Fortinet.NSE5_FNC_AD_7.6.v2026-05-29.q12

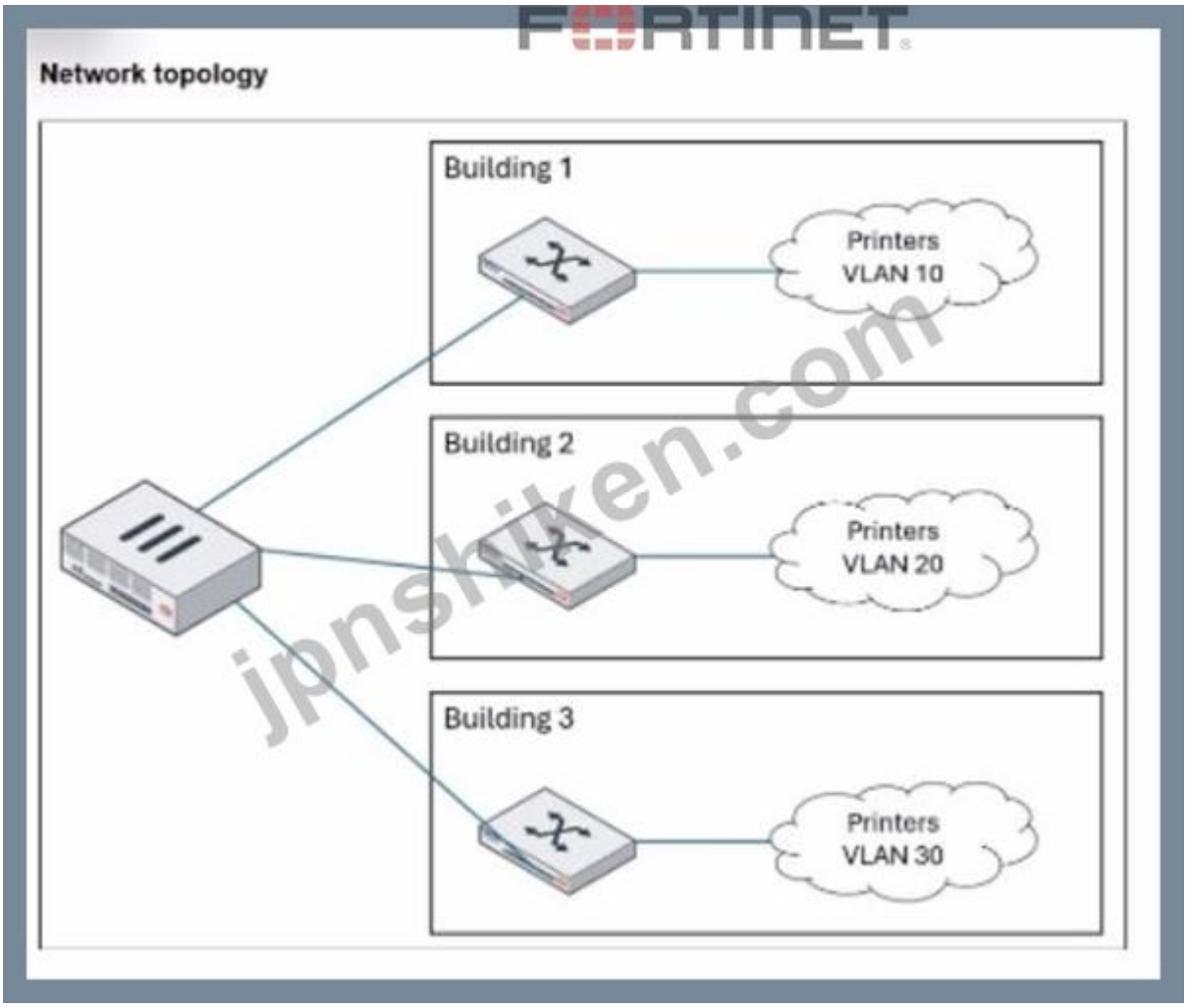
試験コード：	NSE5_FNC_AD_7.6
試験名称：	Fortinet NSE 5 - FortiNAC-F 7.6 Administrator
認証ベンダー：	Fortinet
無料問題の数：	12
バージョン：	v2026-05-29
ページの閲覧量：	105
問題集の閲覧量：	124

https://www.jpnshiken.com/shiken/Fortinet.NSE5_FNC_AD_7.6.v2026-05-29.q12.html

質問: **1**
組織では、大規模な FortiNAC-F の導入を簡素化するために、FortiNAC-F マネージャーを追加したいと考えています。
グローバルに管理できるポリシーの種類はどれですか? (2 つ選択してください。)
A. 認証
B. エンドポイントコンプライアンス
C. サプリカントEasyConnect
D. ネットワークアクセス
正解: **(**正解を表示します**)**
FortiNAC-Fマネージャは、複数の制御 -アプリケーション ℃A）アプライアンスを一元管理し、分散型企業全体で一貫したセキュリティ体制を確保するために設計されています。これを実現するために、マネージャでは、管理者が個々のCAごとにポリシーを設定するのではなく、特定の種類のポリシーをグローバルに定義 -配布できます。
FortiNAC マネージャ ガイドによると、グローバルに管理される主な 2 つのポリシー タイプは次のとおりです。
ネットワークアクセスポリシー (D): これらのポリシーは、ネットワークアクセスに関する ff-Then」ロジックを定義します。管理者は、これらのポリシーをグローバルレベルで管理することで、 請負業者」がどの支社またはキャンパスに接続しても、同じ制限付きアクセスを許可できます。
エンドポイントコンプライアンスポリシー (B): スキャンと設定で構成されるコンプライアンスポリシーをグローバルに管理することで、セキュリティベースラインを統一できます。例えば、グローバルポリシーでは、組織全体のすべてのWindowsデバイスに、本番ネットワークにアクセスする前に、特定のウイルス対策バージョンをインストールしてアクティブ化することを義務付けることができます。
マネージャーは認証イベントの可視性を提供し、ディレクトリデータを同期できますが、特定の認証 A）設定ローカルRADIUSシークレットや特定のLDAPサーバーリンクなど）は、サイト固有のインフラストラクチャに対応するためにCAにローカライズされることがよくあります。サプリカントEasyConnect ℃）はオンボーディング用の機能セットですが、

構造化された グローバルポリシー」エンジンは主にアクセスとコンプライアンスのフレームワークに重点を置いています。
FortiNAC Managerはグローバルポリシー管理機能を備えており、管理対象のすべてのCAアプライアンスにポリシーを作成 配布できます。これには、VLANとACLの割り当てを制御するネットワークアクセスポリシーと、ホストのセキュリティ要件を定義するエンドポイントコンプライアンスポリシーが含まれます。これらのポリシーを一元管理することで、グローバルネットワークファブリック全体でセキュリティ基準が均一に適用されます。- FortiNAC Manager管理ガイド :グローバルポリシー管理の概要。

質問: **2**
展示品を参照してください。



管理者は、FortiNAC-Fを使用して組織全体のプリンタを自動プロビジョニングしたいと考えています。各建物では、プリンタ用に独自のローカルVLANを使用しています。
単一のネットワーク アクセス ポリシーでこれを実現できる FortiNAC-F 機能はどれですか?
A. 動的ホストグループ
B. 論理ネットワーク
C. デバイスプロファイリングルール
D. 優先VLAN指定

正解: **(**正解を表示します**)**
FortiNAC-F 論理ネットワーク機能は、高レベルのセキュリティポリシーと基盤となる物理ネットワークインフラストラクチャの間に抽象化レイヤーを提供するために特別に設計されています。図の建物1、2、3のように、異なる物理的な場所で同じ種類のデバイスに対して異なるローカルVLAN ID（例プリンタの場合はVLAN 10、20、30）が使用されている大規模な導入環境では、建物ごとに個別のポリシーを管理すると、管理オーバーヘッドが大幅に増加します。
論理ネットワークを使用することで、管理者は単一のエンティティ（例えば "プリンター"という論理ネットワーク）を作成し、それを単一のネットワークアクセスポリシーの "アクセス値"として使用できます。この論理ラベルと特定の物理VLANのマッピングは、各ネットワークデバイスのモデル設定レベルで行われます。プリンタがBuilding 1のスイッチに接続すると、FortiNAC-Fはポリシーを評価し、プリンタが "プリンター"論理ネットワークに属する必要があることを識別し、その特定のスイッチのモデル設定をチェックして、そのラベル（VLAN 10）にマッピングされているVLAN IDを確認します。同じプリンタがBuilding 3に移動された場合、同じ単一のポリシーが適用されますが、FortiNAC-FはBuilding 3のスイッチのローカルマッピングに基づいて、プリンタをVLAN 30にプロビジョニングします。
このアーキテクチャ アプローチにより、ローカル ネットワーク トポロジの複雑さや変化に関係なく、ポリシーの一貫性が維持され、管理が容易になります。
論理ネットワークは、ネットワークアクセス要件を一度定義すれば、そのアクセスに異なるVLAN IDを使用する可能性のある多数のネットワークデバイスに適用できる手段を提供します。各管理対象デバイスは、同じ論理ネットワークラベルに対して異なるVLAN IDを使用できます。要件に基づいて論理ネットワークを定義し、管理対象デバイスがモデル構成で構成されている際に、ネットワークをVLAN IDに関連付けることができます。- FortiNAC-F IoT導入ガイド：論理ネットワークの定義

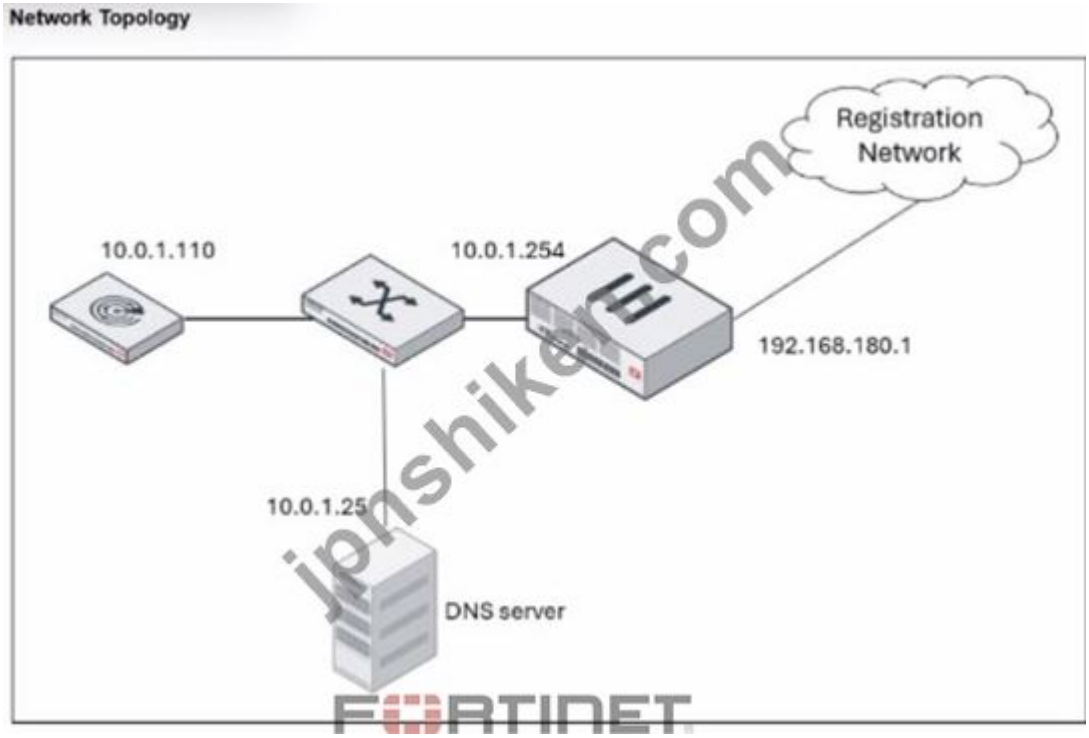
質問**: 3**
ネットワーク管理者は、特定のホストのネットワークアクセスに関する問題をトラブルシューティングしています。管理者は、そのホストに想定とは異なるネットワークアクセスポリシーが割り当てられているのではないかと疑っています。
管理者は、特定のホストに適用されているネットワーク アクセス ポリシーを確認するためにどこを確認すればよいでしょうか。
A. 接続ビュー
B. ホストのポリシー詳細ビュー
C. ポリシーログビュー
D. ホストのポートのポートプロパティビュー
正解: **(**正解を表示します**)**
FortiNAC-F でネットワークアクセスのトラブルシューティングを行う際には、ホストに特定のアクセスレベルが付与された理由を正確に検証する必要があることがよくありま

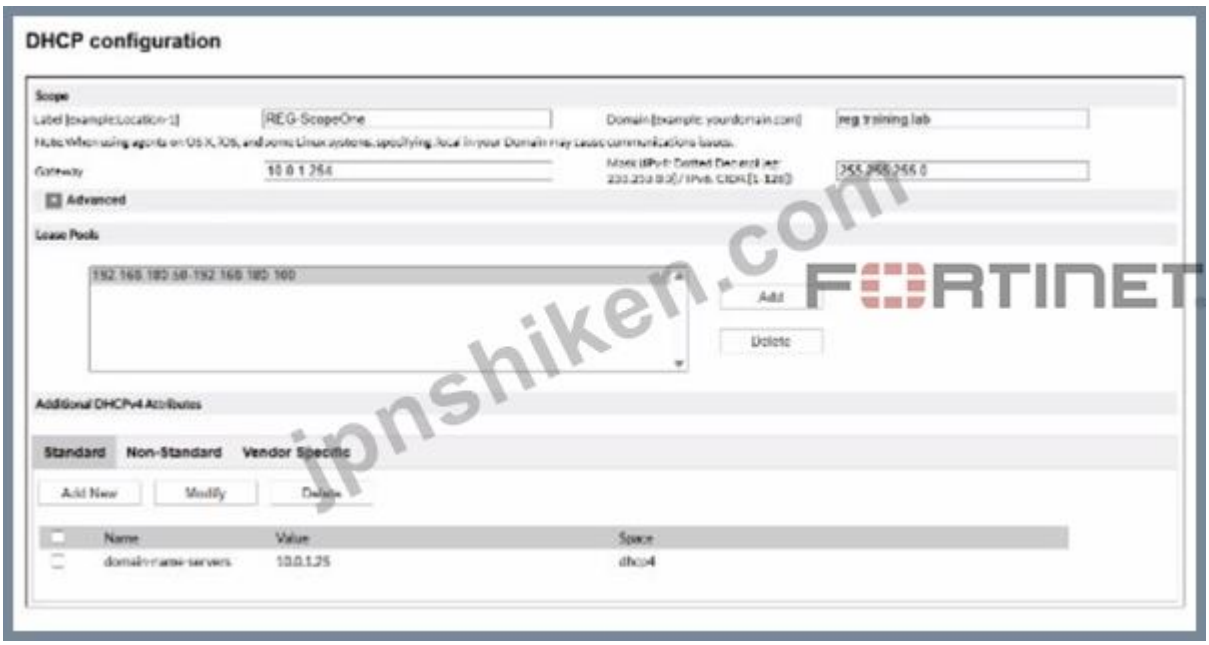
す。FortiNAC-F はポリシーをトップダウンで評価し、最初に一致したポリシーに基づいてアクセスを割り当てるため、管理者は特定の稼働中のエンドポイントにおけるこの評価結果を明確に確認できる必要があります。
ポリシー詳細 (C) ビューは、この目的に特化したツールです。管理UIで 「ホスト」> 「ホスト」 または 「アダプタビュー」) に移動すると、管理者は対象のホストの特定のMACアドレスまたはIPアドレスを検索できます。ホストレコードを右クリックすると、コンテキストメニューが表示され、そこからポリシー詳細を選択できます。このビューでは、特定のホストに対するポリシーエンジンの決定をリアルタイムで確認できます。一致したネットワークアクセスポリシー、一致をトリガーしたユーザー/ホストプロファイル、そして現在適用されているネットワークアクセス設定 (VLAN/ACL) が表示されます。
ポリシーログ (A) はシステム全体のすべてのポリシー遷移の履歴を提供しますが、多くの場合、ログ量が多すぎて単一のホストの現在の状態を効率的に把握することはできません。接続ビュー (B) には物理ポートと基本ステータスが表示されますが、ポリシーロジックの詳細な内訳は表示されません。ポートプロパティ (D) ビューにはスイッチインターフェース自体の設定が表示されますが、これは最終的なアクセス決定を構成する要素の1つにすぎません。
特定のエンドポイントに現在適用されているポリシーを確認するには、 「ポリシー詳細」 ビューを使用します。 「ホスト」> 「ホスト」に移動し、ホストを選択して右クリックし、 「ポリシー詳細」を選択します。このウィンドウには、そのホストレコードに現在適用されている特定のネットワークアクセスポリシー、ユーザー/ホストプロファイル、およびネットワークアクセス構成が表示されます。- FortiNAC-F 管理ガイド :ポリシー詳細とトラブルシューティング。

質問: **4**
管理者は、FortiNAC-F が RADIUS 応答でユーザー定義の RADIUS 属性のグループを返すようにしたいと考えています。
これを実現するにはどの条件を満たす必要がありますか?
A. 要求元デバイスは RFC 5176 をサポートしている必要があります。
B. 着信 RADIUS 要求には、Calling-Station-ID 属性が含まれている必要があります。
C. インベントリ ビュー内のデバイス モデルは、プロキシベースの認証用に構成する必要があります。
D. FortiNAC-F RADIUS サーバー構成で RADIUS アカウンティングを有効にする必要があります。
正解: **(**正解を表示します**)**
FortiNAC-FのRADIUS属性グループ機能により、管理者はネットワークデバイスに返送されるAccess-Acceptパケットに、カスタマイズされたRADIUS属性（特定のVLAN ID、フィルタID、ベンダー固有の属性など）を含めることができます。これは、ネイティブではサポートされていないものの、標準のAVPairsを使用して管理できる 「Generic RADIUS」デバイスをサポートする場合に特に便利です。

FortiNAC-F Generic RADIUS Wired Cookbook および管理ガイドの「RADIUS Attribute Groups」セクションによると、この機能が動作するための重要な前提条件が 1 つあります。それは、着信 RADIUS 要求に Calling-Station-ID 属性が含まれている必要があることです。Calling-Station-ID には通常、接続エンドポイントの MAC アドレスが含まれます。FortiNAC-F はホスト中心のシステムであるため、MAC アドレスを一意の識別子として使用してホスト レコードを検索し、関連付けられているネットワーク アクセス ポリシーを評価し、どの論理ネットワーク (およびどの属性グループ) を適用するかを決定します。着信要求にこの属性がない場合、FortiNAC-F はホストを確実に識別できず、安全機構として、応答にユーザー定義の RADIUS 属性を含めません。これにより、不正な属性が適用されたデバイスや識別できないデバイスが特権アクセスを取得できないようにします。
FortiNAC から返される RADIUS Access-Accept パケットに含める必要がある属性のセットを設定します... 要件: 受信 RADIUS 要求には Calling-Station-Id が含まれている必要があります。そうでない場合、FortiNAC は RADIUS 属性を含めません。この属性は、FortiNAC データベース内でホストとその現在の状態を識別するために使用されます。」- FortiNAC-F 7.6.0 Generic RADIUS Wired Cookbook: RADIUS 属性グループの設定。

質問**: 5**
展示品を参照してください。





管理者は登録分離ネットワークの DHCP スコープを構成しましたが、分離プロセスが機能していません。
設定上の問題は何でしょうか?
A. ドメイン ネーム サーバーの指定が正しくありません。
B. ラベルはシステム予約済みの値を使用します。
C. リース プールに完全なサブネットが含まれていません。
D. スコープに定義されたゲートウェイが正しくありません。
正解: **(**正解を表示します**)**
FortiNAC-Fの導入では、隔離されたホストがFortiNACアプライアンスと確実に通信できるように、隔離ネットワーク（登録 修復など）のDHCPスコープの設定が基盤となるネットワークインフラストラクチャと完全に一致している必要があります。提供されている図では、DHCP設定とネットワークトポロジの間に明らかな矛盾が見られます。
「ネットワークトポロジ」図に示されているように、登録ネットワークはIPアドレス192.168.180.1を持つルータインターフェース（またはサブインターフェース）上に存在します。このアドレスは、登録VLANに配置されたすべてのホストのデフォルトゲートウェイを表します。しかし、「DHCP設定」図では、スコープ「REG-ScopeOne」がゲートウェイ10.0.1.254に設定されています。この10.0.1.254アドレスは、登録サブネットではなく、管理/サービスネットワーク（FortiNACのポート2）に属しています。登録VLAN内のホストがDHCP経由でこの誤ったゲートウェイを受信すると、すべてのオフリンクトラフィックを到達不可能なIPに送信しようとし、キャプティブポータルの読み込みやFortiNACサーバーとの通信ができなくなります。
FortiNAC-F 設定ウィザードリファレンスによると、レイヤー3ネットワークスコープを定義する際、「ゲートウェイ」フィールドには、特定の分離VLANのゲートウェイとして機能するルーターインターフェースのIPアドレスを入力する必要があります。FortiNACアプライアンス自体は通常、別のサブネットに配置され、トラフィックはルーターのDHCPリレー（IPヘルパー）とDNSリダイレクトを介してアプライアンスに送信されます。

レイヤー3ネットワークのスコープを設定する場合、ゲートウェイ値はそのサブネットのルータインターフェースのIPアドレスにする必要があります。これにより、ホストはローカルゲートウェイにアクセスしてトラフィックをルーティングできるようになります。ゲートウェイの設定が間違っていると、ホストはFortiNAC eth1/port2インターフェースにアクセスして登録できなくなります。ゲートウェイが分離VLANのネットワークトポロジと一致していることを確認してください。- FortiNAC-F設定ウィザードリファレンスマニュアル：DHCPスコープ。

質問: **6**
管理者は、すべてのユーザーがネットワークに接続するたびに企業ドメインにログインする企業環境を管理しています。管理者は、ログインスクリプトを活用してFortiNAC-Fエージェントを使用し、エンドポイントの可視性を向上したいと考えています。ログインスクリプトの一部として導入できるエージェントはどれですか？
A. 永続的
B. 溶解可能
C. モバイル
D. パッシブ
正解: **A** (コメントを発表する)
「エンドポイントの可視性強化」が求められる企業ドメイン環境では、Persistent Agent が推奨されます。登録時に一度だけコンプライアンススキャンを実行するための一時的な Dissolvable Agent とは異なり、Persistent Agent は「インストールして常駐する」アプリケーションです。
パーシステントエージェントは、ログインスクリプト、グループポリシーオブジェクト（GPO）、サードパーティ製ソフトウェア管理ツールなど、自動化されたエンタープライズメソッドを通じて配布できるように特別に設計されています。ログインスクリプト経由で導入する場合、エージェントはサイレントインストールされ、FortiNAC-Fサービスインタフェースとの通信を直ちに開始するように設定できます。アクティブになると、ログオンユーザー、インストール済みアプリケーション、アダプタ情報などのホスト詳細情報を報告し、継続的な可視性を提供します。また、Windowsセッションイベント（ログオン/ログオフ）をリッスンし、FortiNAC-Fへの自動シングルサインオン（SSO）登録をトリガーします。これにより、ユーザーがドメインに接続するとすぐにデバイスが識別され、適切なネットワークアクセスポリシーが割り当てられます。
永続エージェントは、ログインスクリプトまたは組織で使用されているその他のソフトウェア配布方法を介してWindowsドメインマシンに配布できます。永続エージェントは常にホストにインストールされたままです。エージェントがインストールされると、バックグラウンドで実行され、FortiNAC管理者が設定した間隔でFortiNACと通信します。- FortiNAC-F管理ガイド：永続エージェントの概要。

質問: **7**

管理者は、FortiNAC-F デバイスを 1+1 HA 構成で導入する際に、共有 IP アドレス オプションを使用することを選択しました。
このタイプの展開ではどの条件を満たす必要がありますか?
A. 分離ネットワーク タイプはレイヤー 3 です。
B. FortiNAC-F デバイス間に直接ケーブル リンクがあります。
C. プライマリ管理インターフェイスとセカンダリ管理インターフェイスは同じサブネット上にあります。
D. 分離ネットワーク タイプはレイヤー 2 です。
正解: **(**正解を表示します**)**
1+1高可用性（HA）構成において、FortiNAC-Fは管理アクセスとして、個別のIPアドレスまたは共有IPアドレス（仮想IPまたはVIPとも呼ばれます）という2つの主要な方法をサポートしています。共有IPオプションはレイヤー2 HA設計の一部であり、現在「アクティブ」または「制御中」状態にあるアプライアンスを常に単一のURLまたはIPアドレスで参照できるようにすることで、管理を簡素化します。
共有IP設定が正しく機能するには、プライマリ管理インタフェースとセカンダリ管理インタフェース（ポート1）が同じサブネット上に配置されている必要があります。これは、共有IPがアクティブユニットの物理インタフェースに動的に割り当てられる論理アドレスであるためです。IPアドレスを所有できるのは一度に1つのユニットのみであるため、共有IPへのARP要求に正しく応答し、どちらのユニットがアクティブであってもゲートウェイへのアクセスを可能にするためには、両方のユニットが同じブロードキャストドメイン（レイヤー2）上に配置されている必要があります。アプライアンスが異なるサブネット上に配置されている場合（レイヤー3 HA設計）、共有IPは異なるネットワークセグメント間で「ワローティング」できないため、使用できません。管理者は各ユニットを固有の物理IPで管理するか、FortiNACマネージャを使用する必要があります。
L2 HA 構成の場合、「共有 IP アドレスを使用する」チェックボックスをオンにし、共有 IP アドレス情報を入力します。プライマリサーバーとセカンダリサーバーが同じサブネットにない場合は、共有 IP アドレスを使用しないでください。共有 IP アドレスは、フェイルオーバーおよびリカバリ中にアプライアンス間で移動するため、両方のユニットが同じネットワーク上に存在している必要があります。- FortiNAC-F 高可用性リファレンスマニュアル：共有IP 構成。

質問: **8**
管理者は、FortiNAC-F デバイスを 1+1 HA 構成で導入する際に、共有 IP アドレス オプションを使用することを選択しました。
このタイプの展開ではどの条件を満たす必要がありますか?
A. 分離ネットワーク タイプはレイヤー 3 です。
B. 分離ネットワーク タイプはレイヤー 2 です。
C. FortiNAC-F デバイス間に直接ケーブル リンクがあります。

D. プライマリ管理インターフェイスとセカンダリ管理インターフェイスは同じサブネット上にあります。
正解: **(**正解を表示します**)**
1+1高可用性（HA）構成において、FortiNAC-Fは管理アクセスとして、個別のIPアドレスまたは共有IPアドレス（仮想IPまたはVIPとも呼ばれます）という2つの主要な方法をサポートしています。共有IPオプションはレイヤー2 HA設計の一部であり、現在「アクティブ」または「制御中」状態にあるアプライアンスを常に単一のURLまたはIPアドレスで参照できるようにすることで、管理を簡素化します。
共有IP設定が正しく機能するには、プライマリ管理インタフェースとセカンダリ管理インタフェース（ポート1）が同じサブネット上に配置されている必要があります。これは、共有IPがアクティブユニットの物理インタフェースに動的に割り当てられる論理アドレスであるためです。IPアドレスを所有できるのは一度に1つのユニットのみであるため、共有IPへのARP要求に正しく応答し、どちらのユニットがアクティブであってもゲートウェイへのアクセスを可能にするためには、両方のユニットが同じブロードキャストドメイン（レイヤー2）上に配置されている必要があります。アプライアンスが異なるサブネット上に配置されている場合（レイヤー3 HA設計）、共有IPは異なるネットワークセグメント間で「ワローティング」できないため、使用できません。管理者は各ユニットを固有の物理IPで管理するか、FortiNACマネージャを使用する必要があります。
L2 HA 構成の場合、「共有 IP アドレスを使用する」チェックボックスをオンにし、共有 IP アドレス情報を入力します。プライマリサーバーとセカンダリサーバーが同じサブネットにない場合は、共有 IP アドレスを使用しないでください。共有 IP アドレスは、フェイルオーバーおよびリカバリ中にアプライアンス間で移動するため、両方のユニットが同じネットワーク上に存在している必要があります。- FortiNAC-F 高可用性リファレンスマニュアル：共有IP 構成。

質問: **9**
管理者は複数のデバイスプロファイリングルールを作成し、データベース内の既存デバイスをすべて評価しました。一部のデバイスはルールに一致したためプロファイリング済みデバイスビューに表示されますが、不明なままであり、プロファイリング済みデバイスビューの登録列には「いいえ」と表示されます。
最も可能性の高い原因は何でしょうか?
A. デバイス プロファイリング ルールの確認オプションが有効になっていません。
B. デバイスが複数のデバイス プロファイリング ルールに一致します。
C. デバイス プロファイリング ルールの登録が手動に設定されています。
D. デバイスには永続エージェントがインストールされており、接続ポイントで PA 最適化が有効になっています。
正解: **A (**コメントを発表する**)**
FortiNAC-Fでは、デバイスプロファイリングルールを使用して、DHCPフィンガープリント、OID、MACプレフィックスなどのフィンガープリントに基づいて、デバイス（IPカメラ、

プリンター、IoTデバイスなど）を自動的に識別・分類します。デバイスがルールに一致すると、「プロファイル済みデバイス」ビューに表示されます。
ただし、ルールに一致しても、デバイスがデータベースに自動的に登録されるわけではありません（ルールでそのように設定されていない場合）。デバイスがビューに表示されているにもかかわらず「不明」のままで、登録列に「いいえ」と表示されている場合は、「確認」または「自動登録」）アクションがトリガーされていないことを示しています。デバイスプロファイリングルールの設定には、「自動承認を許可」または「確認」という設定があります。これが有効になっていない場合、システムはデバイスを識別しますが、管理者が手動で一致を承認するまで、ホストのステータスは「不明」から「登録済み」に変更されません。
これは、システムがそれらの一致に基づいてネットワーク アクセスを自動的に許可する前に、プロファイリング ルールが正確であることを確認するために、初期展開フェーズ中に使用される一般的な「安全」構成です。
デバイスがルールに一致しているにもかかわらず登録されていない場合は、ルール設定を確認してください。「確認」オプション（「方法」または「ルール」設定内）は、一致時にデバイスを自動的に登録するかどうかを決定します。「確認」が有効になっていない場合、管理者が手動でデバイスを昇格させるまで、デバイスは「プロファイル済み」状態のままで、登録ステータスは「いいえ」になります。- FortiNAC-F 管理ガイド：デバイスプロファイリングルール。

質問: **10**
デバイス プロファイリング ルールを作成するときに、デバイスをホスト ビューに登録する 2 つの利点は何ですか (2 つ選択してください)。
A. デバイスは汎用 SNMP デバイスとして管理できます。
B. デバイスには接続ログが保存されます。
C. デバイスをユーザーに関連付けることができます。
D. デバイスの接続ステータスをポーリングできます。
正解: **(**正解を表示します**)**
FortiNAC-F のデバイスプロファイラは、未知の「不正」デバイスを評価し、フィンガープリントと動作に基づいて分類するルールベースのエンジンです。プロファイリングルールがデバイスに一致した場合、管理者はそのデバイスを自動的に登録するようにルールを設定できます。登録プロセスでは、デバイスレコードを主に2つの場所、つまりトポロジビュー（デバイスとして）またはホストビュー（登録済みホストとして）に表示できます。
FortiNAC-F管理ガイドによると、デバイスをホストビューに登録すると、アイデンティティ管理と履歴追跡に大きなメリットがあります。まず、デバイスをユーザー（C）に関連付けることができます。FortiNACデータベースアーキテクチャでは、ホストビューがエンドポイントアイデンティティの主要なリポジトリです。プロファイルされたデバイスをここに配置することで、システムはそのハードウェア（MACアドレス）を特定のユーザーアカウント（従業員、ゲスト、またはシステムレベルの「所有者」）にリンクできます。この関連付け

は、ロールベースアクセス制御（RBAC）とネットワークファブリック全体のアカウンタビリティ追跡に不可欠です。
次に、ホストビューに登録されたデバイスには接続ログ（B）が記録されます。FortiNAC-Fは、すべてのホストレコードの詳細な動作履歴を保持します。これには、デバイスのポートへの接続または切断のすべてのインスタンス、IPアドレスの割り当て、各セッション中に適用された特定のポリシーが含まれます。これらのログは、ネットワーク上のデバイスのライフサイクルを明確に示すため、接続の問題のトラブルシューティングやセキュリティフォレンジック監査に非常に役立ちます。一方、トポロジビューでのみ管理されるデバイスは、通常、インフラストラクチャコンポーネントとして扱われ、個々のセッション履歴ではなくデバイスの可用性に重点が置かれます。
登録され、ユーザーに関連付けられているデバイスは、ホスト ビューに配置され、プロファイルされたデバイス ウィンドウから削除されます。デバイスをホスト ビューに配置すると、接続履歴を追跡したり、デバイスを FortiNAC データベース内の特定の ID またはユーザー レコードに関連付けたりできるようになります。」- FortiNAC-F 管理ガイド: デバイス プロファイラーの仕組み。

質問: **11**
ネットワークインフラストラクチャデバイスの検出中に、インベントリトポロジに疑問符（？）が付いたスイッチのアイコンが表示されます。これは何が原因でしょうか？
A. 検出中に間違った SNMP コミュニティ文字列が入力されました。
B. SNMP ObjectID は FortiNAC-F によって認識されません。
C. 読み取り専用の SNMP コミュニティ サイリングが使用されました。
D. スイッチで SNMP が有効になっていません。
正解: **(正解を表示します)**
FortiNAC-Fのインベントリトポロジでは、検出されたネットワークインフラストラクチャのステータスとモデルを表すために特定のアイコンが使用されます。SNMP経由でスイッチやその他のネットワークデバイスが検出されると、FortiNAC-FはシステムオブジェクトID（sysObjectID）を取得し、特定のメーカーとモデルを識別します。このOIDは、サポート対象のデバイスマッピングの内部データベースと照合されます。
検出されたスイッチに疑問符（？）アイコンが表示される場合、検出プロセスはデバイスとの通信に成功している（つまりSNMP認証情報は正しい）ものの、SNMPオブジェクトIDがFortiNAC-Fの現在のバージョンで認識またはマッピングされていないことを示します。これは基本的に、デバイスが現在のソフトウェアで「サポートされていない」ことを意味します。OIDが不明なため、FortiNAC-FはL2ポーリング（ホスト可視化）やVLANスイッチング（適用などの重要な機能に使用するCLIまたはSNMPコマンドセットを認識できません。この問題を解決するには、管理者は手動で「デバイスマッピングを設定」し、類似の既存モデル、または基本的なL3可視化のみが必要な場合は「汎用SNMPデバイス」にマッピングすることができます。

検出されたデバイスに「?」アイコンが表示されている場合は、現在実行中のバージョンにそのデバイスのシステム OID のマッピングがない（デバイスがサポートされていない）ことを示します。デバイス マッピングは、L2/L3 ポーリング、読み取り、VLAN の切り替えなどの機能を実行してデバイスを管理するために使用されます。」- Fortinet テクニカル ヒント: インベントリでモデル化できないデバイスのオプション。

質問: **12**
複数の FortiNAC-F CA で構成される大規模な環境に FortiNAC-F マネージャを導入すると、どのような 3 つの方法で管理が簡素化されますか? (3 つ選択してください。)
A. グローバルインフラストラクチャデバイスインベントリ
B. グローバルバージョン管理
C. グローバル認証セキュリティポリシー
D. プールされたライセンス
E. グローバルな可視性
正解: **(**正解を表示します**)**
FortiNAC-Fマネージャ（FortiNAC-M）は、複数のFortiNAC-F制御・アプリケーション（CA）アプライアンスが異なる拠点に展開されている大規模分散環境向けの集中管理プラットフォームとして設計されています。FortiNAC-Fマネージャ管理ガイドによると、マネージャを導入することで、以下の3つの点で管理オーバーヘッドが軽減されます。
まず、グローバルバージョン管理（B）を提供します。マネージャーはファームウェアとソフトウェアのアップデートの中央リポジトリとして機能し、管理者は特定のバージョンをすべての管理対象CAに同時にプッシュすることで、ファブリック全体の一貫性を確保できます。次に、プールライセンス（D）を実現します。CAごとに個別のライセンスを購入して管理するのではなく、ライセンスはマネージャーに一元管理されます。マネージャーは、ホスト数に基づいて必要に応じてこれらのライセンスを各CAに配布します。この「フローティング」ライセンスモデルはコストを最適化し、特定のサイトで容量が不足している一方で、他のサイトでは容量が余っているという状況を防ぎます。最後に、グローバルな可視性（E）を提供します。マネージャーは、すべての管理対象CAからのホストとデバイスのデータを単一のコンソールに集約します。この「単一の画面」により、管理者は個々のサーバーにログインすることなく、グローバル組織全体で特定のMACアドレスまたはユーザーを検索できます。
マネージャーは構成テンプレートを支援できますが、認証セキュリティ ポリシー (C) とインフラストラクチャ モデリング (A) は、サイト固有のロジックとパフォーマンスを確保するために、主にローカル CA レベルで管理されます。
FortiNAC マネージャは、複数の FortiNAC-F サーバー (CA) 用の集中管理コンソールを提供します。主な利点は次のとおりです。* ライセンス管理: ライセンスはマネージャ上でプールされ、必要に応じて管理対象の CA に割り当てられます。* ソフトウェア管理: ファームウェアの更新を集中管理し、マネージャからすべての CA にプッシュできます。*

集中監視: 管理対象環境全体のすべてのホスト、アダプタ、イベントをグローバルに表示します。- FortiNAC-F マネージャ管理ガイド: 概要と利点。