Fortinet.FCP_FCT_AD-7.4-JPN.v2026-09-07.q42

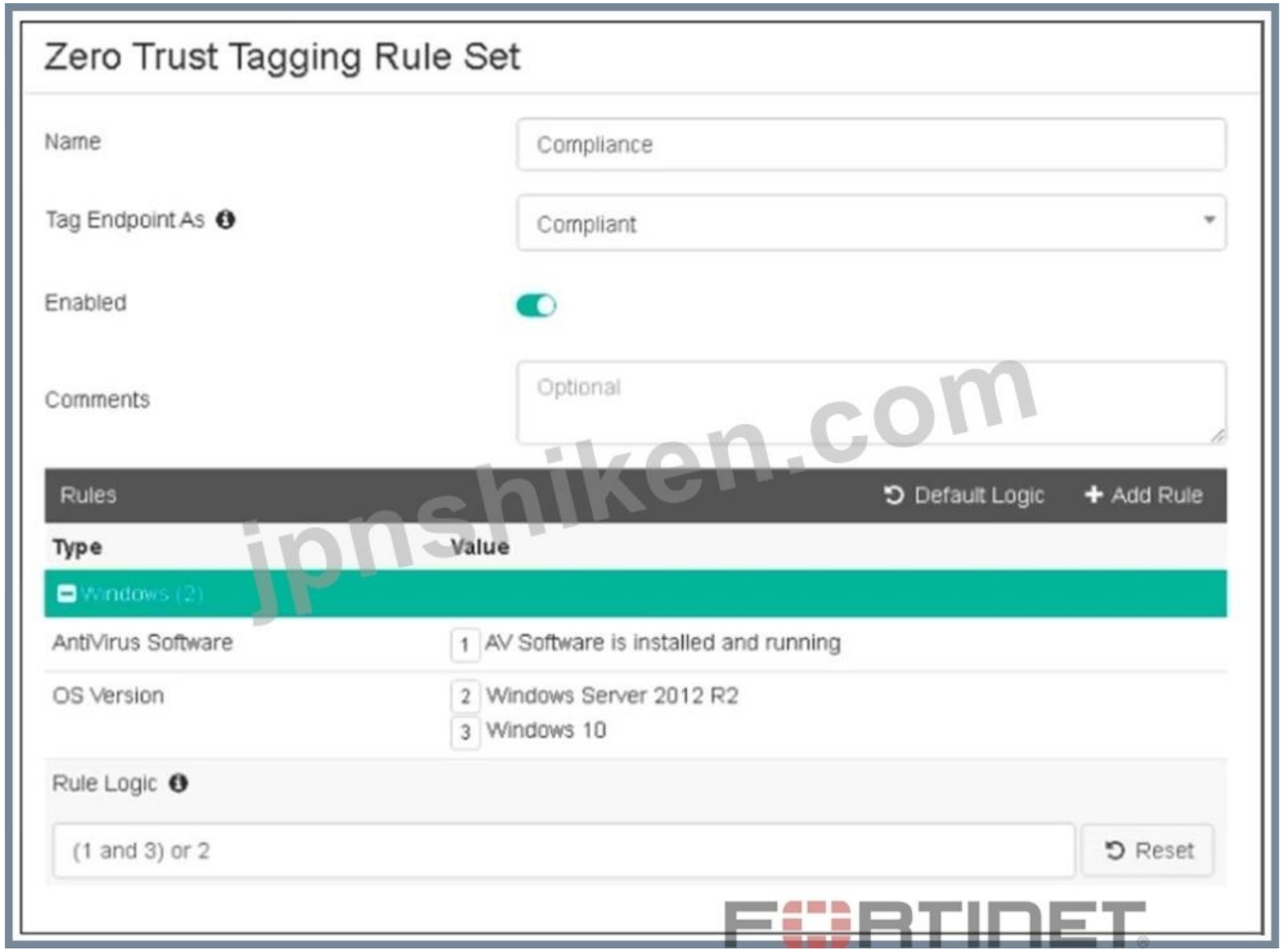
試験コード：	FCP_FCT_AD-7.4-JPN
試験名称：	FCP - FortiClient EMS 7.4 Administrator (FCP_FCT_AD-7.4日本語版)
認証ベンダー：	Fortinet
無料問題の数：	42
バージョン：	v2026-09-07
ページの閲覧量：	110
問題集の閲覧量：	438

https://www.jpnshiken.com/shiken/Fortinet.FCP_FCT_AD-7.4-JPN.v2026-09-07.q42.html

質問: **1**
FortiClient で利用できるウイルス対策スキャンの種類はどれですか (3 つ選択してください)
A. プロキシスキャン
B. フルスキャン
C. カスタムスキャン
D. フロースキャン
E. クイックスキャン
正解: **B,C,E (**コメントを発表する**)**
FortiClient offers several types of antivirus scans to ensure comprehensive protection:
Full scan: Scans the entire system for malware, including all files and directories.
Custom scan: Allows the user to specify particular files, directories, or drives to be scanned.
Quick scan: Scans the most commonly infected areas of the system, providing a faster scanning option.
These three types of scans provide flexibility and thoroughness in detecting and managing malware threats.

質問: **2**
FortiClient エンタープライズ管理サーバーに関して正しい記述はどれですか?
A. ForuGateからエンドポイントの構成情報を受信します。
B. FortiClient ソフトウェアを実行している複数のエンドポイントの集中管理を提供します。
C. タグを使用してエンドポイントのコンプライアンスを強制します
D. クライアント証明書を検証するために、FortiGate から CA 証明書を受信します。
正解: **(**正解を表示します**)**
FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

質問: **3**
ゼロ トラスト タグ付けルール セットの構成を示す展示を参照してください。



ルール セットに関する次の 2 つの記述のうち正しいものはどれですか。(2 つ選択してください。)

A. エンドポイントでは、Windows 10 のみが実行中であることが必要です。

B. エンドポイントでは、AV ソフトウェアのみがインストールされ、実行されている必要があります。

C. エンドポイントでは、ウイルス対策ソフトウェアがインストールされ実行されており、Windows 10 が実行されている必要があります。

D. エンドポイントでは、Windows Server 2012 R2 のみが実行中である必要があります。

正解: **(**正解を表示します**)**

Based on the Zero Trust Tagging Rule Set configuration shown in the exhibit:

The rule set includes two conditions:

AV Software is installed and running

OS Version is Windows Server 2012 R2 or Windows 10

The Rule Logic is specified as "(1 and 3) or 2," meaning:
The endpoint must have antivirus software installed and running and must be running Windows 10.
Alternatively, the endpoint must be running Windows Server 2012 R2.
Therefore, the endpoint must satisfy either:
Antivirus is installed and running and Windows 10 is running.
Windows Server 2012 R2 is running.

質問: **4**
FortiClient はファブリック エージェントとして何を行いますか? (2 つ選択してください。)
A. IOCの判定を提供する
B. 動的ポリシーを作成する
C. アプリケーションインベントリを提供する
D. 応答を自動化する
正解: **C,D (コメントを発表する)**
Forticlient can also automate process of quarantine suspicious or compromised hosts.

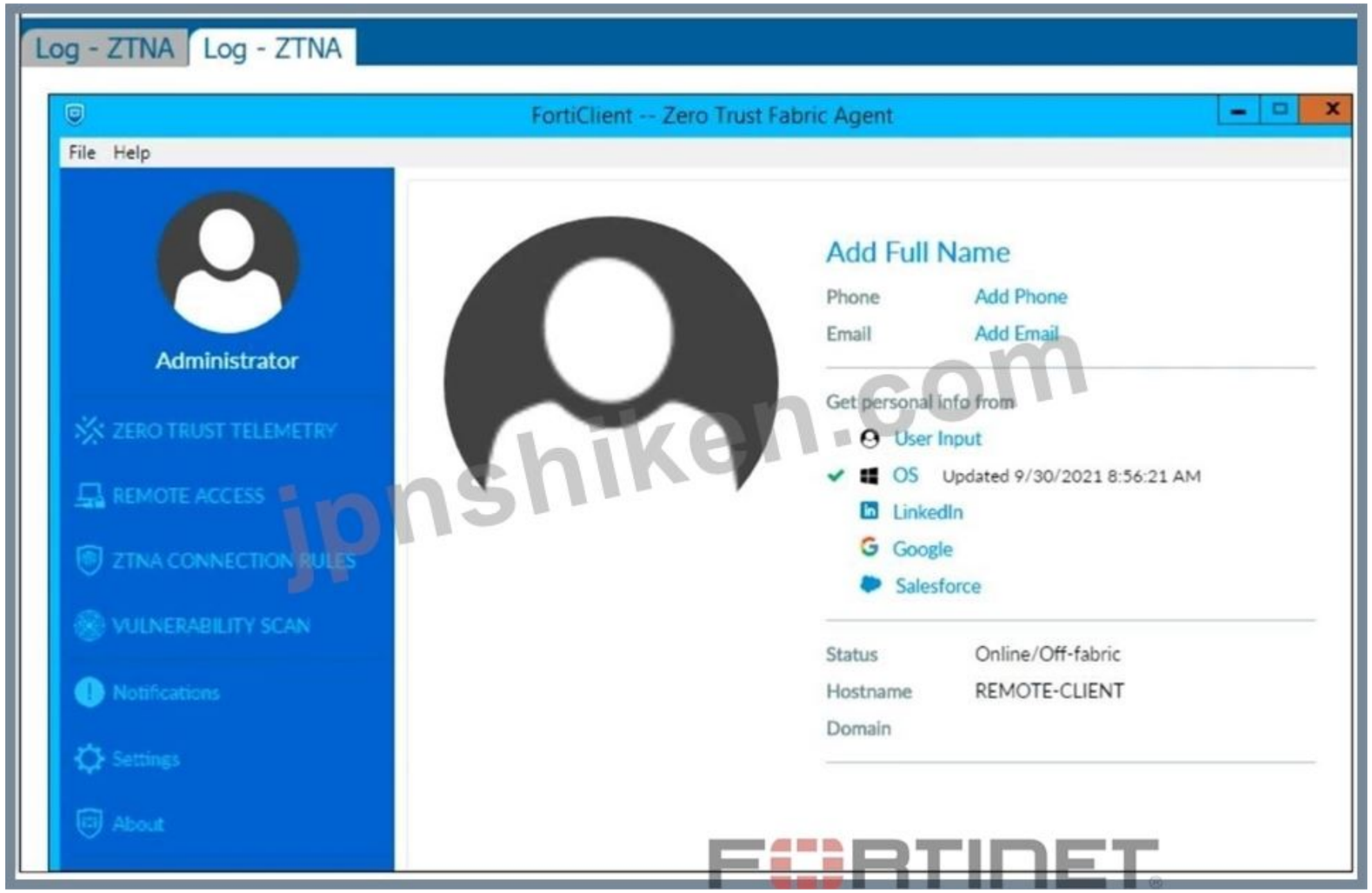
質問: **5**
管理者は Windows Server に FortiClient をインストールします。
リアルタイム保護制御のデフォルトの動作は何ですか?
A. リアルタイム保護ではAVシグネチャデータベースを更新する必要があります
B. リアルタイム保護は、ファイルがローカルで検出されない場合、悪意のあるファイルをFortiSandboxに送信します。
C. リアルタイム保護は無効です
D. リアルタイム保護では、FortiSandboxからシグネチャデータベースを更新する必要があります。
正解: **C (コメントを発表する)**
When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:
Real-time protection is disabled: By default, FortiClient does not enable real-time protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints.
Thus, real-time protection is disabled by default on Windows Server installations.

質問: **6**
FortiClient EMSにおける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内のエンドポイントには、どのポリシーが適用されますか？

A. トレーニングポリシー
B. 販売ポリシーとトレーニングポリシーの両方。これらのポリシーの優先順位はデフォルトポリシーよりも高いため。
C. 最優先されるため、デフォルトポリシーとなります。
D. 販売ポリシー
正解: **(**正解を表示します**)**
Observation of Endpoint Policies:
The exhibit shows multiple endpoint policies with their assigned groups, priority levels, and enabled status.
Evaluating Policy Assignment:
The Training policy is specifically assigned to the "trainingAD.training.lab" group, with a higher priority than the Default policy.
Conclusion:
The correct policy applied to the endpoint in the AD group "trainingAD" is the Training policy (A).

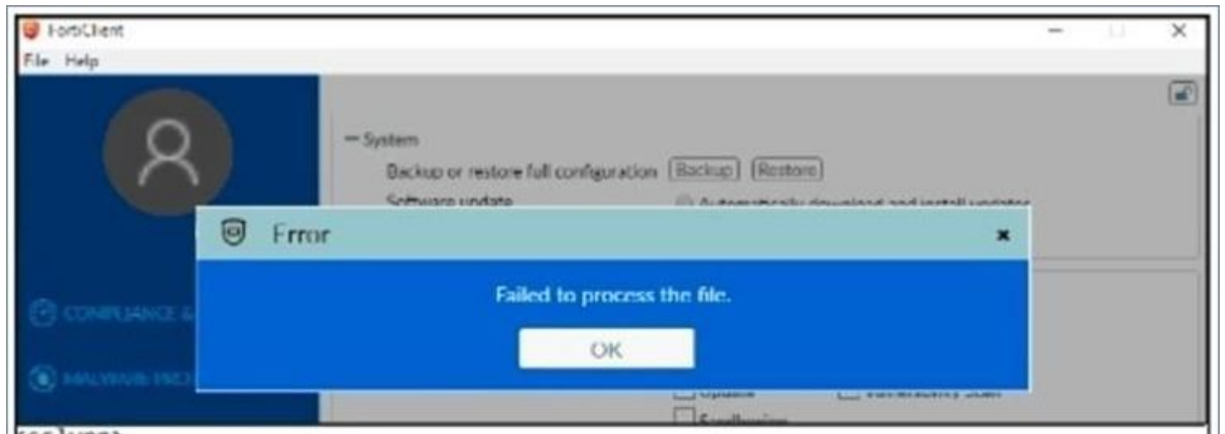
質問: **7**
BYOD(私物端末の業務利用)やリモートユーザーがいる組織では、管理者がFortiClientを導入する必要があります。
管理者はFortiClientを導入するために何を使用できますか？
A. FortiClient ゼロタッチプロビジョニング
B. Microsoft System Center Configuration Manager (SCCM)
C. Microsoft Intune
D. グループポリシーオブジェクト (GPO)
正解: **A (**コメントを発表する**)**
FortiClient zero-touch provisioning is specifically designed to deploy FortiClient to BYOD and remote users without requiring manual installation or corporate device management tools.

質問: **8**
添付資料を参照してください。資料には、ゼロトラストタグモニターとFortiClient GUIのステータスが表示されています。
FortiClient EMSゼロトラストタグモニターでは、Remote-ClientはRemote-Usersとしてタグ付けされています。
FortiClientの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. タグの表示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. FortiClientのシステム設定を変更してタグの表示を有効にします。
C. タグの表示を有効にするためにエンドポイント制御設定を変更します
D. タグの表示を有効にするためにユーザーID設定を変更します
正解: **(**正解を表示します**)**
Based on the exhibits provided:
The "Remote-Client" is tagged as "Remote-Users" in the FortiClient EMS Zero Trust Tag Monitor.
To ensure that the tag "Remote-Users" is visible in the FortiClient GUI, the system settings within FortiClient need to be updated to enable tag visibility.
The tag visibility feature is controlled by FortiClient system settings which manage how tags are displayed in the GUI.
Therefore, the administrator needs to change the FortiClient system settings to enable tag visibility.

質問: **9**
図を参照してください。管理者が変更したXML設定ファイルをFortiClientに復元したところ、図に示すエラーが発生しました。




```
<sslvpn>
    <options>
        <enabled>1</enabled>
        <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
        <dnscache_service_control>0</dnscache_service_control>
        <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
        <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
        <no_dhcp_server_route>0</no_dhcp_server_route>
        <no_dns_registration>0</no_dns_registration>
        <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
    </options>
    <connections>
        <connection>
            <name>Student-SSLVPN</name>
            <description>SSL VPN to Fortigate</description>
            <server>10.0.0.254:10443</server>
            <username />
            <single_user_mode>0</single_user_mode>
            <ui>
                <show_remember_password>0</show_remember_password>
            </ui>
            <password />
            <prompt_username>1</prompt_username>
            <on_connect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_connect>
            <on_disconnect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
```

図に示されているXML設定に基づいて、管理者はXML構成ファイルの問題を解決するために何をする必要がありますか？

A. 管理者は XML 構文エラーを解決する必要があります。

B. 管理者はパスワードを使用してファイルを復号化する必要があります

C. 管理者はファイルサイズを変更する必要があります

D. 管理者はファイルを FortiClient-config conf として保存する必要があります。

正解: **(**正解を表示します**)**

Based on the error message and the XML configuration file shown in the exhibit:

The error "Failed to process the file" typically indicates an issue with the XML syntax.

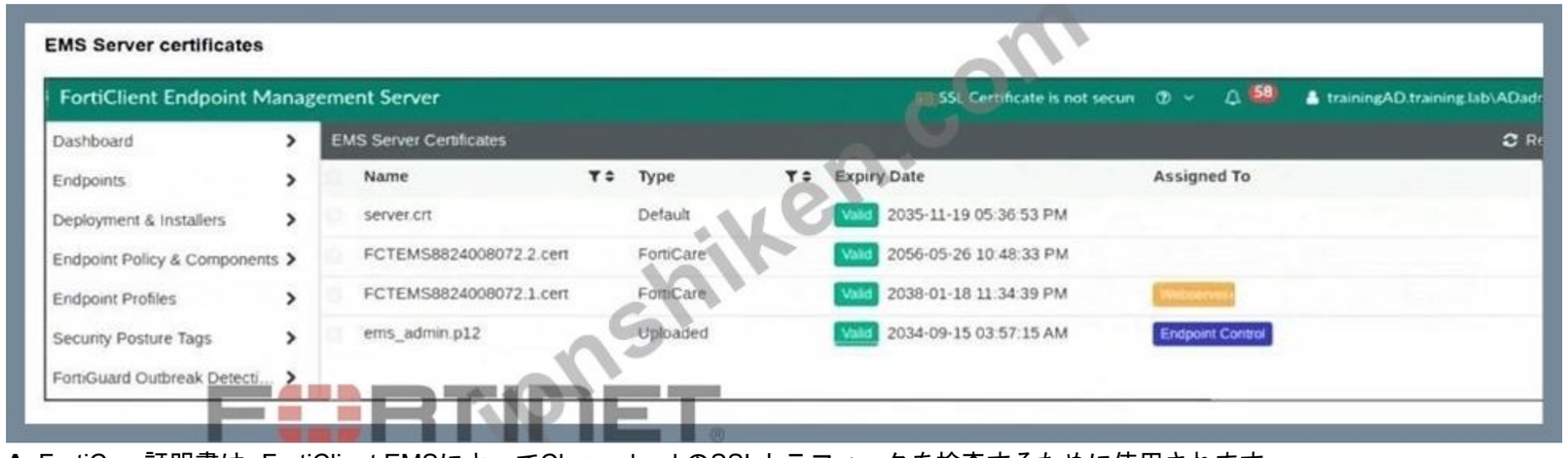
Upon reviewing the XML content, it is crucial to ensure that all tags are correctly formatted, properly opened and closed, and that there are no syntax errors.

Resolving any XML syntax errors will allow FortiClient to successfully process and restore the configuration file.

Therefore, the administrator must resolve the XML syntax error to fix the issue.

質問: **10**

図を参照してください。図に示されているEMSサーバー証明書の構成に当てはまる記述はどれですか？



A. FortiCare証明書は、FortiClient EMSによってChromebookのSSLトラフィックを検査するために使用されます。

B. FortiCare証明書は、エンドポイントとのテレメトリ通信を暗号化するために使用されます。

C. FortiCare証明書は、ゼロトラストネットワークアクセス(ZTNA)のエンドポイントからの証明書要求に署名するために使用されます。

D. FortiCare証明書は、セキュリティファブリックの一部としてFortiGateとの通信に使用されます。

正解: **(**正解を表示します**)**

The FortiCare certificate on FortiClient EMS is used to sign certificate requests from endpoints for ZTNA, enabling secure identity verification and establishing trust between endpoints and the EMS server.

質問: **11**

FortiClient EMS でマルチテナント モードを使用する利点はどれですか (2 つ選択してください)。

A. 各サイトは個別のホスト サーバーによって管理されます。
B. ライセンスはサイト間で共有されます
C. ファブリック コネクタは、FortiClient EMS に接続するために IP アドレスを使用する必要があります。
D. きめ細かなアクセスとセグメンテーションを提供します。
正解: **(**正解を表示します**)**
Understanding Multi-Tenancy Mode:
Multi-tenancy mode allows multiple independent sites or tenants to be managed from a single FortiClient EMS instance.
Evaluating Benefits:
Licenses can be shared among sites, making it cost-effective (B).
It provides granular access and segmentation, allowing for detailed control and separation between tenants (D).
Eliminating Incorrect Options:
Separate host servers managing each site (A) is not a feature of multi-tenancy mode.
The fabric connector's use of an IP address (C) is unrelated to multi-tenancy benefits.

質問: **12**
管理者は、Microsoft AD グループ ポリシーを通じて FortiClient インストールを展開します。インストールが完了すると、すべてのカスタム構成が失われます。
この問題の原因は何でしょうか?
A. FortiClient exeファイルは配布パッケージに含まれています
B. FortiClient MSTファイルが配布パッケージに存在しません
C. FortiClient には配布パッケージにアクセスする権限がありません。
D. FortiClientパッケージがグループに割り当てられていません
正解: **(**正解を表示します**)**
When deploying FortiClient via Microsoft AD Group Policy, it is essential to ensure that the deployment package is correctly assigned to the target group. The absence of custom configuration after installation can be due to several reasons, but the most likely cause is:
Deployment Package Assignment: The FortiClient package must be assigned to the appropriate group in Group Policy Management. If this step is missed, the installation may proceed, but the custom configurations will not be applied.
Thus, the administrator must ensure that the FortiClient package is correctly assigned to the group to include all custom configurations.

質問: **13**
図を参照してください。FortiClientがFortiClient EMSに登録できない原因は何ですか？

A. FortiClient には利用可能なライセンスがありません。
B. FortiClient が証明書チェックに失敗しました。
C. FortiClient はサポートされているバージョンを実行していません。
D. FortiClient は管理対象から除外されています。
正解: **(**正解を表示します**)**
The message "The endpoint is blocked from connecting to EMS" indicates that the FortiClient endpoint has been explicitly excluded from management on FortiClient EMS, preventing registration.

質問: **14**
管理者が FortiClient Cloud 上で FortiGuard Endpoint Forensic Analysis ライセンスを有効化しました。フォレンジック分析について正しい記述はどれですか？
A. エンドポイント上のソフトウェアインベントリを収集するのに役立ちます。
B. 動的なポリシーを実装するのに役立ちます。
C. サイバーセキュリティインシデントへの対応と復旧に役立ちます。
D. FortiClient EMSで利用可能なエンドポイントライセンスについて学ぶのに役立ちます。
正解: **C (**コメントを発表する**)**
The FortiGuard Endpoint Forensic Analysis service provides remote endpoint analysis to assist organizations in responding to and recovering from cyber incidents. Forensic analysts from Fortinet's FortiGuard Labs remotely collect, examine, and present digital evidence and provide a detailed report to help with incident response and recovery efforts.

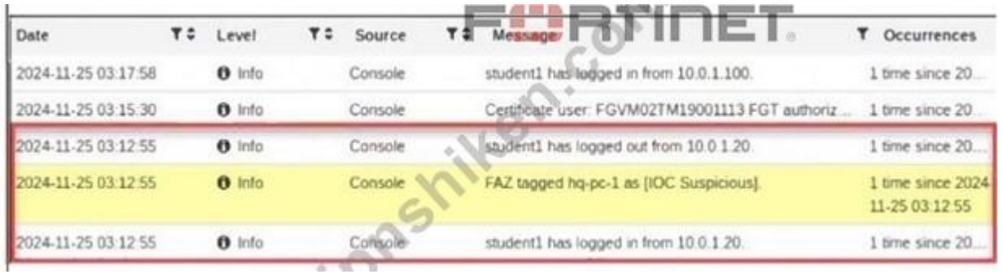
質問: **15**
管理者は、FortiGate、FortiClient EMS、およびFortiAnalyzerを使用して組織のセキュリティファブリックを構成しました。組織は、FortiClient 7.4と最新のアップデートが適用されたウイルス対策ソフトを実行することで、準拠したエンドポイントのみがプライベートサーバーにアクセスできるようにする必要があります。
この結果を得るために、管理者はどのタグを設定する必要がありますか？
A. 布製タグ
B. 分類タグ
C. FortiGuard アウトブレイクアラートタグ
D. セキュリティ態勢タグ
正解: **(**正解を表示します**)**
Security posture tags are used to enforce compliance by identifying endpoints that meet specific security requirements, such as running FortiClient with up-to-date antivirus, and allowing only compliant endpoints access to private servers.

質問: **16**
FortiClient のエクスプロイト対策検出は、エクスプロイトを検出するとどのようなアクションを実行しますか?
A. 侵害されたアプリケーションプロセスを削除します
B. 侵害されたアプリケーションプロセスにパッチを適用します
C. 侵害されたアプリケーションプロセスへのメモリ割り当てをブロックします
D. 侵害されたアプリケーションプロセスを終了します
正解: **D** (コメントを発表する)
The anti-exploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.

質問: **17**
管理者は、エンドポイント情報をFortiGateデバイスと共有するために、ゼロトラストネットワークアクセス(ZTNA)アクセスプロキシソリューションを設定しています。
この解決策を実現するには、どの2つの設定操作を行う必要がありますか？(2つ選択してください。)
A. FortiClient EMS のファブリック デバイス構成に FortiGate の IP アドレスを追加します。
B. FortiClient EMS 上で FortiGate をファブリック コネクタとして認証します。
C. FortiGate の FortiClient EMS コネクタを使用して FortiClient EMS に接続します。
D. FortiGate に ZTNA ライセンスを適用します。
正解: (正解を表示します)
To share endpoint information for ZTNA, the FortiGate must be authorized as a Fabric connector on FortiClient EMS, and the FortiClient EMS connector on FortiGate must be configured to establish the connection and exchange endpoint telemetry.

質問: **18**
FortiClient EMSでマルチテナンシーが有効になっている場合、グローバルサイトへのアクセスのみを許可できる管理者ロールはどれですか？
A. テナント管理者
B. 設定管理者
C. 標準管理者
D. グローバル管理者
正解: (正解を表示します)
The global administrator role in FortiClient EMS has access to the global site only when multitenancy is enabled, allowing management of global settings without tenant-specific permissions.

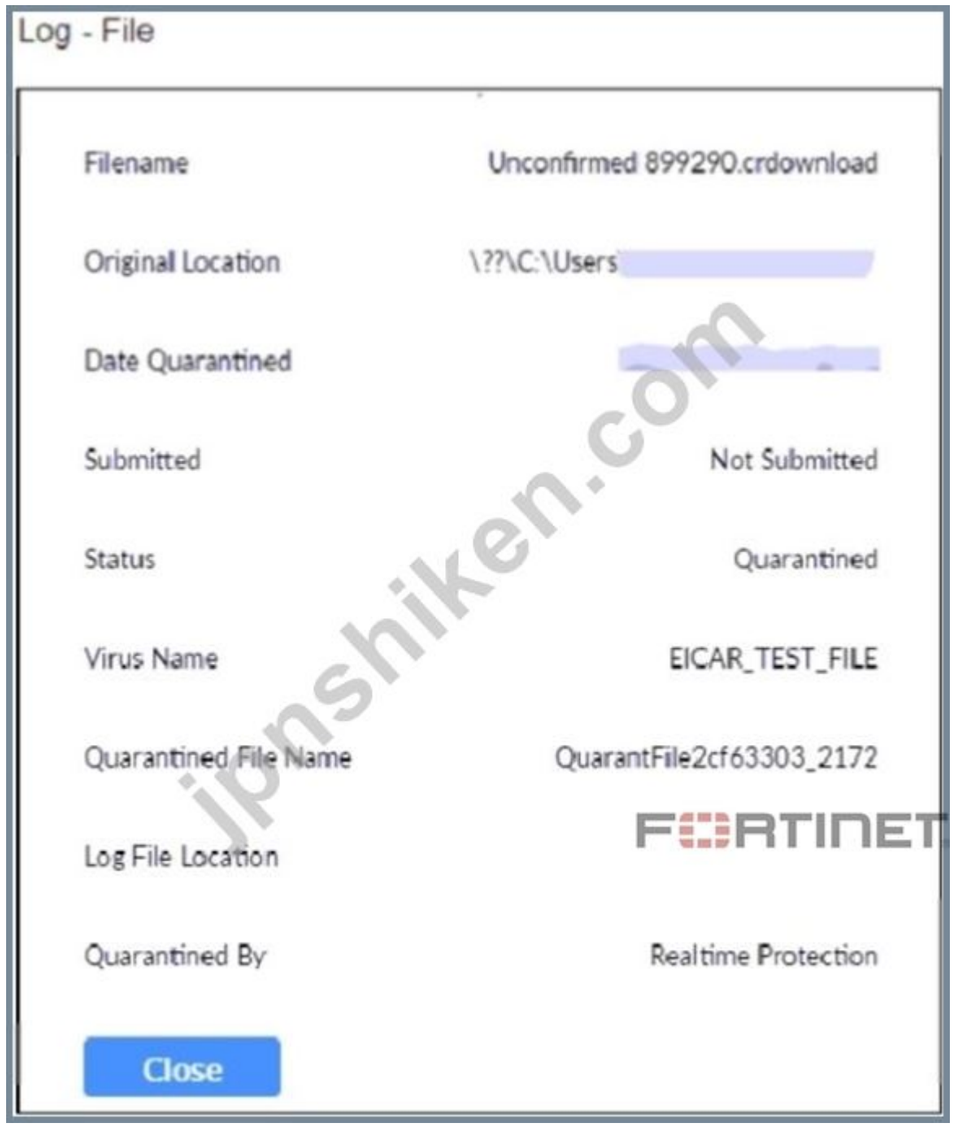
質問: **19**
図を参照してください。エンドポイントが侵害指標(IOC)として疑わしいとタグ付けされているのはなぜですか？



A. エンドポイント hq-pc-1 には、セキュリティ態勢タグ IOC が疑わしいとタグ付けされています。
B. FortiClient EMSファブリックコネクタがFortiAnalyzer上で構成されています。
C. FortiClient EMS 管理者がコンソールを使用して手動でタグ付けしました。
D. FortiAnalyzer の管理者 student1 がプレイブックを実行しました。

正解: **(**正解を表示します**)**
The log shows that FortiAnalyzer (FAZ) tagged the endpoint as [IOC Suspicious] immediately after student1 logged in, indicating that the administrator executed a playbook to automatically tag the endpoint based on the IOC.

質問: **20**
図を参照してください。図に示されているFortiClient togの詳細に基づいて、正しい記述は次のうちどれですか？(2つ選択してください。)



A. ファイル名は未確認 899290.crdownload です。

B. ファイルの状態は隔離されています

C. ファイル名は、さらなる検査のために FortiSandbox に送信されます。

D. ファイルの場所は \??\D:\Users\ です。

正解: **(**正解を表示します**)**

The Filename field clearly shows "Unconfirmed 899290.crdownload."

The Status field shows the file as "Quarantined."
The file is marked "Not Submitted," so it was not sent to FortiSandbox for further inspection.

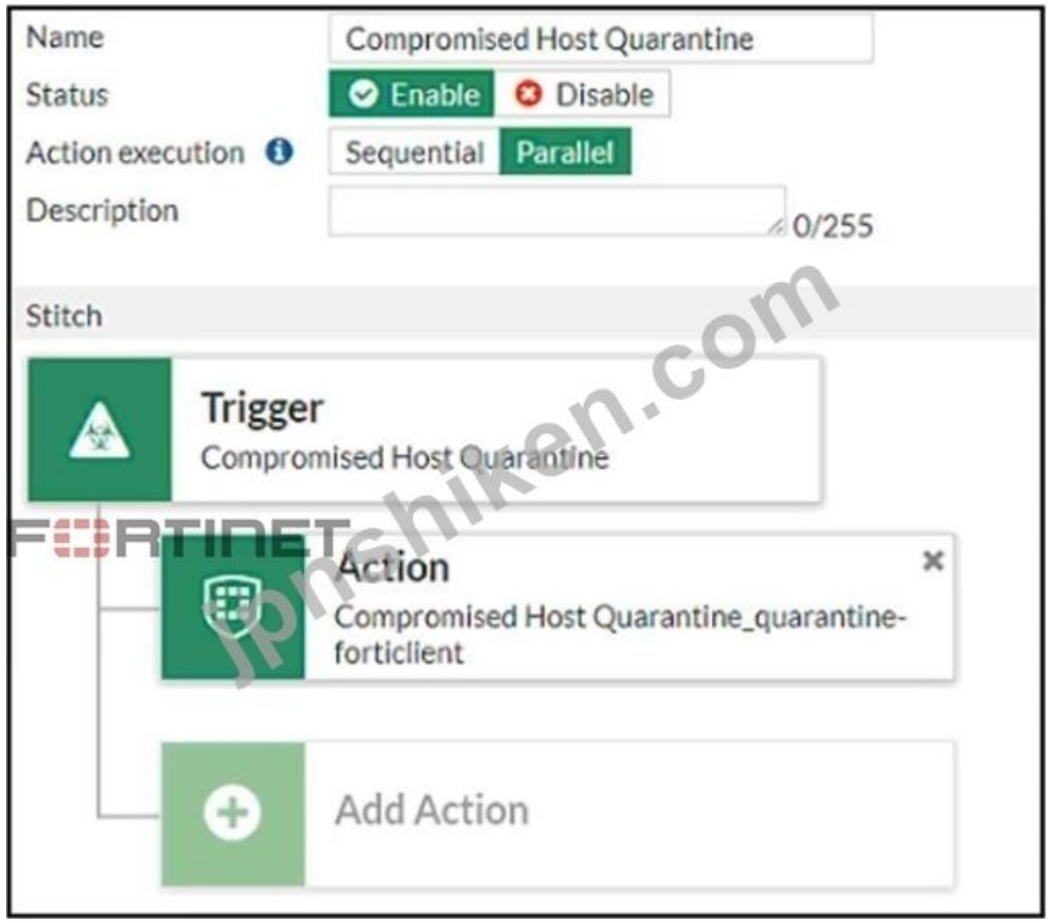
The Original Location shows a path starting with \??\C:\Users, not "??\D:\Users".

質問: **21**

図を参照してください。エンドポイントがゼロトラストネットワークアクセス(ZTNA)サーバーへのアクセスを拒否されたのはなぜですか？

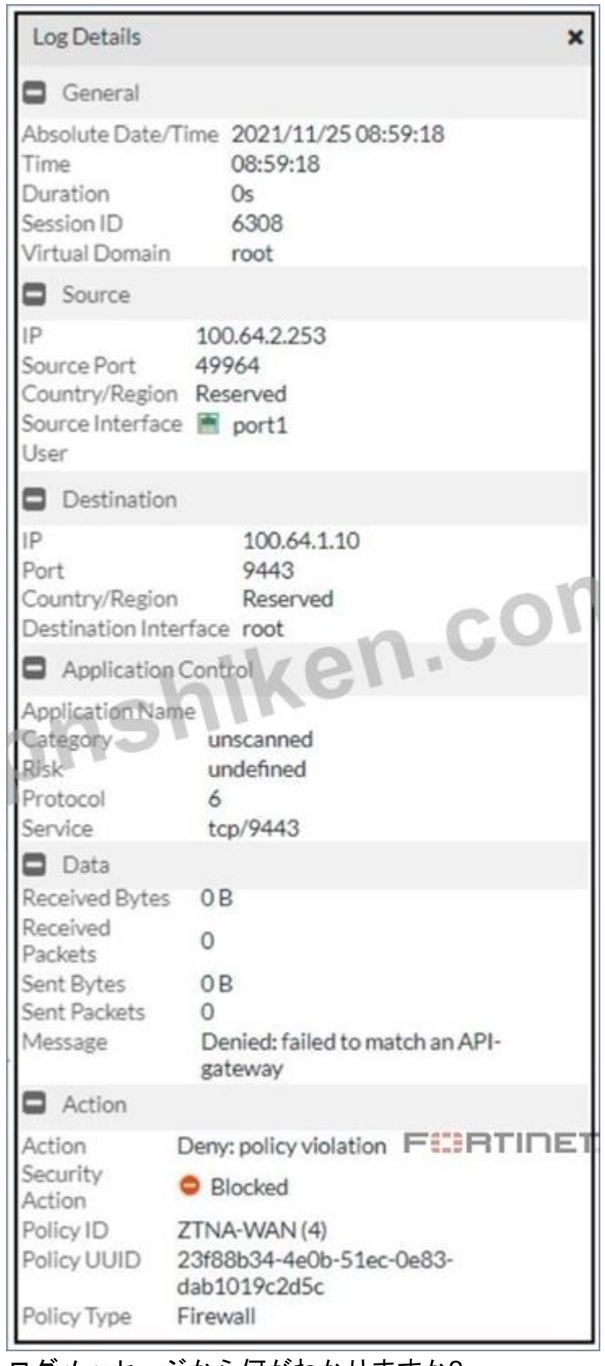
A. FortiGate はユーザー認証情報を検証できませんでした。
B. FortiGate はクライアント証明書を検証できませんでした。
C. エンドポイントのセキュリティ状態が失敗しました。
D. FortiGate に失効したクライアント証明書が提供されました。
正解: **(**正解を表示します**)**
The message indicates that the client certificate is not provided. FortiGate requires a valid ZTNA client certificate to verify the endpoint's identity, and access is denied when the certificate is missing or invalid.

質問: **22**
図を参照してください。Security Fabricの自動化設定に基づいて、侵害されたエンドポイントに対してどのような措置が取られますか？



A. エンドポイントはEMSを通じて隔離されます
B. FortiGate ではエンドポイントが禁止されます
C. 侵害されたエンドポイントに対してメール通知が送信されます
D. エンドポイントはFortiSwitchを通じて隔離されます
正解**: (**正解を表示します**)**
Based on the Security Fabric automation settings shown in the exhibit:
The automation stitch is configured with a trigger for a "Compromised Host." The action specified for this trigger is "Quarantine FortiClient via EMS." This indicates that when an endpoint is detected as compromised, FortiClient EMS will quarantine the endpoint as part of the automation process.
Therefore, the action taken on compromised endpoints will be to quarantine them through EMS.

質問**: 23**
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。



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。

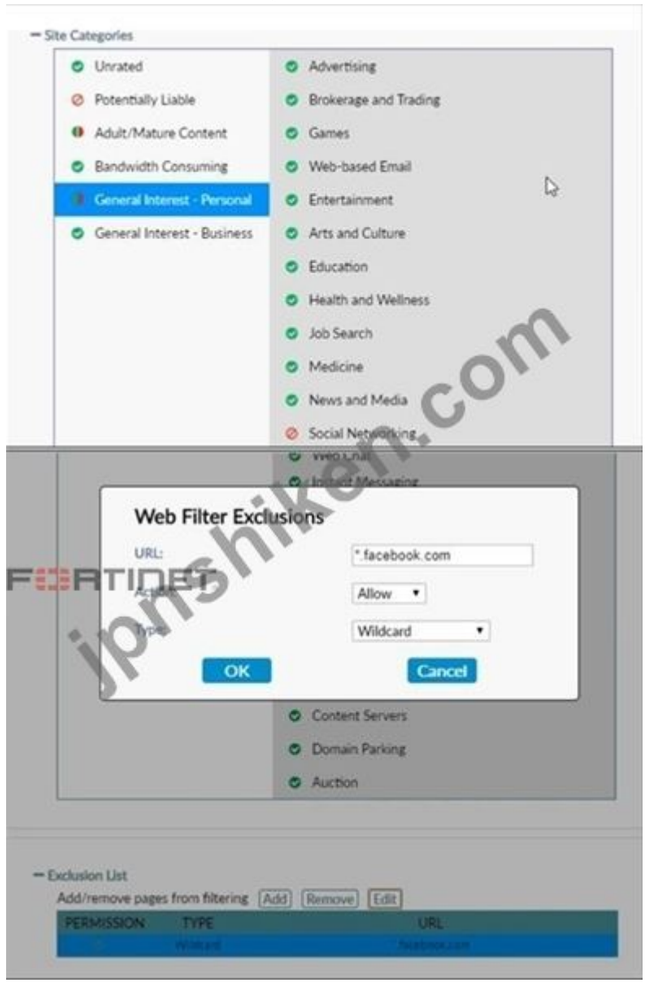
C. リモート ユーザー接続が ZTNA サーバーの構成と一致しません。

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: **(**正解を表示します**)**

Observation of ZTNA Traffic Log:
The log message indicates that the remote user connection was denied due to failure to match a proxy policy.
Evaluating Log Message:
The message suggests that the connection does not match the existing ZTNA rule configuration, leading to the denial.
Conclusion:
The correct conclusion from the log message is that the remote user connection does not match the ZTNA rule configuration (B).

質問: 24
図を参照してください。図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、FortiClientはどのような動作を実行しますか？



A. FortiClient は Facebook へのアクセスを許可します。
B. FortiClient は Facebook および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、ユーザーのFacebookウェブサイトへのウェブアクセスのみを監視します。
D. FortiClient は、ユーザーが Facebook 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: **(**正解を表示します**)**
Observation of Web Filter Exclusions:
The exhibit shows a web filter exclusion for "*.facebook.com" with the action set to "Allow." Evaluating Actions:

This configuration means that FortiClient will allow access to Facebook and its subdomains.
Conclusion:
When users try to access "www.facebook.com," FortiClient will allow the access based on the web filter exclusion settings.

質問: **25**
管理者は、ユーザーにユーザー資格情報の提供を求めることなく、リモート アクセスを簡素化したいと考えています。どのアクセス制御方法がこのソリューションを提供しますか?
A. ZTNAフルモード
B. SSL VPN
C. L2TP
D. ZTNA IP/MACリタリングモード
正解: **A (**コメントを発表する**)**
Simplifying Remote Access:
The administrator wants to simplify remote access without asking users to provide user credentials.
Evaluating Access Control Methods:
ZTNA full mode can provide seamless access by leveraging device identity and posture, eliminating the need for user credentials for each access request.
Other methods like SSL VPN and L2TP typically require user credentials.
Conclusion:
The correct access control method that provides this solution is ZTNA full mode.

質問: **26**
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**)**
The firewall policy matches and redirects client requests to the access proxy VIP.
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration

質問: **27**
管理者がFortiClient EMSコンソールへのWebアクセスを失い、コンソールにアクセスするためのWebページがタイムアウトしています。
管理者はどのようにして問題の調査に必要な情報を収集できるのでしょうか？
A. EMSサーバーでCLI診断ツールを使用します。
B. PostgreSQLサーバーからウェブサーバーのログをダウンロードします。
C. FortiClient EMS GUI の診断ログオプションを使用します。
D. サポートサイトからログジェネレーターをダウンロードし、EMSサーバーで実行します。
正解: **(**正解を表示します**)**
When web access to FortiClient EMS is unavailable, the administrator can use the CLI diagnostic tools on the EMS server to gather system and service information, check the status of services, and investigate connectivity or performance issues.
質問: **28**
セキュリティファブリック内の FortiGate デバイスは、ポリシー適用のため FortiClient EMS からエンドポイント情報を受信する必要があります。エンドポイント情報を同期するために必要なのはどれで

すか？
A. エンドポイントがエンドポイント情報を受信するためには、FortiGate デバイスがゲートウェイ デバイスとして機能する必要があります。
B. FortiGate デバイスは、エンドポイント情報を受信するために FortiClient EMS 上で認証されている必要があります。
C. FortiGate デバイスにはエンドポイント ライセンスが必要です。
D. FortiGate デバイスは FortiClient EMS と同じファームウェア バージョンを実行する必要があります。
正解: **(**正解を表示します**)**
FortiGate devices in the Security Fabric must securely connect and be authorized by the FortiClient EMS to synchronize endpoint and Security Posture tag information. This connection requires establishing a trusted certificate chain to the EMS server and authorizing the FortiGate on the EMS. Once authorized, the FortiGate can pull endpoint information such as dynamic tags from the EMS for policy enforcement.

質問: **29**
FortiClientのフォレンジック分析に当てはまる記述はどれですか？(2つ選択してください。)
A. FortiClient は、悪意のあるアクティビティがトリガーされたときにアラート通知を送信します。
B. 管理者は、目的のエンドポイントの分析を要求する必要があります。
C. フォレンジック調査が完了するまで、エンドポイントは隔離されます。
D. システム設定プロファイルでフォレンジック分析機能を有効にする必要があります。
正解: **(**正解を表示します**)**
FortiClient forensics requires enabling the feature in the system settings profile. When malicious activity is detected, FortiClient generates an alert notification to inform the administrator for further analysis.

質問: **30**
図を参照してください。なぜユーザーはbbc.comにアクセスできないのでしょうか？
FortiClient logs

```
20250226 05:50:24.563 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /
20250226 05:50:24.563 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com
20250226 05:50:24.563 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /
20250226 05:50:24.564 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /
20250226 05:50:24.564 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com / rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.564 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com / Unknown 2025-02-26 05:50:24.564598172
+0100 CET m=+4561.038040408 admin 368039 /opt/google/chrome/chrome}
20250226 05:50:24.601 TZ=+0100 [DEBUG] http2_handler:312 set table size to 65536
20250226 05:50:24.820 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com/favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /favicon.ico
20250226 05:50:24.821 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /favicon.ico
20250226 05:50:24.821 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com /favicon.ico rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.821 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com /favicon.ico Unknown 2025-02-26 05:50:24.82122553
+0100 CET m=+4561.294667764 admin 368039 /opt/google/chrome
```

A. このURLはWebフィルタエンドポイントプロファイルによってブロックされています。
B. エンドポイントは URL FQDN を解決できません。
C. エンドポイントから FortiGuard サーバーにアクセスできません。
D. アプリケーションファイアウォールがGoogle Chromeをブロックしています。
正解: (正解を表示します)
The logs indicate repeated "FortiGuard server down, task dropped" errors, showing that the endpoint cannot reach FortiGuard servers to perform the URL category query. This prevents access because the web filter relies on FortiGuard connectivity.

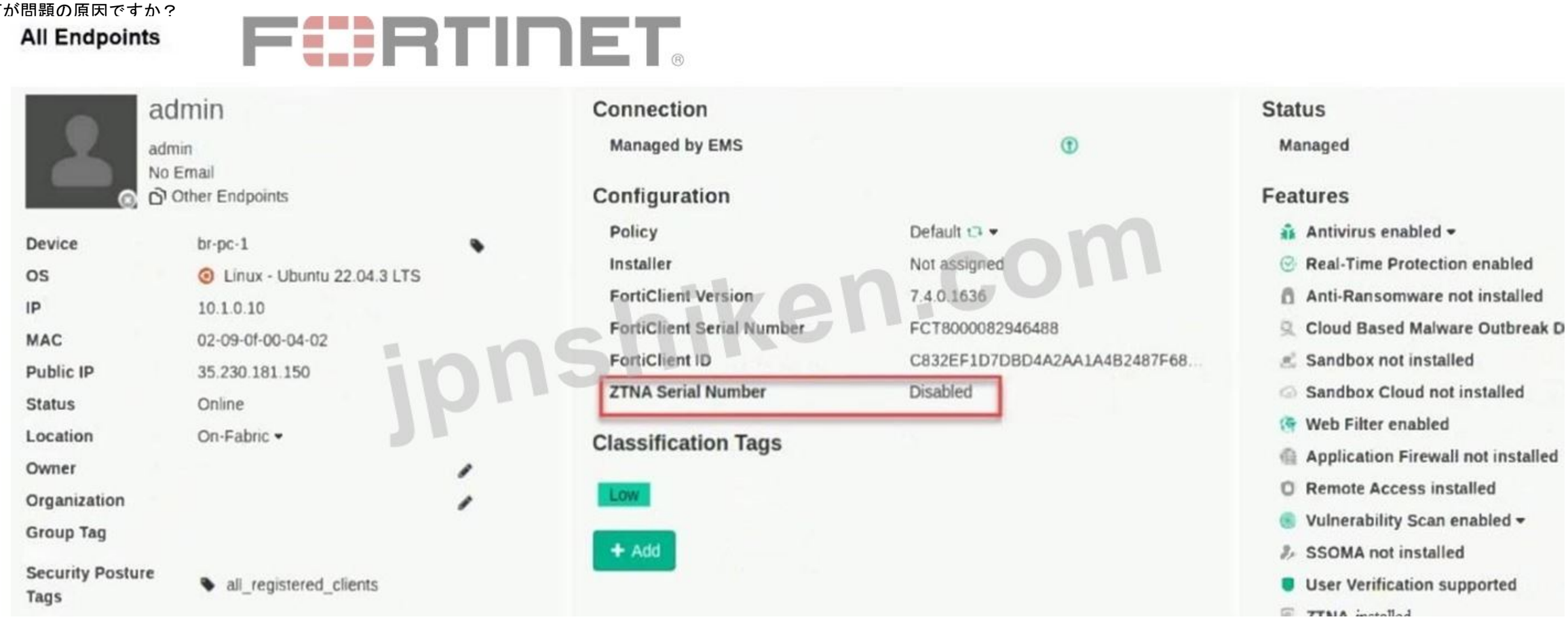
質問: **31**
図を参照してください。FortiGateのCLI出力に基づくと、次のうち正しい記述はどれですか？

A. FortiGateはFortiClient EMSからユーザーグループを取得するように構成されています
B. FortiGateはローカルユーザーグループで構成されています
C. FortiGate は FortiAuthenticator からユーザー グループを取得するように構成されています。
D. FortiGate は AD サーバーからユーザー グループを取得するように構成されています。
正解: (正解を表示します)
Based on the CLI output from FortiGate:
The configuration shows the use of "type fortiems," indicating that FortiGate is set up to interact with FortiClient EMS.
The "server" field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.
The configuration includes an SSL-enabled connection, which is a common setup for secure communication between FortiGate and FortiClient EMS.
Thus, the configuration indicates that FortiGate is set up to pull user groups from FortiClient EMS.

質問: **32**
セキュリティ ファブリック統合における ZTNA 遅延情報を定義するコンポーネントまたはデバイスはどれですか?
A. FortiClient
B. FortiGate
C. FortiClient EMS
D. FortiGate アクセス プロキシ
正解: (正解を表示します)
Understanding ZTNA:
Zero Trust Network Access (ZTNA) requires defining tags for identifying and managing endpoint access.

Evaluating Components:
FortiClient EMS is responsible for managing and defining ZTNA tag information within the Security Fabric.
Conclusion:
The correct component that defines ZTNA tag information in the Security Fabric integration is FortiClient EMS.

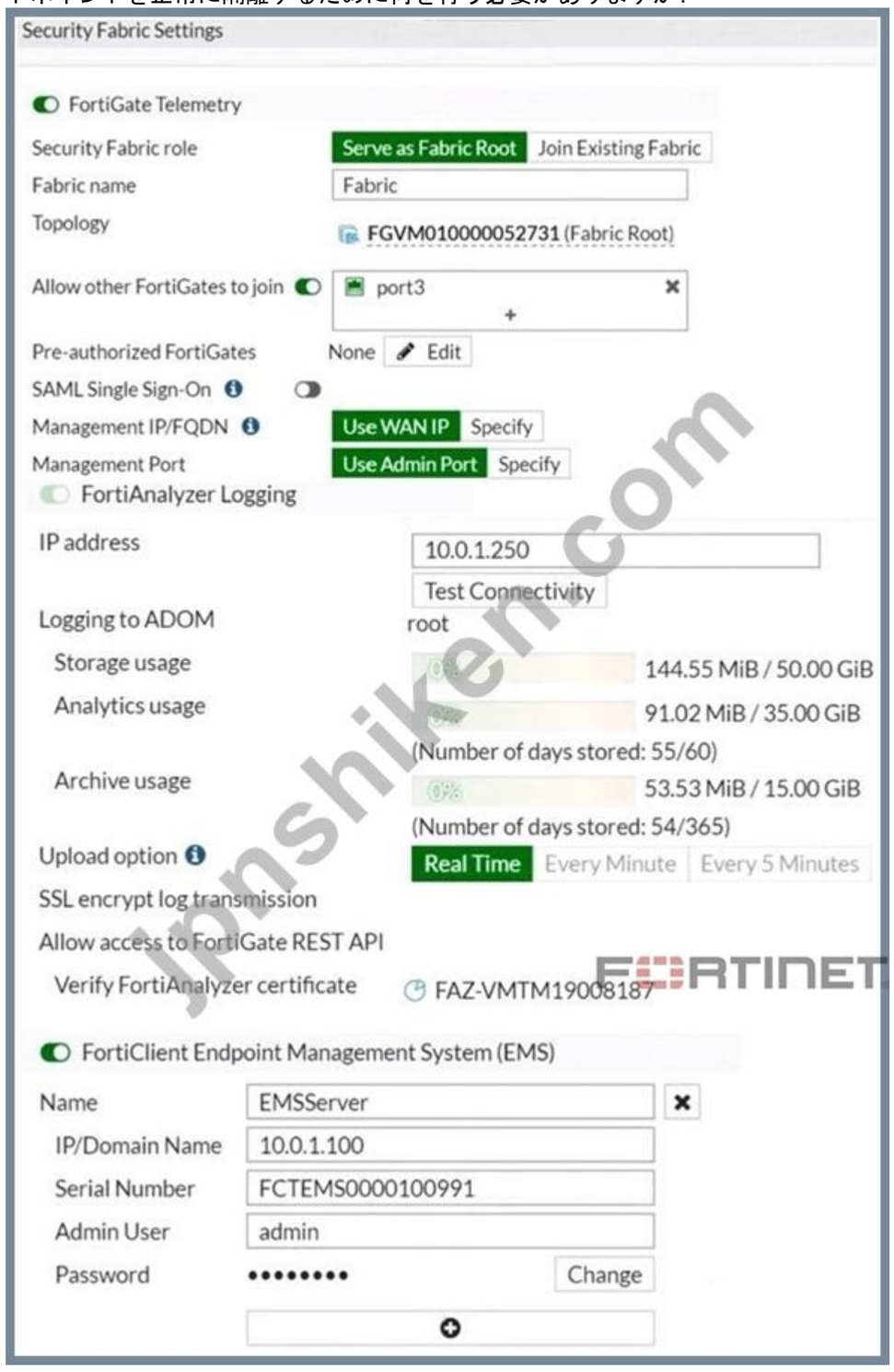
質問: **33**
図を参照してください。エンドポイントbr-pc-1のゼロトラストネットワークアクセス(ZTNA)シリアル番号は無効状態になっています。
何が問題の原因ですか？



A. ZTNA機能はFortiClientにインストールされていません。
B. ZTNAdestinationsエンドポイントプロファイルが無効になっています。
C. FortiClientがFortiClient EMSから切断されたため、ZTNAは無効になっています。
D. ZTNA証明書は管理者によって取り消されました。
正解: **C** (コメントを発表する)
The ZTNA serial number shows as disabled because FortiClient must maintain a connection with FortiClient EMS for ZTNA functionality. If the client is disconnected or cannot communicate with EMS, the ZTNA serial number will appear disabled.

質問: **34**
添付資料を参照してください。添付資料に示されている FortiGate Security Fabric の設定に基づいて、エンドポイントが侵害されたホスト (IoC) として検出された場合、管理者は EMS サーバー上でエン

ドポイントを正常に隔離するために何を行う必要がありますか?



A. 管理者はEMSへのリモートHTTPSアクセスを有効にする必要があります。
B. 管理者はEMSでFQDNを有効にする必要があります。
C. 管理者は FortiAnalyzer 上で FortiGate を承認する必要があります。
D. 管理者はEMSへのSSHアクセスを有効にする必要があります。
正解: **(**正解を表示します**)**
Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:
Enable Remote HTTPS Access to EMS: This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate.
Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

質問: **35**
FortiClientを統合してシングルサインオンモビリティエージェント(SSOMA)機能を使用するには、どのFortinetソリューションと連携できますか？
A. FortiAuthenticator
B. FortiSASE
C. FortiPAM
D. FortiNAC
正解: **A (**コメントを発表する**)**
FortiClient integrates with FortiAuthenticator to use the SSOMA feature, enabling single sign-on for endpoint users and providing seamless authentication for network access.

質問: **36**
管理者は企業内に FortiClient EMS をインストールします。
保護の実施とセキュリティ体制のチェックを担当するコンポーネントはどれですか?
A. FortiClient EMSタグ
B. FortiClientの脆弱性スキャン
C. FortiClient
D. FortiClient EMS
正解: **(**正解を表示します**)**
Understanding FortiClient EMS Components:
FortiClient EMS manages and configures endpoint security settings, while FortiClient installed on the endpoint enforces protection and checks security posture.
Evaluating Responsibilities:
FortiClient performs the actual enforcement of security policies and checks the security posture of the endpoint.
Conclusion:

The component responsible for enforcing protection and checking security posture is FortiClient (C).

質問: **37**
管理者は、リモートユーザーまたはファブリック外ユーザー向けに、ZTNA アクセスにユーザー認証を追加する必要があります。ZTNA に追加する必要がある FortiGate の機能はどれですか？
A. FortiGate FSSO
B. FortiGate証明書
C. FortiGate 明示プロキシ
D. FortiGateエンドポイント制御
正解: **C (**コメントを発表する**)**
FortiGate explicit proxy allows FortiGate to intercept web traffic for authentication purposes.
ZTNA integrates with various FortiGate features to provide secure access and ensure that users are authenticated before accessing resources.
By using an explicit proxy, FortiGate can handle web traffic and enforce authentication policies for remote users who are not directly on the corporate network (off-fabric).

質問: **38**
図を参照してください。なぜトラフィックはゼロトラストネットワークアクセス(ZTNA)サーバーへのアクセスを拒否されたのでしょうか？

WAD Debugs Snippet

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable

[I][p:2090] wad_accept :2403 redirect 90 accepted 100.64.1.1:55958 -> 100.64.0.1:9443 on 123
[I][p:2090] wad_session_context_learn_v4_session:144 Redir session state=0x300 state2=0x0 state_ext=0x0.
[V][p:2090][s:94256] wad_session_start_traffic_timer :620 ses_ctx:0x7f04f65ab408 start traffic timer:3590
[V][p:2090][s:94256] wad_policy_profile_learn :532 app=1 proxy=14, pn=0x7f04f67e1708
[I][p:2090][s:94256] wad_session_context_learn_session_config:464 vf_id=0 ses_ctx=0x7f04f65ab408 policy-id=6,
sec_profile=0x7f04f6952d48 app_type=http
[V][p:2090][s:94259] wad_vs_ssl_port_caps_on_handshake_recv:11235 sp=0x7f04f682dda8/10 recv type=11 len=978
[I][p:2090][s:94259] wad_vs_ssl_access_proxy_on_clt_certs:13548 7:Webserver: received certs from the client.
[I][p:2090][s:94259] wad_ssl_cert_auth_find :73 Found auth_info (stable)
[I][p:2090][s:94259] wad_vs_ssl_access_proxy_on_clt_certs:13552 7:Webserver: cert cache cert(0x7f04f4c1f8b0) authi(0x7f04f4c04b00)
[V][p:2090][s:94259] wad_vs_ssl_access_proxy_on_clt_certs:13557 7:Webserver: vs, Found the cert, and issued by:ems
[V][p:2090][s:94259] wad_vs_ssl_access_proxy_on_clt_certs:13562 7:Webserver: hit the cached auth_result(7)
[I][p:2090][s:94259] wad_vs_ssl_access_proxy_on_clt_certs:13598 7:Webserver: Cert auth success. issued_by: ems
[V][p:2090][s:94259] wad_vs_ssl_port_caps_c2p_on_cert_verify:12386 wsp 0x7f04f682dda8 CertificateVerify signature_scheme 0804
[V][p:2090][s:94259] wad_vs_ssl_port_caps_on_handshake_recv:11235 sp=0x7f04f682dda8/10 recv type=20 len=36
[I][p:2090][s:94259] wad_vs_ssl_port_caps_c2p_on_handshake_done:11878 wsp 0x7f04f682dda8 type 10 handshake done
[I][p:2090][s:94259] wad_vs_http_make :5330 make vs http session
[V][p:2090][s:94259] wad_http_vs_srv_pool_get :1954 get vs server pool.
[V][p:2090] wad_authenticated_user_proc_msg_header:1719 msg=DevQueryResp code=OK seq=6 data_len=317
[V][p:2090] wad_dev_attr_parse_cert_sn :1191 cert_sn=8B311DB0A4724785163678EECF7D5C31903185D9 len=40
[V][p:2090] wad_dev_attr_parse_tag :1179 tag(1)=ZTNA_all_registered_clients_FCTEMS8824008072000000000000000000000000000000 len=76
[V][p:2090] wad_dev_attr_parse_tag :1179 tag(2)=ZTNA_Non-Compliant_FCTEMS8824008072000000000000000000000000000000 len=67
[V][p:2090] wad_dev_query_node_cb :1078 dev resp tid=6, rsp=0x7ffe5b8f46a0
[V][p:2090] wad_dev_cache_find :2286 Looking for key: 'uid.ems_sn.ems_tenant_id':
C832EF1D7DBD4A2AA1A4B2487F6893FC.FCTEMS8824008072.00000000000000000000000000000000
[V][p:2090] wad_fw_policy_match_dev_grp :5112 dev tag matching, info=0x7f04f4df1978, type=dev-id, tag_cnt=2, on_line=1,conf ems-tag size=3
[V][p:2090] wad_fw_policy_match_dev_grp :5140 pol_id = 6 matched dev id = 23
[V][p:2090] wad_fw_policy_match_dev :5202 pol_id = 6 matched = 1
[V][p:2090][s:94259][r:63] wad_http_req_policy_notify :10004 notify policy match: req=0x7f04f5b0ec48 status=1 pid=2090.
[I][p:2090][s:94259][r:63] wad_http_req_policy_set :9779 match policy-id=6(pol_ctx:mth|Ad|7|-d) vd=0(ses_ctx:ct|P|Me|H|C|A1|O) (100.64.1.1:57526@4 -> 10.0.1.20:443@6)
[V][p:2090][s:94259][r:63] wad_https_ap_pol_info_get :9585 policy info created, req=0x7f04f5b0ec48, ses_ctx=0x7f04f65ab408, info=0x7f04f4cfd2c8
[I][p:2090][s:94259][r:63] wad_http_req_proc_policy :9295 ses_ctx:ct|P|Me|H|C|A1|O conn_srv=0 fwd_srv=<nil>
[I][p:2090][s:94259][r:63] wad_auth_inc_user_count :1739 increased user count, quota:128000, n_shared_user:1, vd_used: 1, vd_max: 0, vd_gurantee: 0
[V][p:2090][s:94259][r:63] __wad_hauth_user_node_hold :2375 wad_hauth_user_node_alloc (1641): holding node 0x7f04f4c80bf8
mapping user_node:0x7f04f4c80bf8, user_ip:0x7f04f4c64a78(0), user:0x7f04f4cfd4d0(0)
[V][p:2090][s:94259][r:63] __wad_hauth_user_node_hold :2375 wad_user_node_stats_hold (574): holding node 0x7f04f4c80bf8
[V][p:2090][s:94259][r:63] __wad_hauth_user_node_hold :2375 wad_http_session_upd_user_node (6039): holding node 0x7f04f4c80bf8
[E][p:2090][s:94259][r:63] wad_http_req_proc_policy :9318 POLICY DENIED
[I][p:2090][s:94259][r:63] wad_vs_log_policy_denied :204 7:Webserver: Traffic denied because proxy-policy action is deny. Matched tag: EMS1_ZTNA_Non - Compliant
[I][p:2090][s:94259][r:63] __wad_log_etl :406 size:486 buf:0x5632c3d2b406
[I][p:2090][s:94259][r:63] __wad_http_build_replmsg_resp :780 Generating replacement message. ZTNA deny. repmsg_id 90
[V][p:2090][s:94259][r:63] wad_mem_c_malloc :138 size 32770 exceeds max_elm_size (18392); not using bucket
```

A. FortiGate でクライアント証明書を検証できませんでした。

B. リモートユーザーのユーザー認証に失敗しました。
C. トラフィックがどのプロキシ ポリシーにも一致しませんでした。
D. セキュリティ態勢タグが拒否ポリシーに一致しました。
正解: **D (**コメントを発表する**)**
The debug logs indicate that the traffic was denied because the endpoint's security posture tags did not meet the required policy, resulting in a ZTNA deny action due to non-compliance.

質問: **39**
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製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. Microsoft SCCM
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**)**
Administrators can use several third-party tools to deploy FortiClient:
Microsoft SCCM (System Center Configuration Manager): SCCM is a robust tool used for deploying software across large numbers of Windows-based systems. It supports deployment of FortiClient through its software distribution capabilities.
Microsoft Active Directory GPO (Group Policy Object): GPOs are used to manage user and computer settings in an Active Directory environment. Administrators can deploy FortiClient to multiple machines using GPO software installation settings.
These tools provide centralized and scalable methods for deploying FortiClient across numerous endpoints in an enterprise environment.

質問: **40**
FortiClient EMSコンソールログに関する記述のうち、正しいものはどれですか？
A. FortiClient EMS 管理者がエンドポイント プロファイルをすべてのグループに割り当てました。
B. FortiClient EMS管理者がエンドポイントプロファイルを作成しました。
C. FortiClient EMS 管理者がゲートウェイ リストをすべてのグループに割り当てました。
D. FortiClient EMS管理者が、すべてのグループに新しいFortiClientインストールを展開しました。
正解: **B (**コメントを発表する**)**
This is directly indicated in sample FortiClient EMS questions related to the console logs and endpoint profiles, where the correct choice from similar options is the creation of an endpoint profile by the administrator, not assigning profiles or gateway lists to all groups or deploying new FortiClient installations to all groups.

質問: **41**
管理者は、ドメインに参加しているエンドポイントに対してFortiClientの初期展開を実行する必要があります。
導入にはどの方法が推奨されますか？
A. ドメインエンドポイントを設定して、インストーラーをFortiClientクラウドサービスから直接ダウンロードします。
B. FortiClientインストーラーを含むすべてのドメインユーザーにメールを送信します。
C. FortiClient EMS にドメインエンドポイントをインポートし、FortiClient インストーラーをエンドポイントに展開します。
D. グループポリシーオブジェクト (GPO) を使用して、ドメインエンドポイントに FortiClient をインストールします。
正解: **(**正解を表示します**)**
質問: **42**
図を参照してください。エンドユーザーがtwitter.comにアクセスできないのはなぜですか？

A. アプリケーションファイアウォールのエンドポイントプロファイルによってブロックされています。
B. Webフィルタエンドポイントプロファイルの除外リストによってブロックされています。
C. これらは、Webフィルタエンドポイントプロファイル内のFortiGuardカテゴリによってブロックされています。
D. マルウェア対策エンドポイントプロファイルの拒否リストによってブロックされています。
正解: **(**正解を表示します**)**

The block message indicates that the URL is denylisted by FortiClient. This occurs when FortiGuard categories in the web filter profile restrict access to specific websites, such as twitter.com, based on policy.