Cisco.300-715J.v2026-08-14.q212

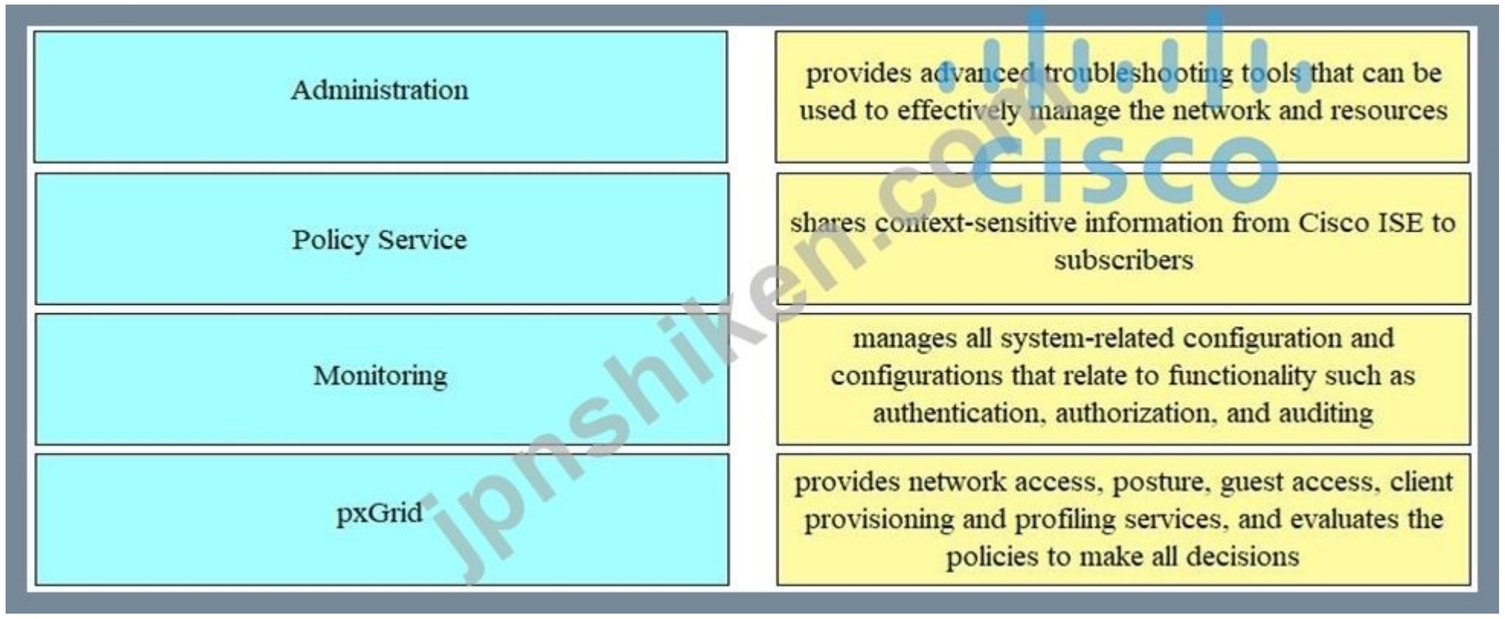
試験コード：	300-715J
試験名称：	Implementing and Configuring Cisco Identity Services Engine (300-715日本語版)
認証ベンダー：	Cisco
無料問題の数：	212
バージョン：	v2026-08-14
ページの閲覧量：	102
問題集の閲覧量：	2277

https://www.jpnshiken.com/shiken/Cisco.300-715J.v2026-08-14.q212.html

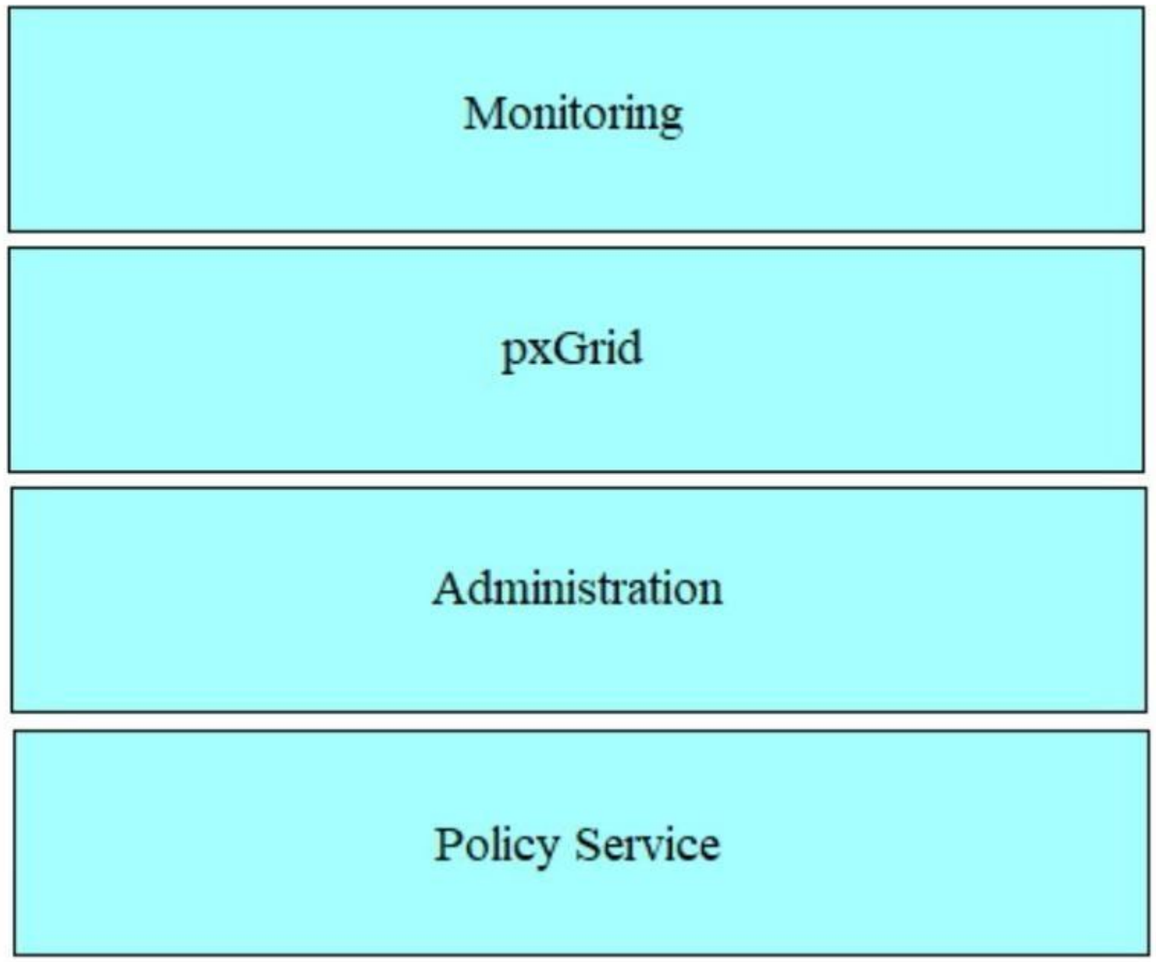
質問: **1**
Cisco ISEを使用してネットワークアクセス制御を行う環境でプロファイリングを設定する場合、組織はレイヤ2で情報を収集するために非独自プロトコルを使用する必要があります。
SPANパケットをCisco ISEに転送せずにこの情報を提供するプローブはどれですか？(2つ選択してください)
(2つ選択してください。)
A. DHCP SPANプローブ
B. SNMPクエリプローブ
C. NetFlowプローブ
D. 半径プローブ
E. DNSプローブ
正解: **(**正解を表示します**)**
https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

質問: **2**
承認ポリシーを構成する場合、管理者は、ポリシー条件として使用されるドメインに存在する特定のActiveDirectoryグループを確認できません。ただし、同じドメインにある他のグループが表示されますこの問題の原因は何ですか？
A. グループは存在しますが、条件として手動で入力する必要があります
B. Cisco ISEは、組み込みグループのみを認識し、ユーザが作成したグループは認識しません。
C. CiscoISEのADジョインポイントへの接続に失敗しています
D. グループはADジョインポイントの下のCiscoISEに追加されません
正解: **D (**コメントを発表する**)**

質問: **3**
ドラッグアンドドロップ問題
左側のCisco ISEノードタイプを、右側の適切な用途にドラッグしてください。


Administration
provides advanced troubleshooting tools that can be used to effectively manage the network and resources
Policy Service
shares context-sensitive information from Cisco ISE to subscribers
Monitoring
manages all system-related configuration and configurations that relate to functionality such as authentication, authorization, and auditing
pxGrid
provides network access, posture, guest access, client provisioning and profiling services, and evaluates the policies to make all decisions

正解:



Explanation:
Monitoring = provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources Policy Service = provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Administration = manages all system-related configuration and configurations that relate to functionality such as authentication, authorization, auditing, and so on pxGrid = shares context-sensitive information from Cisco ISE to subscribers
https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_011.html#ID57

質問: 4
ポリシーサービスノードの冗長性は、展開でどのように実現されますか？
A. VIPを有効にする
B. NADのRADIUSサーバーリストを利用する
C. ノードグループを作成する
D. プライマリノードとセカンダリノードの両方を展開する

正解: **B** (コメントを発表する)
Node groups are optional and they enhance the profiler service mostly. The redundancy of PSN availability is dictated by the Radius Server list order on the NAD.
https://community.cisco.com/t5/network-access-control/ise-node-groups/td-p/3514849

質問: **5**
先日、ユーザーのノートパソコンが盗難に遭いました。IT部門はユーザーのために代替機を発注し、出荷前にベンダーからデバイスのMACアドレス04.57:47:34 35 0Aを入手しました。Cisco ISEにMACアドレスを追加する際の正しい手順はどれですか？
A. MACアドレスは、.csvファイルとインポートオプションを使用して手動でインポートすることのみ可能です。
B. MACアドレスはREST APIを使用して手動でインポートすることのみ可能です。
C. MAC アドレスは、[コンテキスト可視性] > [エンドポイント] の下にある + 記号を使用して手動で追加できます。
D. MACアドレスは、デバイスがネットワークに接続した後にのみ許可されます。
正解: (正解を表示します)

質問: **6**
ある企業がローカルネットワークに新しいCiscoスイッチを導入しています。ネットワークエンジニアは、スイッチとCisco ISEの間でTACACS+を　設定する必要があります。スイッチとCisco ISEの両方で必須となる設定値は何ですか？
A. 鍵暗号化キー
B. CoAポート
C. 共有された秘密
D. 認証プロファイル
正解: (正解を表示します)
The shared secret is the mandatory matching value that must be configured on both the switch (in the TACACS+ server config) and in Cisco ISE (when adding the network device). It's used to encrypt TACACS+ communications between the two.

質問: **7**
ネットワーク管理者は、Cisco ISEの展開をパイロットから本番に変更し、JVMのメモリ使用率が大幅に増加したことに気づきました。管理者は、これがノード間のレプリケーションによるものであると考えています。パフォーマンスの低下を最小限に抑えるために何を構成する必要がありますか？
A. 設定ミスがないかプロファイリングポリシーを確認します
B. エンドポイント属性フィルターを有効にする
C. 再認証間隔を変更します。
D. CiscoISEが最新のプロファイラフィードアップデートで更新されていることを確認します
正解: (正解を表示します)
Enabling the EndPoint Attribute Filter will have the Cisco ISE profiler only to keep significant attributes and discard all other attributes. Significant attributes are those used by the Cisco ISE system or those used specifically in a endpoint profiling policy or rule.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_cisco_ise_endpoint_profiling_policies.html#ID481

質問: **8**
RADIUSとTACACS+の　暗号化処理方法の違いは何ですか？
A. RADIUSはユーザー名とパスワードのフィールドのみを暗号化しますが、TACACS+は　パケット全体を暗号化します。

B. RADIUSはパケット全体を暗号化しますが、TACACS+は　ユーザー名とパスワードのフィールドのみを暗号化します。
C. RADIUSはパスワードフィールドのみを暗号化しますが、TACACS+は　パケット全体を暗号化します。
D. RADIUSはパケット全体を暗号化しますが、TACACS+は　パスワードフィールドのみを暗号化します。
正解: **(**正解を表示します**)**

質問: **9**
企業ネットワークへのアクセスが許可される前に、エンドポイントに最新バージョンのウイルス対策アップデートがインストールされていることを保証する Cisco ISE ソリューションはどれですか?
A. プロファイリング サービス
B. 脅威サービス
C. プロビジョニング サービス
D. ポスチャ サービス
正解: **(**正解を表示します**)**

質問: **10**
デバイス管理におけるTACACS +とRADIUS の2つの利点は何ですか？ 2つ選択してください）
A. TACACS +はサービスタイプを提供し、RADIUSは提供しません
B. TACACS +はUDP を使用し、RADIUSはTCPを使用します
C. TACACS +は802.1Xをサポートし、RADIUSはMABをサポートします
D. TACACS +にはコマンド許可がありますが、RADIUSにはありません。
E. TACACS +はペイロード全体を暗号化し、RADIUSはパスワードのみを暗号化します。
正解: **D,E (**コメントを発表する**)**

質問: **11**
組織は、BYODプロセスを改善して、CiscoISEがBYODエンドポイントに証明書を発行できるようにしたいと考えています。現在、アクティブな認証局があり、CiscoISEに置き換えることは望んでいません。この目標を達成するには、Cisco ISE内で何を設定する必要がありますか？
A. OCSPプロファイルを追加し、ルート認証局をセカンダリとして構成します。
B. ルート認証局をトラストストアに追加し、認証を有効にします。
C. 証明書署名要求を作成し、ルート認証局に署名してもらいます。
D. SCEPプロファイルを作成して、CiscoISEをルート認証局にリンクします。
正解: **(**正解を表示します**)**

質問: **12**
エンジニアが新しい Cisco ISE ノードを構成しています。Cisco ISE は、脅威および脆弱性アダプタから受信した脅威および脆弱性の属性に基づいて認証の判断を行う必要があります。どのペルソナを有効にする必要がありますか？
A. pxGrid
B. ポリシーサービス
C. 管理
D. モニタリング
正解: **A (**コメントを発表する**)**

To enable Cisco ISE to make authorization decisions based on threat and vulnerability attributes received from external sources, the pxGrid persona must be enabled. pxGrid (Platform Exchange Grid) is a Cisco ISE service that facilitates communication between ISE and third-party systems for the exchange of context-based information such as threat intelligence, vulnerabilities, and device posture.
How pxGrid Works:
1. pxGrid provides a framework for integrating external systems like threat intelligence platforms or vulnerability scanners with Cisco ISE.
2. These systems send threat and vulnerability data to Cisco ISE via pxGrid.
3. Cisco ISE uses this information to enforce dynamic authorization policies, such as quarantining or restricting access for compromised devices.

質問: **13**
Cisco ISEノードからMABユーザーの非アクティブアクティブタイマーを動的に割り当てるために使用されるRADIUS属性はどれですか？
A. セッションタイムアウト
B. アイドルタイムアウト
C. RADIUSサーバータイムアウト
D. 終了処理
正解: **B (**コメントを発表する**)**

質問: **14**
エンジニアは、認証が不要なポータルへのゲストのWebリダイレクトを設定し、ネットワークアクセスを許可する前にゲストが利用規約に同意する必要があるようにする必要があります。この要件を満たすには、Cisco ISEでどのタイプのゲストポータルを設定する必要がありますか？
A. スポンサー提供
B. カスタム
C. 自己登録
D. ホットスポット
正解: (正解を表示します)

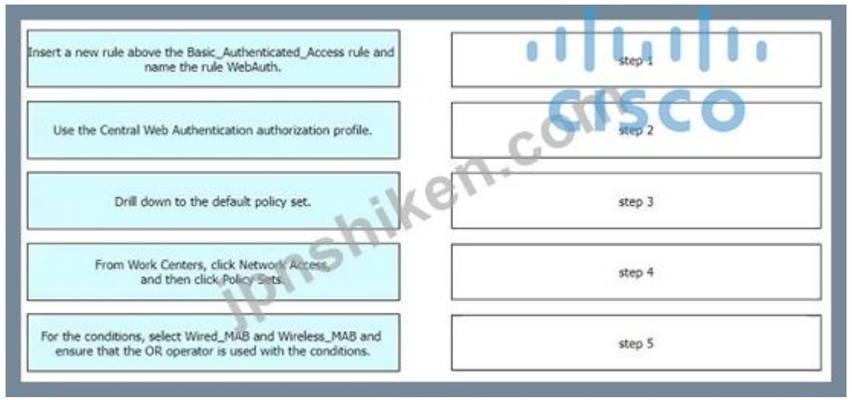
質問: **15**
エンジニアはCisco ISEを導入した後、認証ポリシーでActive Directoryの情報を使用するようにActive Directoryを設定する必要があります。
この目標を達成するために、Active Directoryグループに加えて、どの2つのコンポーネントを構成する必要がありますか？(2つ選択してください)
A. LDAP外部IDソース
B. 外部アイデンティティのライブラリ条件：外部グループ
C. Active Directory 外部 ID ソース
D. アイデンティティソースシーケンス
E. IDグループのライブラリ条件: ユーザーIDグループ
正解: (正解を表示します)

質問: **16**
管理者が、分散 Cisco ISE 環境で PSN を置き換えました。エンドポイントが認証されると、デバイスは適切なプロファイルまたは属性を取得せず、その結果、正しいポリシーにヒットしません。これは、以前の PSN で正しく機能していました。エンドポイントを確実に特定するには、どのアクションを実行する必要がありますか?
A. プロファイリング サービスが新しい PSN で実行されていることを確認します。
B. MnT ノードがセッションを追跡していることを確認します。
C. PSN が受信している認証要求の形式が正しくないことを確認します。

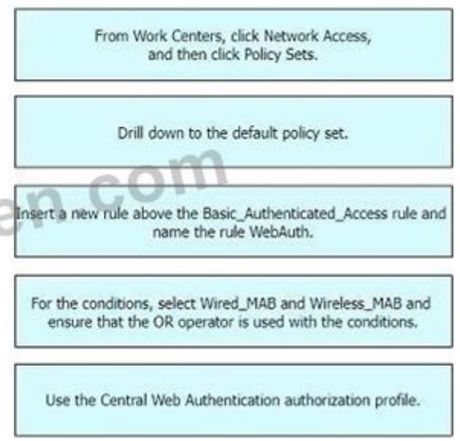
D. スイッチと PSN の間で使用される共有秘密を確認します。
正解: (正解を表示します)

質問: **17**
ネットワークセキュリティ管理者は、ゲストユーザーが以下の手順で無線接続を使用してネットワークに接続する際に、Web認証構成を設定する必要があります。
- 最初のMABリクエストがCisco ISEノードに送信されます。
Cisco ISE は、以下の場合に URL リダイレクト認証プロファイルで応答します。
エンドポイントIDストアにユーザーのMACアドレスが登録されていません。
- URLリダイレクトにより、ユーザーにAUP同意ページが表示されます
ユーザーが任意のURLにアクセスしようとしたとき。
管理者はCisco ISEでどの認証を設定する必要がありますか？
A. 中央Web認証を備えたNAD
B. デバイス登録 WebAuth
C. ローカルWeb認証を備えたWLC
D. ローカルWeb認証を備えた有線NAD
正解: (正解を表示します)

質問: **18**
ドラッグアンドドロップ問題
図を参照してください。エンジニアは、Cisco ISEで図に一致するWeb認証アクセスポリシーを作成する必要があります。このタスクを実行するには、左側の設定手順を右側にドラッグアンドドロップして順番に並べ替えてください。



正解:



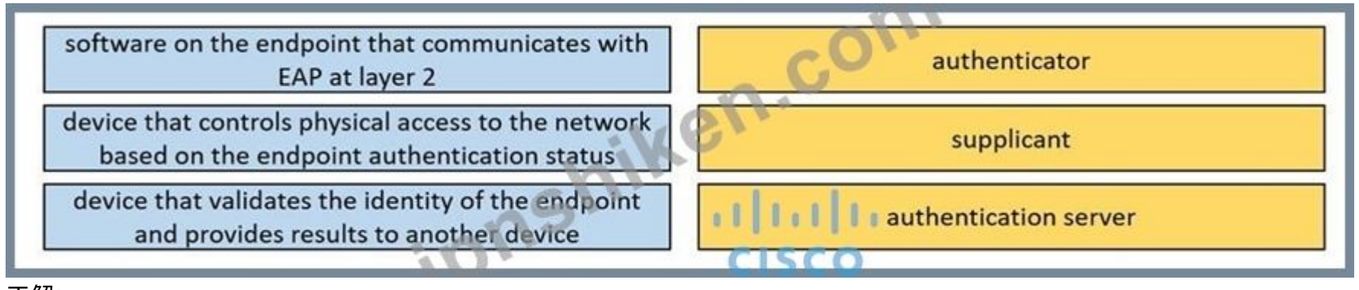
質問: **19**
中規模の展開でサポートされるPSNノードの最大数はいくつですか。
A. 3
B. 5
C. 2
D. 8
正解: **(**正解を表示します**)**
Five nodes for Cisco ISE below 3.0.
Six nodes for Cisco ISE 3.0 above.

質問: **20**
エンジニアがLDAPを使用して、プリンタエンドポイントの一括インポートをCisco ISEローカルデータベースに実行しています。デバイスが 不明」としてプロファイルされないようにするには、どのLDAPフィールドを設定する必要がありますか？
A. MACアドレスオブジェクトクラス
B. プロフィール属性名
C. MACアドレスプロファイルクラス

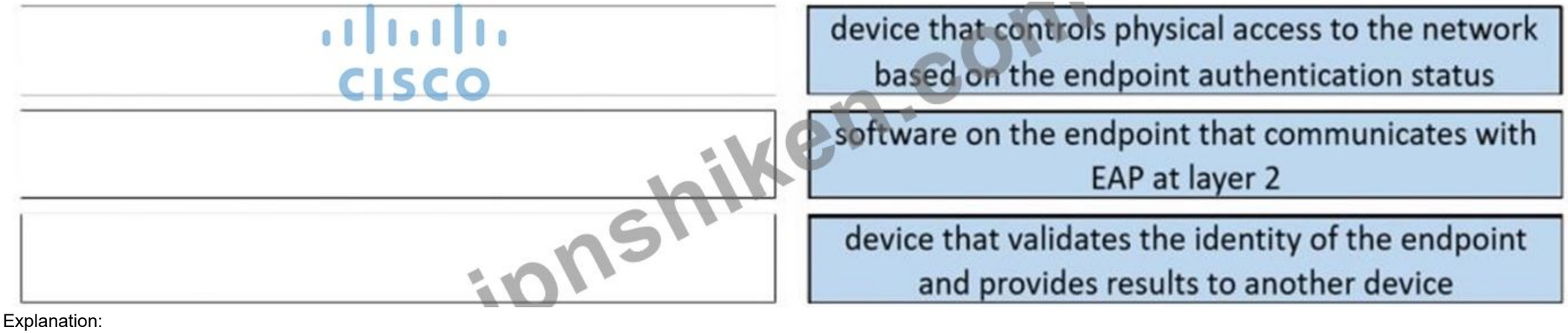
D. デバイスプロファイル名
正解: **B** (コメントを発表する)
When importing printer endpoints via LDAP, Cisco ISE requires the correct Profile Attribute Name to map LDAP data to the appropriate profiling policy. This ensures that the endpoints match an existing profiling condition rather than being classified as Unknown.

質問: **21**
管理者がCiscoスイッチでTACACS+を　設定しているが、Cisco ISEでユーザー認証ができない。
設定には正しいキーである Cisc039712287 が含まれています。しかし、スイッチは Cisco ISE インスタンスから応答を受信していません。
AAA構成を検証し、TACACS+サー　バーの問題点を特定するには、どのような手順を踏む必要がありますか？
A. test aaa group tacacs+ admin <key> legacy コマンドを使用して、サーバーへの到達可能性を確認します。
B. test aaa group radius server CUCS user admin pass <key> legacy コマンドを使用して、サーバー上のユーザー アカウントをテストします。
C. test aaa authentication admin <key> legacy コマンドを使用して、キーの値が正しいことを検証します。
D. test aaa authorization admin drop legacy コマンドを使用して、認証ポリシーが正しいことを確認します。
正解: **A** (コメントを発表する)
https://medium.com/training-course-ccna-security-210-260/ccna-security-part-3-implementing-aaa-in-cisco-ios-4b13ab285f51

質問: **22**
ドラッグアンドドロップ問題
左側の説明文を、右側の802.1Xの構成要素にドラッグしてください。



正解:



Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec- user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

質問: **23**
Cisco ISE エンジニアが、ネットワークのマシン認証で使用する証明書認証プロファイルを作成しています。エンジニアは、ユーザーが提示した証明書を Active Directory に保存されている証明書と比較できるようにしたいと考えています。これを実現するには、どのような手順が必要ですか？
A. CAPに主題の別名と一般名を追加する
B. MS-CHAPv2 を使用します。これはマシン認証情報を提供し、それを Active Directory に保存されている認証情報と照合します。
C. ユーザーが提示したパスワードハッシュと、Active Directoryに保存されているハッシュを比較用に設定します。
D. バイナリ比較を実行するオプションを有効にします。
正解: **(**正解を表示します**)**
Binary comparison must be enabled in the certificate authentication profile so Cisco ISE can directly compare the certificate presented by the machine with the certificate stored in Active Directory during machine authentication.

質問: **24**
組織は、Cisco ISE 展開にノードを追加しており、プライマリおよびセカンダリ PAN および MnT ノードとして指定された 2 つのノードがあります。組織には 4 つの PSN もあります 管理者がこの展開にさらに 2 つの PSN を追加しようとしていますが、そのうちの 1 つを追加する際に問題が発生しています 問題は何ですか?
A. このように構成されている場合、Cisco ISE キューブに含めることができる PSN は 5 つだけです。
B. 現在の PAN は最大 4 つのノードしか追跡できません
C. 新しいノードの 1 つを pxGrid ノードとして指定する必要があります
D. 新しいノードは、展開に追加する前にプライマリに設定する必要があります
正解: **(**正解を表示します**)**

質問: **25**
Cisco ISEのどのモジュールに、OPSWATが提供するベンダー名、製品名、および属性のリストが含まれていますか？
A. コンプライアンスモジュール
B. クライアントプロビジョニングモジュール
C. エンドポイントセキュリティモジュール
D. 姿勢モジュール
正解: **A (**コメントを発表する**)**
The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.
https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/admin_guide/b_ise_admin_3_1/b_ISE_admin_31_compliance.html

質問: **26**
エンジニアがCisco ISEの段階的な導入に低影響モードを使用し、認証前にネットワークに接続しようとしています。この場合、どのアクセスが拒否されますか？
A. HTTP
B. DNS
C. EAP
D. DHCP
正解: **(**正解を表示します**)**
HTTP is the most reasonable answer. User that tried to connect needs to connect to DNS, DHCP and of course EAP.

質問: **27**
ある組織がCisco ISEのポスチャサービスを導入しており、ネットワークにアクセスしようとするすべてのWindowsおよびMacコンピュータにホストベースのファイアウォールが設置されていることを確認する必要があります。
彼らのデバイスには複数のベンダーのファイアウォールアプリケーションが搭載されているため、ポリシーを作成するエンジニアは、特定のアプリケーションチェックを使用してセキュリティ状態を検証することができません。
このような姿勢チェックを可能にするには、どのような対策を講じるべきでしょうか？
A. ファイルレジストリ条件を使用して、ファイアウォールが正しくインストールされ、実行されていることを確認します。
B. 複合条件を使用して、Windows または Mac のネイティブファイアウォールアプリケーションを検索します。
C. デフォルトのファイアウォール条件を有効にして、ベンダーのファイアウォール アプリケーションをチェックします。
D. デフォルトのアプリケーション条件を有効にして、インストールされているアプリケーションを識別し、ファイアウォールアプリを検証します。
正解: **(**正解を表示します**)**
The Firewall condition checks if a specific Firewall product is enabled on an endpoint. The list of supported Firewall products is based on the OPSWAT support charts. You can enforce policies during initial posture and Periodic Reassessment (PRA). Cisco ISE provides default Firewall conditions for Windows and macOS.
https://community.cisco.com/t5/security-knowledge-base/ise-posture-prescriptive-deployment- guide/ta-p/3680273#toc-hId-1256947692

質問: **28**
証明書要求を生成せずに、証明書プロビジョニングポータルを使用してCisco ISEでシングル署名を生成するための2つの要件は何ですか？　2つ選択してください）
A. デバイスMACのCSVファイルの場所
B. 証明書テンプレートを選択します
C. ハッシュ方法を選択します
D. 一般名を入力します
E. デバイスのIPアドレスを入力します
正解: **B,D (**コメントを発表する**)**
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200534-ISE-2-0-Certificate-Provisioning-Portal.html

質問: **29**
ネットワークエンジニアが、接続しているデバイスに関する詳細情報を取得するために、CiscoワイヤレスLANコントローラを設定しています。この情報は、認証ポリシーで使用するためにCisco ISEに送信する必要があります。このタスクを実行するには、CiscoワイヤレスLANコントローラでどのプロファイリングメカニズムを設定する必要がありますか？
A. ICMP
B. DHCP
C. CDP
D. DNS
正解: **(**正解を表示します**)**
DHCP Profiling: The WLC can be configured to relay DHCP information that it obtains when devices request IP addresses. This DHCP data includes attributes such as vendor class identifiers and other DHCP options, which are valuable for Cisco ISE to accurately classify and profile the connecting devices. The information gathered through DHCP profiling helps in enforcing the correct authorization policies based on the device type.

質問: **30**
図を参照してください。エンジニアがクライアントを設定していますが、Cisco ISEへの認証ができません。
トラブルシューティング中に、各ポートの認証状態を表示するために、show authentication sessionsコマンドが実行されました。
認証の問題を特定するのに役立つ追加情報を提供するコマンドはどれですか？

Interface	MAC Address	Method	Domain	Status Fg	Session ID
Gi1/0/6	0024.142d.e471	mab	UNKNOWN	Auth	C0A829020000000C2BBAF5D3
Gi1/0/1	0050.5698.0720	dot1x	UNKNOWN	Unauth	C0A8290200000152BCD0BE7

A. 認証セッションの出力を表示する
B. 認証セッションを表示する
C. 認証セッションの表示 インターフェース Gil/0/1 出力
D. 認証セッションインターフェース Gi1/0/1 の詳細を表示します
正解: (正解を表示します)

質問: **31**
Cisco ISE仮想アプライアンスでサポートされているVMwareの機能はどれですか？(2つ選択してください。)
A. VMのコールドマイグレーション
B. OVFサポート
C. マルチベンダー統合
D. VMハードウェアバージョン7以上
E. VMスナップショット
正解: (正解を表示します)
When deploying Cisco ISE as a virtual appliance on a VMware platform, there are specific VMware features that are supported and recommended:
VM Cold Migration:
Cisco ISE supports cold migration. This means that the virtual appliance can be moved from one host to another while it is powered off. Cold migration is a supported method for relocating the virtual machine in the event of hardware maintenance or upgrades.
OVF Support:
Cisco ISE is distributed as an OVF (Open Virtualization Format) package. This format is supported by VMware environments, making it straightforward to deploy the ISE virtual appliance using standard VMware tools.

質問: **32**
Cisco ISEにおける高速ユーザー切り替えに関するMicrosoftのセキュリティポリシー推奨事項は何ですか？
A. BOYD姿勢エージェントを無効化します。
B. Cisco Secure Clientのポスチャエージェントを有効にする。
C. 高速なユーザー切り替えを有効にする。
D. 高速ユーザー切り替えを無効にする。
正解: (正解を表示します)

Microsoft's security policy recommends disabling fast user switching to reduce the risk of unauthorized access. Fast user switching allows multiple user sessions to remain active simultaneously, which can potentially leave a system vulnerable if one session is compromised.
Disabling this feature ensures that when a user logs off, the session is fully terminated, thereby reducing the security risk.
In the context of Cisco ISE and endpoint compliance, this recommendation aligns with best practices to enforce strict user session control and ensure that endpoints are fully compliant before granting network access.

質問: **33**
Cisco ISEでポスチャを設定する際に、Cisco ISEとクライアント間で開いている必要があるポートはどれですか？(2つ選択してください)。
A. TCP 8906
B. TCP 443
C. DTCP80
D. TCP 8905
E. TCP 8443
正解: **(**正解を表示します**)**

質問: **34**
有効なゲストポータルタイプとは何ですか？
A. Sponsored-Guest
B. My Devices
C. Sponsor
D. Captive-Guest
正解: **A (**コメントを発表する**)**
Hotspot Guest portal: Network access is granted without requiring any credentials. Usually, an Acceptance of User Policy (AUP) must be accepted before network access is granted.
Sponsored-Guest portal: Network access is granted by a sponsor who creates accounts for guests, and provides the guest with login credentials.
Self-Registered Guest portal: Guests can create their own account credentials, and may need sponsor approval before they are granted network access.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_guest.html#ID32

質問: **35**
エンジニアは、企業のCisco ISE環境内のすべてのポータルに対して、新しい証明書を作成して署名する必要があります。企業側は、この環境ではワイルドカード証明書がブロックされていると報告しています。
技術者は証明書に署名する前に、どのような行動をとらなければならないか？
A. Cisco ISEモニタリングノードのFQDNに対してDNS AAAAレコードを作成します。
B. 各ポータルのFQDNをCSRのSANフィールドに追加する
C. 各ポータルの FQDN を CSR の CN フィールドに追加します。
D. Cisco ISE管理ノードのFQDNのDNS AAAレコードを作成します。
正解: **B (**コメントを発表する**)**
When wildcard certificates are not allowed, every portal FQDN must be explicitly listed. This requires adding each portal's FQDN to the SAN (Subject Alternative Name) field of the CSR so that the resulting certificate is valid for all ISE portals after signing.

質問: **36**
ネットワークエンジニアは、スイッチがCiscoISEの標準的なWeb認証をサポートできるようにすることを任されています。これには、認証時にURLリダイレクトをプロビジョニングする機能が含まれている必要があります。この要件を満たすには、どの2つのコマンドを入力する必要がありますか。 2つ選択してください）

A. IP httpsecure-authentication
B. IPhttpサーバー
C. IPhttpリダイレクト
D. Ip http secure-server
E. IPhttp認証
正解: **B,D** (コメントを発表する)
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111001.html

質問: **37**
ISE 管理者は、IP 電話に接続されたスイッチ ポートがデバイスからのパケットを 30 分間検出しない場合は常に、MAB エンドポイントの非アクティブ タイマーを変更して認証セッションを終了する必要があります。このタスクを達成するには、どのアクションを実行する必要がありますか?
A. 認証タイマー再認証サーバーコマンドをスイッチポートに追加します。
B. authentication timer inactivity 3600 コマンドをスイッチポートに追加します。
C. Radius サーバーのアイドル タイムアウトを IP Phone エンドポイントの 3600 秒に変更します。
D. Cisco ISE でセッション タイムアウトを 3600 秒に設定します。
正解: **C** (コメントを発表する)
The inactivity timer for MAB can be statically configured on the switch port, or it can be dynamically assigned using the RADIUS Idle-Timeout attribute (Attribute 28). Cisco recommends setting the timer using the RADIUS attribute because this approach lets gives you control over which endpoints are subject to this timer and the length of the timer for each class of endpoints.
For example, endpoints that are known to be quiet for long periods of time can be assigned a longer inactivity timer value than chatty endpoints.
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/MAB/MAB_Dep_Guide.html#wp392385

質問: **38**
Cisco ISEのポスチャを設定する際のポスチャ要件を構成する2つの要素は何ですか？
(2つ選択してください)
A. 更新
B. 是正措置
C. クライアントプロビジョニングポータル
D. 条件
E. アクセスポリシー
正解: (正解を表示します)
Create Client Posture Requirements
You can create a requirement in the Requirements window where you can associate user-defined conditions and Cisco defined conditions, and remediation actions. Once created and saved in the Requirements window, user-defined conditions and remediation actions can be viewed from their respective list windows.
https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_compliance.html#task_52F2E45628EF43C889B5559AF657B884

質問: **39**

ネットワーク管理者が、Cisco ISE と連携してネットワークアクセス制御を行うための新しいアクセススイッチを設定しています。再認証タイマーには集中型サーバーを使用する必要があります。このタスクを実行するには、どのような設定が必要ですか？
A. Cisco ISE を設定して、スイッチの設定を新しいタイマーに置き換えます。
B. スイッチ上で認証定期コマンドを発行します。
C. スイッチ上で認証タイマーの再認証サーバーコマンドを発行します。
D. Cisco ISEを設定して、一定期間後にアクセスをブロックします。
正解: **C** (コメントを発表する)

質問: **40**
管理者が Cisco ISE で変更を行い、CoA パケットをネットワーク デバイスに送信してすでに認証されているエンドポイントに新しい権限を適用する必要があります。この目標を達成するには、どの IOS コマンドをデバイスに設定する必要がありますか?
A. AAA サーバー半径の動的作成者
B. 認証コマンド disable-port
C. aaa nas ポート拡張
D. 認証コマンド バウンスポート
正解: (正解を表示します)

質問: **41**
管理者は、ゲストおよびBYOD認証のためにCisco ISEで使用する新しいサードパーティ製ネットワークデバイスを追加する必要があります。これを実現するには、ネットワークデバイスプロファイルでどの2つの機能を設定する必要がありますか？(2つ選択してください。)
A. URLリダイレクト
B. CoAタイプ
C. SNMPコミュニティ
D. TACACS
E. dACL
正解: (正解を表示します)

質問: **42**
姿勢チェックに利用できる条件を3つ挙げてください。(3つ選択してください。)
A. アプリケーション
B. サービス
C. オペレーティングシステム
D. 証明書
E. ファイル
正解: **A,B,E** (コメントを発表する)

質問: **43**
ネットワークエンジニアは、監視プラットフォームから、スイッチポートに複数のセッションが存在するというアラートを受信しました。この問題を解決するには、Cisco ISEを使用したRADIUS CoAを使用する必要があります。どのRADIUS CoA構成を使用すべきでしょうか？
A. 例外

B. 再認証
C. CoA用
D. ポートバウンス
正解: (正解を表示します)

質問: **44**
エンジニアは、ゲストがネットワーク アクセスを取得するためにコードを入力する必要があるゲストにインターネット アクセスを提供するように Cisco ISE を設定する必要があります。どのアクションが目標を達成しますか?
A. スポンサー ポータルを 1 つのアカウントで構成し、アクセス コードをパスワードとして使用します。
B. ゲストが個人用アクセス コードを作成できるように、自己登録ゲスト ポータルを構成します。
C. ゲスト アクセス用にホットスポット ポータルを構成し、アクセス コードを要求します。
D. ユーザーの認証をバイパスし、アクセス コードを承認する BYOD ポリシーを作成します。
正解: (正解を表示します)

質問: **45**
管理者は、Cisco ISEのBYODポータルを使用して、Ciscoスイッチに接続するmacOSエンドポイントをオンボーディングする必要があります。認証方法は、以下の要件を満たすように設定する必要があります。
- Cisco ISE は、ID 証明書を提供することで自身を識別します。
終点。
- エンドポイントは、Cisco ISEのID証明書を検証します。
- エンドポイントは、以下の署名を持つエンドポイントID証明書を提供します。
Cisco ISE から Cisco ISE へ。
- Cisco ISE はエンドポイント証明書の有効性を確認し、
エンドポイントはネットワークへの接続を許可されています。
どのプロトコルを設定する必要がありますか？
A. EAP-TLS
B. EAP-GTC
C. EAP-FAST
D. EAP-TTLS
正解: **A** (コメントを発表する)
The described onboarding process requires mutual authentication between the endpoint and Cisco ISE using certificates. The Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) protocol is the best choice because it supports:
1. Mutual Authentication:
Cisco ISE presents its identity certificate to the endpoint, which validates it.
■
The endpoint presents its identity certificate, signed by Cisco ISE, to the Cisco ISE server.
■
2. Certificate-Based Authentication:
EAP-TLS relies on X.509 certificates for both the client and server, meeting the requirements
■
outlined in the scenario.
3. Secure Communication:
TLS ensures that communication between the client and server is encrypted and secure.
■

質問: **46**
管理者が、Cisco ISEが稼働しているネットワークに、IP電話専用のスイッチを追加しようとしています。
これらの電話機は802.1Xによる認証機能を備えていません。
認証のために各スイッチポートで必要なコマンドは何ですか？
A. バイパスMACを有効にする
B. dot1xシステム認証制御
C. 息子
D. ネットワーク認証を有効にする
正解: **(**正解を表示します**)**
Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.
Before standalone MAB support was available, MAB could be configured only as a failover method for 802.1x authentication. Standalone MAB is independent of 802.1x authentication.
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-config- mab.html

質問: **47**
クライアントプロビジョニングの機能は何ですか？
A. クライアントプロビジョニングにより、エンドポイントが適切なポスチャエージェントを確実に受信します。
B. クライアントプロビジョニングは、クライアント上のファイルの存在、日付、およびバージョンをチェックします。
C. クライアントプロビジョニングは、ディクショナリ属性を値でチェックします。
D. クライアントプロビジョニングにより、アプリケーションプロセスがエンドポイントで実行されていることが保証されます。
正解: **A (**コメントを発表する**)**

質問: **48**
Active Directoryの参加および脱退操作に共通のアクセス許可はどれですか。
A. マシンアカウントがまだ存在しない場合は、ドメインにCisco ISEマシンアカウントを作成します
B. ドメインからCisco ISEマシンアカウントを削除します。
C. Cisco ISEマシンアカウントに属性を設定します
D. Active Directoryを検索して、Cisco ISEマシンアカウントがすでにex.stsであるかどうかを確認します。
正解: **(**正解を表示します**)**
tab -> Active Directory Account Permissions Required to Perform Various Operations
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/ise_active_directory_integration/b_ISE_AD_integration_2x.html

質問: **49**

Active Directoryグループを設定する際に、管理者が取得しようとしているグループ名が、別のグループ名と重複している場合があります。正しいグループを取得するには、どのような操作が必要ですか？
A. MIBエントリを利用して目的のグループを識別します。
B. SIDをグループの識別子として使用します。
C. 両方のグループを選択し、TCTポインタを使用して適切なグループを識別します。
D. MAB を 1 つのグループを使用するよう設定し、802 1x を競合するグループを使用するように設定します。
正解: **B** (コメントを発表する)

質問: **50**
Cisco ISEの分散展開環境で2つのノードがあり、セカンダリノードの登録が解除された場合、何が起こりますか？
A. プライマリノードが再起動します
B. セカンダリノードが再起動します。
C. プライマリノードがスタンドアロンになる
D. 両方のノードが再起動します。
正解: (正解を表示します)
Only the secondary restart to become standalone.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html#ID185

質問: **51**
新しい従業員がワークステーションをCiscoIPPhoneに接続しました。ネットワーク管理者は、ユーザがワークステーションを企業ネットワークから切断したときに、Cisco IPPhoneがオンラインのままであることを確認したいと考えています。この要件を満たすCoA構成はどれですか。
A. ポートバウンス
B. 再認証
C. NoCoA
D. 切断
正解: (正解を表示します)
The Reauth option may be sufficient for cases where no VLAN or address change is expected following reauthorization of the current session.
If multiple endpoints are detected on a wired switchport, ISE will automatically revert to using the Reauth option to avoid service disruption of other connected devices. A common example is a workstation connected to an IP phone where a port bounce would interrupt communications for both workstation and phone.

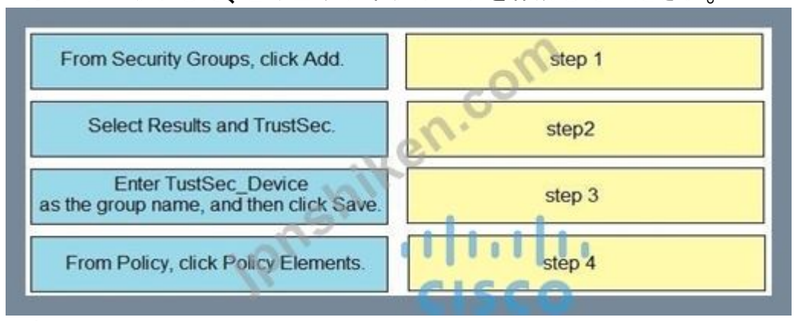
質問: **52**
Cisco ISEはどのような場合にアドバンストライセンスを割り当てますか？
A. 高可用性管理者ノード
B. dACL適用によるゲストサービス
C. 動的デバイスプロファイリング
D. SGA強制によるエンドポイント認証
正解: (正解を表示します)

質問: **53**

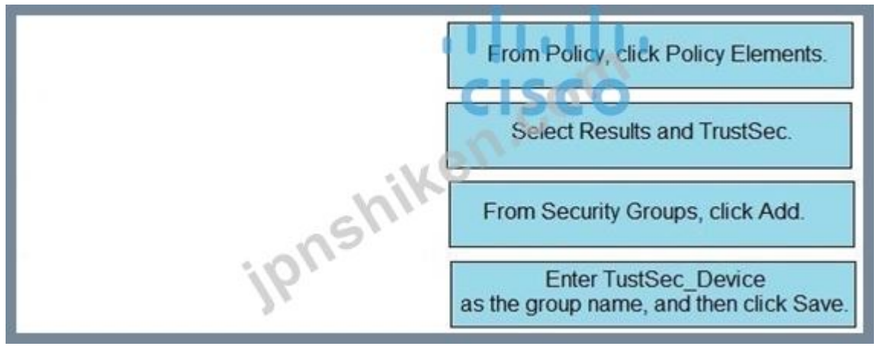
Cisco ISE環境では、管理者はワイヤレスゲストユーザーの認証方法をローカルアカウントからSAMILに変更する必要があります。SAMLプロトコルを使用する場合、ゲストポータルは外部IDプロバイダサーバーで従業員を認証するように構成する必要があります。以下の構成が実行されました。
- SAML統合用の二次的な自己登録型ゲストポータルを作成しました
- ワイヤレスゲストユーザー向けのプライマリゲストポータルを作成しました
- SAML IDプロバイダーで必要な設定をすべて構成しました
サーバ
- IdPメタデータをCisco ISE SAML IDプロバイダプロファイルにインポートしました。実行する必要のあるアクションはどれですか？(2つ選択してください。)
A. スポンサーポータルで従業員アカウントを作成します。
B. スポンサーポータルの設定
C. ISEでSAML IDプロバイダを作成します。
D. プライマリゲストポータルの認証方法として、SAML IDプロバイダを設定します。
E. セカンダリゲストポータルの認証方法として、SAML IDプロバイダを設定します。
正解: **D,E** (コメントを発表する)

質問: **54**
TACACS+の2　つの特徴は何ですか？(2つ選択してください)
A. UDPポート49を使用します。
B. 認可機能と認証機能を兼ね備えています。
C. TCPポート49を使用します。
D. パスワードのみを暗号化します。
E. 認可機能と認証機能を分離します。
正解: (正解を表示します)

質問: **55**
ドラッグアンドドロップ問題
エンジニアはCisco ISEでCisco TrustSecを設定する必要があります。エンジニアはActive Directoryとの統合を完了しますが、セキュリティグループを作成する必要があります。左側の設定手順を右側の手順にドラッグアンドドロップして、セキュリティグループを作成してください。



正解:



質問: **56**
企業は、BYODポリシーを改善し、特定の基準に基づいてアクセスを制限しようとしています。会社のサブネットは、建物ごとに編成されています。場所に基づいてアクセスするには、どの属性を使用する必要がありますか？
A. 静的グループ割り当て
B. IPアドレス
C. デバイス登録ステータス
D. MACアドレス
正解: **A** (コメントを発表する)

質問: **57**
図を参照してください。エンジニアは、インターフェース VLAN 10 上の IP アドレス 10.1.100.6 を持つ Cisco ISE ポリシー サービス ノードに DHCP プローブを送信するように Cisco スイッチを設定する必要があります。どのコード スニペットが設定を完了しますか？

```
interface Vlan10
   ip address 10.1.10.1 255.255.255.0
   ip helper-address 10.1.100.100
```

A. ip helper-address 10.1.10.6
B. ip helper-address 10.1.100.6
C. ip dhcp-relay 10.1.100.6
D. ip dhcp-address 10.1.100.6
正解: **(**正解を表示します**)**
The config already has one helper-address (10.1.100.100, likely the DHCP server). You simply add a second ip helper-address line pointing to the ISE PSN at 10.1.100.6 - Cisco IOS supports multiple helper-addresses on the same interface, and ISE uses the DHCP probe (port 67) for device profiling.

質問: **58**

エンジニアは、Cisco ISE を使用してデバイス管理を展開する必要があります。各部門は Cisco ISE 内で独自のグループと権限を必要とし、一部の部門は特定のデバイスへのアクセスのみを必要とします。エンジニアはデバイス管理サービスを有効にし、ユーザー ID グループを作成します。
エンジニアは次にネットワーク機器で何を設定する必要があるでしょうか？
A. SNMP設定
B. 高度なTrustSec設定
C. TACACS認証設定
D. RADIUS認証設定
正解: **(**正解を表示します**)**
Device Administration in Cisco ISE uses TACACS+ for authentication and authorization of administrators. After enabling the Device Admin service and configuring identity groups, the network devices must be configured with TACACS authentication settings so they can authenticate admin logins and receive per-department privileges and command sets from ISE.

質問: **59**
ネットワーク エンジニアは、シン クライアントが起動時に PXE を使用してシステム イメージをダウンロードする有線ネットワーク環境で、Cisco ISE を使用して 802.1x を展開する必要があります。スイッチ ポートを構成する必要があるモードはどれですか?
A. 制限あり
B. モニター
C. クローズ
D. 低影響
正解: **(**正解を表示します**)**

質問: **60**
あるエンジニアがWindows 10エンドポイントのポスチャポリシーを設定しており、各ADグループのユーザーが準拠するために満たすべき条件が異なるようにしたいと考えています。
この課題を達成するためには、何をしなければならないのか？
A. 各ADグループに対してシンプルな条件を設定し、各ユースケースの姿勢ポリシーでそれを使用する。
B. 姿勢要件を変更して、ユースケースごとに AD グループを使用し、それらの要件を姿勢ポリシーで使用します。
C. ポリシーセット内の認証ポリシーを使用して、各 AD グループをそれぞれの姿勢ポリシーでグループ化します。
D. さまざまなポリシーに必要なユーザーグループを特定し、それぞれのポリシーを要件にマッピングするサービス条件を作成する。
正解: **(**正解を表示します**)**

質問: **61**
図を参照してください。スイッチのCLIでトラブルシューティング出力を表示するには、どのコマンドを入力しますか？

A. 認証セッションを表示 mac 000e.84af.59af 詳細
B. 認証登録を表示する
C. show authentication interface gigabitethemet2/0/36
D. 認証セッションを表示する方法
正解: (正解を表示します)
show authentication sessions [handle handle-number | interface type number | mac mac-address | method method-name interface type number | session-id session-id]
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

質問: **62**
ある組織が既存のゲストネットワークをCisco ISEに移行しようとしており、現在のデータベースには1000人のゲストユーザーが登録されています。この情報をCisco ISEデータベースに手動で入力するリソースがありません。
この課題を効率的に達成するためには、何をすべきでしょうか？
A. CSVファイルを使用してゲストアカウントをインポートします
B. SOLを使用して既存のデータベースをCisco ISEに接続します
C. JSONファイルを使用してゲストアカウントの移行を自動化します
D. XMLファイルを使用して、既存のフォーマットをCisco ISEのフォーマットに合わせるように変更します。
正解: (正解を表示します)
https://community.cisco.com/t5/network-access-control/ise-2-4-guest-user-import-csv-template- guest-type-and-state/td-p/3686005

質問: **63**
ネットワークエンジニアが、セキュリティグループタグに基づいてトラフィックをフィルタリングする必要のあるネットワークデバイスを、ルーティングされたセキュリティポリシーを使用して構成していますか？
A. cts承認リスト

B. CTSの役割に基づく執行
C. CTSキャッシュを有効にする
D. cts ロールベース ポリシー優先度静的
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16/sec-usr-cts-xe-16-book/sec-cts-sgacl.html

質問: **64**
組織は、スイッチの802 1X構成を標準化し、スイッチポートの静的ACLを削除すると同時に、Cisco ISEがスイッチにどのアクセスを提供するかを通信できるようにしたいと考えています。このタスクを実行するには、何を構成する必要がありますか。
A. 承認ポリシー内のセキュリティグループタグ
B. クライアントのスイッチの拡張アクセスリスト
C. クライアントの情報に基づくスイッチのポートセキュリティ
D. 許可プロファイル内の動的アクセスリスト
正解: **D** (コメントを発表する)
SGTs are usable where Trust Sec is deployed, the question simply asks about a better way of handling ACLs, substitute for Static ACLs should be Dynamic ACLs configured on ISE Authorisation Profiles.
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/212419-configure- per-user-dynamic-access-contro.html

質問: **65**
エンジニアがスタティック SGT 分類を設定しています。認証が無効で、サードパーティのスイッチが使用されている場合、どの構成を使用する必要がありますか?
A. VLAN から SGT へのマッピング
B. IP アドレスから SGT へのマッピング
C. L3IF から SGT へのマッピング
D. サブネットから SGT へのマッピング
正解: (正解を表示します)
The method of sending out IP to SGT mappings from ISE is particularly useful if the access switch does not support TrustSec.
https://community.cisco.com/t5/security-knowledge-base/segmentation-strategy/ta-p/3757424

質問: **66**
管理者は、クライアントプロビジョニングポリシーでCisco ISEポスチャエージェントを設定しており、クライアントと対話するポスチャポリシーが監視されていることを確認する必要があり、エンドユーザはネットワーク使用規則に準拠する必要があります。この目標を達成しますか？ （2つ選択してください）
A. AnyConnect
B. サプリカント
C. Cisco ISE NAC
D. PEAP
E. 姿勢エージェント
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administrati on/guide/b_AnyConnect_Administrator_Guide_4-0/configure-posture.html
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_configure_client_provisioning.html#task_D1C2E8ECE

1D 54D259C01BCBF0A5822F1

質問: **67**
ユーザーがエンドポイントのIPアドレスとMACアドレスを確実にバインドできるように、ARPキャッシュをCisco ISEプロファイルサービスで機能させるには、どの2つのプローブを有効にする必要がありますか？ 2つ選択してください。）
A. NetFlow
B. SNMP
C. HTTP
D. DHCP
E. RADIUS
正解: **(**正解を表示します**)**
Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry the IP addresses and the MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html

質問: **68**
管理者は、802 1Xで使用するためにスイッチポートを構成しています。ポートが音声および複数のデータエンドポイントを許可するために何をする必要がありますか？
A. authenticationhost-modemulti-authコマンドを使用してポートを設定します
B. データデバイスをポートに接続し、その背後に電話を接続します。
C. ポートでコマンドauthenticationhost-modemulti-domainを使用します
D. ハブをスイッチポートに接続して、認証後に複数のデバイスがアクセスできるようにします
正解: **(**正解を表示します**)**
The multi-domain host mode allows both a data device and a voice device to authenticate on the same port (e.g., a phone and a computer). It is commonly used in scenarios where IP phones and computers share a port.

質問: **69**
シスコ デバイスにはマルチ認証モードで設定されたポートがあり、SGT_0422048549 の SGT が割り当てられたホストからの接続のみを受け入れています。VLAN トランク リンクは最大 8 つの VLAN をサポートしています。これらの制限の理由は何ですか?
A. デバイスは、SXP スピーカーとして機能せずにインライン タギングを実行しています。
B. デバイスは、SXP スピーカーとして機能しながら、MIME タギングを実行しています。
C. IP サブネット アドレスは SGT に動的にマッピングされます。
D. IP サブネット アドレスは、SGT に静的にマッピングされます。
正解: **A (**コメントを発表する**)**
The following restrictions are applicable when running Cisco TrustSec in enforcement mode or inline tagging mode. These restrictions do not apply when these switches are used as an SXP speaker:
- An IP subnet address cannot be statically mapped to a Security Group Tag (SGT).
- If a port is configured in multi-authentication mode, all hosts connecting to that port must be assigned the same SGT.
- Cisco TrustSec enforcement mode on a VLAN trunk line supports only up to eight VLANs. If more than eight VLANs are configured on a VLAN trunk link and Cisco TrustSec is enabled on those VLANs.
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/sxp_conf ig.html#Restriction%20for%20SGT%20Exchange%20Protocol

質問: **70**
エンジニアは、システムの状態更新を設定する必要があります。その目的は、事前に定義された最新のチェック項目とオペレーティングシステム情報が更新されていることを確認することです。これらのチェックは定期的に実施する必要があります。
Cisco ISEインターフェースのどの部分で、エンジニアはコンプライアンスモジュールに必要な変更を加えるのでしょうか？
A. 管理 > システム > 設定 > 更新 > スケジュール
B. 管理 > システム > 設定 > 更新 > 姿勢
C. 管理 > システム > 設定 > 姿勢 > 更新
D. 管理 > システム > 設定 > 姿勢 > 更新 > スケジュール
正解: **(**正解を表示します**)**

質問: **71**
分散型Cisco ISE展開では、どのノードがサポートされますか？
A. セッションフェイルオーバー用の管理ノード
B. セッションフェイルオーバー用のポリシーサービスノード
C. PxGridサービスの監視ノード
D. 自動フェイルオーバー用のポリシーサービスノード
正解: **(**正解を表示します**)**

質問: **72**
CiscoISEが作成する2つのデフォルトエンドポイントIDグループはどれですか。 2つ選択してください）
A. ブロックリスト
B. エンドポイント
C. プロファイル
D. 許可リスト
E. 不明
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html Default Endpoint Identity Groups Created for Endpoints Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system. Cisco ISE creates the following endpoint identity groups:
Blacklist--This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are block listed in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
GuestEndpoints--This endpoint identity group includes endpoints that are used by guest users.
Profiled--This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.
RegisteredDevices--This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list.
You can edit, delete, and block these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blocked in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blocked devices to a URL, which displays
"Unauthorised Network Access", a default portal page to the blocked devices.

Unknown--This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.
In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled identity group:
Cisco-IP-Phone--An identity group that contains all the profiled Cisco IP phones on your network.
Workstation--An identity group that contains all the profiled workstations on your network.

質問: **73**
ネットワーク管理者がCisco ISEにネットワークアクセスデバイスを追加します。セキュリティ侵害が発生した後、管理チームはすべてのネットワークデバイスが特定の基準に準拠することを義務付けます。すべてのネットワークデバイスはCisco ISEを介して認証を行う必要があります。一部のデバイスは、デフォルト以外のCoAポートを使用します。
Cisco ISEで設定する必要がある項目は何ですか？
A. 指定されたポートを備えたネットワークデバイス
B. ポートが指定されたネットワークアクセスマネージャ
C. ポートが指定されたネットワークデバイスグループ
D. ポートが指定されたネットワークデバイスプロファイル
正解: **(**正解を表示します**)**
In Cisco ISE, network access devices (NADs) are individually configured under the Network Devices section. Each network device entry includes details such as IP address, shared secret, and optional ports for RADIUS and CoA (Change of Authorization) communications.
Since some of the devices are using nondefault CoA ports, the administrator must specify the correct port information for each device. This configuration ensures that Cisco ISE can properly communicate with and manage these devices using the appropriate CoA port settings.

質問: **74**
802.1X認証を有効にするには、どのインターフェースレベルのコマンドが必要ですか？
A. dot1x pae認証器
B. dot1xシステム認証制御
C. 認証ホストモードシングルホスト
D. aaa server radius dynamic-author
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/dot1x.html

質問: **75**
ドラッグアンドドロップ問題
エンジニアは、Cisco ISE のローカル内部データベースに新しいユーザーを設定し、そのユーザーが Cisco ISE ネットワーク上のリソースとサービスにアクセスできるようにする必要があります。左側の設定手順を右側の手順にドラッグアンドドロップしてください。

Click Identities, and then click Users.	Step 1
Click Add (+) to create a new user.	Step 2
Enter the user details, and then click Save.	Step 3
Click Administration, and then click Identity Management.	Step 4

正解:

Click Administration, and then click Identity Management.

Click Identities, and then click Users.

Click Add (+) to create a new user.

Enter the user details, and then click Save.

質問: **76**

RADIUSとTACACS+の　違いは何ですか？

A. RADIUSはAAを分離し、TACACS+は　認証と認可を組み合わせます。

B. RADIUSはマルチプロトコルをサポートしていますが、TACACS+はIP　のみをサポートしています。

C. RADIUSはUDPポート1812と1813を使用し、TACACS+はUDP　　ポート1645と1646を使用します。

D. RADIUSはパスワードのみを暗号化し、TACACS+は　すべてのパケットを暗号化します。

正解: **(**正解を表示します**)**

One key difference between RADIUS and TACACS+ lies in their encryption mechanisms and the scope of their encrypted data:

RADIUS:

Encrypts only the password field in the packet.

■

The rest of the packet, including attributes such as usernames, accounting information, and

■

authorization data, is sent in cleartext.

Uses UDP ports 1812 for authentication and 1813 for accounting (originally 1645 and 1646 for

■

older implementations).

Primarily focuses on authentication and accounting, with limited control over authorization.

■

TACACS+:

Encrypts the entire packet (except the header), ensuring that all sensitive data, including

■

usernames and accounting information, is secure.
Uses TCP port 49, which provides reliable transmission and ensures packet delivery.
■
Separates authentication, authorization, and accounting (AAA) functions, offering granular
■
control over each phase.

質問: **77**
ネットワーク管理者は、クライアントマシンのクライアントプロビジョニングリソースポリシーを構成しており、ネットワークに接続しようとするときに、エージェントポップアップがクライアントに表示されることを確認する必要があります。これを可能にするために追加する必要のある構成項目はどれですか。
A. 承認ポリシーのクライアントプロビジョニングURL
B. システムにインストールされる一時的なエージェント
C. ネットワーク接続をプロキシするリモートポスチャエージェント
D. クライアントへのAPI接続
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_configure_client_provisioning.html#ID1405 It is mandatory to include the client provisioning URL in authorization policy to enable the agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

質問: **78**
エンドポイントを正常に認証するには、Cisco ISEとネットワークアクセスデバイスの間で何を一致させる必要がありますか？
A. SNMPバージョン
B. 共有秘密
C. 証明書
D. プロファイル
正解: **(**正解を表示します**)**
https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_network_devices.html

質問: **79**
エンジニアがCiscoISEを実装しており、802.1Xを設定する必要があります。ポート設定は、ポートベースの認証用に構成されています。この構成を完了するには、どのコマンドを使用する必要がありますか？
A. dot1x pae authenticator
B. dot1x system-auth-control
C. authentication port-control auto
D. aaa authentication dot1x default group radius
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26.pdf

質問: **80**
ネットワーク上のスイッチへのデバイス管理アクセスを提供するために、ポリシーが作成されています。セッションがアクティブに使用されていない場合、10分後にセッションが切断されることを確認する必要があります。この要件を満たすには、どのタスクを構成する必要がありますか？
A. セッションタイムアウト
B. アイドル時間
C. 属性を次のように設定します
D. モニター
正解: **(**正解を表示します**)**

質問: **81**
エンジニアが新しいCisco ISEノードを設定しています。このノードでは、TACACS+経　由でネットワークデバイスへのアクセス認証要求を処理するために、デバイス管理サービスを実行する必要があります。この機能を実行するには、このノードでどのペルソナを有効にする必要がありますか？
A. 管理
B. モニタリング
C. pxGrid
D. ポリシーサービス
正解: **(**正解を表示します**)**

質問: **82**
スタンドアロンの Cisco ISE ノード展開の制限は何ですか?
A. ポリシー サービス ペルソナのみをノードで無効にできます。
B. インストール後にノードのドメイン名を変更することはできません。
C. ペルソナはデフォルトで有効になっており、ノードで編集することはできません。
D. インストール後にノードのホスト名を変更することはできません。
正解: **(**正解を表示します**)**
After you install a Cisco ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas run on it. This node is in a standalone state. You must log in to the Admin portal of the Cisco ISE node to configure it. You cannot edit the personas or services of a standalone Cisco ISE node. You can, however, edit the personas and services of the primary and secondary Cisco ISE nodes. You must first configure a primary ISE node and then register secondary ISE nodes to the primary ISE node.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010.html

質問: **83**
あるエンジニアが、キャンパス全体に有線802.1Xネットワークを構築するプロジェクトを開始した。課題は、認証失敗をCisco ISEにログ記録すると同時に、ユーザーへの影響を最小限に抑えることである。
エンジニアはどのコマンドを設定する必要がありますか？
A. 認証オープン
B. モニターモードが有効
C. 認証ホストモードマルチ認証
D. pae dot1x が有効
正解: **(**正解を表示します**)**

質問: **84**
図を参照してください。このスイッチ構成は、どのようなシナリオに適用されますか？

A. IP電話認証を通過する際
B. 複数のIP電話を接続する場合
C. ハイパーバイザーを使用するユーザーを防止する場合
D. 複数のクライアントが接続されたハブを許可する場合
正解: **(**正解を表示します**)**

質問: **85**
1つの環境に2つのCiscoISEノードが設定されている場合の展開モードは何ですか。
A. 配布
B. アクティブ
C. スタンドアロン
D. 標準
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010.html

質問: **86**
管理者は、エンドポイントのブラウザバージョンに基づいて、アプリケーションのIPアドレスへのアクセスを制限する必要があります。Cisco ISEプロファイリングサービスとQuestポータルアクセスは、ユーザーエージェントをキャプチャするように構成する必要があります。デバイスセンサー機能を使用してCiscoスイッチからエンドポイントの情報を取得します。以下の構成が実行されました。
- Cisco ISEにスイッチを追加しました
- スイッチにデバイスセンサーを設定しました
Cisco ISEポータルへのアクセスを有効にしました
- ユーザーエンドポイントをCisco ISEポータルに接続するように設定しました
設定を完了するには、次にどのタイプのプローブを有効にする必要がありますか？
A. 半径
B. DHCP
C. SNMP
D. ネットフロー
正解: **(**正解を表示します**)**
Capturing the User-Agent string for profiling requires the RADIUS probe, because User-Agent information is learned from RADIUS authentication exchanges and from Device Sensor RADIUS accounting attributes sent by the switch. Enabling the RADIUS probe allows ISE to receive and use this browser-based profiling data.

質問: **87**
Cisco ISE ノードから MAB ユーザに非アクティブ アクティブ タイマーを動的に割り当てるために使用される RADIUS 属性はどれですか?
A. セッションタイムアウト
B. アイドル タイムアウト
C. 半径サーバーのタイムアウト
D. 終了アクション
正解: **(**正解を表示します**)**
When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When the inactivity timer expires, the switch removes the authenticated session. The inactivity timer for MAB can be statically configured on the switch port, or it can be dynamically assigned using the RADIUS Idle-Timeout attribute

質問: **88**
デフォルトでは、802.IX対応スイッチは認証前にどのトラフィックを許可しますか？
A. スイッチのデフォルトACLで許可されているトラフィック
B. Cisco ISEのポートdACLで許可されたトラフィック
C. すべての交通
D. 交通渋滞なし
正解: **A (**コメントを発表する**)**

質問: **89**
セキュリティチームは、MACアドレス00:47:44:40:54:1Aを持つ不正なエンドポイントがネットワークに接続されていることを特定しました。このエンドポイントのネットワークアクセスを効果的に制限するために、セキュリティエンジニアはCisco ISE内でどのような操作を行う必要がありますか？
A. MACアドレスをエンドポイント隔離リストに追加します。
B. アクセスを拒否するための認証ポリシーを実装します。
C. 再認証を強制する認証ポリシーを作成します。
D. ネットワークスイッチのアクセス制御リストを設定してトラフィックをブロックします。
正解: **(**正解を表示します**)**

質問: **90**
ReAuth に対して CoA がグローバルに有効になっている場合、エンドポイントの CoA をトリガーする 2 つのイベントはどれですか (2 つ選択してください)。
A. エンドポイント dACL を更新しています。
B. Apple-Device から Apple-iPhone へのエンドポイント プロファイルの遷移
C. マイデバイスポータルへのエンドポイントの追加
D. エンドポイントがマイデバイスポータルで紛失としてマークされました
E. エンドポイント プロファイルが不明から Windows 10 ワークステーションに移行しました
正解: **(**正解を表示します**)**

質問: **91**
図を参照してください。ネットワークエンジニアが、Cisco ISCサーバーからダウンロード可能なACLを受け入れるようにスイッチを設定している様子を示しています。
設定を完了するには、どの2つのコマンドを実行すればよいですか？(2つ選択してください)

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
```

A. aaa authorization auth-proxy default group radius
B. RADIUSサーバーVSA Sand認証
C. radius-server属性8 include-in-access-req
D. IPデバイス追跡
E. dot1xシステム認証制御
正解: **(**正解を表示します**)**
radius server vsa send authentication is enabled by default on IOS 15.X and later versions.
To configure a switch to accept downloadable ACLs from a Cisco ISE server, the following two commands are required:
ip device tracking: This command enables the switch to track IP device information, which is needed for the ISE server to provide dynamic access policies based on a device's IP address.
dot1x system-auth-control: This command enables 802.1X authentication on the switch and allows the switch to forward authentication requests to the ISE server.

質問: **92**
管理者は、ネイティブ サプリカント プロファイルを Cisco ISE ポスチャ エージェントで使用するように設定しており、有線デバイスを使用して接続をテストして、使用可能なプロファイル設定を判断する必要があります。このタスクを実行するには、どの 2 つの構成設定を使用する必要がありますか? 2つ選んでください。）
A. 許可されたプロトコル
B. プロキシ ホスト/IP
C. 認証モード
D. セキュリティ
E. 証明書テンプレート
正解: **A,E (**コメントを発表する**)**

質問: **93**
ネットワーク管理者は現在、Cisco ISEを使用して、8021Xを介してデバイスとユーザーを認証しています。EAP-TLSを使用してデバイスとユーザーを認証する必要もあります。これを実現するには、CiscoISEで構成する必要のある2つの追加コンポーネントはどれですか。2つ選択してください。）
A. ネットワークデバイスグループ
B. CAサーバにマップするシリアル番号属性
C. IDストアにマップする共通名属性
D. 証明書認証プロファイル
E. EAP認証プロファイル
正解: **(**正解を表示します**)**

Certificate Authentication Profile: A Certificate Authentication Profile needs to be configured in Cisco ISE. This profile specifies the requirements for client certificates, such as certificate types, acceptable certificate authorities (CAs), and other certificate validation criteria.
EAP Authorization Profile: An EAP Authorization Profile must be configured in Cisco ISE. This profile defines the authorization policies and access privileges for devices and users authenticated using EAP-TLS. It specifies the network resources, VLAN assignments, and other attributes that should be applied to the authenticated devices and users.

質問: **94**
ゲスト ポータルを構成するときにゲスト アクセス経由でインターネットにアクセスできることを確認するために検証する必要がある 2 つのアクションはどれですか? （2つ選んでください。）
A. ゲスト ユーザーがブラウザを開くと、認証ページにリダイレクトされます。
B. ゲスト デバイスは正しい SSID に正常に関連付けられます。
C. ゲスト デバイスは、WLAN で内部ネットワークにアクセスできます。
D. Cisco ISE は、ゲスト認証が成功すると CoA を送信します。
E. ゲスト デバイスは、ネットワーク ファイル共有に接続できます。
正解: **A,D (**コメントを発表する**)**

質問: **95**
管理者は、ネットワークを通過するトラフィックに関するメタデータ情報を収集して、ホストの可視性を高めようとしています。この情報は、ネットワークアクセスポリシーを使用できるように、CiscoISEを使用するデバイスのプロファイリングポリシーを作成するために使用されます。このタスクを実行するには何をする必要がありますか。
A. CiscoISE内でRADIUSプロファイリングプローブを設定します
B. CiscoISEアプライアンスに送信されるようにNetFlowを設定します。
C. CiscoISEアプライアンスで使用するようにSNMPを設定します
D. CiscoISE内でDHCPプローブを設定します
正解: **(**正解を表示します**)**
DHCP can be one of the most useful data sources for an endpoint device. A primary use of DHCP in profiling has been to capture the device MAC address, but it can also be used to capture other probes as well. The true value in the DHCP probe is that many other attributes can be gleaned to help identify the type of endpoint. As HTTP carries User-Agent field, DHCP requests carry a Class-Identifier field that helps identify the operating system of a device. Some organizations have been known to use a custom DHCP Class-Identifier string to help identify a device as a corporate asset.

質問: **96**
50,000 を超える同時アクティブ エンドポイントを持つ企業に推奨される Cisco ISE 導入モデルはどれですか?
A. 専用 PSN を備えたプライマリおよびセカンダリ PAN/MnT/pxGrid ノードによる中規模展開
B. すべてのペルソナを実行する完全に分散されたノードによる大規模な展開
C. 共有 PSN を持つプライマリおよびセカンダリ PAN/MnT/pxGrid ノードによる中規模展開
D. 1 つのプライマリ ノードと 1 つのセカンダリ ノードですべてのペルソナを実行する小規模な展開
正解: **(**正解を表示します**)**

質問: **97**
Cisco ISEハードウェアアプライアンスでゼロタッチプロビジョニングを行うには、どのメディアタイプを使用する必要がありますか？
A. バーチャルメディア
B. ネットワーク
C. USB
D. CD/DVD

正解: **C** (コメントを発表する)
Cisco ISE hardware appliances support zero-touch provisioning using a USB drive that contains the required configuration file. This is the mandatory media type for ZTP on ISE physical appliances.

質問: **98**
Cisco ISEモニタリングノードについて、正しくない記述はどれですか？
A. ローカルコレクターエージェントは、自身およびポリシーサービスノードにログを送信するように構成されているすべてのNADからローカルにログを収集します。
B. ローカルコレクターエージェントプロセスは、インライン姿勢ノードのみを実行します。
C. Cisco ISEは、すべてのノードにわたる分散ログ収集をサポートし、ローカルデータの収集、集約、集中相関、およびストレージを最適化します。
D. ローカルコレクターバッファは、収集したデータをsyslogとして指定されたCisco ISEモニタリングノードに転送します。モニタリングノードが管理画面でグローバルに定義されると、ISEノードは自動的に設定されたモニタリングノードの1つまたは両方にログを送信します。
正解: (正解を表示します)

質問: **99**
NetFlow バージョン 9 プローブに Cisco ISE が使用するデフォルト ポートは何ですか?
A. UDP 9999
B. UDP 9996
C. UDP 9998
D. UDP 9997
正解: (正解を表示します)

質問: **100**
組織は、Oseo ISEでのプロファイリングを改善するために、システムに新しいプロファイリングプローブを追加しています。プローブは、エンドポイントとそれらが接続されているポートに関する情報を受信するための共通のネットワーク管理プロトコルをサポートする必要があります。これを実現するには、ネットワークデバイスで何を構成する必要がありますか。ゴール？
A. ARP
B. SNMP
C. WCCP
D. ICMP
正解: **B** (コメントを発表する)
https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hId-790343135

質問: **101**
EAP-TLSとPEAP-TLSをサポートする2つの外部IDストアはどれですか？ 2つ選択してください。）
A. Active Directory
B. RADIUS トークン
C. 内部データベース
D. RSA SecurID
E. LDAP
正解: **A,E** (コメントを発表する)
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure- eap-tls-authentication-with-is.html

質問: **102**
Cisco ISEのデフォルトの管理者ログイン名とパスワードは何ですか？
A. admin/admin
B. ISEAdmin/admin
C. admin/cisco
D. admin/デフォルトパスワードなし--adminパスワードはセットアップ時に設定されます
正解: **(**正解を表示します**)**

質問: **103**
エンジニアは、Cisco Temporal Agentワークフローを使用してポスチャポリシーを設定する必要があります。要件を満たすために、エンジニアはどの2つの設定を適用する必要がありますか？(2つ選択してください。)
A. セキュアクライアントポスチャモジュールを設定します。
B. クライアントプロビジョニングポリシーを設定します。
C. 姿勢要件を作成します。
D. 姿勢条件を作り出す。
E. クライアントプロビジョニングリソースを設定します。
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/admin_guide/b_ise_admin_3_1/b_ISE_admin_31_compliance.html#AnyConnect_Temporal_Ag ent_Workflow_For_Windows

質問: **104**
BYOD(私物端末の業務利用)用の証明書を設定する際に考慮すべき点は何ですか？
A. Cisco ISE BYODにはエンドポイント証明書が必須です
B. AndroidエンドポイントはESTを使用するが、他のオペレーティングシステムは登録にSCEPを使用する
C. CNフィールドにはエンドポイントホスト名が入力されます。
D. SANフィールドにはエンドユーザー名が入力されます
正解: **C (**コメントを発表する**)**
When configuring certificates for Bring Your Own Device (BYOD), it is important to consider populating the CN (Common Name) field with the endpoint host name. The CN field should contain the host name or FQDN (Fully Qualified Domain Name) of the endpoint device. This allows the certificate to be properly validated when the device connects to the network. The CN field helps ensure that the device is correctly identified and authorized for network access.

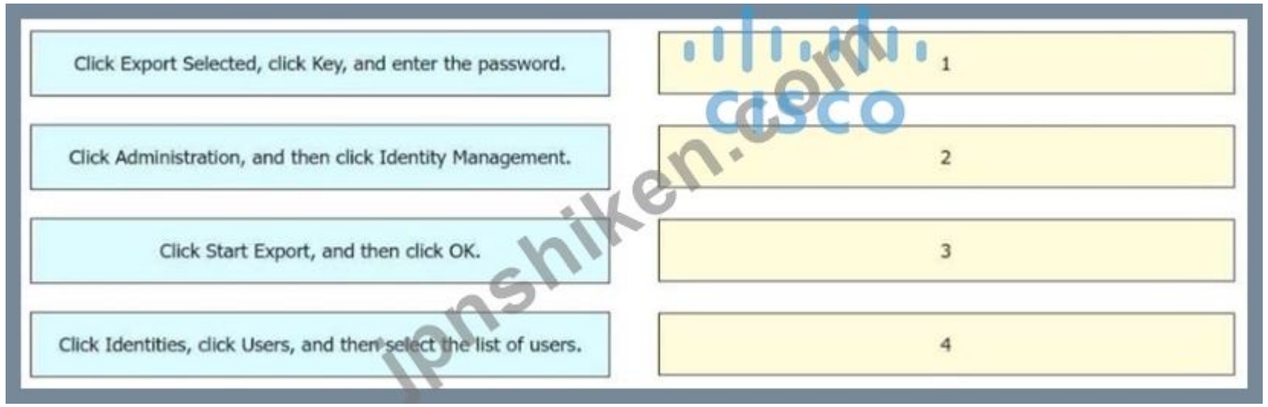
質問: **105**
エンジニアは、Cisco TrustSec ポリシーを適用するように Cisco ISE および Cisco Catalyst スイッチを設定します。エンジニアは、新しいデバイスに対して、ステージング、プレプロダクション、およびプロダクションの各環境で TrustSec ポリシーを展開することにより、無停止の展開方法を使用する必要があります。設定を完了するには、どの操作を実行する必要がありますか？
A. ステージング、プレプロダクション、プロダクションの各ステージで、新しいデバイスに異なるセキュリティグループタグを設定します。
B. Cisco ISEでポリシーマトリックスを設定し、新しいデバイスをポリシーマトリックスに割り当てます。
C. 新しいデバイスでセキュリティグループタグ交換プロトコルを設定し、デバイスをグループとしてCisco ISEと統合します。
D. 新しいデバイスをステージング、プリプロダクション、およびプロダクションのネットワークデバイスグループに統合します。
正解: **(**正解を表示します**)**

質問: **106**

あるエンジニアは、Cisco ISEのGUIからエンドポイントIDグループの管理を容易にしたいと考えている。
Cisco ISE の [ID 管理] メニューから、エンジニアは名前に 「Android」を含むエンドポイント ID グループを一覧表示できる必要があります。エンジニアはどのタスクを実行する必要がありますか？
A. 名前が 「Android」と等しいという条件で高度なフィルターを作成して保存します。
B. 名前が 「Android」と等しいという条件でクイックフィルターを作成して保存します。
C. Android という名前のアイデンティティ グループを作成し、親グループを profiled に設定します。
D. Android という名前の ID グループを作成し、そのグループに Android デバイスのみを追加します。
正解: (正解を表示します)

質問: **107**
管理者は、Cisco ISEプロファイラサービスを使用して、特定のデバイスタイプとオペレーティングシステムバージョンを持つレガシーWindowsエンドポイントにネットワークアクセスを提供する必要があります。ISEプロファイラサービスとアクセススイッチは、DHCPトラフィックのdhcp-class-identifier属性とparameters-request-list属性を使用してエンドポイントを識別するように構成する必要があります。以下の構成が実行されました。
Cisco ISEでDHCPプローブを有効にしました
Cisco ISE PSNインターフェイスをDHCPパケットを受信するように設定しました。
- カスタムプロファイリング条件で属性を設定しました
- カスタムプロファイリングポリシーを設定しました
- アクセスを許可する認証ルールを設定しました
どの操作を行うと設定が完了しますか？
A. Cisco ISE PSNインターフェイスを設定して、SPAN DHCPトラフィックを受信するようにします。
B. スイッチを設定して、DHCP トラフィックのコピーを Cisco ISE PSN に送信するようにします。
C. Cisco ISEプライマリサーバーでDHCP SPANプローブを有効にします。
D. スイッチを設定して、DHCP パケットを Cisco ISE PSN に中継します。
正解: (正解を表示します)
To ensure Cisco ISE receives the necessary DHCP traffic for profiling, the access switches must be configured to send copies of DHCP traffic to the Cisco ISE Policy Service Node (PSN). This enables ISE to analyze DHCP attributes and accurately profile the endpoints.

質問: **108**
ドラッグアンドドロップ問題
エンジニアは、Cisco ISEで現在設定されているユーザーを含む、パスワードC1$c0438563935で暗号化されたCSV形式のファイルをエクスポートする必要があります。このタスクを完了するには、左側の手順を右側の手順にドラッグアンドドロップしてください。



正解:

質問: **109**
管理者が新しい Cisco ISE PSN を分散展開に追加しました。管理者が認証要求を受け入れてエンドポイントを正しくプロファイリングし、それらをそれぞれのエンドポイント ID グループに追加するために有効にする必要がある 2 つの機能はどれですか? (2つ選択)
A. セッション サービス
B. エンドポイント属性フィルター
C. ポスチャ サービス
D. プロファイリング サービス
E. 半径サービス
正解: **A,D (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html#reference_94D3872F7DED4522909A3FF3ECFCDB23
Policy Service Check this check box to enable any one or all of the following services:

Enable Session Services: Check this check box to enable network access, posture, guest, and client-provisioning services.
Enable Profiling Service: Check this check box to enable the Profiling service.

質問: **110**
管理者は、ISEを外部認証ソースとしてActive Directoryに接続し、ファイアウォールを通過する適切なポートを許可する必要があります。このタスクを実行するには、どの2つのポートを開く必要がありますか？ （2つ選択してください）
A. TELNET 23
B. LDAP 389
C. HTTP 80
D. HTTPS 443
E. MSRPC 445
正解: (正解を表示します)
These are the important ports to open in AD implementation.
https://cloudinfrastructureservices.co.uk/active-directory-ports/

質問: **111**
ネットワークアクセス制御を提供するための新しいCisco ISEインフラストラクチャが構築されています。Cisco Discovery Protocolを使用する場合、Cisco ISEによるプロファイリングに関連してどのような情報が収集されますか？
A. RADIUSセッション属性
B. デバイスID
C. DHCPセッション属性
D. アイデンティティグループ
正解: (正解を表示します)

質問: **112**
エンジニアはゲストパスワードポリシーを構成しており、ブルートフォース攻撃を軽減するためにパスワードの複雑さの要件が設定されていることを確認する必要があります。このポリシーを完了する2つの要件はどれですか？ （2つ選択してください）
A. パスワードの最小長
B. gpasswordの有効期限
C. アクティブなユーザー名の制限
D. アクセスコード制御
E. ユーザー名の有効期限
正解: (正解を表示します)

質問: **113**
組織がスイッチポートにローカルでSGACLを設定しているにもかかわらず、役員グループのユーザーがネットワークに接続すると、想定とは異なるレベルのネットワークアクセス権限が付与されてしまう場合があります。Cisco ISEが認証フェーズ後にSGACLをスイッチにプッシュする際、スイッチはどのようにしてユーザーにどのアクセス権限を付与するかを決定するのでしょうか？
A. 動的にダウンロードされたポリシーは、すべての場合においてローカルポリシーを上書きします。
B. 政策は統合されますが、地方政策が優先されます。
C. ポリシーは統合されますが、動的にダウンロードされたポリシーが優先されます。

D. ローカルポリシーは、すべての場合において動的にダウンロードされたポリシーよりも優先されます。
正解: (正解を表示します)

質問: **114**
CiscoISE分散環境内の管理者が担う2つの役割はどれですか。 2つ選択してください。）
A. スタンバイ
B. プライマリ
C. セカンダリ
D. バックアップ
E. アクティブ
正解: (正解を表示します)

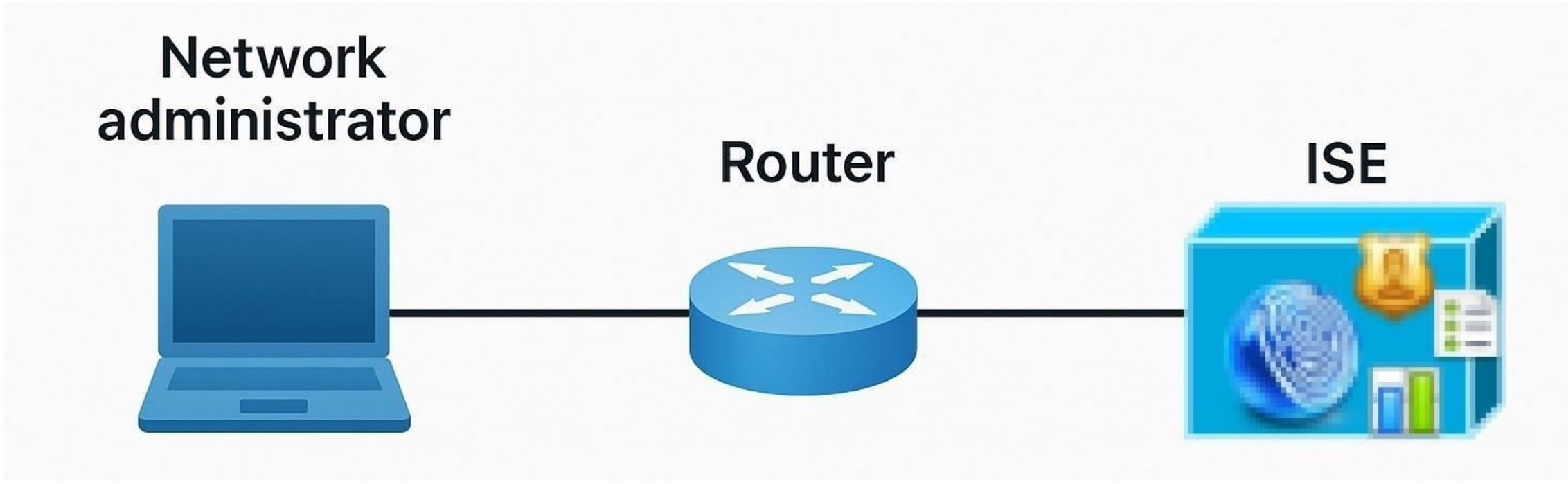
質問: **115**
あるエンジニアが、企業向けに新しいCisco ISE環境を導入しています。企業は、この導入環境でTACACS+を　使用することを希望しています。エンジニアは、Cisco ISEにデバイス管理ライセンスが付与されていることを確認しました。TACACS+の　動作を有効にするには、何を設定する必要がありますか？
A. デバイス管理ワークセンター
B. デバイス管理展開設定
C. デバイス管理サービス
D. デバイス管理者ポリシー設定
正解: (正解を表示します)
The Device Admin service must be explicitly enabled on the Cisco ISE node to activate TACACS+ functionality. Even with a Device Administration license installed, TACACS+ operations will not run until this service is turned on under the node's service settings.

質問: **116**
TACACS+とRADIUS　の違いは何ですか？(2つ選択してください。)
A. TACACS+ はコネクション指向トランスポートを使用し、RADIUS はコネクションレストランスポートを使用します。
B. TACACS+は　パスワードのみを暗号化し、RADIUSはパケットペイロード全体を暗号化します。
C. TACACS+は　複数のプロトコルをサポートしますが、RADIUSはIPトラフィックのみをサポートします。
D. TACACS+ は 802.1X ネットワークアクセス制御をサポートし、RADIUS は MAB のみをサポートします。
正解: (正解を表示します)

質問: **117**
管理者は、8021XをバイパスしてMABを使用することになっているエンドポイントのトラブルシューティングを行っています。エンドポイントは802.1Xをバイパスし、MABを使用してネットワークアクセスを正常に取得しています。ただし、エンドポイントはIPアドレスを取得できないため、通信できません。何が問題ですか？
A. CiscoISEのDHCPプローブが期待どおりに機能していません。
B. 802.1Xタイムアウト期間が長すぎます。
C. エンドポイントがCiscoISEで認証するために間違ったプロトコルを使用しています。
D. ポートのACIがHTTPトラフィックをブロックしています
正解: (正解を表示します)
Based on numerous deployment experiences, the recommendation is to set the tx-period value to

10 seconds to provide the most optimal time for MAB devices. Setting the value below 10 seconds may result in unwanted behavior, and setting the value greater than 10 seconds may result in DHCP timeouts.

質問: **118**
ドラッグアンドドロップ問題
図を参照してください。エンジニアは、ルーターにサインインするすべての管理者に対して、Cisco ISEをTACACS+サー バーとして使用できるよう設定する必要があります。ユーザーは、TACACS+サー バー経由でTelnet パスワードを変更できる必要があります。左側の設定手順を右側の手順にドラッグアンドドロップしてください。



Enable Password Change Control.	step 1
Open Work Centers, open Device Administration, and then open Settings.	step 2
Select Enable Telnet Change Password.	step 3
Open the Session Key Assignment tab, and then click Save.	step 4

正解:

Open Work Centers, open Device Administration, and then open Settings.

Enable Password Change Control.

Select Enable Telnet Change Password.

Open the Session Key Assignment tab, and then click Save.

質問: **119**
図を参照してください。エンジニアが、802.1Xをサポートしていないプリンタを含むネットワークに802.1Xを導入しようとしています。現在のCisco IOSスイッチのポート構成を図に示します。
プリンターの認証を可能にするために、他にどのコマンドが必要ですか？

```
switchport mode access
switchport access vlan 10
switchport voice vlan 20
authentication event fail action next-method
authentication host-mode multi-auth
authentication order mab dot1x
authentication port-control auto
authentication violation restrict
snmp trap mac-notification change added
snmp trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 10
snmp trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 10
```

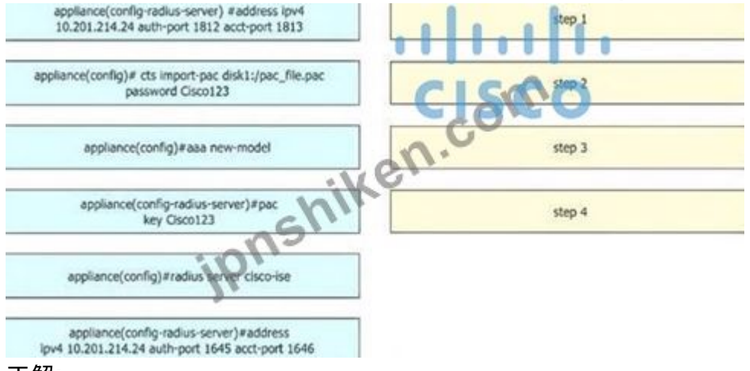
A. dot1q
B. dotx
C. mac
D. 息子
正解: **D** (コメントを発表する)
The command mab needs to be added to enable MAC Authentication Bypass, which allows devices that don't support 802.1X (like printers) to authenticate using their MAC address instead.
The config already has authentication order mab dot1x (telling the switch to try MAB first, then
802.1X), but without the mab command explicitly enabled on the interface, MAB won't actually run.

質問: **120**
エンジニアは、802.1Xをサポートしないcisco IP電話にネットワークアクセスを提供するために、Cisco ISEプロファイラサービスを使用する必要があります。Cisco ISEは、アクセススイッチデバイスのセンサー情報システム記述とプラットフォームタイプを使用してCisco IP電話をプロファイリングし、アクセスを許可するように構成されています。
スイッチの設定を完了するには、どの2つのプロトコルを設定する必要がありますか？(2つ選択してください。)
A. SNMP
B. EAPOL
C. LLDP
D. STP
E. CDP
正解: **C,E** (コメントを発表する)
A Device Sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by the Device Sensor can come from these protocols:
- CDP
- LLDP
- DHCP
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure- Device-Sensor-for-ISE-Profilin.html

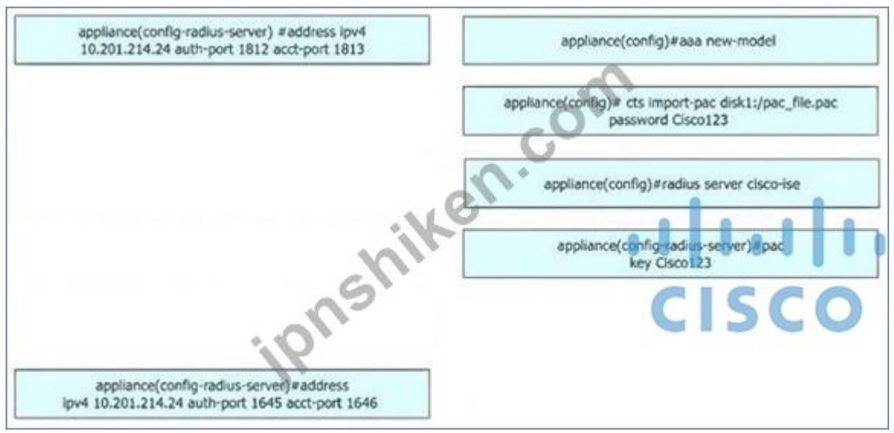
質問: **121**
管理者は、Cisco Adaptive Security ApplianceファイアウォールにSSHを使用してアクセスするユーザーを認証するようにCisco ISEを設定する必要があります。ソリューションは以下の要件を満たす必要があります。

- ユーザー認証にはローカルのCisco ISEデータベースを使用する必要があります
- ユーザーが実行するASAコマンドは検証されなければならない
以下の設定が実行されました。
Cisco Adaptive Security Applianceファイアウォールを追加しました
- 設定済みのユーザーアカウント
Cisco ISEでデバイス管理サービスを有効にする
TACACSプロファイルを設定しました
- 認証ポリシーを設定しました
- Cisco Adaptive Security Applianceファイアウォールを設定しました
認証と認可
Cisco ISEで必ず実行しなければならない操作はどれですか？(2つ選択してください。)
A. ユーザーIDグループを設定します。
B. 認証プロファイルを設定します。
C. ローカル認証を有効にする。
D. TACACSコマンドセットを設定します。
E. 認証プロファイルを設定します。
正解: **(**正解を表示します**)**

質問: **122**
ドラッグアンドドロップ問題
セキュリティエンジニアがCisco CatalystスイッチをCisco TrustSecを使用するように設定します。エンジニアは、スイッチをCisco ISEで認証するためのPACキーを定義する必要があります。左側のコマンドを右側にドラッグアンドドロップして順番に並べ替えてください。すべてのオプションを使用するわけではありません。



正解:



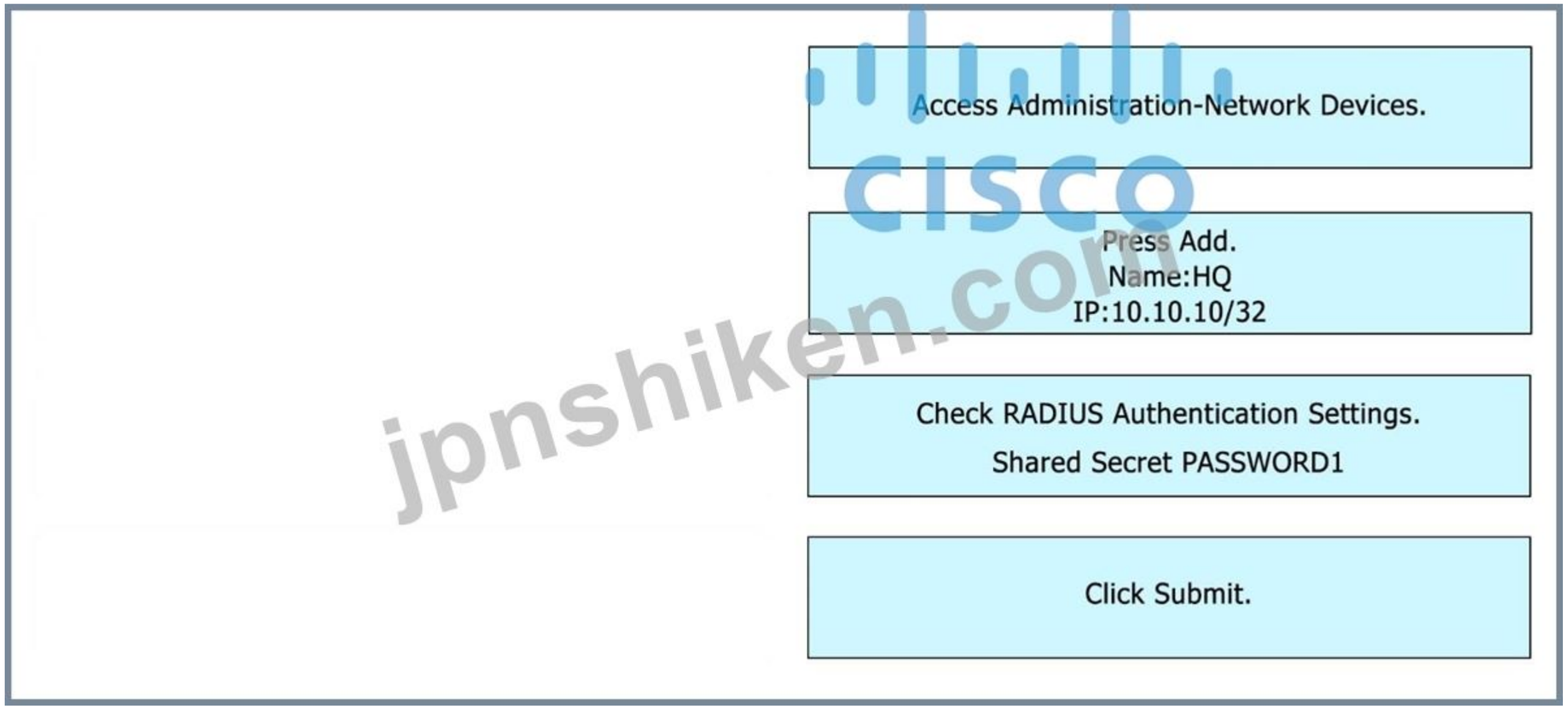
質問: **123**
エンジニアが802.1Xを構成し、ポリシーセットをテストしています。認証後、一部のエンドポイントにはアクセス拒否メッセージが表示されますが、ネットワークへのアクセスは引き続き許可されます。この問題が発生する原因は何ですか？
A. エンドポイントの認証結果には、アクセスを許可するdACLが含まれます。
B. スイッチポートは、認証イベントサーバーのデッドアクション許可VLANで構成されています。
C. エンドポイントの認証結果には、信頼できるセキュリティグループタグが含まれます。
D. スイッチポートは認証を開いた状態で構成されています。
正解: **(**正解を表示します**)**

質問: **124**
Cisco IOS デバイスで Cisco TrustSec を設定する際、エンジニアはデバイス同士が認証できるように、CTS デバイス ID とパスワードを設定する必要があります。しかし、設定が完了しても、デバイスが正しく認証されない場合があります。デバイス ID とパスワードが正しいにもかかわらず、このような問題が発生する原因は何でしょうか？
A. EAP-FASTが有効になっていません。
B. SGTマッピングは定義されていません。
C. デバイスエイリアスが一致しません。
D. デバイスに構成 cts 認証情報 trustsec verify 1 がありません。
正解: **(**正解を表示します**)**
The Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST.

質問: **125**
ドラッグアンドドロップ問題
ネットワークエンジニアは、TACACS+デ　バイス管理のために、HQ-IDF100という名前のCiscoスイッチをCisco ISEに追加する必要があります。共有シークレットはPASSWORD1、IPアドレスは10.10.10.10です。
左側の設定手順を右側の手順にドラッグ＆ドロップしてください。

Press Add. Name:HQ IP:10.10.10/32	step 1
Access Administration-Network Devices.	step 2
Check RADIUS Authentication Settings. Shared Secret PASSWORD1	step 3
Click Submit.	step 4

正解:



質問: **126**
Cisco ISEでレポートを確認する際、TACACS+認　証とRADIUS認証のどちらが優れている点は何ですか？
A. TACACS+はIPsec　で安全な通信を行い、RADIUSはDTLS暗号化を使用します。
B. TACACS+ は認証遅延を削減し、RADIUS は追加のパケット ヘッダーを追加することで遅延を増加させます。
C. TACACS+ はコマンド アカウンティングを提供し、RADIUS は認証と認可を組み合わせます。
D. TACACS+ は SSL 証明書を使用しますが、RADIUS は暗号化機能を持っていません。
正解: **(**正解を表示します**)**
TACACS+ provides command accounting, allowing Cisco ISE to log every command executed by an administrator, which is highly useful for audit and compliance reports. In contrast, RADIUS combines authentication and authorization in a single process and does not support per- command accounting. This makes TACACS+ preferable for detailed administrative activity reporting.

質問: **127**
ネットワークセキュリティ管理者は、Cisco ISEをActive Directoryと統合する必要があります。管理者は休暇操作を実行する必要があります。この要件を満たすために、Active Directoryでどのような操作が必要ですか？
A. ドメインからISEマシンアカウントを削除します。
B. ドメインからISEユーザーアカウントを削除します。
C. ドメインにISEマシンアカウントを作成します。
D. Active Directory を検索して、管理者ユーザーアカウントが存在するかどうかを確認します。
正解: **(**正解を表示します**)**

Remove the ISE machine account from the domain.
This is the correct action because the machine account represents Cisco ISE in AD. Removing it effectively disconnects ISE from the domain.

質問: **128**
Cisco ISE は、ポスチャとクライアント プロビジョニング用の管理者証明書をどのポートに提示しますか?
A. TCP/8000
B. TCP/8080
C. TCP/8905
D. TCP/8999
正解: **C (**コメントを発表する**)**
Cisco ISE presents the Admin certificate for posture and client provisioning on TCP port 8905.
This port is used to securely communicate with endpoints during posture assessment and provisioning processes.

質問: **129**
802.1X認証プロセスのどのコンポーネントが、ID認証情報を提供し、レイヤ2でEAPを使用して通信しますか？
A. 認証サーバー
B. 認証器
C. 認証データベース
D. 嘆願者
正解: **D (**コメントを発表する**)**
In the 802.1X authentication framework, the supplicant is the device or software application that provides the identity credentials (such as a username and password or digital certificate) during the authentication process. It communicates with the authenticator using the Extensible Authentication Protocol (EAP) at Layer 2.
The supplicant is essential for initiating the authentication process and ensures secure communication of identity credentials via EAP.

質問: **130**
RADIUS ではサポートされているが TACACS+ ではサポートされていない 2 つの認証プロトコルは? 2つ選んでください。）
A. EAP
B. チャップ
C. PAP
D. MSCHAPV2
E. MSCHAPv1
正解: **(**正解を表示します**)**

質問: **131**
TACACS+とRADIUS　プロトコルのトラフィックの違いは何ですか？
A. TACACS+ はトランスポート層で UDP を使用し、RADIUS はトランスポート層で TCP を使用します。
B. TACACS+ は各 AAA 機能を分離し、RADIUS は認証と認可を統合します。
C. TACACS+ はパスワードのみを暗号化し、RADIUS はパケットのペイロード全体を暗号化します。
D. TACACS+ はネットワーク層で IP トラフィックのみをサポートしますが、RADIUS は複数のプロトコルをサポートします。
正解: **(**正解を表示します**)**

One of the key differences between TACACS+ and RADIUS lies in how they handle the AAA (Authentication, Authorization, and Accounting) functions:
TACACS+:
■
TACACS+ separates the AAA functions into distinct processes. This means that authentication, authorization, and accounting are handled independently, providing more granular control over each process. TACACS+ encrypts the entire payload (except for the header), offering a higher level of security for the transmitted data.
RADIUS:
■
In contrast, RADIUS combines the authentication and authorization processes into a single step, which can limit flexibility. Additionally, in RADIUS, only the user password is typically encrypted in the packet payload; the rest of the information, including accounting data, is sent in clear text.

質問**: 132**
BYODフロー中に、Microsoft Windows PCはどこからネットワークセットアップアシスタントをダウンロードしますか？
A. Cisco App Store
B. Microsoft App Store
C. Cisco ISE directly
D. Native OTA functionality
正解**: (**正解を表示します**)**
https://ciscocustomer.lookbookhq.com/iseguidedjourney/BYOD-configuration

質問**: 133**
802.1X の導入時に、エンジニアは接続先のエンドポイントに問題を引き起こすことなく、認証失敗を特定する必要があります。これを実現するには、どのコマンドを使用すればよいでしょうか？
A. dotlxシステム認証制御
B. dotlx pae認証
C. 認証オープン
D. 認証ポート制御自動
正解**: C (**コメントを発表する**)**
authentication open gives the administrator the possibility to have connected endpoint even if they fail the authentication.

質問**: 134**
ネットワーク管理者は、プライマリciscoISEノードのバックアップ設定からセカンダリciscoISEノードを設定して、高可用性ペアを作成しています。CiscoISECA証明書とキーは、プライマリCisco ISEから手動でバックアップし、セカンダリCiscoISEにコピーする必要があります。これが機能するために最も発行されるコマンドはどれですか。
A. 証明書をコピーする伊勢
B. アプリケーションは伊勢を構成します
C. 証明書構成伊勢
D. 証明書をインポートする伊勢
正解**: (**正解を表示します**)**
https://community.cisco.com/t5/network-access-control/ise-certificate-import-export/m-p/3847746

質問**: 135**
図を参照してください。エンジニアは、Cisco Wireless LANコントローラ上で中央Web認証を設定し、ワイヤレスネットワークに接続されているすべてのゲストに対してCisco ISEを使用するようにする必要があります。コンポーネントは以下のように設定されます。
- Cisco ワイヤレス LAN コントローラ

- Cisco ISE 上の認証プロファイル
- Cisco IS の認証ルール

Cisco ISEで次に設定する必要がある項目は何ですか？

A. 承認ポリシー
B. 会計プロファイル
C. 認証プロファイル
D. 承認ルール

正解: **A** (コメントを発表する)

質問: **136**

管理者は、一時的なネットワークプリンタのネットワークアクセスを設定する責任を負います。
管理者は認証にプリンタのMACアドレス50:40:16:89:0:ABのみを使用する必要があります。
どの認証方法がこのタスクを達成できますか？

A. 姿勢
B. プロファイリング
C. MAB
D. 802.1x

正解: **C** (コメントを発表する)

MAC Authentication Bypass (MAB) is the authentication method that uses the MAC address of a device (such as a printer) to grant network access when 802.1X is not supported. The administrator can configure ISE to authenticate the printer using its MAC address.

質問: **137**

最近のネットワーク障害のため、ネットワークデバイスへのすべてのアクセスをCisco ISEで一元的にログ記録および追跡する必要があります。デバイス管理サービスを有効にする必要があるノードはどれですか？
A. PSN 1つ
B. 各PSN
C. PAN 1台
D. 各PAN
正解: **B** (コメントを発表する)

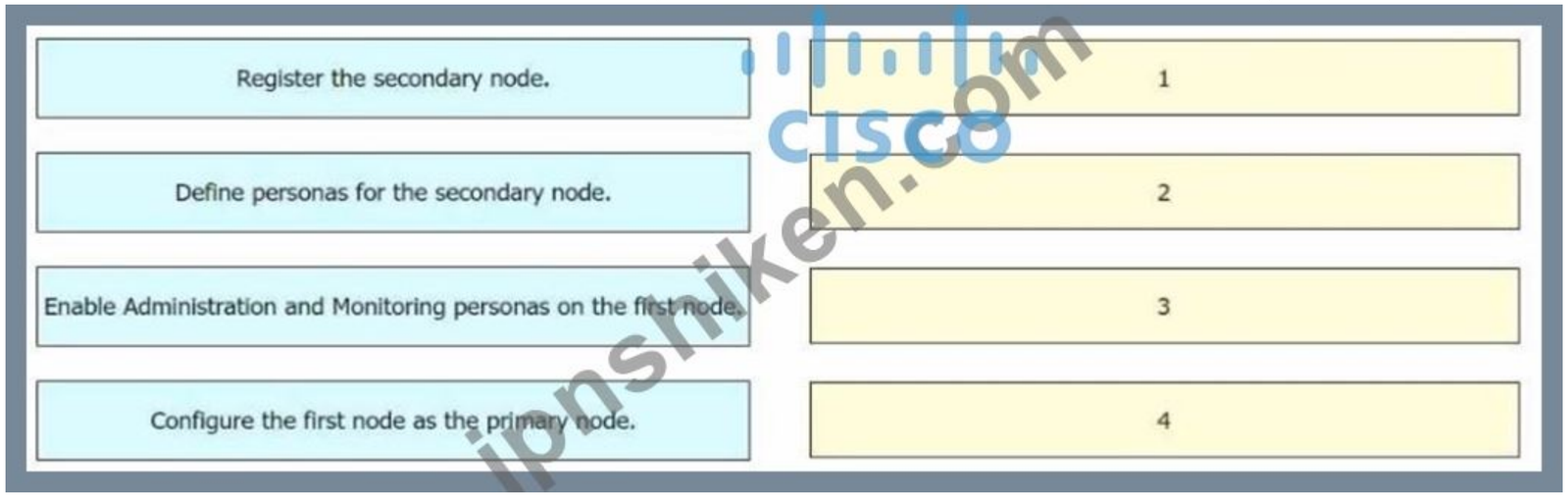
質問: **138**
エンジニアが非標準ポートを使用してWeb認証を構成しており、トラフィックを正しいポートにリダイレクトするためのスイッチが必要です。このタスクを実行するには、どのコマンドを使用する必要がありますか？
A. permit tcp any any eq <port number>
B. aaa group server radius proxy
C. ip http port <port number>
D. aaa group server radius
正解: **C** (コメントを発表する)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/command/nm-https-cr-book/nm-https-cr-cl-sh.html#wp2154019954

質問: **139**
802 1X対応ネットワークに参加しようとするエンドポイントエージェントを指す用語はどれですか。
A. オーセンティケーター
B. EAPサーバー
C. クライアント
D. サプリカント
正解: **D** (コメントを発表する)

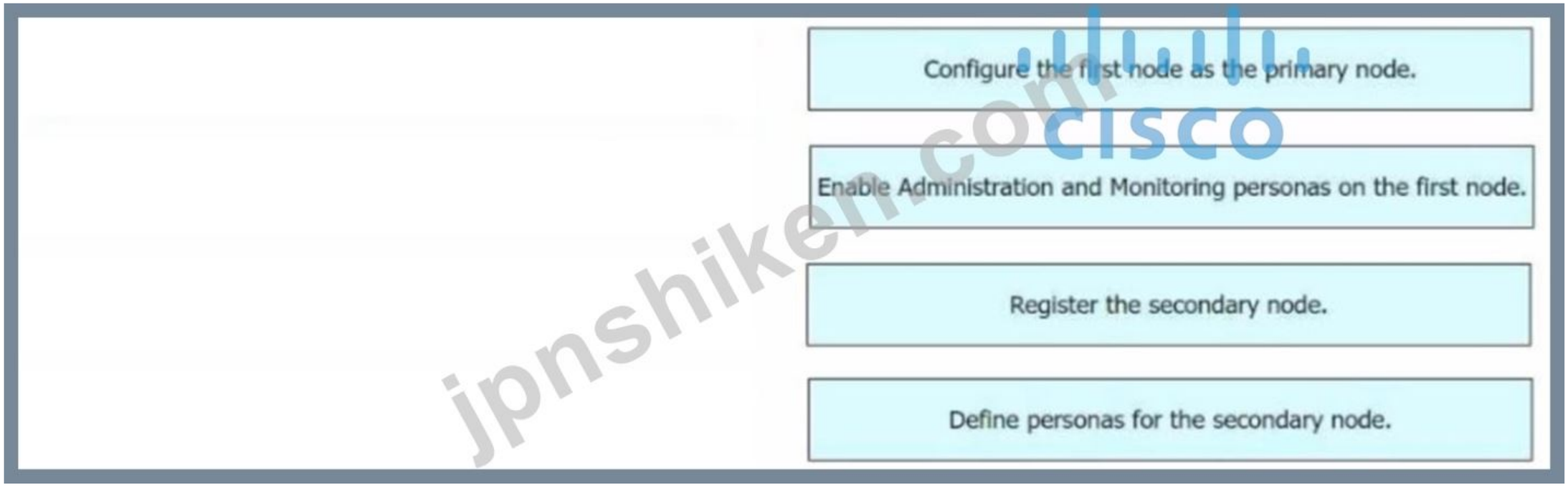
質問: **140**
管理者は、ネットワークアクセスを必要とするMACアドレス11:22 33:44:55:AAのIoTコネクタをデプロイしています。コネクタを適切にプロファイリングするために、Cisco ISEで新しいカスタムプロファイリングポリシーを設定する必要があります。要件を満たすために設定する必要がある条件はどれですか？
A. Radius_Called_Station-ID_ENDSSWITH_
B. MAC_MACAddress_CONTAINS_
C. DHCP_dhcpCacheDeviceID_CONTAINS_
D. MAC_OUI_ENDSWITH_
正解: (正解を表示します)
When creating a custom profiling policy in Cisco ISE for a specific device - such as an IoT connector identified by its MAC address - the profiling condition must accurately match the attribute that is reliably reported by the network access device. In many scenarios, especially with Cisco devices, the Called-Station-Id attribute in RADIUS messages contains the MAC address of the connecting device. However, due to the way some devices or controllers format this attribute, extra characters or prefixes may be appended. Using the condition "ENDSSWITH" ensures that the policy will correctly match the tail end of the Called-Station-Id string to the expected MAC address, regardless of any additional formatting at the beginning.
Radius_Called_Station-ID_ENDSSWITH_<MAC ADDRESS>
This condition tells ISE to examine the Called-Station-Id attribute from RADIUS messages and check whether it ends with the specified MAC address. This is a common and reliable method for profiling devices where the MAC address might be appended to additional text.

質問: **141**
Active Directoryグループを設定するとき、あいまいなグループ名を解決するためにCisco ISEは何を使用しますか？
A. TGT
B. SID
C. OMAB
D. MIB
正解: **(**正解を表示します**)**

質問: **142**
ドラッグアンドドロップ問題
左側の構成手順を右側の手順にドラッグアンドドロップして、分散展開で2つのCisco ISEノードをインストールします。



正解:



Explanation:
https://www.ciscopress.com/articles/article.asp?p=2812072

質問: **143**
ネットワークエンジニアが、Cisco ISE の内部 CA 上で新しい証明書テンプレートを設定し、ネットワークに登録する必要のある BYOD デバイスに証明書をプロビジョニングしようとしています。登録後にデバイスを識別するために、証明書の SAN フィールドには何を設定する必要がありますか？
A. 一般名
B. MACアドレス
C. メールアドレス
D. ユーザープリンシパル名
正解: **(**正解を表示します**)**

質問: **144**
ネットワーク管理者がフロントデスクの受付アカウントをCisco ISEゲストサービススポンサーグループに追加したところです。
Cisco ISEゲストスポンサーポータルを使用して、受付ではどのゲストサービスを提供できますか？
A. ゲストユーザーのアクティビティを追跡します
B. ゲストユーザーの認証設定を構成します
C. ゲストユーザーアカウントの作成と管理
D. Cisco ISEへのゲストユーザーの認証
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/sponsor_guide/b_spons_SponsorPortalUserGuide_21/Support_Guests.html

質問: **145**
エンジニアはプロファイリングを使用して、エンドポイントがどのようなアクセス権限を受け取る必要があるかを判断しています。Cisco ISEとネットワークデバイスの両方で802.1Xとプロファイリングの設定を行った後でも、エンドポイントは認証前にプロファイリングを実行しません。
このようなことが起こっている理由を2つ挙げてください。(2つ選択してください。)
A. クローズドモードでは、認証前に属性の収集が制限されます。
B. スイッチでNetFlowが有効になっていないため、属性は収集されません。
C. クローズドモードが有効になっているため、HTTPプローブが誤動作しています。
D. スイッチはRADIUS経由で属性を収集していますが、プローブがそれらを送信していません。
E. SNMPプローブが有効になっていません。
正解: **(**正解を表示します**)**

質問: **146**
セキュリティチームは有線ネットワークのセキュリティ強化を希望しています。ネットワーク上のMACアドレス00:43:08:50:64:60を持つ旧型プリンタは802.1Xをサポートしていません。Cisco ISEがこのMACアドレスのMABをサポートするには、認証ポリシーの 許可された認証プロトコル」リストでどの設定を有効にする必要がありますか？
A. EAP-TLS
B. PAP
C. MS-CHAPv2
D. プロセスホスト検索
正解: **D (**コメントを発表する**)**

質問: **147**
エンジニアは、ネットワークにアクセスするためにすでに認証されているエンドポイントに対して CoA を発行するように Cisco ISE サーバを設定する必要があります。ポートに複数のアクティブなセッションがある場合でも、セッションに CoA オプションを適用する必要があります。このタスクを実行するには、何を構成する必要がありますか?
A. Cisco ISE システム プロファイリング設定の Reauth CoA オプションが有効
B. ポート バウンス CoA オプションが有効になっているエンドポイント プロファイリング ポリシー
C. No CoA オプションが有効になっているエンドポイント プロファイリング ポリシー
D. Cisco ISE システム プロファイリング設定のポート バウンス CoA オプションが有効
正解: **(**正解を表示します**)**

質問: **148**
中央Web認証を許可するには、Cisco ISE認証ポリシーでどの構成が必要ですか？
A. MAB、ユーザーが見つからない場合は続行
B. MAB、認証に失敗した場合は続行
C. Dot1x、ユーザーが見つからない場合は続行
D. Dot1x、認証が失敗した場合は続行
正解: **A (**コメントを発表する**)**
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central- web-auth-00.html

質問: **149**

AireOSコントローラーでワイヤレスユーザーの中央Web認証をトリガーするには、WLAN内のどの高度なオプションを有効にする必要がありますか？
A. AAAオーバーライド
B. DHCPサーバー
C. 静的IPトンネリング
D. インターフェースACLを上書き
正解: **A** (コメントを発表する)

質問: **150**
Cisco ISEに脆弱性のエンドポイントをスキャンするオプションを提供するものは何ですか？
A. 許可ポリシー
B. 認証ポリシー
C. 認証プロファイル
D. 認可プロファイル
正解: (正解を表示します)
Configure Authorization Profile
The authorization profile in Cisco ISE now includes an option to scan endpoints for vulnerabilities.
You can choose to run the scan periodically and also specify the time interval for these scans.
After you define the authorization profile, you can apply it to an existing authorization policy rule or create a new authorization policy rule.
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010100.html

質問: **151**
ネットワーク全体でセキュリティグループタグを転送する方法は何ですか？
A. すべてのネットワークデバイスで802.1AEを有効にする
B. IPヘッダーにセキュリティグループタグを埋め込む
C. セキュリティグループタグを802.1Qヘッダーに埋め込む
D. セキュリティグループタグ交換プロトコル
正解: (正解を表示します)

質問: **152**
ネットワークエンジニアは、エンドポイントをチェックするポリシールールを設定する必要があります。このポリシーでは、ディスク暗号化が有効になっていること、および適切なバージョンのウイルス対策ソフトウェアがインストールされていることを確認する必要があります。エンジニアは、このルールにどのような設定を適用する必要がありますか？
A. 複合姿勢条件
B. 辞書の単純条件
C. 辞書複合条件

D. 単純な姿勢条件
正解: **(**正解を表示します**)**

質問: **153**
Windowsベースのデバイスは、どのプラットフォームからネットワークアシスタントをダウンロードしますか？
A. マイクロソフトアプリストア
B. Cisco ISE
C. ネイティブOS
D. シスコのダウンロードサイト
正解: **(**正解を表示します**)**
A Windows-based device downloads the Network Assistant Manager from Cisco ISE. During the BYOD onboarding process, ISE serves the necessary agent software directly to the endpoint.

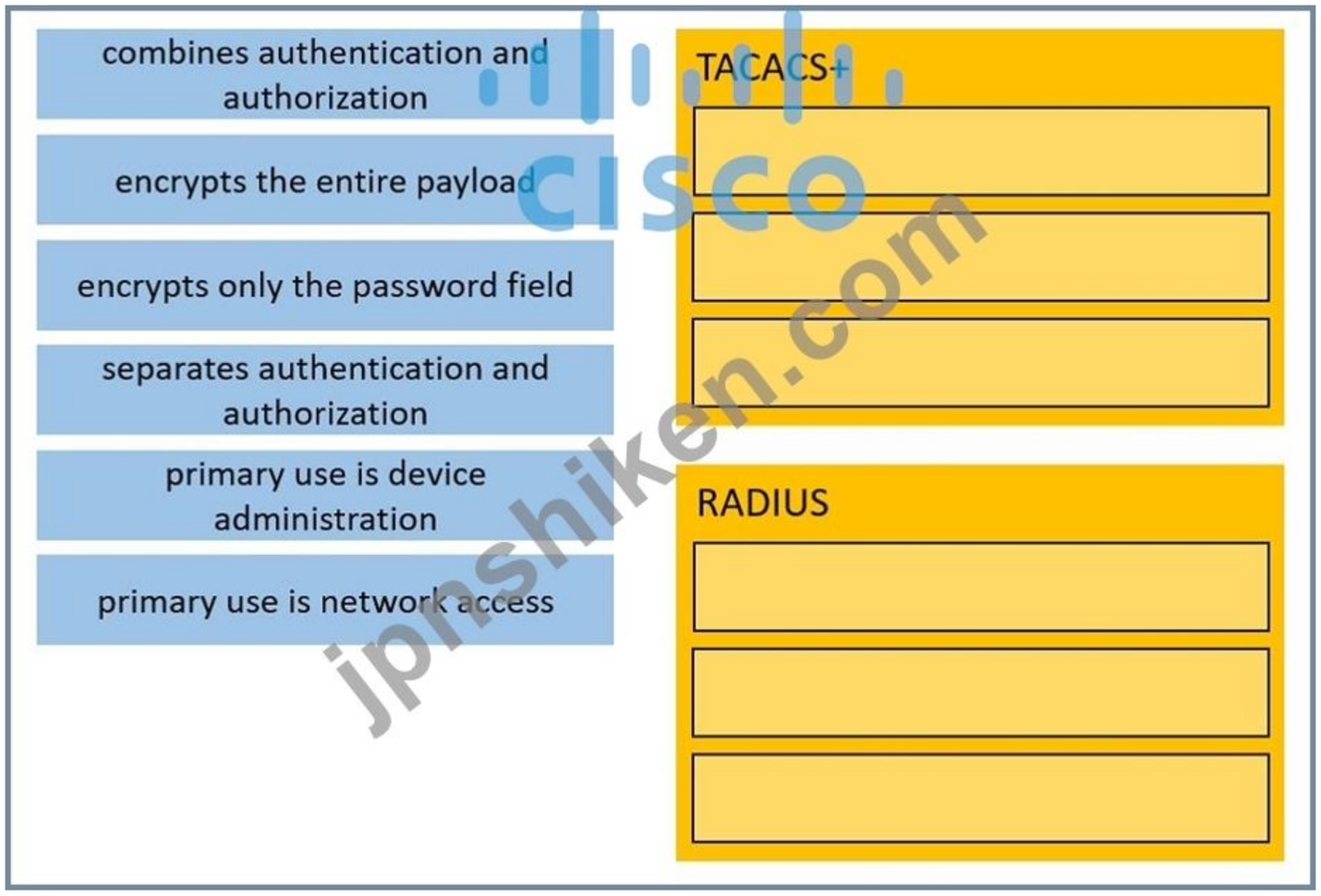
質問: **154**
管理者がCiscoISEでポスチャを設定していて、ネットワークにアクセスしようとしているワークステーションに特定のサービスが存在することを確認したいと考えています。この目標を達成するには、何を構成する必要がありますか？
A. OPSWATAPIバージョンを使用してアプリケーションの姿勢条件を作成します。
B. OPSWATAPIバージョンを使用して複合姿勢条件を作成します。
C. OPSWATAPI以外のバージョンを使用してレジストリポスチャ条件を作成します。
D. OPSWATAPI以外のバージョンを使用してサービスポスチャ条件を作成します。
正解: **(**正解を表示します**)**

質問: **155**
Cisco ISEがパスワードタイプでサポートする外部IDストアはどれですか？(2つ選択してください。)
A. RADIUSトークンサーバー
B. OBDC
C. TACACS+トー　クンサーバー
D. SQL
E. LDAP
正解: **(**正解を表示します**)**

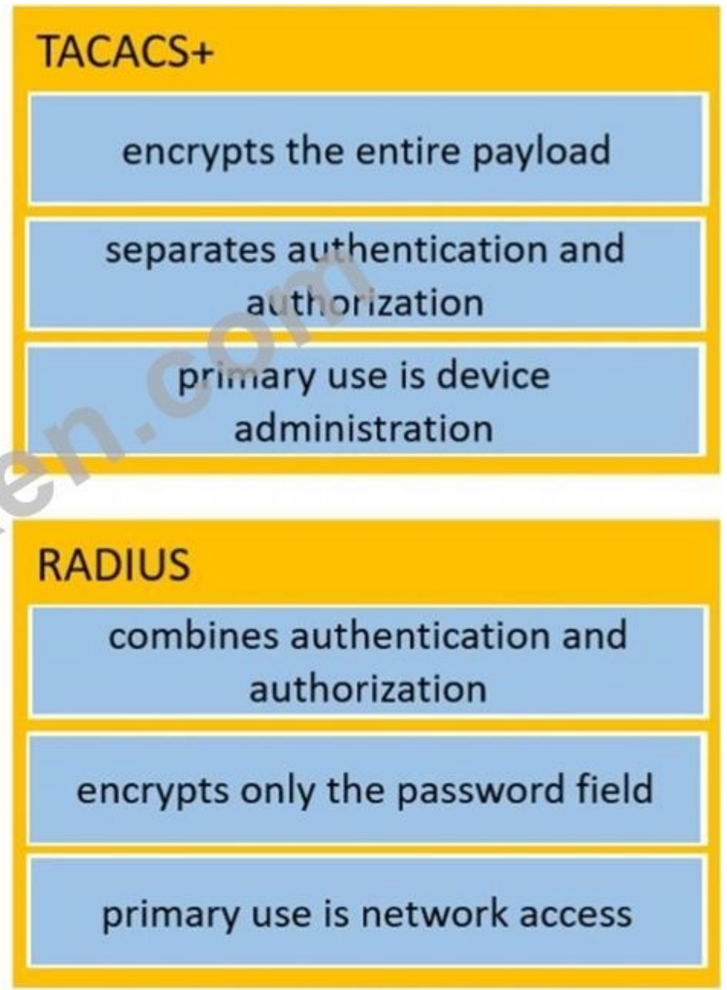
質問: **156**
TACACS +プロファイルのCisco ISE共通タスクサポートに含まれる2つのタスクタイプはどれですか。 2つ選択してください。）
A. 火力
B. WLC
C. IOS
D. ASA
E. シェル
正解: **B,E (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-

1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0100010.html TACACS+ Profile TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:
Common tasks
Custom attributes
There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)--Task Attribute View and Raw View. Common tasks can be entered using the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.
The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However, the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:
Shell
WLC
Nexus
Generic
The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using a equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

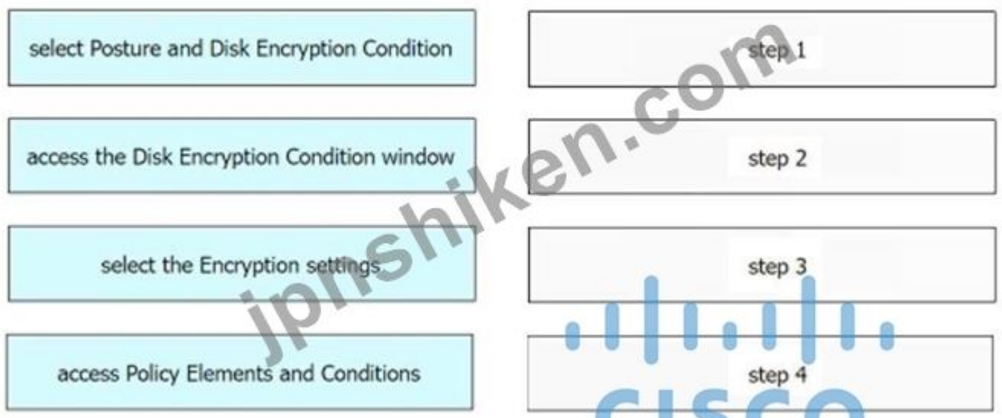
質問: **157**
ドラッグアンドドロップ問題
左側の説明文を、システム認証、認証、およびアカウンティングを実行するために使用される右側のプロトコルにドラッグアンドドロップしてください。


combines authentication and authorization
encrypts the entire payload
encrypts only the password field
separates authentication and authorization
primary use is device administration
primary use is network access
TACACS+
RADIUS

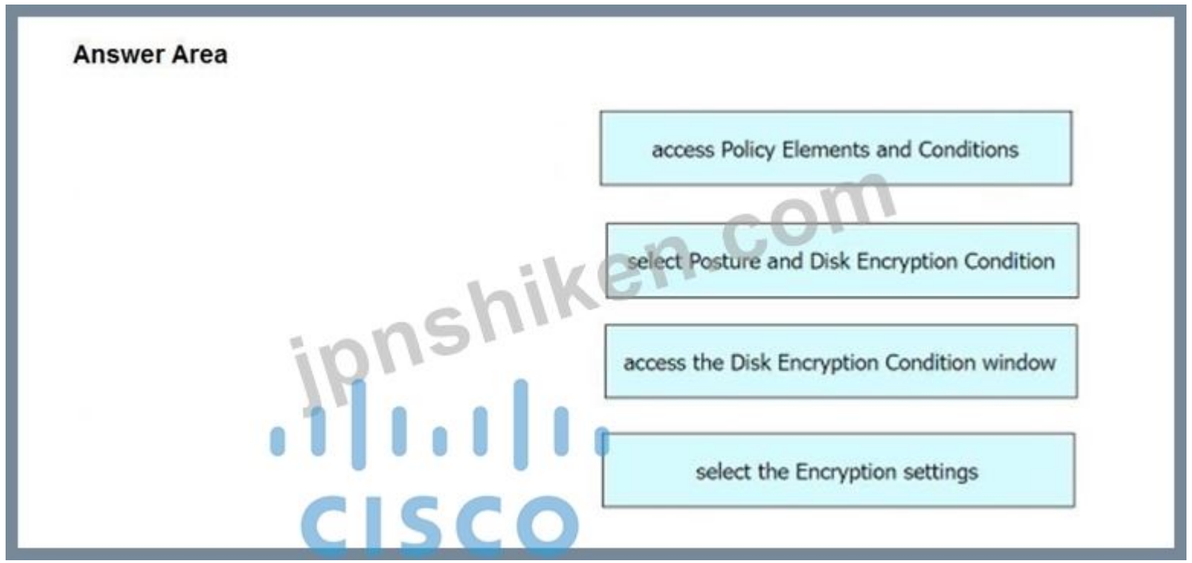
正解:



質問: **158**
ドラッグアンドドロップ問題
エンジニアは、Cisco ISE 上でコンプライアンス ポリシーを設定し、すべてのエンドポイントの C ドライブに最新の暗号化ソフトウェアが実行されていることを確認する必要があります。このタスクを実行するには、左側の設定手順を右側の順序にドラッグ アンド ドロップしてください。



正解:



質問: **159**
エンドポイントが認証され、プロファイリングされ、適切なエンドポイントIDグループに追加されるようにするには、管理者はCisco ISEの展開において、どの2つのサービスを有効にする必要がありますか？
(2つ選択してください。)
A. TACACS
B. セッション
C. 半径
D. 姿勢
E. プロファイリング
正解: **B,E** (コメントを発表する)

Cisco ISE needs the session-related service to process authentication flows and the profiling service to identify the endpoint and place it into the appropriate endpoint identity group.
In Cisco ISE, profiling must be enabled on the deployment node, and the endpoint must then be categorized into the profiled identity group based on the profiling policy results.

質問: **160**
スイッチング環境を担当するネットワークエンジニアは、TrustSecインライン方式でセキュリティグループタグを適切に伝播させるために、新しいスイッチをプロビジョニングする必要があります。ネットワークエンジニアは、スイッチ上でどのCLIコマンドを入力してSGTのタグ付けをグローバルに有効にする必要がありますか？
A. cts ロールベース sgt-map
B. cts sxp を有効にする
C. cts ロールベースの執行
D. ctsマニュアル
正解: **(**正解を表示します**)**

質問: **161**
ネットワークエンジニアが最近、リモートブランチルータをTACACS+を　使用して企業ファイアウォールの背後にある中央Cisco ISEサーバに認証するように設定しました。この設定変更後、エンジニアはルータへのSSHセッションを再度開き、ログイン試行がCisco ISEに送信されていることを確認しましたが、ログイン試行は失敗しました。Cisco ISEのTACACSライブログには接続試行が表示されておらず、ファイアウォール管理者はCisco ISEのIPアドレス宛てのsyslogおよびSNMPトラフィックは確認できたものの、TACACS+ト　ラフィックは確認できませんでした。ログイン失敗の原因となっている設定ミスはどれでしょうか？
A. ルーター上の aaa server グループにホストが定義されていません。
B. ルーターにCisco ISEサーバーへのルートがありません。
C. ルーター上の tacacs source-interface コマンドが間違ったインターフェースを参照しています。
D. ルーターに入力された Cisco ISE サーバー用の共有シークレットが間違っています。
正解: **(**正解を表示します**)**

質問: **162**
スイッチでのip http serverコマンドの目的は何ですか？
A. スイッチでMAB認証を有効にします
B. スイッチでdot1x認証を有効にします。
C. Web認証のためにユーザーのhttpsサーバーを有効にします
D. スイッチがユーザーをWeb認証にリダイレクトできるようにします。
正解: **D (**コメントを発表する**)**

質問: **163**
TACACSと比較した場合、RADIUSの主な機能は何ですか？
A. RADIUSはコマンド認証をサポートしていますが、TACACSはコマンドをサポートしていません。
B. RADIUSはコマンドアカウンティングをサポートしていますが、TACACSは開始/停止アカウンティングのみをサポートしています。
C. RADIUSは複数の特権レベルをサポートしますが、TACACSは1つの特権レベルのみをサポートします。
D. RADIUSはネットワークアクセス用のAAAを提供し、TACACSはデバイス管理用のAAAを提供します。
正解: **(**正解を表示します**)**

質問: **164**
Cisco ISEノードのデフォルト設定では、どの役割がデフォルトで有効になっていますか？

A. 管理およびPokeyサービス
B. インライン姿勢のみ
C. 政策サービスの監視および管理
D. 管理専用
正解: **(**正解を表示します**)**

質問: **165**
ネットワークセキュリティ管理者は、Cisco ISEをActive Directoryと統合する必要があります。管理者は参加操作を実行する必要があります。セキュリティ管理者はどのような操作を行う必要がありますか？
A. Active Directory を検索して、管理者ユーザーアカウントが存在するかどうかを確認します。
B. ドメインからISEマシンアカウントを削除します
C. Cisco ISEをActive Directoryドメインに参加させる
D. ドメインからCisco ISEユーザーアカウントを削除します。
正解: **(**正解を表示します**)**
To integrate Cisco Identity Services Engine (ISE) with Active Directory (AD), the ISE node must join the AD domain. This enables Cisco ISE to authenticate users and devices against the directory and enforce policies based on AD attributes.
Steps to Perform the Join Operation:
1. Navigate to Administration > Identity Management > External Identity Sources > Active Directory in the Cisco ISE GUI.
2. Provide the AD domain name and ensure network connectivity to the AD servers.
3. Use an AD account with appropriate privileges (often a domain admin or delegated account with join permissions) to perform the join operation.
4. After successful domain join, Cisco ISE can query the AD for user and group information.

質問: **166**
管理者は、新しい医療ビルのネットワークデバイスをCiscoISEに追加しています。これらのデバイスは、それらを介して接続するエンドポイントに対して個別にポリシーを作成できるように、「メディカルスイッチ」として識別しているネットワークデバイスグループに含まれている必要があります。この目標を達成するには、CiscoISE内のネットワークデバイスでどの設定項目を変更する必要がありますか。
A. デバイスタイプをメディカルスイッチに変更します。
B. デバイスプロファイルをMedicalSwitchに変更します。
C. モデル名をMedicalSwitchに変更します。
D. デバイスの場所をMedicalSwitchに変更します。
正解: **A (**コメントを発表する**)**
It should be Device Type, Medical Switch could be located on any floor or any room.

質問: **167**
Cisco ISE の管理者が、ユーザーエンドポイント認証に使用する中央 Web 認証を設定しています。クライアントはゲスト ポータルにアクセスしてログインし、アクセス権を取得できませんが、DNS は正常に機能しており、ゲスト ポータルは有効になっています。アクセス権を取得するには、他に何を設定する必要がありますか？
A. ファイアウォールでTCP/8443ポートを許可します。

B. HTTPからHTTPSへのリダイレクトを設定します。
C. ゲストポータルがTCP/8443でリッスンするように設定します。
D. 任意のクライアントIP範囲からのリダイレクトを許可します。
正解: **(**正解を表示します**)**

質問: **168**
エンジニアがCisco ISEでスポンサーポータルを設定しています。認証フローはKerberosを使用する外部ソースに渡る必要があります。この要件を満たすには、どのタイプの外部データベースを使用する必要がありますか？
A. 半径
B. SAML
C. Active Directory
D. LDAP
正解: **C (**コメントを発表する**)**
Kerberos authentication is only supported through Active Directory in Cisco ISE. Therefore, when a Sponsor portal must authenticate against an external source using Kerberos, the external identity database must be Active Directory.

質問: **169**
物理アプライアンス上のZTPでサポートされているファイル設定方法はどれですか？
A. cfg
B. 画像
C. はい
D. iso
正解: **(**正解を表示します**)**

質問: **170**
Cisco ISEとWLCを使用して中央Web認証を設定するには、WLCで何を設定する必要がありますか。
A. NAC状態オプションをSNMPNACに設定します。
B. コマンドでip access-groupwebauthを使用します。
C. NAC状態オプションをRADIUSNACに設定します。
D. radius-server vsa sendauthenticationコマンドを使用します。
正解: **(**正解を表示します**)**

質問: **171**
Microsoft Hyper-VでZTP構成ファイルを使用してCisco ISEをデプロイする場合、どのファイル拡張子が必要ですか？
A. .img
B. .tar
C. .iso
D. .txt
正解: **C (**コメントを発表する**)**

質問: **172**
UDPプロトコルの特徴は何ですか？
A. UDPはサーバーのダウンを検出できます。
B. UDPはベストエフォート型の配信を提供します
C. サーバーが遅いときにUDPが検出できる
D. UDPは存在しないサーバーに関する情報を提供します
正解: (正解を表示します)
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

質問: **173**
管理者は、Active DirectoryプローブからのAD-Join-Point属性とAD-Operating-System属性を使用してユーザーアクセスを提供するように、Cisco ISEプロファイリングサービスとCiscoスイッチデバイスセンサー機能を構成する必要があります。以下の構成が実行されました。
- 必要なCiscoワイヤレスLANコントローラをすべて設定しました
設定
- Active Directoryプローブを有効にしました
- カスタムプロファイリングポリシーを設定しました
Cisco ISEをActive Directoryに接続しました。
- フルアクセス権限を持つ認証ルールを設定しました
設定を完了するには、どの2つの操作を行う必要がありますか？(2つ選択してください。)
A. カスタムプロファイリング条件を設定します。
B. RADIUSプローブを有効にします。
C. プロファイリング論理プロファイルを設定します。
D. SNMPプローブを有効にします。
E. エンドポイントのIDグループを設定します。
正解: (正解を表示します)

質問: **174**
エンジニアは、Cisco ISE 上で AD グループメンバーシップを利用するポリシーを開発する必要があります。ポリシー内で AD グループを作成するには、エンジニアはどのタイプのポリシー要素を設定する必要がありますか？
A. 辞書
B. 条件
C. 結果
D. スマートコンディション
正解: (正解を表示します)

質問: **175**
Cisco ISEノードはどのようなペルソナを想定できますか？
A. ポリシーサービス、ゲートキーピング、およびモニタリング
B. 管理、政策サービス、監視
C. 管理、政策サービス、ゲートキーピング

D. 管理、監視、ゲートキーピング
正解: **B** (コメントを発表する)
https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_dis_deploy.html The persona or personas of a node determine the services provided by a node. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring. The menu options that are available through the administrative user interface are dependent on the role and personas that an ISE node assumes. See Cisco ISE Nodes and Available Menu Options for more information.

質問: **176**
あるエンジニアが、病院の既存の無線環境にCisco ISEを導入しようとしています。顧客からの要件は、WLCが中央Web認証にCisco ISEを使用することです。
同社は、WLCと連携して患者記録への無線アクセスを患者の部屋のみに制限するCisco MSEも使用しています。この統合をサポートするために、Cisco ISEの認証プロファイルでどのオプションを選択する必要がありますか？
A. 地図上の位置
B. アクセスタイプ
C. トラックムーブメント
D. サービステンプレート
正解: **A** (コメントを発表する)
To support the integration of Cisco ISE with a Cisco Mobility Services Engine (MSE) and a Wireless LAN Controller (WLC) for restricting access based on the location of a patient, the MAP Location option must be selected in the Authorization Profile in Cisco ISE.
The MAP Location option allows Cisco ISE to leverage location information provided by the MSE.
This ensures that authorization policies are dynamically applied based on the endpoint's physical location, such as restricting access to patient records to specific rooms in the hospital.

質問: **177**
エンジニアは、シスコ以外のネットワークデバイスで使用するためにCiscoISE内でTACACS+を　設定しています。ユーザーに適切なアクセス権が与えられるように、Access-Accept応答で特別な属性を送信する必要があります。これを達成するために何を構成する必要がありますか？
A. さまざまな役割を定義するためのカスタムアクセス条件
B. ユーザーにさまざまなアクセスポリシーを適用するためのdACL
C. 適切なアクセスを提供するためのTACACS+コ　マンドセット
D. さまざまな役割を定義するカスタム属性を持つシェルプロファイル
正解: (正解を表示します)

質問: **178**
Cisco ISE管理者は、ゲストエンドポイント登録が1日だけ有効であることを確認する必要があります。ゲストポリシーフローをテストすると、管理者は、Cisco ISEが1日後にゲストエンドポイントIDストアのエンドポイントを削除せず、アクセスを許可することを確認します。その期間の後のゲストネットワーク。この問題の原因となっている構成はどれですか？
A. ゲストアクセス用に設定されたRADIUSポリシーは、同じデバイスの繰り返し認証を許可するように設定されています
B. ゲストポータル設定でアクセス期間が7日に設定されています
C. ゲストアカウントのパージポリシーは15日に設定されています
D. ゲストデバイスのエンドポイントパージポリシーは30日に設定されています
正解: **D** (コメントを発表する)

質問: **179**

エンジニアがネットワーク上のMABから802.1Xにユーザーを移行しています。これは、ユーザーへの影響を最小限に抑えて、通常の営業時間内に実行する必要があります。どのCoAメソッドを使用する必要がありますか？
A. セッションの再認証
B. ポートバウンス
C. ポートのシャットダウン
D. セッションの終了
正解: **A** (コメントを発表する)

質問: **180**
管理者は、Cisco ISEで使用する新しいプローブを設定しており、メタデータを使用してエンドポイントのプロファイルを作成したいと考えています。メタデータには、業界標準のプロトコル情報ではなく、エンドポイントに関連するトラフィック情報が含まれている必要があります。これらの要件を満たすには、どのプローブを有効にする必要がありますか？
A. NetFlowプローブ
B. DNSプローブ
C. DHCPプローブ
D. SNMPクエリプローブ
正解: (正解を表示します)
http://www.network-node.com/blog/2016/1/2/ise-20-profiling

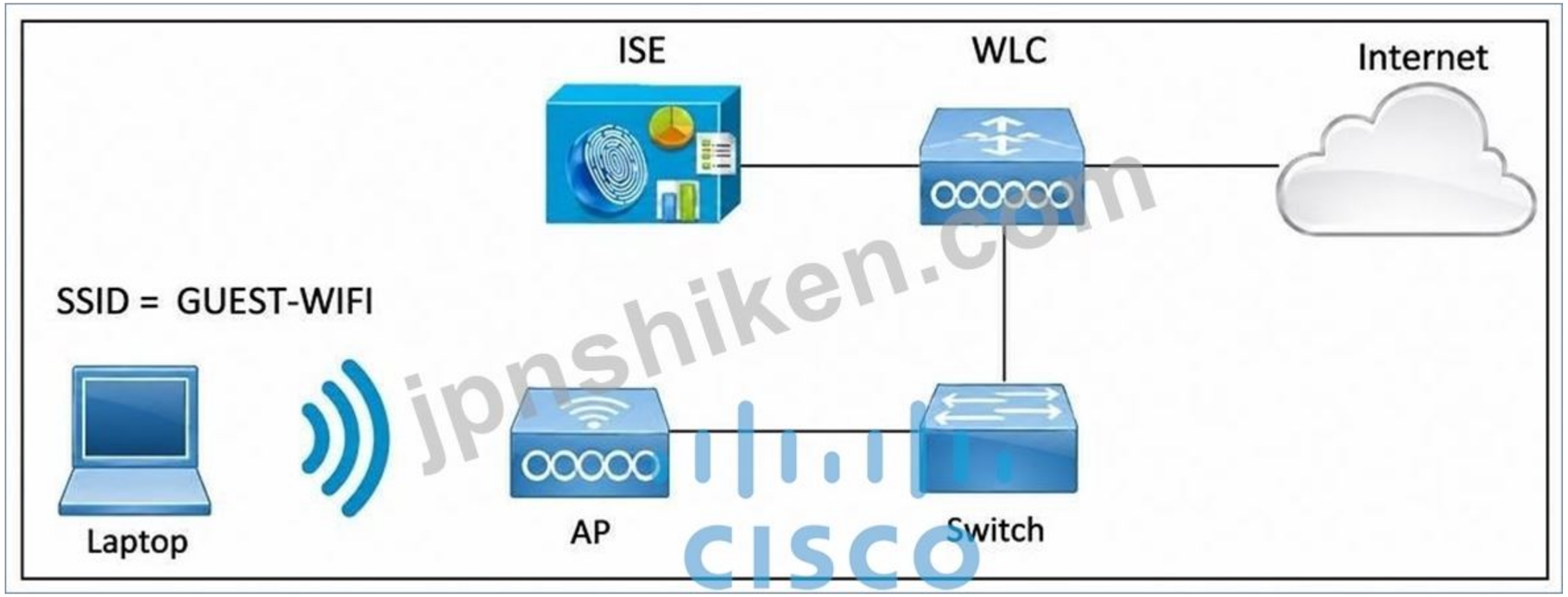
質問: **181**
エンジニアは、TACACS+ を有効にするために必要な CLI コマンドをデバイスに追加した後、SSH を使用してスイッチに接続することができません。デバイス管理ライセンスが Cisco ISE に追加され、必要なポリシーが作成されました。スイッチへのアクセスを有効にするには、どのアクションが必要ですか?
A. SSH に使用される RSA キーペアは、TACACS+ を有効にした後に再生成する必要があります。
B. スイッチをネットワーク デバイスとして Cisco ISE に追加し、TACACS+ を使用するように設定する必要があります。
C. スイッチで 802.1X 認証を構成する必要があります。
D. ip ssh source-interface コマンドをスイッチに設定する必要があります。
正解: **B** (コメントを発表する)

質問: **182**
管理者は、CiscoISEのプロファイリングサービスがクローズモードで許可ポリシーに使用できるようにします。エンドポイントが接続すると、アクセスが制限されるため、プロファイリングプローブは情報を収集し、CiscoISEは正しいプロファイルを割り当てることができます。CiscoISE内のデフォルト値を使用しています。ただし、新しいプロファイルのため、デバイスはアクセスを変更しません。何が問題ですか'？
A. 再認証設定のデフォルトのプロファイラー構成はNoCoAに設定されています
B. クローズドモードでは、CDPが有効になっていないとプロファイリングは機能しません。
C. プロファイリングプローブは、デバイスプロファイルを変更するのに十分な情報を収集できません
D. プロファイラーフィードが新しい情報をダウンロードしていないため、プロファイラーは非アクティブです
正解: (正解を表示します)

質問: **183**
エンジニアは、Cisco ISEでデバイスがブロックリストに追加された際に表示されるメッセージを変更する必要があります。新しいメッセージには、静的コンテンツと動的コンテンツの両方を含める必要があります。以下の設定は既に完了しています。
ポータルで使用する証明書を設定します。
- デバイスポータル管理設定とブロックリストポータルを編集します
設定。
証明書グループのタグと表示言語を設定します。
Cisco ISEで次に実行すべき設定操作は何ですか？
A. HTMLによるポータルカスタマイズを有効にする。
B. HTMLとJavaScriptを使用してポータルのカスタマイズを有効にする。
C. ポータルページのカスタマイズ設定を編集します。
D. オプションコンテンツ領域を編集します。
正解: **(**正解を表示します**)**
Cisco ISE blocklist portal messaging that mixes static and dynamic content requires portal customization that supports both HTML and JavaScript.
The blocklist portal is one of the end-user portals that can be customized through the portal text content, and Cisco's portal customization guidance specifically notes HTML and JavaScript support for these web portals.

質問: **184**
ラップトップが盗まれ、ネットワークエンジニアがそれをブロックリストエンドポイントIDグループに追加しました。ラップトップをリダイレクトしてアクセスを制限するには、新しいCiscoISE展開で何を行う必要がありますか。
A. 承認ポリシー内で[DenyAccess]を選択します。
B. ポート8443へのアクセスがACL内で許可されていることを確認します。
C. ポート8444へのアクセスがACL内で許可されていることを確認します。
D. 認証ポリシー内で[認証が失敗した場合]で[DROP]を選択します。
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010000.html

質問: **185**
図を参照してください。エンジニアはCisco ISEでゲストアクセス設定を構成する必要があります。



これらの設定は既に完了しています。
- ワイヤレス LAN コントローラを設定し、ネットワーク デバイスとして追加します
Cisco ISE。
エンドポイントIDグループと自己登録ゲストタイプを作成します。
- SMTPと登録フォームを設定して認証情報を送信する
メール。
要件を満たすために、Cisco ISEで次に設定する必要があるプロファイルの種類はどれですか？(2つ選択)
(2つ選択してください。)
A. インターネットアクセスを許可する認証プロファイル
B. インターネットアクセスを許可する認証プロファイル
C. ユーザーをゲストポータルにリダイレクトするための認証プロファイル
D. ユーザーをスポンサーポータルにリダイレクトするための認証プロファイル
E. ゲストポータルを許可する認証プロファイル
正解: **(**正解を表示します**)**
A typical self-registration guest lifecycle in Cisco ISE requires two separate Authorization Profiles to handle the user before and after authentication:
The Redirect Phase (Option C): When an unauthenticated guest first associates with the GUEST- WIFI SSID shown in image_039618.jpg, Cisco ISE needs to intercept their traffic. You must configure an Authorization Profile that passes the URL redirection attributes and a redirection ACL back to the WLC. This forces the user's web browser to load the self-registration guest portal.
The Access Phase (Option A): Once the user successfully registers and logs into the portal, Cisco ISE sends a Change of Authorization (CoA) to update the session. A second Authorization Profile must be configured to grant the endpoint full or limited internet access (typically by removing the redirection constraints and applying a standard permit policy).

質問: **186**

MACアドレス04:85:70:26:64:ABのエンドポイントがネットワークへの接続を試みます。セキュリティ管理者は、認証前にDHCPやDNSなどのサービスへのアクセスが制限されるようにしたいと考えています。ネットワークへのフルアクセスは、認証が成功した場合にのみ許可されます。
802.1X認証。要件を満たすために、管理者はどのISE展開モードを設定すべきでしょうか？
A. モニターモード
B. 低衝撃モード
C. オープンモード
D. クローズモード
正解: (正解を表示します)

質問: **187**
RADIUS と比較した TACACS+ の 2 つの違いは何ですか？ 2つ選んでください。）
A. TACACS+ はコネクションレス トランスポート プロトコルを使用しますが、RADIUS はコネクション型トランスポート プロトコルを使用します。
B. TACACS+ はコネクション型トランスポート プロトコルを使用しますが、RADIUS はコネクションレス型トランスポート プロトコルを使用します。
C. TACACS+ はユーザーごとに複数のセッションをサポートしますが、RADIUS はユーザーごとに 1 つのセッションをサポートします。
D. TACACS+ はパケット ペイロード全体を暗号化しますが、RADIUS はパスワードのみを暗号化します。
E. TACACS+ はパスワードのみを暗号化しますが、RADIUS はパケット ペイロード全体を暗号化します。
正解: (正解を表示します)

質問: **188**
ネットワークエンジニアは、Cisco ISE導入の事前調査フェーズにあり、ネットワークを検出する必要があります。ネットワーク監視には、既存のネットワーク管理システムが使用されています。
情報を収集するために、どのタイプのプローブを構成する必要がありますか？
A. NMAP
B. 半径
C. SNMP
D. ネットフロー
正解: (正解を表示します)
When there's an existing network management system (NMS) already doing network monitoring, the appropriate ISE probe is SNMP - specifically the SNMP Query probe, which allows ISE to query network devices (switches, WLCs) to gather endpoint information such as MAC addresses, connected ports, and VLAN data.
SNMP integrates naturally with an existing NMS infrastructure during the discovery phase. The other options are distractors: NMAP is active scanning, RADIUS requires authentication events to already be flowing, and NetFlow is for traffic analysis rather than endpoint discovery.

質問: **189**
管理者がCisco ISEで初めて姿勢評価を設定しています。クライアントプロビジョニングポリシーのエージェント構成にSecure Clientを使用するには、Cisco ISEにどの2つのコンポーネントをアップロードする必要がありますか？(2つ選択してください。)
A. セキュアクライアントネットワーク可視化モジュール
B. SecureClientProfie.xml ファイル
C. セキュアクライアントコンプライアンスモジュール
D. セキュアクライアントエージェントイメージ
E. SecureClientProtie.xsd ファイル
正解: (正解を表示します)

質問: **190**
ネットワークエンジニアは、ホワイトリストに登録されたデバイスを手動で削除する必要があります。Cisco ISEエンドポイントデータベースから削除するには、どのようにすればよいでしょうか？
A. 管理 > ID管理 > エンドポイントIDグループ > プロファイル済み
B. 管理 > ID管理 > グループ > エンドポイントIDグループ
C. 管理 > ID管理 > グループ > エンドポイントIDグループ > プロファイル済み
D. 管理 > ID管理 > エンドポイントIDグループ
正解: **B** (コメントを発表する)
To remove a device that has been allowlisted manually on Cisco ISE, the correct answer is option
- Administration > Identity Management > Groups > Endpoint Identity Groups. This option allows you to view and edit the endpoint identity groups that are configured on Cisco ISE, and to delete any device that belongs to a specific group.

質問: **191**
Cisco ISEでTACACS+機　能を有効にするには、どの2つの機能を使用する必要がありますか？(2つ選択してください。)
A. デバイス管理ライセンス
B. サーバーシーケンス
C. 外部TACACSサーバー
D. コマンドセット
E. デバイス管理サービス
正解: (正解を表示します)

質問: **192**
エンジニアは、VMware上で動作するCisco ISE仮想アプライアンス上で、プロファイリング専用のインターフェイスを使用してHTTPプローブを設定する必要があります。このインターフェイスは、VMネットワークポートグループに割り当てられます。
エンジニアは、Cisco ISE VMとVMのネットワーク設定のみにアクセスできるユーザーアカウントでハイパーバイザーにログインしています。このインターフェイスがSPANトラフィックを受け入れるようにするには、どのセキュリティ設定を変更する必要がありますか？
A. vSwitch プロパティで、プロミスキャス モードをポート グループから継承するように設定します。
B. vSwitchのプロパティでプロミスキャスモードを 'Accept」に設定します。
C. ポートグループのプロパティでプロミスキャスモードを 'Accept」に設定します。
D. ポートグループのプロパティで、プロミスキャスモードをvSwitchから継承するように設定します。
正解: (正解を表示します)

質問: **193**
組織は、Cisco ISE展開を分割して、デバイス管理機能をmam展開から分離したいと考えています。これを機能させるには、管理者は新しい展開の一部となるノードの登録を解除する必要がありますが、このオプションのボタンはグレー表示されています。この動作の原因となっている構成はどれですか。
A. ノードの1つがアクティブなPSNです。
B. ノードの1つはプライマリPANです
C. すべてのノードがPAN自動フェイルオーバーに参加します。
D. すべてのノードがアクティブに同期されています。
正解: **B** (コメントを発表する)

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html#ID185

質問: **194**
エンジニアは、Cisco ISE を使用して、サポートできないエンドポイントにネットワーク アクセスを提供する必要があります。
802.1X。エンドポイントMACアドレスは、エンドポイントIDグループを設定することで許可リストに登録する必要があります。以下の設定が実行されました。
- allowlist という名前の ID グループを設定しました
- エンドポイントを、互換性のないMACアドレスを使用するように構成しました
802.1Xデバイス
- エンドポイントを許可リストIDグループに追加しました
MABユーザー向けの認証ポリシーを設定しました
何を設定する必要がありますか？
A. 設定されたポリシーに基づいて、許可リストのIDグループに一致する論理プロファイル
B. PermitAccess権限を持ち、許可リストIDグループに一致する認証プロファイル
C. PermitAccess権限を持ち、許可リストIDグループに一致する認証ポリシー
D. PermitAccess権限を持ち、許可リストIDグループに一致する認証プロファイル
正解: (正解を表示します)
Since the endpoints cannot support 802.1X, they must be authenticated using MAC Authentication Bypass (MAB). The authentication policy has already been configured for MAB users, meaning ISE will attempt to authenticate based on the MAC address. However, to grant network access to these devices, an authorization policy is required.
Authorization Policy determines what level of access should be granted after authentication. The policy must match devices in the allowlist identity group and apply the PermitAccess permission, allowing them onto the network.

質問: **195**
エンジニアがネットワークアクセス制御の姿勢評価を設定しており、評価条件としてサービス条件を使用できるエージェントを使用する必要があります。エージェントはユーザーの操作を妨げないようにバックグラウンドプロセスとして実行されるべきですが、実行されるとユーザーに表示されてしまいます。何が問題なのでしょうか？
A. 評価を実施するための適切な許可が臨時代理人に与えられていなかった
B. ポスチャモジュールはSCCMでインストールする代わりに、ヘッドエンドを使用して展開されました。
C. ユーザーに修復が必要だったため、エージェントが通知に表示されました
D. エンジニアは「Anyconnect」姿勢エージェントを使用していますが、「Stealth Anyconnect姿勢エージェント」を使用する必要があります。
正解: (正解を表示します)

質問: **196**
エンジニアが、Cisco ISE の段階的導入における低影響モードをテストしています。認証前にホストがネットワークに接続しようとした場合、どのタイプのトラフィックが拒否されますか？
A. EAP
B. DNS
C. HTTP
D. DHCP
正解: (正解を表示します)

質問: **197**
Cisco ISE を使用して BYOD を構成するにあたり、管理者は、より良いユーザー エクスペリエンスを提供するために、接続するデバイスに証明書を発行することを検討しています。すべてが Cisco ISE のローカル環境である必要があるため、外部 CA サーバーはこの目的には使用できません。これを実現するには、どのような手順が必要ですか？
A. エンドポイントがローカル AD サーバーに正しい証明書を照会できるように、MS SCEP を構成します。
B. Cisco ISE内部CAを設定して、BYODネットワークに接続する各エンドポイントに証明書を発行します。
C. 認証時にエンドポイントに証明書を発行するために、キャプティブポータルネットワークアシスタントを使用します。
D. BYODポータルのサブCAとしてISEを使用し、証明書発行のためにユーザーをルートCAにリダイレクトします。
正解: **(**正解を表示します**)**

質問: **198**
dot1x system-auth-controlコマンドは何をしますか？
A. ネットワークアクセススイッチが802.1xセッションを追跡しないようにします
B. 802.1xをグローバルに有効にします
C. ネットワークアクセスデバイスインターフェイスで802.1xを有効にします
D. ネットワークアクセススイッチに802.1xセッションを追跡させます。
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380-configuration/dot1x.html

質問: **199**
管理者は、ユーザーがTACACS +を使用してネットワークデバイスにログインするときに、ネットワークデバイスに同じレベルのアクセスを許可する必要があります。ただし、管理者は、異なるコマンドを必要とする3つのユーザーロールのいずれかに基づいて特定のコマンドを制限する必要があります。Cisco ISEを使用していますか？
A. 1つのシェルプロファイルと複数のコマンドセットを作成します。
B. 複数のシェルプロファイルと複数のコマンドセットを作成します。
C. 1つのシェルプロファイルと1つのコマンドセットを作成します。
D. 複数のシェルプロファイルと1つのコマンドセットを作成します
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0100010.html
https://www.youtube.com/watch?v=IlZwB71Szog&ab_channel=JasonMaynard

質問: **200**
ネットワーク管理者は、Cisco ISEを使用して、エンドポイントに正しいバージョンのアンチウイルスがインストールされているかどうかを確認する必要があります。この機能を許可するには、どのアクションを実行する必要がありますか。
A. ウイルス対策バージョンの確認に使用するネイティブサプリカントプロファイルを構成します
B. ウイルス対策バージョンを確認するためにHostScanパッケージをエンドポイントにプッシュするようにCiscoISEを設定します。

C. エンドポイントのアンチウイルス情報をCisco ISEに送信するために、CiscoAnyConnectネットワーク可視性モジュールコンフィギュレーションプロファイルを作成します。
D. コンプライアンスモジュールおよび関連する設定ファイル用にCiscoISE内にCiscoAnyConnect設定を作成します
正解: (正解を表示します)
When using posture assessment, it is critical to keep the compliance modules as up to date as possible. Many TAC cases are opened due to an endpoint failing posture checks. The remedy for such cases is simply to update the ISE and AnyConnect compliance modules because the client is running a newer version of some antivirus software, and a new compliance module is required to detect that new version correctly.
AnyConnect Configuration: These configurations are built per operating system (Windows and macOS) and control what AnyConnect modules should be provisioned through the CPP and what PROFILES should be leveraged per module.
AnyConnect Posture Profile: This is the posture configuration for the SYSTEM SCAN MODULE, where you control all aspects of the posture module, but it is not called a configuration; rather, it is called a profile for alignment with the AnyConnect naming convention in Cisco's ASA.

質問: **201**
管理者がエンドポイントのCSVリストを編集しており、Cisco ISEにリストをインポートする前に、一部のデバイスのプロファイルを無期限に再設定したいと考えています。リストを再インポートする前に、デバイスのどのフィールドとブール値を変更する必要がありますか？
A. ポリシー割り当てフィールドと静的割り当てフィールドの値がFALSEに設定されています
B. ポリシー割り当てフィールドと静的割り当てフィールドの値がTRUEに設定されています
C. IDグループ割り当てフィールドと静的割り当てフィールドの値がFALSEに設定されています
D. IDグループ割り当てフィールドと静的割り当てフィールドの値がTRUEに設定されています
正解: (正解を表示します)
To allow devices to continue being dynamically reprofiled, the CSV must set Static Assignment = FALSE, and the field that controls this behavior is the Identity Group Assignment field. This ensures ISE does not lock the device into a static group and can reprofile it indefinitely.

質問: **202**
エンジニアは、ネットワーク内のCisco ISEの新しい分散展開を設計しており、管理ノードのフェールオーバーオプションを検討しています。管理ノードが常にポリシーの構成に使用できることを確認する必要があります。この機能を有効にするための要件は何ですか？
A. 1つのポリシーサービスノードと1つの監視およびトラブルシューティングノード
B. 1つのプライマリ管理ノードと1つの監視およびトラブルシューティングノード
C. デプロイメント内の1つのプライマリ管理者ノードと1つのセカンダリ管理者ノード
D. 1つのポリシーサービスノードと1つのセカンダリ管理ノード
正解: (正解を表示します)

質問: **203**
次のうち、Cisco ISEのプロファイリングデータを取得する方法ではないものはどれですか？
A. HTTP
B. DNS
C. SNMPクエリ
D. 半径
E. アクティブスキャン
F. ネットフロー
正解: (正解を表示します)

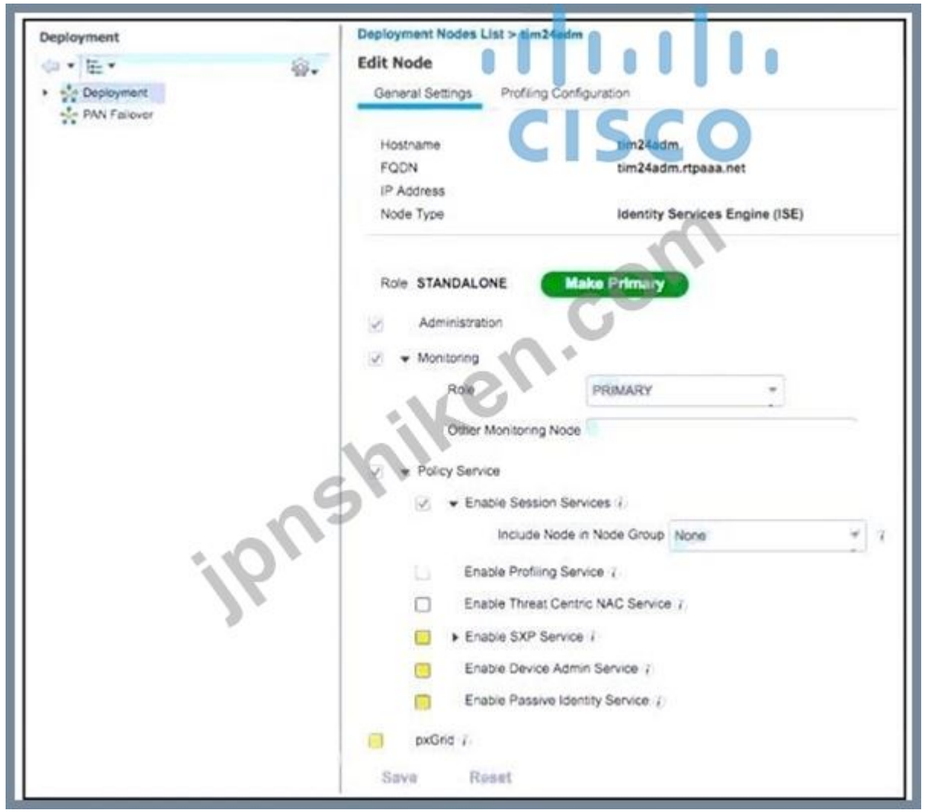
質問: **204**
スポンサーがスポンサーポータルからゲストアカウントを一括作成するには、どの2つの方法を選択すべきでしょうか？
A. ランダム
B. 月刊
C. デイリー
D. 輸入品
E. 既知
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/sponsor_guide/b_spons_SponsorPortalUserGuide_20/Create_Guest___Accounts.html#task_5 AD3C531980C4597A43A442F37EF2DFE

質問: **205**
エンジニアが、会社の有線ネットワークへのアクセス制御に802.1X認証を使用するため、Cisco ISEを導入しようとしています。会社経営陣からの要望は、社内スイッチへの802.1X導入時にユーザーへの影響を最小限に抑えることです。この要望を満たすために、段階的な802.1X導入において最初にどのモードを使用すべきでしょうか？
A. 低負荷
B. 開く
C. 閉店
D. モニター
正解: **(**正解を表示します**)**

質問: **206**
デバイス登録プロセス中のエンドポイント属性の有効なステータスは何ですか?
A. ブロックリスト
B. 不明
C. 保留中
D. アクセス拒否
正解: **C (**コメントを発表する**)**

質問: **207**
組織内では、CiscoISEで新しいポリシーを作成する必要があります。ネットワークへのアクセスを許可する前に、特定のウイルス対策アプリケーションがインストールされているだけでなく、マシン上で実行されていることを検証する必要があります。このポリシーが機能するために、管理者はどのポスチャ条件を設定する必要がありますか？
A. ファイル
B. レジストリ
C. サービス
D. アプリケーション
正解: **(**正解を表示します**)**

質問: **208**
図を参照してください。Cisco ISEがアクティブユーザーのグループメンバーシップ情報を公開し、Cisco Firepowerデバイスと共有できるようにするには、どのチェックボックスを有効にする必要がありますか？



A. デバイス管理サービスを有効にする
B. SXPサービスを有効にする
C. パッシブIDサービスを有効にする
D. pxGrid
正解: **D** (コメントを発表する)

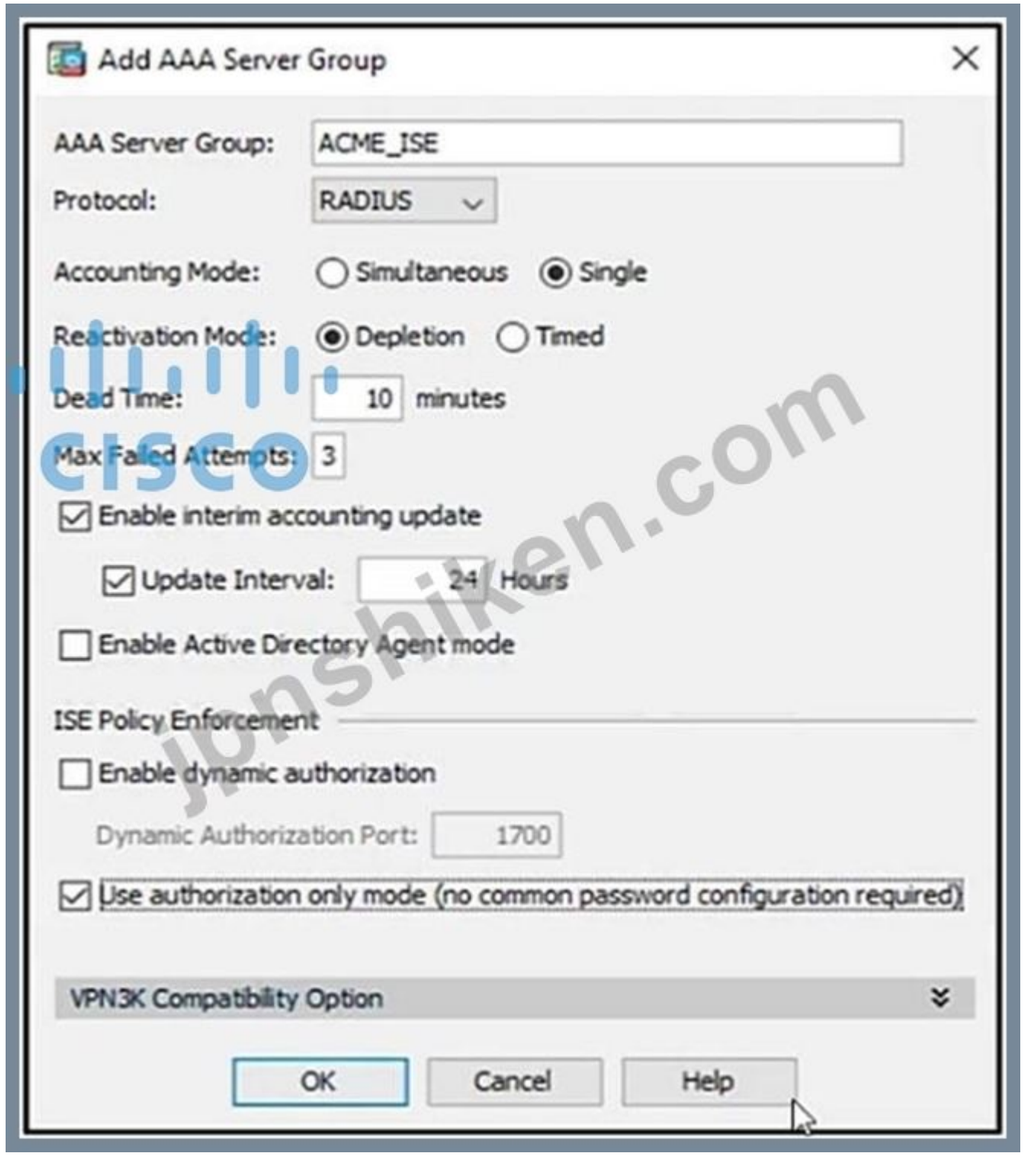
質問: **209**
Cisco ISE管理者は、クローズドモードで特定のエンドポイントがネットワークにアクセスするのを制限する必要があります。要件は、アクセスを制限するためにCiscoISEにエンドポイントを一元的に保存させることです。このタスクを達成するために何をしなければならないか」
A. 各MACアドレスを手動でブロックリストIDグループに追加し、アクセスを拒否するポリシーを作成します
B. 各デバイスのプロファイルポリシーの論理プロファイルを作成し、承認ポリシーを介してそれをブロックします。
C. cdpCacheDeviceId属性を使用して、各エンドポイントのプロファイリングポリシーを作成します。
D. アクセスを拒否するポリシーに各IPアドレスを追加します。
正解: (正解を表示します)
To accomplish this task, the Cisco ISE administrator must follow these steps:
- Create a blocklist identity group.
- Add each MAC address of the endpoints that must be restricted from accessing the network to the blocklist identity group.
- Create a policy that denies access to the blocklist identity group.

- Apply the policy to the network access devices.

質問: **210**
自動フェイルオーバーをサポートしていないCisco ISEノードはどれですか？
A. インライン姿勢ノード
B. 監視ノード
C. ポリシーサービスノード
D. 管理者ノード
正解: **(**正解を表示します**)**
The administration persona can take on any one of the following roles: Standalone, Primary, or Secondary. If the primary Administration ISE node goes down, you have to manually promote the secondary Administration ISE node. There is no automatic failover for the Administration persona.

質問: **211**
Cisco ISEのゲストサービスをサポートしないシナリオはどれですか？
A. ローカルWeb認証を備えた有線NAD
B. ローカルWeb認証機能を備えた無線LANコントローラ
C. 中央Web認証機能を備えた無線LANコントローラ
D. 中央Web認証を備えた有線NAD
正解: **C (**コメントを発表する**)**

質問: **212**
図を参照してください。エンジニアがリモートアクセスVPNを構成し、AAAにCisco ISEを使用するように設定している際に、接続エンドポイントに対してポスチャチェックを実行する必要があります。エンドポイントが接続されると、最初の認証結果を受信し、コンプライアンススキャンに進みます。
このAAA構成で、ネットワークへの準拠したアクセスを可能にするには、何をする必要がありますか？



A. 姿勢認証を、デフォルトで不明なステータスになるように設定します。
B. CoAポート番号を修正する
C. 認証専用モードが有効になっていないことを確認してください
D. AAAサーバーグループ内で動的認証を有効にする
正解: **D (**コメントを発表する**)**
RFC 3576 and its successor RFC 5176 defined a new enhancement to RADIUS known as Dynamic Authorization Extensions to RADIUS, more commonly called Change of Authorization (CoA).