 5 GHz 無線で 30% 以下です。
E. Cisco DNA Center は、AP ヘルス スコアに干渉を含めません。
正解: **(**正解を表示します**)**
Cisco DNA Center is likely ignoring the interference detected by the AP because it includes only Cisco CleanAir interferers in the AP health score (option C), and the interference is less than or equal to 30% on the
5 GHz radio (option D). Cisco DNA Center's AP health score algorithm may not consider interference that falls below a certain threshold or interference that is not identified as a CleanAir event. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, particularly the chapters on Cisco DNA Center and CleanAir technology.

質問: **102**
エンジニアは、RADIUS サーバーの内部データベースを利用して、ワイヤレス ネットワークに 802.1x 認証を実装しました。一部のクライアントから、接続できないことが報告されました。トラブルシューティングの結果、PEAP 認証が失敗していることが判明しました。デバッグは、サーバーが Access-Reject メッセージを送信していることを示しました。認証を解決するには、どのアクションを実行する必要がありますか?
A. サーバーで構成されているユーザー パスワードを使用します。
B. クライアントでのサーバー証明書の検証を無効にします。
C. ユーザー アカウントと一致するようにクライアント証明書を更新します。
D. CA からのクライアント証明書をサーバー証明書に置き換えます。
正解: **(**正解を表示します**)**
If PEAP authentication is failing and the server is sending an Access-Reject message, one possible action to resolve the issue is to disable the server certificate validation on the client. This means that the client device will not check the authenticity of the RADIUS server's certificate, which can sometimes resolve connection issues, especially if there is a problem with the certificate chain or trust settings. However, this should be done with caution as it reduces the

security of the authentication process. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

質問: **103**
Cisco DNA Center で使用される Cisco Aironet アクティブ センサーの AP モデルはどれですか?
A. 1800年代
B. 3600e
C. 3800 秒
D. 4800i
正解: **(**正解を表示します**)**
The Cisco Aironet 1800s Active Sensor is designed to work with Cisco DNA Center. It is a compact, flexible sensor that provides insights into the wireless network's health and is used for proactive monitoring and troubleshooting. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, which includes information on Cisco DNA Center and compatible AP models.

質問: **104**
EAP プロセス中、特にクライアント認証セッションに関連して、どの暗号化キーが RADIUS サーバーからアクセス ポイントに送信されますか?
A. WPA キー
B. セッションキー
C. 暗号化キー
D. 共有秘密鍵
正解: **B (**コメントを発表する**)**
During the Extensible Authentication Protocol (EAP) process, the RADIUS server generates an encrypted session key after the client's identity is authenticated. This session key is sent to the access point to encrypt data frames between the client and the access point. It ensures that each session has a unique encryption key, enhancing security. References: Look for information on EAP and RADIUS in the CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **105**
顧客は、Cisco Catalyst 9800シリーズ ワイヤレス コントローラからCisco APへのセキュアなワイヤレス ネットワークをリモート ユーザーに提供する必要があります。企業のWLANは、インターネット経由で特定の場所に提供され、ローカルに設置されたIP電話をサポートする必要があります。この設定を実現する2つのアクションはどれですか? (2つ選択してください)
A. 物理インターフェースにNATを設定する
B. リモートLANの下でリモートLANを構成する
C. Flex プロファイルで Office Extend AP を有効にする
D. WLAN でローカルスイッチングを有効にする

E. Flexグループを作成し、APを追加する
正解: **B,C** (コメントを発表する)

質問: **106**
セキュリティポリシーでは、ITサブネットからのコントローラのWeb管理トラフィックのみを許可するように規定されています。テスト中に、エンジニアがゲストユーザー向けのWeb認証を使用してWLANに接続しようとしましたが、ワイヤレスクライアントブラウザでページがタイムアウトします。問題の原因は何ですか？
A. コントローラに実装された CPU ACL がゲスト クライアントからの HTTP/HTTPS トラフィックをブロックしています。
B. Web 認証リダイレクトは CPU ACL ではサポートされていません。
C. コントローラに設定されている DNS サーバーが正しくありません。
D. Web 認証リダイレクトは Internet Explorer でのみサポートされており、クライアントは Google Chrome を使用しています。
正解: **A** (コメントを発表する)
The issue is likely caused by the CPU ACL on the controller, which is blocking HTTP/HTTPS traffic from the guest clients. When a WLAN with Web Authentication is used, the wireless client's browser is redirected to a web page for authentication. If the CPU ACL is configured to only allow controller web management traffic from the IT subnet, it may inadvertently block the necessary HTTP/HTTPS traffic for the Web Authentication process, leading to a timeout on the wireless client browser. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, specifically the sections discussing CPU ACLs and their impact on network traffic.

質問: **107**
検出中に、ファブリック対応WLANコントローラ5台のうち1台が正しく検出されません。ファイアウォールルールはすべてのコントローラで同じです。どの要素が欠けていますか？
A. SNMPトラップ
B. SNMP管理
C. NETCONF
D. YANG
正解: (正解を表示します)

質問: **108**
大規模ネットワークを管理しているお客様がロケーションサービスを実装しました。負荷が高いため、WLCからNMSP経由で送信されるデータのロードバランシングが必要です。APのデータフローを最適化するには、複数のCMXサーバ間で負荷を分散する必要があります。この要件を満たすCMXの構成はどれですか？
A. cmxctl config 機能フラグ nmsplb.cmx-ap-grouping true
B. cmxctl config 機能フラグ nmsplb.cmxgrouping true
C. cmxctl config 機能フラグ nmsplb.cmx-loadbalance true
D. cmxctl config 機能フラグ nmsplb.cmx-rssi-distribute true
正解: **(正解を表示します)**
To load balance the data coming through NMSP from the WLCs and spread the load between multiple CMX servers, the configuration cmxctl config feature flags nmsplb.cmx-ap-grouping true should be used. This enables the load balancing feature and helps optimize the data flow for APs in a large network environment. References: The configuration for load balancing in CMX is explained in the certification guide, which outlines the commands and flags necessary to manage data flow efficiently.
Reference: https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_command/cmxcli106/cmxcli1051_chapter_010.html#wp7273815000
https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894-optimize-cmx-performance.html

質問: **109**
ある企業が仮想会議ソリューションとしてWebExの利用を開始しました。WebExの利用によって増加するトラフィック量を既存の無線ネットワークがサポートできなくなるのではないかと懸念されています。エンジニアは、会議の高品質を確保するために、このアプリケーションのQoS値を確認する必要があります。このタスクを達成するには、何を実装する必要がありますか？
A. QoS優先コールインデックス
B. UPからDSCPへのマップ
C. AVCプロファイル
D. WLANサービス品質プロファイル
正解: **C (コメントを発表する)**
Application Visibility and Control (AVC) profiles must be implemented to remark the QoS value for WebEx traffic. AVC profiles allow the network to identify different applications and provide the appropriate QoS treatment, ensuring high-quality meetings. References := (CCNP Enterprise Wireless Design ENWLSD 300-
425 and Implementation ENWLSI 300-430 Official Cert Guide)
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKEWN-3003.pdf

質問: **110**

企業は最近、AireOS コントローラを使用してすべての従業員が利用できる音声およびビデオ ソリューションを導入しました。従業員はラップトップでこのサービスを使用する必要がありますが、ユーザーは、ワイヤレス ネットワークに接続したときのサービスが悪いと報告しています。帯域幅を消費するプログラムを特定して制限する必要があります。トラフィックの認識に役立つ WLAN の設定はどれですか?

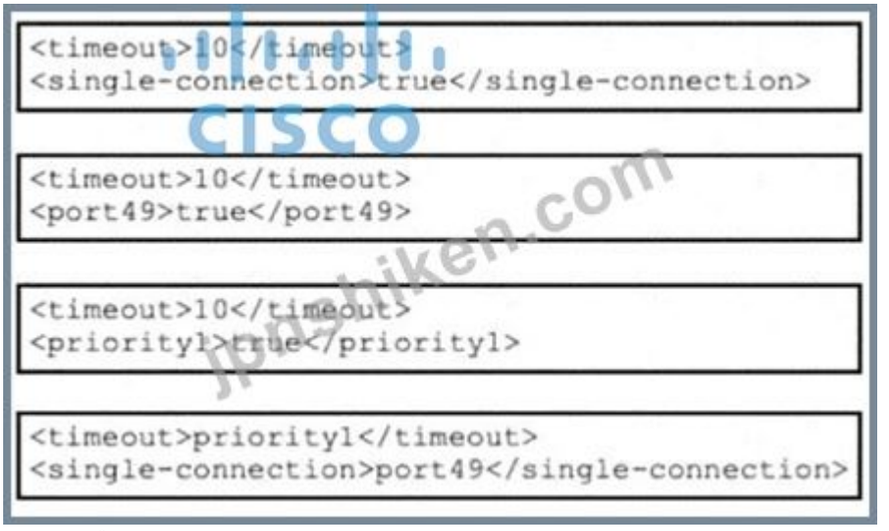
A. NetFlow モニター
B. AVC プロファイル
C. QoS プロファイル
D. アプリケーションの可視性

正解: **(**正解を表示します**)**

Application Visibility and Control (AVC) profiles in AireOS controllers allow the identification and management of bandwidth consumption by different applications. By using AVC, administrators can set policies to prioritize or restrict bandwidth for specific applications, thus ensuring that critical services like voice and video are not adversely affected by bandwidth-heavy programs. References: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

質問: **111**

別紙を参照してください。ネットワーク管理者は、TACACS+を　使用してGUIおよびCLIへの管理アクセスを保護するために、Cisco Catalyst C9800-80 WLCにデバイスアクセス制御を実装する必要があります。管理者は、PythonスクリプトでNETCONFを使用してWLCを直接設定し、TACACS+サーバを定義しています。このサーバは、GUIおよびCLIアクセスの認証を処理します。192.168.1.100のTACACS+サー　バには、WLCからの認証要求のプライマリサーバとなるようにするための特別な設定が必要です。管理者は、共有秘密鍵Cisco123がサーバ設定と一致し、タイムアウトが10秒に設定されていることを確認しました。スクリプトを完成させるには、コード内のボックスにどのXMLコードスニペットを配置する必要がありますか？



A. オプションB
B. オプションD
C. オプションC

D. オプションA
正解: **D** (コメントを発表する)

質問: **112**
エンジニアは、Cisco FlexConnect グループ内の AP をアップグレードしたいと考えています。このアップグレードを実行するには、FlexConnect AP アップグレード設定を使用します。グループ内で MAC アドレスが最も小さい各モデルの AP のうち 1 つが、コントローラから直接アップグレードを受信する必要があります。この直接アップグレードを実現するには、どのアクションが必要ですか？
A. グループから AP を削除します。
B. アップグレード前にすべての AP を再起動します。
C. マスター AP を異なるグループに割り当てます。
D. マスター AP を設定しません。
正解: (正解を表示します)
The FlexConnect AP Upgrade feature allows for a selective upgrade process within a FlexConnect group. By not setting any master APs, the WLC will automatically select one AP of each model with the lowest MAC address to receive the upgrade directly from the controller. This ensures that the upgrade is distributed efficiently across different AP models in the group without manual intervention.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **113**
お客様がCisco Catalyst 9800シリーズ ワイヤレス コントローラとCisco 802.11axAPを使用しています。経営陣から、ワイヤレスネットワーク上にあるデバイスの種類を確認する機能が求められています。どの2種類のローカルデバイスプロファイリングを使用する必要がありますか？ 2つ選択してください）
A. MACアドレスOUI
B. 無線
C. 無線サプリカント
D. DHCP
E. IPアドレス
正解: **A,D** (コメントを発表する)

質問: **114**
エンジニアは、SSID の不正封じ込めを実装する必要があります。封じ込めに使用する AP の最大数はいくつですか?
A. 1
B. 2
C. 3

D. 4
正解: **(**正解を表示します**)**
For rogue containment on an SSID, it's recommended to use two access points for containment (Option B).
Using more than two can lead to unnecessary interference and potential disruption of service for legitimate users, while using just one may not be effective enough in containing the rogue SSID.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide) Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_Detection.html

質問: **115**
エンジニアが2台のWLCにマルチキャストを設定しています。コントローラは物理的に異なる場所にあり、それぞれ約500台の無線クライアントを処理します。設定中にCAPWAPマルチキャストグループアドレスをどのように割り当てるべきですか？
A. 各 WLC には、一意のマルチキャスト グループ アドレスを割り当てる必要があります。
B. 各 WLC 管理アドレスは同じマルチキャスト グループに属している必要があります。
C. 両方の WLC に同じマルチキャスト グループ アドレスを割り当てる必要があります。
D. 各 WLC 管理アドレスは、異なるマルチキャスト グループに属している必要があります。
正解: **A (**コメントを発表する**)**
When configuring multicast for two WLCs in different physical locations, each handling around 500 wireless clients, it is important to assign a unique multicast group address to each WLC. This ensures that multicast traffic is properly segregated and managed within each controller's network.
References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

質問: **116**
Cisco MSE とワイヤレス LAN コントローラ間のデフォルトの NMSP エコー間隔は?
A. 10 秒
B. 15秒
C. 30 秒
D. 60秒
正解: **B (**コメントを発表する**)**
The default NMSP echo interval between Cisco MSE and a Wireless LAN Controller is 15 seconds. This interval determines how frequently the MSE sends echo messages to the WLC to maintain the NMSP connection and ensure that the link is active and operational. References := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide) Reference:
https://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide

/msecg_ch4_CAS.html

質問: **117**
ある企業では、リモートブランチに既存のシスコ無線ソリューションを導入しており、制御トラフィックとデータトラフィックは中央でスイッチングされています。Wi-Fiを使用する際にクライアントトラフィックをローカルでスイッチングするための新しいソリューションが必要です
音声デバイス専用に使用される新しい SSID は、VLAN 25 という名前のオンサイト音声 VLAN にマッピングする必要があります。
AP に接続するスイッチ インターフェイスのどの構成が要件を満たしていますか?
A. スイッチポートモードトランクスイッチトランクネイティブVLAN 25
B. スイッチポートモードアクセス スイッチポートアクセスVLAN 25 スイッチポートアクセス音声VLAN 25 スイッチポートモードトランク
C. スイッチポートモードアクセス スイッチポートアクセスVLAN 25
D. スイッチポートトランク許可VLANにVLAN 25を追加
正解: **(**正解を表示します**)**

質問: **118**
ある企業は、有線および無線ネットワークにおける不正なAPの存在を懸念しています。この企業はCisco Catalyst Center（旧DNA Center）ソリューションを導入しています。どの機能を有効にする必要がありますか？
A. 不正管理アプリケーション パッケージ
B. 近隣支援ローミング
C. スニファーパッケージ
D. モニターモードパッケージ
正解: **A (**コメントを発表する**)**

質問: **119**
お客様はCisco Catalyst 9800シリーズ ワイヤレスコントローラでディープパケットインスペクションを使用する必要があります。詳細には、すべてのワイヤレスクライアントの使用状況の詳細を含める必要があります。この要件を満たすには、AVCをどこで設定する必要がありますか？
A. join tag
B. WLAN
C. AP join
D. RF tag
E. policy profile
正解: **E (**コメントを発表する**)**

質問: **120**

エンジニアは、ユーザーに802.1X認証を許可するように自律APを設定しています。RADIUSサーバーのポリシーでは、EAP-TLS認証のみが許可されています。エンジニアは、APのSSIDのクライアント認証設定でどの認証方法を選択する必要がありますか？

A. オープン

B. 共有

C. ネットワークEAP

D. ウェブ

正解: **(**正解を表示します**)**