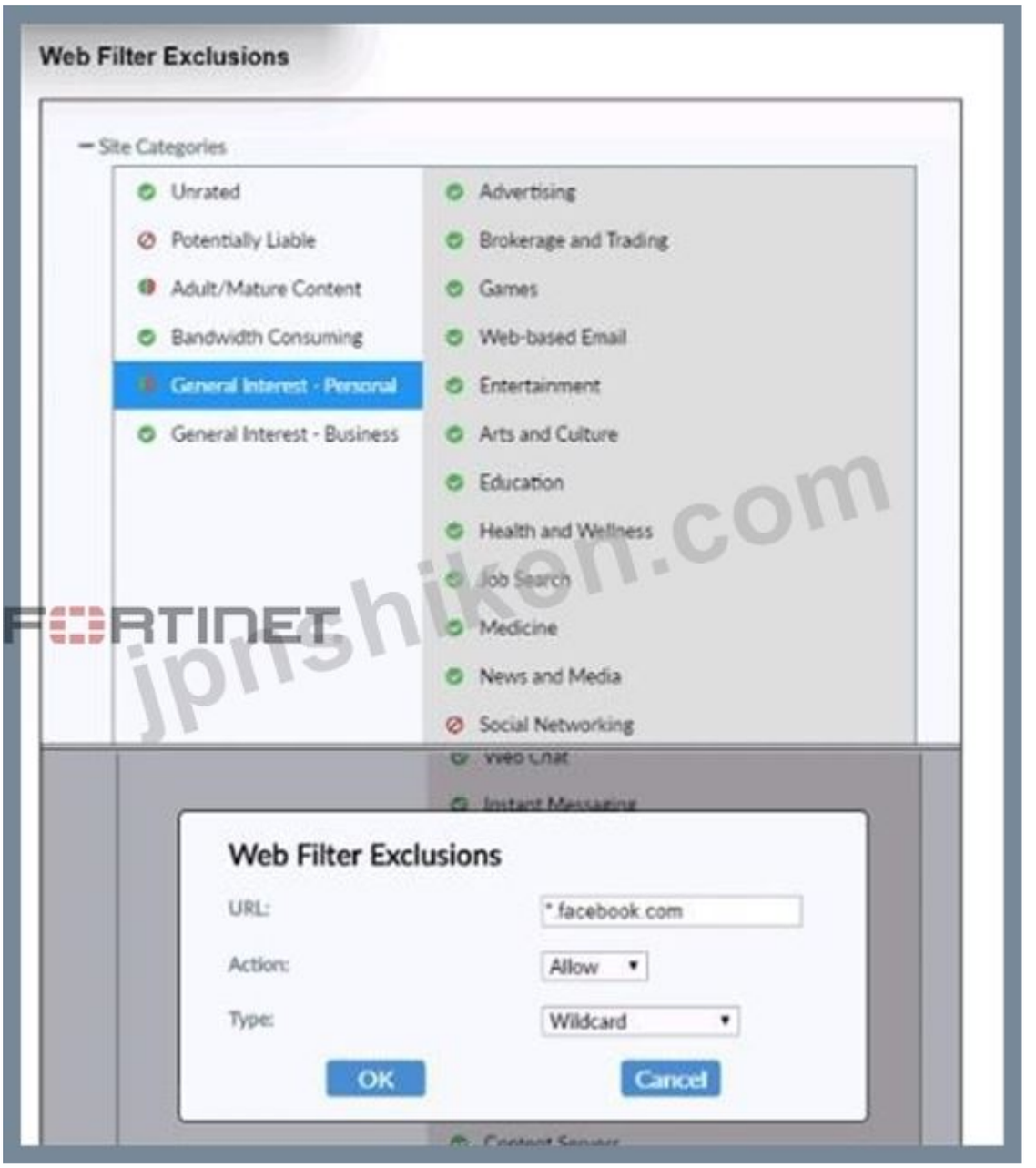
Fortinet.FCP_FCT_AD-7.4.v2026-03-23.q23

試験コード：	FCP_FCT_AD-7.4
試験名称：	FCP - FortiClient EMS 7.4 Administrator
認証ベンダー：	Fortinet
無料問題の数：	23
バージョン：	v2026-03-23
ページの閲覧量：	105
問題集の閲覧量：	263

https://www.jpnshiken.com/shiken/Fortinet.FCP_FCT_AD-7.4.v2026-03-23.q23.html

質問: **1**
管理者が FortiClient を導入するために使用できるサードパーティ ツールはどれですか (2 つ選択してください)。
A. Microsoft Windows インストーラー
B. B. マイクロソフト SCCM
C. C. Microsoft Active Directory GPO
D. QRコードジェネレーター
正解: **(正解を表示します)**
管理者は、いくつかのサードパーティ ツールを使用して FortiClient を展開できます。
* Microsoft SCCM（System Center Configuration Manager）SCCMは、多数のWindowsベースシステムにソフトウェアを導入するための堅牢なツールです。ソフトウェア配布機能を通じてFortiClientの導入をサポートします。
* Microsoft Active Directory GPO（グループ ポリシー オブジェクト）GPO は、Active Directory 環境におけるユーザーとコンピュータの設定を管理するために使用されます。管理者は、GPO ソフトウェアのインストール設定を使用して、FortiClient を複数のマシンに導入できます。
これらのツールは、エンタープライズ環境内の多数のエンドポイントに FortiClient を展開するための集中化されたスケーラブルな方法を提供します。
参考文献
* FortiClient EMS 7.2 学習ガイド、FortiClient 導入セクション
* SCCM と GPO を使用した FortiClient の導入に関する Fortinet のドキュメント

質問: **2**
展示品を参照してください。



展示に示されている設定に基づいて、ユーザーが www facebook com にアクセスしようとしたときに FortiClient はどのようなアクションを実行しますか?

A. FortiClient は Facebook へのアクセスを許可します。

B. FortiClient は Facebook とそのサブドメインへのアクセスをブロックします。

C. FortiClientはFacebookウェブサイトへのユーザーのウェブアクセスのみを監視します

D. FortiClientは、Facebookのウェブサイトにアクセスする前に、ユーザーに警告メッセージを表示します。

正解: **B** (コメントを発表する)

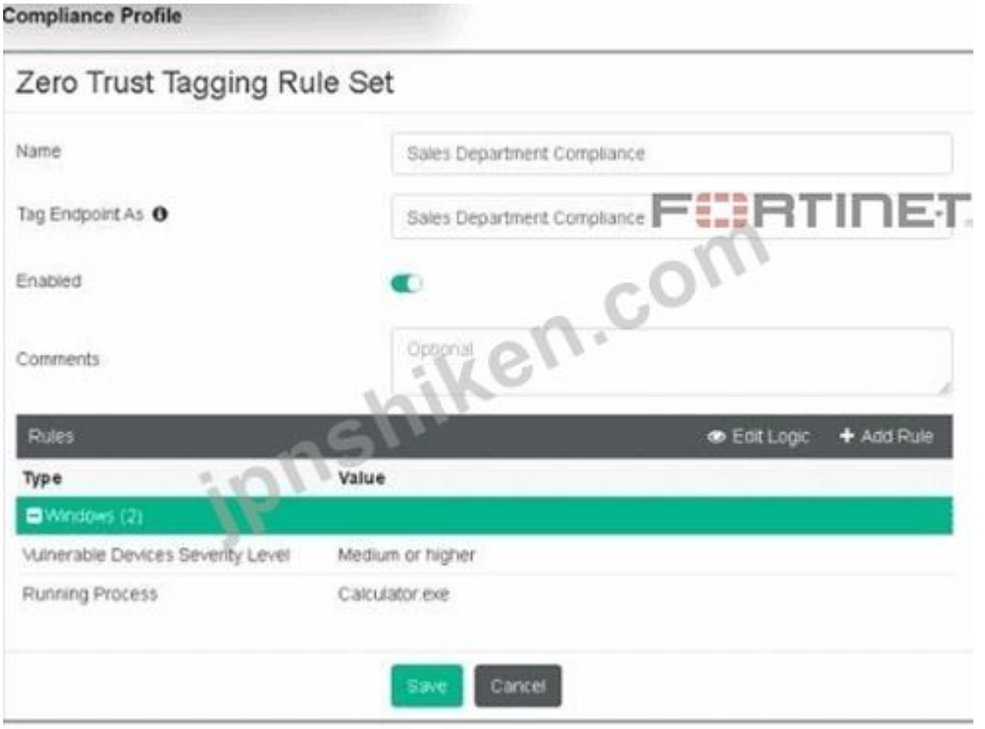
* Webフィルタ除外の観察:

* この図では、アクションが 「許可」に設定された 「*.facebook.com」に対する Web フィルターの除外を示しています。

* アクションの評価:

* この構成は、FortiClient が Facebook とそのサブドメインへのアクセスを許可することを意味します。
* 結論：
* ユーザーが「www.facebook.com」にアクセスしようとすると、FortiClient は Web フィルターの除外設定に基づいてアクセスを許可します。
参考文献:
学習ガイドからの FortiClient Web フィルターの構成と除外に関するドキュメント。

質問: **3**
展示品を参照してください。



図に示されている設定に基づいて、エンドポイントを準拠させるために管理者が実行する必要がある 2 つのアクションはどれですか。(2 つ選択してください。)
A. Web フィルター プロファイルを有効にします。
B. エンドポイントで計算機アプリケーションを実行します。
C. FortiSandboxを統合して感染ファイル解析を行う
D. 脆弱性が「高」以上と評価されたアプリケーションにパッチを適用します。
正解: **B,D (**コメントを発表する**)**
* コンプライアンスプロファイルの観察:
* 図に示されているコンプライアンス プロファイルには、脆弱性の重大度レベルと実行プロセス (Calculator.exe) に関するルールが含まれています。
* コンプライアンスのためのアクションの評価:
* エンドポイントを準拠させるには、管理者は脆弱性の重大度レベルが中以上 (D) であることを確認する必要があります。

* さらに、Calculator.exe アプリケーションがエンドポイント (B) で実行されている必要があります。
* 誤った選択肢を排除する:
* Web フィルタ プロファイル (A) を有効にすることは、表示されているコンプライアンス ルールとは関係ありません。
* 指定されたコンプライアンス プロファイルでは、FortiSandbox (C) の統合は必須ではありません。
* 結論：
* 正しいアクションは、エンドポイントで Calculator アプリケーションを実行し (B)、脆弱性が高以上と評価されたアプリケーションにパッチを適用する (D) ことです。
参考文献:
学習ガイドからの FortiClient EMS コンプライアンス プロファイル構成ドキュメント。

質問: **4**
FortiClient の包括的なエンドポイント保護に関する正しい記述はどれですか?
A. 電子メールスパムからシステムを保護するのに役立ちます
B. システムをデータ損失から保護するのに役立ちます。
C. DDoS からシステムを保護するのに役立ちます。
D. マルウェアなどの高度なセキュリティの脅威からシステムを保護するのに役立ちます。
正解: **(**正解を表示します**)**
FortiClientは、Windows、Mac、Linuxベースのデスクトップ、ノートパソコン、ファイルサーバー、そしてiOSやAndroidなどのモバイルデバイスに包括的なエンドポイント保護を提供します。高度なセキュリティテクノロジーでシステムを保護し、すべてを単一の管理コンソールから管理できます。

質問: **5**
Security Fabric 統合を通じて ZTNA タグ情報を共有するコンポーネントまたはデバイスはどれですか?
A. FortiGate
B. FortiGate アクセス プロキシ
C. FortiClient
正解: **A (**コメントを発表する**)**
FortiClient EMS は、Security Fabric 統合を通じて ZTNA タグ情報を共有するコンポーネントです。
ZTNAタグは、FortiGateアプリケーションゲートウェイへの入力としてFortiClient EMSから同期されます。これらのタグは、ZTNAポリシーでセキュリティポスチャチェックとして使用し、特定のセキュリティ基準が満たされているかどうかを確認できます。FortiClient EMSは、FortiGate、FortiManager、FortiAnalyzerなど、ファブリック内の複数のデバイス間でZTNAタグを共有できます。また、FortiClient EMSは、同じFortiGateデバイス上の複数のVDOM間でZTNAタ

グを共有することもできます。FortiClient EMSは、ファブリックデバイス設定1でZTNAタグの共有動作を制御するように設定できます。
FortiGateは、ZTNAタグを用いてZTNAポリシーを適用するデバイスです。FortiGateは、ファブリックコネクタを介してFortiClient EMSからZTNAタグを受信できます。また、FortiGateはZTNAポータルを通じてZTNAサービスを公開できるため、ユーザーはFortiClientをインストールすることなくアプリケーションにアクセスできます。さらに、FortiGateはSaaSアプリケーションのアクセス制御のためのZTNAインラインCASBも提供できます2。
FortiGate アクセス プロキシは、FortiGate を ZTNA トラフィックのプロキシとして機能させる機能です。FortiGate アクセス プロキシは、アプリケーション サーバーの前面に導入することで ZTNA 保護を提供できます。また、アプリケーション サーバーの背面に導入することで ZTNA の可視性を提供することもできます。FortiGate アクセス プロキシは、ZTNA タグを使用してユーザーとデバイスを識別および認証できます2。
FortiClientは、ZTNAサービスに接続するエンドポイントソフトウェアです。FortiClientは、エンドポイントのセキュリティポスチャに基づいて、FortiClient EMSにZTNAタグを登録できます。また、FortiClientはZTNAタグを使用して、FortiGateによって公開されたZTNAサービスにアクセスすることもできます。さらに、FortiClientはZTNAタグを使用して、ZTNAインラインCASB2を備えたSaaSアプリケーションにアクセスすることもできます。
参考文献:
* テクニカルヒント: 同じ FortiClient EMS サーバーに接続されたセキュリティ ファブリック内の複数の vdom または複数の FortiGate ファイアウォール間で共有される ZTNA タグの動作
* FortiClient ZTNAタグの同期
* アプリケーションアクセスを制御するゼロトラストネットワークアクセス（ZTNA）

質問: **6**
FortiClient EMS 管理者は、コンプライアンス チェックのために FortiClient に追加のセキュリティを実装しています。
管理者は、脆弱性の重大度レベルに基づいてエンドポイントを検出するためにどのタグを構成できますか?
（1つ選択してください）
A. アウトブレイクアラートタグ
B. 分類タグ
C. ファブリックタグ
D. セキュリティポスチャタグ
正解: **(正解を表示します)**
FortiClient EMS 7.2/7.4 管理ガイドおよび ZTNA 導入ガイドによれば、管理者はセキュリティ ポスチャ タグ (最新バージョンでは Zero Trust Network Access (ZTNA) タグとも呼ばれます) を構成して、脆弱性の重大度レベルなどの特定のコンプライアンス基準に基づいてエンドポイントを検出し、グループ化することができます。
1. 脆弱性に対するセキュリティポスチャタグの仕組み:

* タグ付けルール: EMS のセキュリティ ポスチャ タグ (またはゼロ トラスト タグ) セクションで、管理者は新しいルール セットを作成し、ルールを追加します。
* ルール タイプ: 管理者は、脆弱なデバイスのルール タイプを選択します。
* 重大度レベル: このルールでは、管理者は重大度レベル(重大、高など)を指定できます。
、中、または低）。EMS は、脆弱性スキャンによってその重大度レベルに一致するかそれを超える脆弱性が少なくとも 1 つ検出されたエンドポイントに、タグを動的に適用します。
* 動的グループ化: これらのタグを使用すると、エンドポイントを動的にグループ化することができ、その後、FortiGate と同期して、デバイスの現在のセキュリティ体制に基づいてアクセス制御を実施できます。
2. 他の選択肢が間違っている理由:
* A. アウトブレイク アラート タグ: FortiGuard アウトブレイク アラートはタグ付けに使用できますが、すべての脆弱性の重大度レベルに一般的なメカニズムを提供するのではなく、特定の「アウトブレイク」または現在活発に活動している注目度の高い脅威に対して脆弱なエンドポイントを特にターゲットにします。
* B. 分類タグ: これらのタグは通常、脆弱性スキャンに基づくリアルタイムのセキュリティ態勢コンプライアンスではなく、より広範なエンドポイント識別 (部門や場所など) やレポート用の FortiAnalyzer への情報送信に使用されます。
* C. ファブリック タグ: 「ファブリック」は通常、Fortinet デバイス (セキュリティ ファブリック) 間の統合を指します。
タグはファブリック全体で共有されますが、ポスチャに基づいてエンドポイント検出用に EMS 内で構成された特定のタグは、セキュリティ ポスチャ/ゼロ トラスト タグとして分類されます。
3. カリキュラム参考文献:
* FortiClient EMS管理ガイド ゼロトラストタグ付けルールのセクション） :
脆弱なデバイス」ルール タイプとその重大度オプション。
* EMS 学習ガイド (コンプライアンスと脆弱性): これらのタグを使用して、エンドポイントがネットワークへのアクセスを許可する前に最低限のセキュリティ標準を満たしていることを確認する方法について説明します。

質問**: 7**
ZTNA テレメトリを通じてデバイスのステータス情報を共有するコンポーネントまたはデバイスはどれですか?
A. FortiClient EMS
B. フォーティゲート
C. FortiClient
D. FortiGate アクセス プロキシ
正解**: (**正解を表示します**)**
FortiClient は FortiClient EMS と直接通信し、ZTNA テレメトリを通じてデバイスのステータス情報を継続的に共有します。

質問: **8**

展示品を参照してください。

ウェブサーバーのホスティングサービスを提供しています。エンドポイントがテストファイル (testfile.txt) をダウンロードしますが、FortiClientによってブロックされます。

エンドポイントでファイルにアクセスできるようにするには、どの構成を使用できますか? (回答を 1 つ選択してください)

A. FortiClient を使用してファイルへのアクセスを直接復元します。

B. Web フィルタ プロファイルの除外リスト内の Web サーバー URL を許可します。

C. マルウェア保護プロファイルから testfile.txt を除外します。

D. FortiClient EMS の隔離管理の許可リストにファイルを追加します。

正解: **(正解を表示します)**

FortiClient EMS 7.2/7.4 管理ガイド (特に隔離管理およびマルウェア対策のセクション) によると、ブロックされたファイルを復元し、悪意のあるファイルとしてフラグ付けされないようにするための正しい管理ワークフローは、EMS サーバーの隔離管理機能を使用することです。

1. 展示物の分析

* イベント タイプ: この図は、testfile.txt というファイルにマルウェア: EICAR_TEST_FILE のフラグが付けられたウイルス対策イベントを示しています。

* 場所:ファイルはローカルユーザーディレクトリ(C:\Users\administrator\Desktop\Resources\testfile.txt)。

* システム状態: エンドポイントは EMS によって管理されています (ポリシー: デフォルトと EMS ステータス アイコンで示されます)。

2. オプションDが正しい選択である理由:

* 集中管理：管理された環境では、管理者はEMSコンソールを使用してセキュリティインシデントを監視します。隔離されたファイルを復元するには、「隔離管理」> 「ファイル」に移動する必要があります。

* 許可リストと復元アクション: 特定のブロックされたファイル (testfile.txt) を選択し、[許可リストと復元] をクリックすると、次の 2 つのことが同時に発生します。

* 復元:EMS は、FortiClient エンドポイントにコマンドを送信し、ファイルをローカルの隔離フォルダから解放して元のパスに戻します。

* 許可リスト: ファイルのハッシュが許可リスト ([隔離管理] > [許可リスト] で管理) に追加され、今後のリアルタイム スキャンまたはオンデマンド スキャン中に FortiClient がファイルを再隔離することを防ぎます。

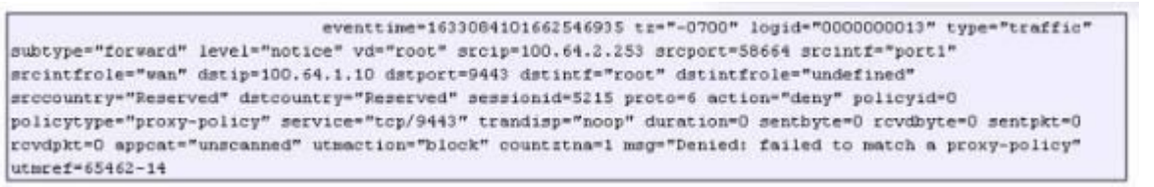
* アクセシビリティ: これは、ファイルがセキュリティ エンジンによってすぐに再ブロックされないようにしながら、エンドポイントでファイルを 『アクセス可能」にするための文書化された方法です。
3. 他の選択肢が間違っている理由:
* A. FortiClientを使用して直接アクセスを復元する:FortiClientにはローカル隔離タブがありますが、
集中的なセキュリティ ポリシーの適用を確実にするために、クライアントが EMS によって管理されている場合、『リリース」ボタンは通常、グレー表示または制限されます。
* B. 除外リストでウェブサーバーのURLを許可する :この図は、ウェブフィルターイベントではなく、ウイルス対策/マルウェアイベントを示しています。ファイルはすでにローカルディスクにダウンロードされており、リアルタイム保護エンジンによってブロックされているため、ウェブフィルターURLの除外はローカルファイルのブロックには影響しません。
* C. マルウェア対策プロファイルから testfile.txt を除外する :マルウェア対策プロファイルにパスの除外を追加することは、ディレクトリの今後のスキャンを阻止する有効な方法ですが、既に隔離されたファイルを自動的に復元するわけではありません。既存のブロックに対する適切なワークフローは、まず隔離管理ツールを使用することです。

質問: **9**
FortiClient EMS の展開プロファイルを示す展示を参照してください。

管理者が FortiClient EMS で展開プロファイルを作成する場合、展開プロファイルに関するどの記述が正しいですか。
A. 展開 2 は、AD グループとワークグループの両方で FortiClient をアップグレードします。
B. Deployment-1 は、新しい AO グループ エンドポイントに FortiClient をインストールします。
C. デプロイメント 2 は、AD グループとワークグループの両方に FortiClient をインストールします。
D. Deployment-1 はワークグループ上の FortiClient のみをアップグレードします。
正解: **A** (コメントを発表する)
* 展開プロファイル分析:
* Deployment-1 には 『初回インストール」パッケージがあり、優先度 1 で 『すべてのグループ」に割り当てられていますが、有効になっていません。
* Deployment-2 には 『To-Upgrade」パッケージがあり、 『すべてのグループ」と 『trainingAD」の両方に割り当てられています。
『training.lab」というファイルが作成され、優先度は 2 に設定され、有効になっています。

* 展開2の評価:
* 展開2では、「すべてのグループ」と「trainingAD.training.lab」の両方のFortiClientが有効化され、これらのグループに割り当てられているため、両方のグループでFortiClientをアップグレードします。これにはAD（Active Directory）グループとワークグループの両方が含まれます。
* 結論：
* Deployment-2 は、割り当てられたすべてのグループとワークグループで FortiClient をアップグレードするように設定されているため、正解は A です。
参考文献:
学習ガイドからの FortiClient EMS の展開およびプロファイルのドキュメント。

質問: **10**
FortiGate 上の ZTNA トラフィック ログの出力を示す図を参照してください。


```
eventtime=1633084101662546935 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=100.64.2.253 srcport=58664 srcintf="port1"
srcintfrole="wan" dstip=100.64.1.10 dstport=9443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=5215 proto=6 action="deny" policyid=0
policytype="proxy-policy" service="tcp/9443" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: failed to match a proxy-policy"
utmref=65462-14
```

ログメッセージから何がわかりますか?
A. リモート ユーザー接続がローカル入力ポリシーと一致しません。
B. リモート ユーザー接続が ZTNA ルール設定と一致しません。
C. リモート ユーザー接続が ZTNA サーバーの構成と一致しません。
D. リモート ユーザー接続が ZTNA ファイアウォール ポリシーと一致しません。
正解: **B (**コメントを発表する**)**
* ZTNAトラフィックログの観察:
* ログ メッセージは、プロキシ ポリシーに一致しなかったため、リモート ユーザー接続が拒否されたことを示します。
* ログメッセージを評価しています:
* メッセージは、接続が既存の ZTNA ルール構成と一致していないことを示しており、拒否につながっています。
* 結論：
* ログ メッセージからの正しい結論は、リモート ユーザー接続が ZTNA ルール構成と一致していないということです (B)。
参考文献:
学習ガイドからの ZTNA トラフィック ログ分析および構成ドキュメント。

質問: **11**
管理者は、BYOD とリモート ユーザーが存在する組織に FortiClient を導入する必要があります。管理者は FortiClient を展開するために何を使用できますか? (1 つの回答を選択してください)
A. FortiClientゼロタッチプロビジョニング
B. Microsoft システム センター構成マネージャー (SCCM)
C. Microsoft Intune

D. グループ ポリシー オブジェクト (GPO)
正解**: (**正解を表示します**)**
FortiClient EMS 管理者学習ガイドおよび Fortinet ドキュメント ライブラリ (バージョン 7.2/7.4) によると、BYOD (Bring Your Own Device) およびリモート ユーザーに FortiClient を展開する最も効果的な方法は、Microsoft Intune (またはその他のサポートされているモバイル デバイス管理 - MDM ソリューション) を使用することです。
1. Microsoft Intune (回答 C) が正しい選択である理由:
* クラウドベースのアクセシビリティ：従来、オンプレミスのインフラストラクチャにアクセスするためにローカルのActive Directory（AD）ドメインへの直接接続やVPNを必要とするGPOやSCCMとは異なり、Microsoft Intuneはクラウドベースの MDMです。そのため、企業ネットワークに常駐していないリモートユーザーにとって、Intuneは最適な選択肢となります。
* BYOD管理：Intuneは、BYOD環境で一般的に使用される様々なオペレーティングシステム（Windows、macOS、iOS、Android）を管理するために特別に設計されています。管理者は、FortiClientインストールパッケージと登録構成（invitation_codeやems_serverの詳細など）をクラウド経由でユーザーのデバイスに直接プッシュできます。
* EMSとの統合：FortiClient EMS 7.2/7.4には、Intuneとの統合に関する具体的なドキュメントが用意されています。管理者はEMSでカスタムMSIまたは.pkgインストーラーを作成し、Intuneにアップロードすることで、Intuneのアプリ構成ポリシーを使用してEMSへのテレメトリ接続を自動化できます。
2. このシナリオで他のオプションが不適切である理由:
* A. FortiClient ゼロタッチ プロビジョニング: FortiClient はゼロタッチ プロビジョニング (特にモバイルまたは FortiCloud 経由) をサポートしていますが、組織の広範な BYOD およびリモート フリートの「展開ツール」というコンテキストでは、サードパーティのリモート デバイス上の初期ソフトウェア パッケージのスタンドアロン展開メカニズムではなく、Intune などの MDM によって促進される機能またはプロセスであることが一般的です。
* B. Microsoft SCCM：SCCM（現在はMicrosoft Configuration Managerの一部）はオンプレミスのインフラストラクチャに大きく依存しており、通常は企業所有のドメイン参加デバイスに使用されます。リモートユーザーの「管理対象外」BYODデバイスの管理に関しては、Intuneほど柔軟性がありません。
* D. グループポリシーオブジェクト（GPO）GPOを使用するには、デバイスがActive Directory（AD）ドメインに参加している必要があります。BYODデバイスは通常、ドメインに参加しておらず、リモートデバイスはポリシー更新時にVPN経由で接続されていない限りGPOの更新を受信できないため、この特定のユースケースには適していません。
3. カリキュラム参考文献:
* EMS管理ガイド（展開セクション）AD経由でアクセスできないエンドポイントの場合/Workgroups (リモートおよび BYOD をカバー) の場合、管理者はインストーラー リンク メソッドまたは MDM (Microsoft Intune など) を使用する必要があります。

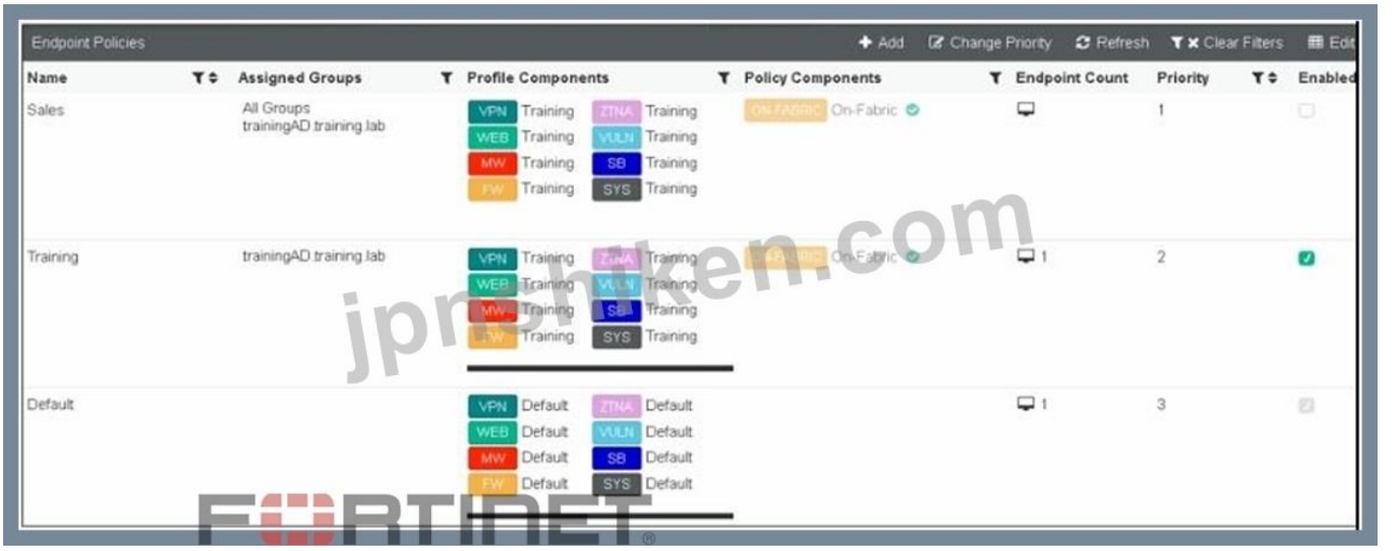
* FortiClient の Intune 展開ガイド: リモート ユーザーがアプリをインストールすると、正しい EMS インスタンスに自動的に登録されるように、Intune から FortiClient アプリに渡される構成キー (cloud_invite_code、ems_server など) の具体的な使用方法を詳しく説明します。

質問: **12**
新しい Chrome Book が学校のネットワークに接続されます。
EMS 管理者は、Google Chromebook エンドポイントにインストールされた FortiClient Web フィルタ拡張機能を管理するためにどのコンポーネントを使用できますか?
A. FortiClient EMS
B. FortiClientサイトカテゴリ
C. FortiClient顧客URLリスト
D. FortiClient Web フィルター拡張機能
正解: **D (**コメントを発表する**)**
Google Chromebook エンドポイントにインストールされている FortiClient Web フィルタ拡張機能を管理するために、EMS 管理者は次のコンポーネントを使用できます。
* FortiClient EMS (エンタープライズ管理サーバー) は、さまざまなエンドポイントにわたる複数の FortiClient インストールを管理および制御するように設計されています。
* EMS は、Web フィルタリング構成を含むエンドポイント ポリシーの集中管理を提供します。
* EMS 管理者は、EMS コンソールを通じて Chromebook 上のウェブ フィルタ ポリシーを設定および適用できます。
したがって、FortiClient EMS は、Google Chromebook エンドポイント上の Web フィルター拡張機能を管理するための適切なコンポーネントです。
参考文献
* FortiClient EMS 7.2 学習ガイド、Chromebook 管理セクション
* Chromebook 向け FortiClient EMS および Web フィルタリングに関する Fortinet のドキュメント

質問: **13**
管理者がFortiGateでZTNA構成を設定します。ファイアウォールポリシーについて正しい記述はどれですか？
A. クライアント要求をアクセス プロキシにリダイレクトします。
B. アクセス プロキシを使用します。
C. ZTNA サーバーを定義します。
D. エンドポイントへのアクセスを制御するために ZTNA タグのみを使用します。
正解: **(**正解を表示します**)**
「ファイアウォール ポリシーはクライアント要求を照合し、アクセス プロキシ VIP にリダイレクトします」https://docs.fortinet.com
/document/fortigate/7.0.0/新機能/194961/基本的なZTNA構成

質問: **14**

FortiClient EMSエンドポイントポリシー



FortiClient EMS上の複数のエンドポイントポリシーを示す図を参照してください。ADグループtrainingADのエンドポイントにはどのポリシーが適用されていますか？

A. トレーニングポリシー

B. セールスポリシーとトレーニングポリシーの両方。優先度がデフォルトポリシーよりも高いため。

C. 最も優先度が高いため、デフォルトのポリシーです。

D. 販売ポリシー

正解: **(**正解を表示します**)**

* エンドポイントポリシーの遵守:

* この図には、複数のエンドポイント ポリシーと、それらに割り当てられたグループ、優先度レベル、および有効なステータスが表示されます。

* ポリシー割り当ての評価:

* トレーニング ポリシーは、デフォルト ポリシーよりも高い優先度で、「trainingAD.training.lab」グループに明確に割り当てられます。

* 結論：

* AD グループ「trainingAD」内のエンドポイントに適用されている正しいポリシーは、トレーニング ポリシー (A) です。

参考文献:

学習ガイドからの FortiClient EMS ポリシー構成および優先度管理ドキュメント。

質問: **15**

展示品を参照してください。

展示に示されている FortiClient の詳細に基づいて、正しいと思われる 2 つの記述はどれですか。(2 つ選択してください。)

A. ファイル名は、さらに検査するために FortiSandbox に送信されます。

B. ファイルの場所は \??\D:\Users\ です。

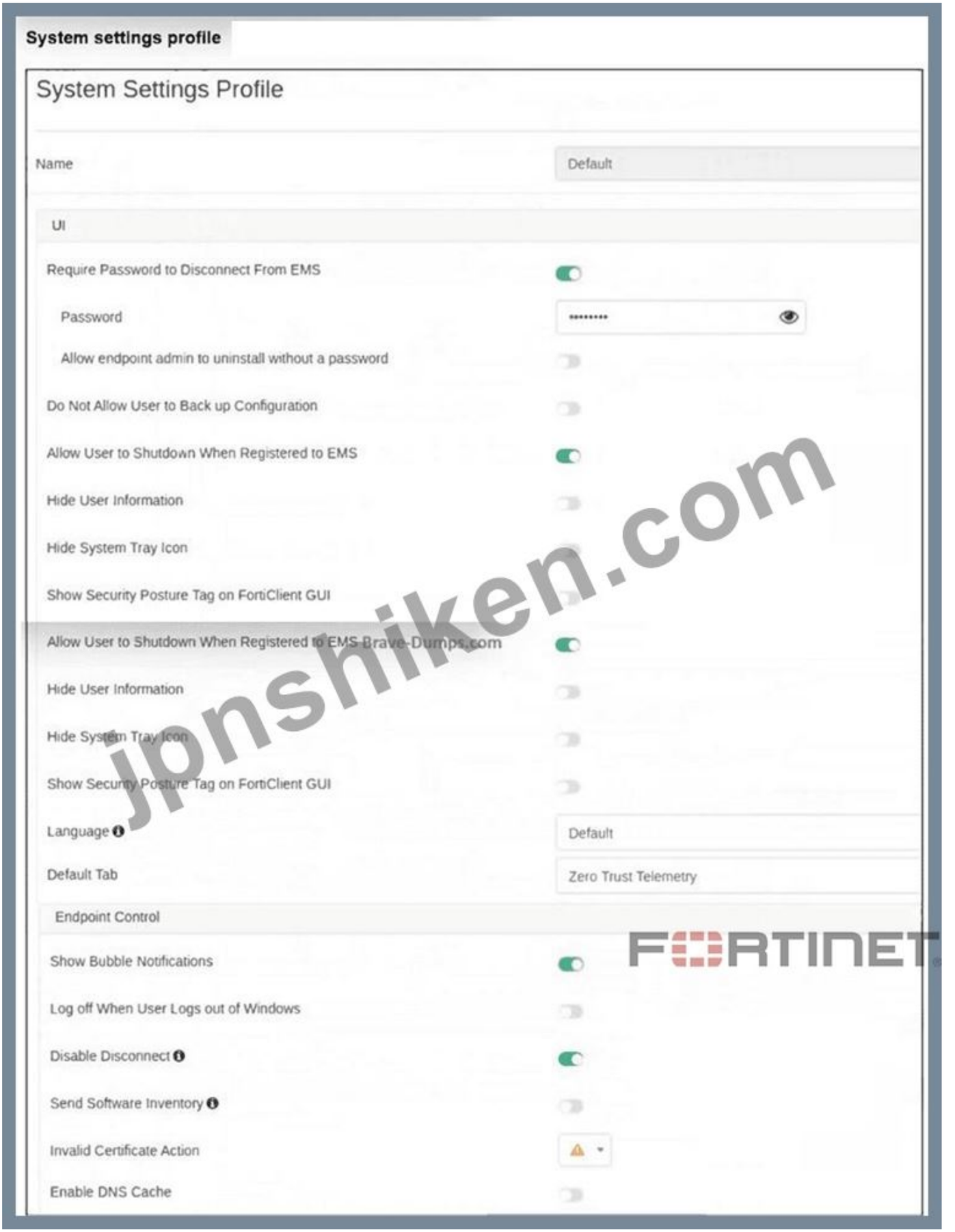
C. ファイル名は未確認です 899290.crdovnload。

D. ファイルのステータスは隔離されています

正解: **C,D (**コメントを発表する**)**

質問: **16**

展示品を参照してください。



無効な証明書を持つ FortiClient が FortiClient EMS に接続している場合、どのような動作が予想されますか? (1 つの回答を選択してください)

A. FortiClient は FortiClient EMS への接続をブロックされています。

B. FortiClient では、FortiClient EMS に接続するために追加のパスワードが必要です。
C. FortiClient はエンドユーザーに警告メッセージを表示します。
D. FortiClient EMS は有効な証明書を FortiClient にプッシュします。
正解**: (**正解を表示します**)**
FortiClient EMS 7.2/7.4 管理ガイドおよびシステム設定プロファイルの提供された展示に基づいて、無効な証明書接続の予想される動作は、無効な証明書アクション設定によって決定されます。
1. 展示物の分析
* 場所:展示では、システム設定プロファイル (具体的には「デフォルト」プロファイル) が表示されます。
* 設定:エンドポイント制御セクションの下部で、無効な証明書アクションフィールドが構成されます。
* 選択されたアクション: 無効な証明書アクションのドロップダウンには警告アイコン（感嘆符付きのオレンジ色の三角形）が表示されます。FortiClient EMS GUIでは、このアイコンは「警告」アクション。
2. 検証済みの行動（オプションC）
エンドポイント通信セキュリティに関するカリキュラム文書によると、
* 警告アクションの動作:無効な証明書アクションが警告に設定されている場合、EMS サーバー証明書が信頼されていない、期限が切れている、またはホスト名が一致しない場合に、FortiClient はエンド ユーザーに警告メッセージを表示するように指示されます。
* ユーザープロンプト: 警告メッセージは、セキュリティ上のリスクがあるにもかかわらず接続を続行するか、試行を終了するかをユーザーに明示的に尋ねます。
* 接続ロジック: ユーザーが手動で警告を受け入れると、FortiClient はテレメトリ接続を確立し、その特定のサーバーに対するプロンプトが繰り返し表示されるのを避けるために、将来のセッションのために証明書を「記憶」します。
3. 他の選択肢が間違っている理由
* A. FortiClient がブロックされています: この動作は、管理者がプロファイルで「拒否」アクションを選択した場合にのみ発生します。
* B. 追加のパスワードが必要: 展示の上部に表示されているパスワード フィールドは、「EMS から切断するにはパスワードが必要」用であり、ユーザーが手動で登録解除することを防ぎますが、証明書エラーを回避または解決するものではありません。
* D. EMS は有効な証明書をプッシュします:EMS は、失敗した TLS ハンドシェイクを解決するために有効な ID 証明書を「プッシュ」することはできません。有効な証明書は、管理者が EMS サーバーに手動でインストールする必要があります。

質問: 17
FortiClient Web フィルターでサイト カテゴリが無効になっている場合、エンドポイントを悪意のある Web アクセスから保護するために使用できる機能はどれですか。
A. リアルタイム保護リスト
B. ウイルス対策ソフトで悪質なウェブサイトをブロックする
C. FortiSandbox URLリスト
D. Web除外リスト
正解: (正解を表示します)
* Webフィルター機能:
* FortiClient Web フィルターでサイト カテゴリが無効になっている場合でも、エンドポイントは悪意のある Web アクセスから保護する必要があります。
* 代替保護機能:
* Web 除外リストを使用すると、悪意のあることがわかっている特定の URL を管理およびブロックできるため、サイト カテゴリが有効になっていなくても、Web アクセスを制御および保護することができます。
* 結論：
* このシナリオでエンドポイントを保護するために使用できる正しい機能は、Web 除外リスト (D) です。
参考文献:
学習ガイドからの FortiClient Web フィルターの構成と機能。

質問: 18
展示品を参照してください。

展示に示されている設定に基づくと、FortiClient の動作に関するどの記述が Hue ですか。

A. ユーザーがファイルをリソース フォルダーにコピーすると、FortiClient は感染したファイルをスキャンします。

B. FortiClient は感染した接続を隔離し、スキャン後に後で確認します。

C. FortiClient は感染したファイルをスキャンせずに Resources フォルダにコピーします。

D. FortiClient は感染したファイルをスキャンした後にブロックして削除します。

正解: (正解を表示します)

添付資料の設定に基づき、FortiClientはファイルがシステムにダウンロードまたはコピーされる際にスキャンするように設定されています。つまり、ユーザーが Resources」フォルダ（除外リストに含まれていない）にファイルをコピーした場合、FortiClientはこれらのファイルの感染をスキャンします。設定に記載されている除外パス C:\Users\Administrator\Desktop\Resources」は、この特定のフォルダにコピーされたファイルはスキャンされないことを示していますが、質問は Resources」フォルダが除外パスと同じではないことを示唆しているため、FortiClient は実際にファイルの感染をスキャンします。

質問: **19**

FortiClient のクイックスキャン オプションの機能は何ですか?

A. 現在実行中のプログラムとドライバーをスキャンして脅威を検出します

B. すべてのファイル、実行可能ファイル、DLL、およびドライバを含む完全なシステム スキャンを実行します。

C. ユーザーは、ローカル ハード ディスク ドライブ (HDD) 上の特定のファイル フォルダーを選択して、脅威をスキャンできます。

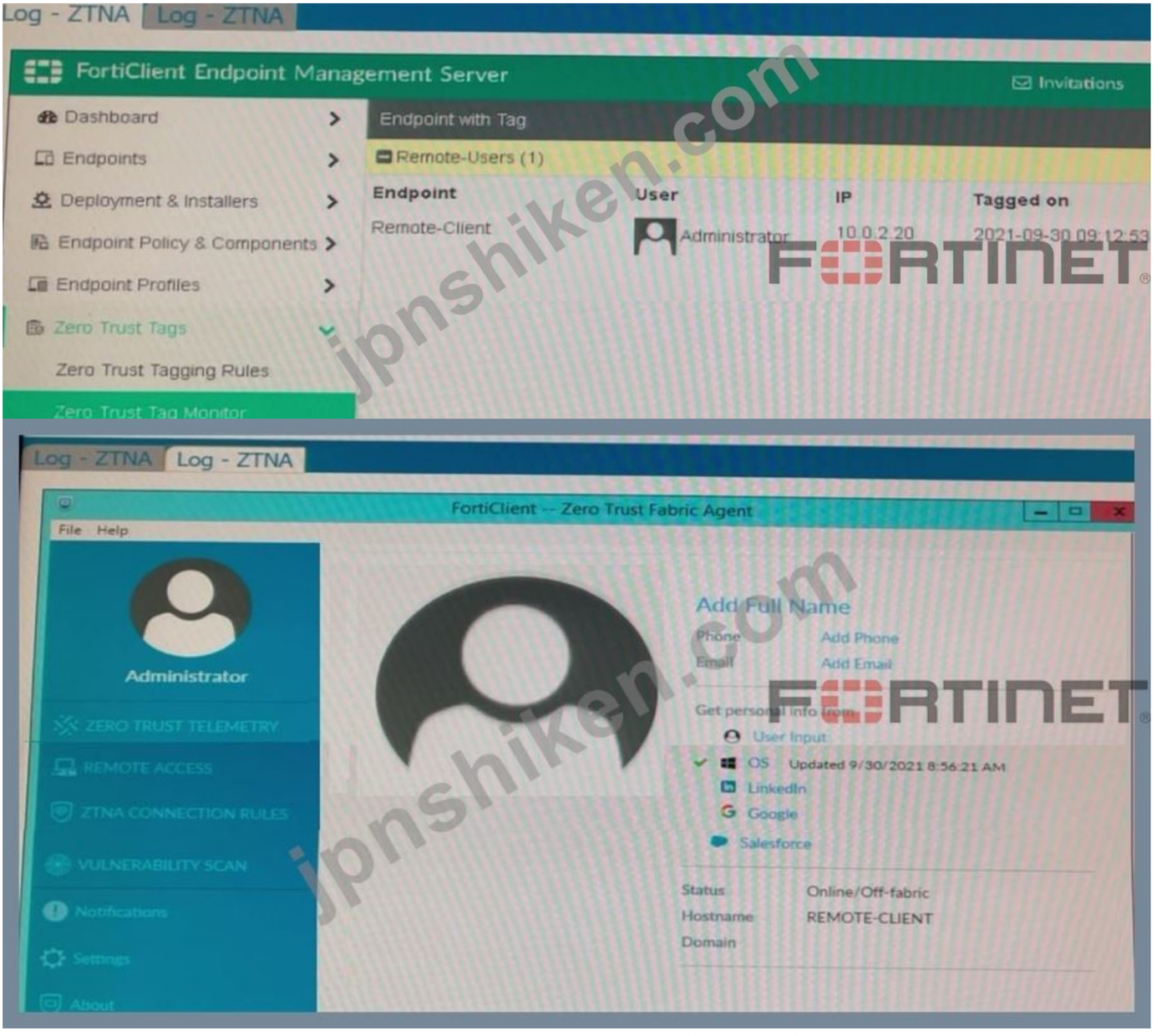
D. 実行可能ファイル、DLL、および現在実行中のドライバーをスキャンして脅威を検出します。

正解: (正解を表示します)

* クイックスキャン機能について:

* FortiClient のクイック スキャン オプションは、システムの特定の要素をすばやくスキャンして脅威を検出するように設計されています。
* スキャン範囲の評価:
* クイック スキャンは、現在実行中の実行可能ファイル、DLL、およびドライバーを特にターゲットとし、システムのアクティブなコンポーネントを迅速に評価します。
* 結論：
* 正解は D です。FortiClient のクイック スキャン オプションの機能を正確に説明しているからです。
参考文献:
学習ガイドからの FortiClient スキャン オプションのドキュメント。

質問: **20**
展示物を参照してください。



Zero Trust Tag Monitor と FortiClient GUI のステータスを表示します。

リモート クライアントは、FortiClient EMS Zero Trust タグ モニターでリモート ユーザーとしてタグ付けされます。
FortiClient GUI にタグを表示するには、管理者は何をする必要がありますか?
A. タグの可視性を有効にするためにタグ付けルールのロジックを更新します
B. B. FortiClientのシステム設定を変更してタグの可視性を有効にする
C. エンドポイント制御設定を変更してタグの可視性を有効にします
D. ユーザーID設定を変更してタグの表示を有効にする
正解: (正解を表示します)
提供された展示品に基づくと、次のようになります。
* Remote-Client」は、FortiClient EMS Zero Trust タグ モニターでは Remote-Users」としてタグ付けされます。
* タグ Remote-Users」が FortiClient GUI に表示されるようにするには、FortiClient 内のシステム設定を更新してタグの表示を有効にする必要があります。
* タグの可視性機能は、GUI でのタグの表示方法を管理する FortiClient システム設定によって制御されます。
したがって、管理者はタグの可視性を有効にするために FortiClient システム設定を変更する必要があります。
参考文献
* FortiClient EMS 7.2 学習ガイド、ゼロトラスト タグ付けセクション
* タグ管理と可視性設定に関するFortiClientドキュメント

質問: **21**
FortiClientエンドポイントユーザーがWindowsコマンドプロンプトから使用できるVPNタイプはどれですか？ 2つ選択してください）
A. L2TP
B. PPTP
C. IPSec
D. SSL VPN
正解: (正解を表示します)
FortiClient は、Windows コマンド プロンプトから次の VPN タイプを開始することをサポートしています。
* IPSec VPN:FortiClient は、コマンドライン命令を使用して IPSec VPN 接続を確立できます。
* SSL VPN:FortiClient は、Windows コマンド プロンプトからの SSL VPN 接続の開始もサポートします。
これら 2 つの VPN タイプは、FortiClient が提供する特定のコマンド ライン パラメータを使用して構成および開始できます。
参考文献
* FortiClient EMS 7.2 学習ガイド、VPN 構成セクション
* FortiClient VPN のコマンドライン オプションに関する Fortinet ドキュメント

質問: **22**
FortiClient EMS と Active Directory (AD) の統合に関する次の 2 つの記述のうち正しいものはどれですか。(2 つの回答を選択してください)
A. FortiClient EMS は AD サーバーに対して完全な読み取り/書き込みアクセス権を持ちます。
B. ドメイン エンドポイント上の FortiClient インストールは、FortiClient EMS から展開できます。
C. エンドポイント プロファイルは、ドメイン グループに基づいてエンドポイントに割り当てることができます。
D. インポートされたADエンドポイントはFortiClient EMS上で直接削除できません
正解: **B,C (**コメントを発表する**)**
FortiClient EMS 7.2/7.4 管理ガイドおよび EMS 管理者学習ガイドに基づいて、Active Directory (AD) との統合により、いくつかの自動管理機能が提供されます。
1. 真実の陳述の分析:
* B. ドメインエンドポイントへの FortiClient のインストールは、FortiClient EMS から展開できます。
* FortiClient EMS を使用すると、管理者は AD 経由で検出された Windows エンドポイント専用の展開プロファイルを作成できます。
* 展開プロファイル内で AD 管理者の資格情報を提供することにより、EMS は、ソフトウェアがまだインストールされていないドメインに参加しているエンドポイントに FortiClient MSI インストーラーをリモートでプッシュできます。
* C. エンドポイント プロファイルは、ドメイン グループに基づいてエンドポイントに割り当てることができます。
* AD 統合の主な利点は、エンドポイント ポリシーを特定の AD 組織単位 (OU) またはセキュリティ グループにマップできることです。
* エンドポイント ポリシーが AD グループに割り当てられると、そのグループに属するすべての FortiClient エンドポイントは、そのポリシー内で定義されている関連セキュリティ プロファイル (ウイルス対策、Web フィルター、VPN など) を自動的に受け取ります。
2. 他の選択肢が間違っている/二次的な理由:
* A. FortiClient EMS は AD サーバー上で完全な読み取り/書き込みアクセス権を持ちます。
* カリキュラムでは、LDAP/AD 接続は読み取り専用であると明示的に記載されています。
* EMS は、AD オブジェクトを変更したり、ユーザーを作成したり、グループ メンバーシップを変更したりすることはできません。AD サーバーから EMS データベースに情報を同期するだけです。
* D. インポートされた AD エンドポイントは、FortiClient EMS 上で直接削除できません。
* 機能的な意味では技術的には正しいですが (同期されたエンドポイントを削除すると、AD OU から削除されない限り、次の同期時に再度追加されます)、カリキュラムでは通常、統合の主な機能 特徴」である B と Cas を優先します。
* ガイドでは、同期の競合を防ぐために、エンドポイント ペインの 削除」アクションは非ドメインデバイスに制限されていると指定されていることに注意してください。
3. 統合機能の概要:

* 同期スケジュール:EMS は定期的に AD と同期し (デフォルトでは 10 分ごと)、エンドポイントリストを更新します。
* ポリシーの自動化: ユーザーまたはコンピューターを AD 内の別のグループに移動すると、EMS は新しいグループに割り当てられたポリシーに基づいてセキュリティ体制を自動的に更新します。

質問**: 23**
中間者 (MITM) 攻撃を軽減するために、FortiClient と FortiClient EMS 間の SSL 接続ネゴシエーション中に検証されるセキュリティ属性はどれですか? (回答を 1 つ選択してください)
A. シリアル番号 (SN)
B. 一般名 (CN)
C. 場所 (L)
D. 組織 (O)
正解**: B (**コメントを発表する**)**
SSL/TLS エンドポイント通信セキュリティに関する FortiClient EMS 管理者学習ガイド (7.2/7.4 バージョン) および Fortinet ドキュメント ライブラリによると、中間者 (MITM) 攻撃を軽減するために SSL 接続ネゴシエーション中に検証される主な属性は共通名 (CN) です。
1. SSL接続ネゴシエーションとMITM軽減
* 検証プロセス:FortiClientがFortiClient EMSサーバーとのテレメトリ接続を確立しようとすると、SSLハンドシェイクが行われます。FortiClientは、悪意のある傍受者 (MITM) ではなく、正当なサーバーと通信していることを確認するために、サーバーの証明書を検証します。
* 共通名 (CN) の役割: 証明書内の共通名 (またはサブジェクト代替名 - SAN) は、クライアントが接続しようとした FQDN (完全修飾ドメイン名) または IP アドレスと一致する必要があります。
* セキュリティ強制:CN/SANがサーバーの想定アドレスと一致しない場合、FortiClientは不一致を検出します。プロファイルの「無効な証明書に対するアクション」(警告またはブロックなど)の設定に応じて、安全なセッションの確立を阻止し、中間者攻撃者がEMSサーバーになりすますことを阻止します。
2. 他の選択肢が間違っている/二次的な理由
* A. シリアル番号 (SN): すべての証明書には固有のシリアル番号が付与されますが、これは主に証明機関 (CA) による追跡と失効のために使用されます。FortiOS 7.2.4以降では、特定の制限付きVPNチェックにシリアル番号を使用できますが、なりすましを防止するために特定のホストを識別するコアSSLネゴシエーションメカニズムは、CN/SANフィールドに依存しています。
* C. 場所 (L) および D. 組織 (O): これらは証明書のサブジェクト内の説明フィールドであり、地理情報と企業情報を提供します。SSL/TLSプロトコルでは、接続ネゴシエーション中にホストのIDを検証したり、中間者攻撃 (MITM) を緩和したりする機能的な用途には使用されません。
3. カリキュラム参考文献
* EMS管理ガイド (システム設定プロファイル) クライアントがEMSサーバー証明書を検証する方法について詳しく説明しています。接続が信頼されるためには、サーバーアドレスが証明書の識別フィールド (CN/SAN) と一致している必要があることが規定されています。

* FortiGate/FortiOS 7.2.4 の新機能: FortiClient EMS コネクタが「CN フィールドに基づいて EMS サーバー証明書の更新を信頼する」ようになり、継続的な安全な通信が確保されるようになった具体的な機能強化について説明します。