Fortinet.FCP_FAZ_AN-7.4.v2025-02-10.q53

試験コード:	FCP_FAZ_AN-7.4
試験名称:	FCP - FortiAnalyzer 7.4 Analyst
認定資格:	Fortinet
無料問題数:	53
バージョン:	v2025-02-10
アクセス数:	500
ページビュー数:	530
https://www.jpnpdf.com/Fortinet.FCP_FAZ_AN-7.4.v2025-02-10.q53-mondaishu.html	

最新問題: **1**
FortiAnalyzer の動作モードに関する次の記述のうち、正しいものはどれですか? (2 つ選択してください。)
A. コレクター モードで実行している場合、FortiAnalyzer はログを syslog サーバーに転送できます。
B. FortiAnalyzer は、HA 用に設定されていない限り、デフォルトでコレクター モードで実行されます。
C. FortiAnalyzer がコレクター モードで実行されているときにレポートを作成および編集できます。
D. FortiAnalyzeer デバイスを両方のモードで実行するトポロジでは、パフォーマンスが向上します。
Answer: B,D (メーッセージを残す**)**
FortiAnalyzer には、アナライザー モードとコレクター モードという 2 つの主要な動作モードがあります。各モードには特定の目的があり、異なる機能があります。
* オプション A - コレクター モードで Syslog サーバーにログを転送する:
* コレクター モードでは、FortiAnalyzer は Fortinet デバイスからログを収集しますが、ログを処理または分析しません。代わりに、ログをアナライザー モードの他の FortiAnalyzer ユニットまたは特定の保存場所に転送します。ただし、ログを syslog サーバーに転送することは、コレクター モードの機能ではありません。ログは通常、他の FortiAnalyzer デバイスに保存されるか、送信されます。
* 結論:誤り。
* オプション B - HA 用に設定されていない限り、デフォルト モードはコレクター モードです。
* FortiAnalyzer を最初にセットアップすると、高可用性 (HA) セットアップの一部として構成されない限り、デフォルトでコレクター モードで実行されます。高可用性 (HA) セットアップの一部として構成されている場合は、アナライザー モードに設定されます。

コレクター モードでは、分析よりもログの収集と保存を優先し、分析をネットワーク内の他のデバイスにオフロードします。
* 結論:正解です。
* オプション C - コレクター モードでのレポートの作成と編集:
* コレクター モードでは、FortiAnalyzer にはレポートを作成または編集する機能がありません。このモードはログの収集と転送のみに重点が置かれており、分析とレポートの生成はアナライザー モードで動作する FortiAnalyzer ユニットに任されています。
* 結論:誤り。
* オプション D - トポロジの両方のモードでのパフォーマンスの向上:
* FortiAnalyzer デバイスをネットワーク トポロジにコレクタ モードとアナライザ モードの両方で導入すると、パフォーマンスが向上します。コレクタ モードのデバイスはログ収集を処理するため、ログの処理、分析、レポート作成に重点を置くアナライザ モードのデバイスの負荷が軽減されます。このタスクの分離により、リソースの使用が最適化され、ログ管理の全体的な効率が向上します。
* 結論:正解です。
結論：
* 正解:B. FortiAnalyzer は、HA および D 用に設定されていない限り、デフォルトでコレクター モードで実行されます。両方のモードで実行される FortiAnalyzer デバイスを含むトポロジにより、パフォーマンスが向上します。
* これらの回答は、FortiAnalyzer の動作モードの機能とデフォルト構成、および混合モード トポロジによってパフォーマンスを向上させる方法を正しく説明しています。
参考文献:
* FortiAnalyzer 7.4.1 の動作モード (コレクターとアナライザー) とそれぞれの機能に関するドキュメント。

最新問題**: 2**
作成したプレイブックを実行する前に、なぜ数分間待たなければならないのでしょうか?
A. FortiAnalyzer では、他のプレイブックが実行されていないことを確認するためにその時間が必要です。
B. FortiAnalyzer は現在のプレイブックをバックアップするためにその時間を必要とします。
C. FortiAnalyzer は新しいプレイブックをデバッグするためにその時間を必要とします。
D. FortiAnalyzer は新しいプレイブックを解析するためにその時間を必要とします。
Answer: (解答を表示する**)**

最新問題**: 3**
ローカル以外の管理者が単一の LDAP グループ内の任意のユーザー アカウントを使用して FortiAnalyzer に認証できるようにするには、FortiAnalyzer でどの 2 つの設定を構成する必要がありますか? (2 つ選択してください。)
A. リモートLDAPサーバー
B. ローカルワイルドカード管理者アカウント

C. LDAPグループへのアクセスを制限する信頼されたホストプロファイル
D. 管理者グループ
Answer: A,B (メーッセージを残す**)**

最新問題**: 4**
登録済みのログ記録デバイスを 1 つの ADOM から新しい ADOM に移動した後、次の CLI コマンドを実行する目的は何ですか?
sql-local rebuild-adom <新しいADOM名>を実行します。
A. 移動したデバイスの分析ログを新しいADOMに取り込み、レポートを実行できるようにする
B. デバイスの分析ログを古いデータベースから削除する
C. アーカイブログを新しいADOMに移行するには
D. ディスククォータの強制をデフォルトにリセットする
Answer: A (メーッセージを残す**)**

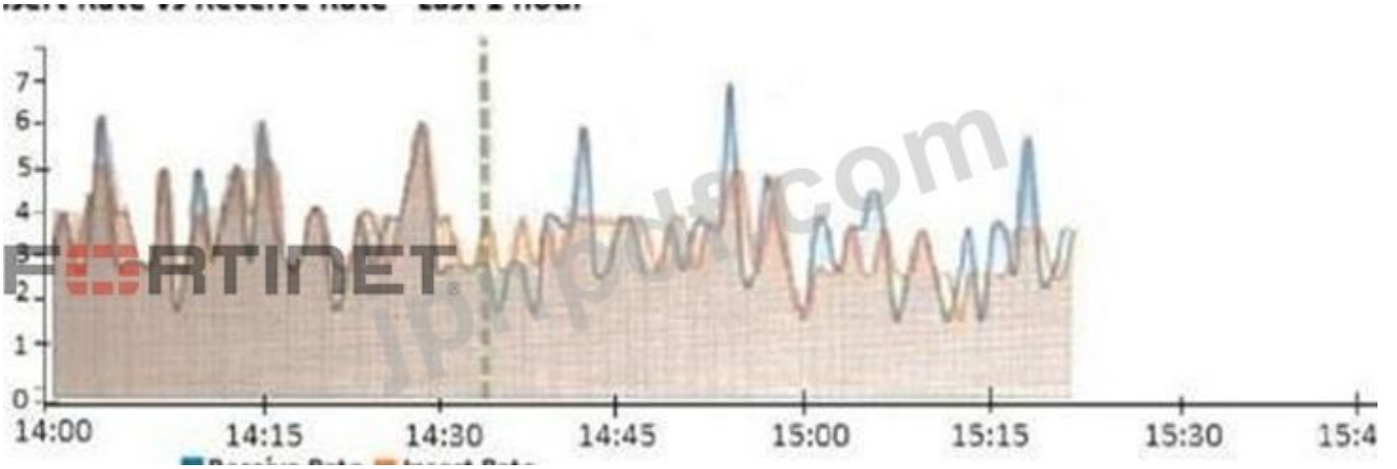
最新問題**: 5**
アナリストとしての役割の一環として、同じパラメータを使用してログ ビューを頻繁に検索していることがわかります。
検索フィルターを繰り返し定義する代わりに、時間を節約するにはどうすればよいでしょうか?
A. カスタムダッシュボードを構成します。
B. カスタム ビューを構成します。
C. データセレクターを構成します。
D. マクロを設定し、デバイス グループに適用します。
Answer: B (メーッセージを残す**)**
FortiAnalyzer のログ ビューで同じ検索パラメータを頻繁に使用する場合は、再利用可能なフィルタまたはビューを設定すると、かなりの時間を節約できます。各オプションの分析は次のとおりです。
* オプション A - カスタムダッシュボードを構成する:
* カスタム ダッシュボードは、ネットワーク アクティビティ、パフォーマンス、脅威データに関するさまざまなウィジェットや概要を表示するのに便利ですが、ログ ビューの特定の検索フィルターを保存するようには設計されていません。
* 結論:誤り。
* オプション B - カスタムビューを構成する:
* FortiAnalyzer のカスタム ビューを使用すると、アナリストは特定の検索フィルターと構成を保存できます。
カスタム ビューを設定すると、頻繁に使用する検索パラメータを保持しておき、毎回フィルターを再適用しなくてもすばやくアクセスできます。このオプションは、定期的なログ検索のプロセスを効率化するために特別に設計されています。
* 結論:正解です。
* オプション C - データセレクターを構成する:

* データ セレクターは、FortiAnalyzer レポートおよびウィジェットの特定の種類のデータを定義するために使用されます。
これらはレポートでは役立ちますが、ログ ビューでログ検索パラメータを保存して再利用するためのものではありません。
* 結論:誤り。
* オプション D - マクロを構成してデバイス グループに適用する:
* FortiAnalyzer のマクロは通常、ログ検索フィルターの保存ではなく、自動化タスクに使用されます。
デバイス グループにマクロを適用しても、特定のログ ビュー検索パラメータを保存するという要件は満たされません。
* 結論:誤り。
結論：
* 正解:B. カスタム ビューを構成します。
* カスタム ビューを使用すると、特定の検索フィルターを保存できるため、ログ ビューで頻繁に使用されるパラメーターにすばやくアクセスできます。
参考文献:
* ログ検索用のカスタム ビューの作成と使用に関する FortiAnalyzer 7.4.1 ドキュメント。

最新問題: **6**
どのログが Contained ステータスのイベントを生成しますか?
A. action=pass の IPS ログ。
B. action=quarantine の AV ログ。
C. WebFilter ログは action=dropped になります。
D. action=blocked の AppControl ログ。
Answer: B (メーッセージを残す**)**

最新問題: **7**
FortiAnalyzer はどの機能を一元管理しますか? (3 つ選択してください)
A. 脆弱性評価
B. コンテンツのアーカイブ化/データマイニング
C. グラフィカルレポート
D. セキュリティログ分析/フォレンジック
E. ネットワーク分析
Answer: B,C,D (メーッセージを残す**)**

最新問題: **8**
展示品をご覧ください。



14:35 のデータポイントは何を示していますか?

A. FortiAnalyzer は、ログの受信よりも速くログをインデックスしています。

B. sqlplugind デーモンは、インデックス作成で 1 ログ先を行っています。

C. FortiAnalyzer はログをドロップしています。

D. FortiAnalyzer は、古いログをインデックス化できるように、一時的にログの受信を停止しました。

Answer: (解答を表示する**)**

最新問題**: 9**

2 つの FortiAnalyzer デバイスで構成された HA クラスタのファームウェアをアップグレードする場合、正しい記述はどれですか。

A. 最初にセカンダリ デバイスをアップグレードし、次にプライマリ デバイスをアップグレードします。

B. 両方の FortiAnalyzer デバイスが同時にアップグレードされます。

C. コンソール接続のみを使用してファームウェアのアップグレードを実行できます。

D. クラスタ ファームウェアのアップグレード中に通常の FortiAnalyzer 操作が中断されないように、uninterruptible-upgrade を有効にすることができます。

Answer: A (メーッセージを残す**)**

最新問題**: 10**

別添を参照:

21:20 のデータポイントは何を示していますか?
A. FortiAnalyzer は、ログの受信よりも速くログをインデックスしています。
B. fortilogd デーモンは 1 ログ分インデックスを先行しています。
C. 受信遅延が大きいため、SQL データベースを再構築する必要があります。
D. FortiAnalyzer は受信したログを一時的にバッファリングして、古いログを最初にインデックス化できるようにしています。
Answer: (解答を表示する**)**
この図には、受信レートと挿入レートという 2 つのメトリックを時間の経過とともに追跡するグラフが表示されています。これら 2 つのレートは、FortiAnalyzer でのログ処理の動作を理解する上で非常に重要です。
受信レートと挿入レートを理解する:
受信速度: これは、FortiAnalyzer が接続されたデバイスからログを受信する速度です。
挿入レート: これは、FortiAnalyzer が保存および分析のためにログをデータベースにインデックス (挿入) するレートです。
21:20のデータポイント:
21:20 には、挿入レート ラインが受信レート ラインより上にあり、FortiAnalyzer がログを受信するよりも速い速度でデータベースにログを挿入していることを示しています。この状況は、FortiAnalyzer が受信ログに対応できており、バックログまたは一時的に受信したログを新しいログの受信よりも速く処理している可能性があることを示しています。
オプション分析:
オプション A - FortiAnalyzer がログの受信よりも速くログをインデックス化しています: これは、挿入レートが受信レートを超えている 21:20 のシナリオを正確に表しています。これは、FortiAnalyzer がその時点でログを効率的に処理しており、処理のバックログがないことを示しています。
オプション B - fortilogd デーモンはインデックス作成で 1 ログ先を行っています: データは fortilogd デーモンのログ数に関する具体的な情報ではなく、レートのみを提供します。このオプションは正しくありません。
オプション C - SQL データベースの再構築が必要: 受信ラグが大きいということは、受信ログとインデックス ログのバックログが発生していることを意味します。これは通常、受信レートが挿入レートを大幅に上回っている場合に発生しますが、この場合は当てはまりません。
オプション D - FortiAnalyzer は、古いログを最初にインデックスするためにログを一時的にバッファリングしています。このシナリオでは、バッファリングの兆候はありません。バッファリングは通常、受信レートが挿入レートよりも高い場合に発生し、インデックス作成の遅れのために FortiAnalyzer がログを一時的に保存していることを示します。
結論：
正解: A. FortiAnalyzer は、ログの受信よりも速くログをインデックス化しています。
21:20 のグラフでは、受信レートよりも挿入レートが高く、FortiAnalyzer によるログ処理が効率的であることがわかります。
参照：

ログ処理メトリック、受信レート、挿入レート インジケーターに関する FortiAnalyzer 7.4.1 ドキュメント。

最新問題: **11**
FortiAnalyzer で侵害されたホストを表示す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. FortiAnalyzer デバイスに接続されている FortiGate デバイスのインターフェースでデバイス検出を有効にします。
B. FortiAnalyzer を FortiGuard にサブスクライブして、ローカル脅威データベースを最新の状態に保ちます。
C. FortiGate デバイスのファイアウォール ポリシーで Web フィルタリングを有効にし、これらのログが FortiAnalyzer に送信されることを確認します。
D. すべてのエンドポイントが FortiAnalyzer から到達可能であることを確認します。
Answer: B,C (メーッセージを残す**)**

最新問題: **12**
FortiAnalyzer ログ転送に関して正しい記述はどれですか? (2 つ選択してください。)
A. 集約モードでは、ログを syslog サーバーや CEF サーバーにも転送できます。
B. 転送モードと集約モードの両方で、デバイス間のログの暗号化がサポートされます。
C. 集約モードでは、ログとコンテンツ ファイルが保存され、スケジュールされた時間に別の FortiAnalyzer デバイスにアップロードされます。
D. 転送モードでは、ログは他の FortiAnalyzer デバイスにのみリアルタイムで転送されます。
Answer: B,C (メーッセージを残す**)**

最新問題: **13**
ログ ビューでは、チャート ビルダー機能を使用して、フィルターされた検索結果に基づいてデータセットとチャートを作成できます。同様に、FortiView ではどの機能を使用できますか?
A. レポートチャートにエクスポート
B. カスタムチャートにエクスポート
C. PDF にエクスポート
D. チャートビルダーにエクスポート
Answer: (解答を表示する**)**

最新問題: **14**
ファブリック コネクタを使用する 2 つの利点は何ですか? (2 つ選択してください。)
A. FortiAnalyzer がパブリック クラウド アカウントにログをリアルタイムで送信できるようになります。
B. ファブリック コネクタを使用すると冗長性を向上させることができます。
C. クラウド プラットフォームにログを送信するために追加のライセンスは必要ありません。

D. ファブリック コネクタを使用する方が、API を使用したサードパーティのポーリングを使用するよりも効率的です。
Answer: A,B (メーッセージを残す**)**

最新問題**: 15**
管理者が次の設定を構成しました:
設定システムグローバル
ログチェックサム md5-auth を設定する
終わり
このコマンドを実行することの意味は何ですか?
A. このコマンドは、パスワードをログ ファイルに記録し、暗号化します。
B. このコマンドはFortiAnalyzerと他のデバイス間のログ転送を暗号化します
C. このコマンドは、ログ ファイルの MD5 ハッシュ値と認証コードを記録します。
D. このコマンドは、ログ ファイルの MD5 ハッシュ値を記録します。
Answer: C (メーッセージを残す**)**

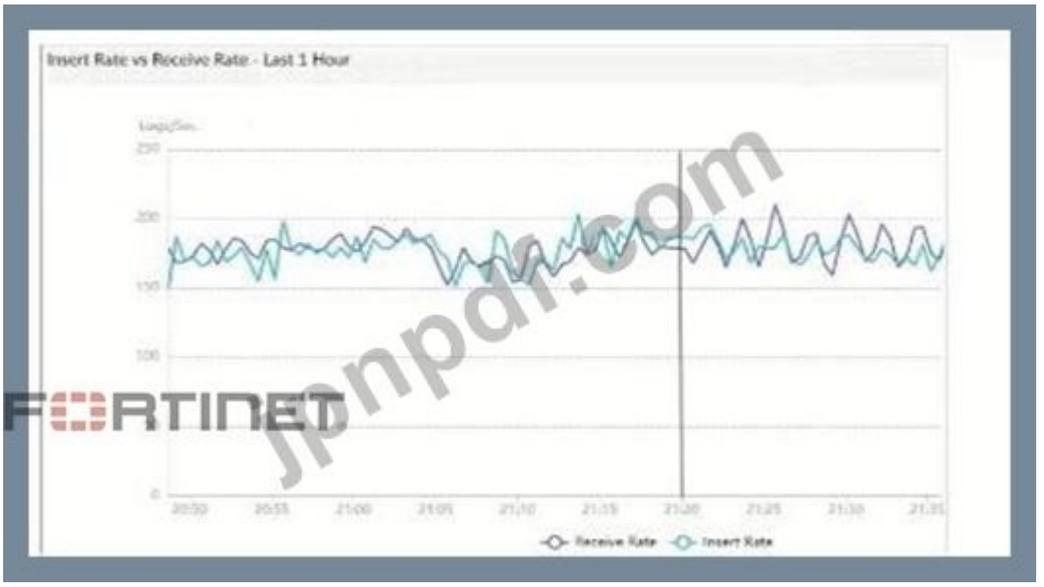
最新問題**: 16**
展示する。

Event	Event Status	Event Type	Severity
bujyqttatbsd.fndhere.org (1)	Mitigated	Web Filter	Low
Web request to suspicious destination from 10.0.3.20 blocked	Mitigated	Web Filter	Low

表示されたイベントに関するどの記述が正しいですか?
A. リスク源は分離されています。
B. セキュリティ リスクはブロックまたはドロップされました。
C. セキュリティ イベントのリスクは未解決であると見なされます。
D. このイベントからインシデントが作成されました。
Answer: B (メーッセージを残す**)**
FortiOS および FortiAnalyzer ログ システムでは、イベントの [イベント ステータス] 列のステータスが 軽減済み」の場合、通常、システムが特定された脅威に対処するためのアクションを実行したことを示します。この場合、Web フィルターは疑わしい宛先への Web 要求をブロックし、イベント ステータス 軽減済み」は、セキュリティ リスクを中和またはブロックするためのアクションが正常に実行されたことを確認します。
回答の選択肢を確認してみましょう。
* オプション A: リスク源は分離されています。
* これは正しくありません。 分離」は、FortiGate がソース デバイスがネットワークと通信するのを防ぐためにさらに手順を実行したことを意味します。このイベント ステータスには分離の兆候はありません。
* オプション B: セキュリティ リスクがブロックまたは削除されました。

* これは正解です。Web フィルタ イベント タイプとそれに付随する説明とともに、 軽減」ステータスは、FortiGate または FortiAnalyzer が疑わしい Web 要求を正常にブロックまたはドロップしたことを意味しており、 軽減」という用語に該当します。
* オプション C: セキュリティ イベントのリスクは未解決であると見なされます。
* これは誤りです。オープン ステータスは、何のアクションも実行されていないか、脅威がまだ存在していることを示します。 軽減済み」ステータスは、脅威が対処されたことを示します。
* オプション D: このイベントからインシデントが作成されました。
* このオプションは、表示されている内容から判断すると正しくないか明らかではありません。FortiAnalyzer または FortiGate は特定のイベントをインシデントにエスカレートできますが、ここでは示されていません。
参考文献:
* FortiOS 7.4.1 および FortiAnalyzer 7.4.1 のドキュメントでは、ログ内の 軽減」ステータスは、特に Web フィルタおよびセキュリティ ポリシー ログで、特定された脅威が通常、イベントに関連付けられたアクションをブロックまたはドロップすることによって処理されたことを意味すると規定されています。

最新問題: **17**
別添を参照:



21:20 のデータポイントは何を示していますか?

A. FortiAnalyzer は、ログの受信よりも速くログをインデックスしています。
B. fortilogd デーモンは 1 ログ分インデックスを先行しています。
C. 受信遅延が大きいため、SQL データベースを再構築する必要があります。
D. FortiAnalyzer は受信したログを一時的にバッファリングして、古いログを最初にインデックス化できるようにしています。
Answer: A (メーッセージを残す)
この図には、受信レートと挿入レートという 2 つのメトリックを時間の経過とともに追跡するグラフが表示されています。これら 2 つのレートは、FortiAnalyzer でのログ処理の動作を理解する上で非常に重要です。
* 受信レートと挿入レートを理解する:
* 受信速度: これは、FortiAnalyzer が接続されたデバイスからログを受信する速度です。
* 挿入レート: これは、FortiAnalyzer が保存および分析のためにログをデータベースにインデックス付け (挿入) するレートです。
* 21:20のデータポイント:
* 21:20 に、挿入レート ラインが受信レート ラインを上回っています。これは、FortiAnalyzer がログを受信するよりも速い速度でデータベースにログを挿入していることを示しています。この状況は、FortiAnalyzer が受信ログに対応できており、バックログまたは一時的に受信したログを新しいログの受信よりも速く処理している可能性があることを示しています。
* オプション分析:
* オプション A - FortiAnalyzer がログの受信よりも速くログをインデックス化している: これは、挿入レートが受信レートを超えている 21:20 のシナリオを正確に表しています。これは、FortiAnalyzer がその時点でログを効率的に処理しており、処理のバックログがないことを示しています。
* オプション B - fortilogd デーモンは 1 ログ分インデックス処理が先行しています: データは fortilogd デーモンのログ数に関する具体的な情報ではなく、レートのみを提供します。このオプションは正しくありません。
* オプション C - SQL データベースの再構築が必要: 受信ラグが大きい場合、受信ログとインデックス ログにバックログがあることを意味します。これは通常、受信レートが挿入レートを大幅に上回っている場合に発生しますが、この場合は当てはまりません。
* オプション D - FortiAnalyzer は古いログを最初にインデックスするためにログを一時的にバッファリングしています: このシナリオではバッファリングの兆候はありません。バッファリングは通常、受信レートが挿入レートよりも高い場合に発生し、インデックス作成の遅れのために FortiAnalyzer がログを一時的に保存していることを示します。
結論：
* 正解:A. FortiAnalyzer は、ログの受信よりも速くログをインデックス化します。
* 21:20 のグラフでは、受信レートよりも挿入レートが高く、FortiAnalyzer によるログ処理が効率的であることがわかります。
参考文献:

* ログ処理メトリック、受信レート、挿入レート インジケーターに関する FortiAnalyzer 7.4.1 ドキュメント。

最新問題: **18**
展示する。

表示されたイベントに関するどの記述が正しいですか?
A. リスク源は分離されています。
B. セキュリティ リスクはブロックまたはドロップされました。
C. セキュリティ イベントのリスクは未解決であると見なされます。
D. このイベントからインシデントが作成されました。
Answer: B (メーッセージを残す**)**
FortiOS および FortiAnalyzer ログ システムでは、イベントの [イベント ステータス] 列のステータスが 軽減」になっている場合、通常、システムが特定された脅威に対処するためのアクションを実行したことを示します。この場合、Web フィルターは疑わしい宛先への Web 要求をブロックし、イベント ステータス 軽減」は、セキュリティ リスクを中和またはブロックするためのアクションが正常に実行されたことを確認します。
回答の選択肢を確認してみましょう。
オプション A: リスク源は分離されています。
これは正しくありません。 分離」は、FortiGate がソース デバイスがネットワークと通信するのを防ぐためにさらに手順を実行したことを意味します。このイベント ステータスには分離の兆候はありません。
オプション B: セキュリティ リスクがブロックまたは削除されました。
これは正解です。Web フィルタ イベント タイプとそれに付随する説明とともに、 軽減」ステータスは、FortiGate または FortiAnalyzer が疑わしい Web 要求を正常にブロックまたはドロップしたことを意味しており、 軽減」という用語に該当します。オプション C: セキュリティ イベントのリスクは未解決であると見なされます。
これは正しくありません。オープン ステータスは、アクションが実行されなかったか、脅威がまだ存在していることを示します。 軽減済み」ステータスは、脅威が対処されたことを示します。
オプション D: このイベントからインシデントが作成されました。
このオプションは、表示されている内容から判断すると正しくないか、明らかではありません。FortiAnalyzer または FortiGate は特定のイベントをインシデントにエスカレートできますが、ここでは示されていません。
参照：
FortiOS 7.4.1 および FortiAnalyzer 7.4.1 のドキュメントでは、ログ内の 軽減」ステータスは、特に Web フィルタおよびセキュリティ ポリシー ログで、特定された脅威が通常、イベントに関連

付けられたアクションをブロックまたはドロップすることによって処理されたことを意味すると規定されています。

最新問題: **19**
FortiAnalyzer で RAID を使用する目的は何ですか?
A. ADOM間のデータ分離を提供する
B. ログをバックアップする
C. ログデータに冗長性を導入する
D. 分析データとアーカイブデータを分離する
Answer: C (メーッセージを残す**)**

最新問題: **20**
コマンド diagnose sql status sqlplugind を実行するのはなぜですか?
A. 現在のhcacheサイズを表示する
B. SOLクエリ接続とhcacheステータスを表示します
C. データベースログの挿入ステータスを確認する
D. 現在実行中のSQLプロセスを一覧表示する
Answer: (解答を表示する**)**

最新問題: **21**
プレイブックには合計 5 つのタスクが含まれています。管理者がプレイブックを実行すると、5 つのタスクのうち 4 つは正常に完了しましたが、1 つのタスクは失敗しました。
プレイブックを実行した後のステータスはどうなりますか?
A. 注意が必要
B. アップストリームが失敗しました
C. 失敗
D. 成功
Answer: (解答を表示する**)**
FortiAnalyzer では、プレイブックが実行されると、各タスクのステータスがプレイブック全体のステータスに影響します。タスクの結果に基づいて次のことが起こります。
* すべてのタスクが成功したときのステータス:
* すべてのタスクが正常に完了すると、プレイブックのステータスは 成功」とマークされます。
* 一部のタスクが失敗した場合のステータス:
* プレイブック内の 1 つ以上のタスクが失敗し、他のタスクが成功した場合、プレイブックのステータスは通常、 注意が必要」に変わります。このステータスは、プレイブックの実行は完了したが、1 つ以上のタスクが失敗したため確認が必要であることを示します。
* これは、上流のタスクが依存していることが多い初期のタスクでの重大なエラーのためにプレイブックを続行できない場合に使用される completeFailedstatus とは異なります。
* オプション分析:

* A. 注意が必要: プレイブックは完了しましたが、部分的に成功しており、レビューが必要なタスクがあるため、これは正解です。
* B. Upstream_failed: このステータスは、前提条件または 「上流」タスクが失敗したためにタスクを実行できない場合に使用されます。5 つのタスクのうち 4 つが完了したため、この場合は当てはまりません。
* C. 失敗: このステータスは、プレイブックが完全に失敗したことを意味し、5 つのタスクのうち 1 つだけが失敗したシナリオとは一致しません。
* D. 成功: すべてのタスクが正常に完了した場合、このステータスが適用されますが、この場合は当てはまりません。
結論：
* 正解:A. 注意が必要
* プレイブックのステータスは完了したことを表していますが、タスクの 1 つでエラーが発生したため、管理者は失敗したタスクを確認するよう求められます。
参考文献:
* プレイブックの実行ステータスとタスク エラー処理に関する FortiAnalyzer 7.4.1 のドキュメント。

最新問題**: 22**
CLI コマンド # diagnose test application oftpd 3 は、何を判断するのに役立ちますか?
A. FortiAnalyzer に届くログ（ある場合）
B. 登録されているデバイスと登録されていないデバイス
C. 有効化および設定されているADOM
D. FortiAnalyzerに接続しているデバイスとIPアドレス
Answer: (解答を表示する**)**

最新問題**: 23**
プレイブックの実行が失敗したとみなされるのはいつですか?
A. すべてのタスクが失敗した場合
B. プレイブックが別のADOMからインポートされた場合
C. 少なくとも1つのタスクが失敗した場合
D. プレイブックが無効になっている場合
Answer: C (メーッセージを残す**)**

最新問題**: 24**
FortiAnalyzer でデータベースにクエリを実行する場合、どの SQL クエリが正しい順序ですか?
A. $log から devid を選択し、GROUP BY devid WHERE 'user',,' users1' を指定します。
B. $log から devid 'user',, USER1' を選択し、devid によってグループ化します。
C. SELECT devid WHERE 'user'-' USER1' FROM $log GROUP By devid
D. $log から devid を選択し、'user'=' GROUP BY devid を実行します。
Answer: D (メーッセージを残す**)**

FortiAnalyzer の SQL クエリ構文では、データベースをクエリする一般的な順序は次の標準 SQL 形式に従います。
SELECT <列> FROM <テーブル> WHERE <条件> GROUP BY <列>
* オプション D は、次の構造に正しく従います。
* SELECT devid FROM $log: これは、クエリが $log テーブルから devid 列を選択することを指定します。
* WHERE 'user' = ': クエリのこの部分は、ユーザー列に関連する条件に基づいて結果をフィルター処理することを目的としています。軽微な入力ミスがあるように見えますが (= の後のユーザー値が欠落している可能性があります)、構造的には正しい SQL 順序に準拠しています。
* GROUP BY devid: クエリの最後に正しく配置されている devid ごとに結果をグループ化します。
他の選択肢がなぜ間違っているのか簡単に調べてみましょう。
* オプション A: SELECT devid FROM $log GROUP BY devid WHERE 'user', 'users1'
* これは誤りです。GROUP BY 句が WHERE 句の前に出現し、SQL 構文の順序が正しくないためです。
* オプション B: SELECT FROM $log WHERE devid 'user', USER1' GROUP BY devid
* これは、SELECT ステートメントに列がなく、WHERE 句の構文が不正であるため、正しくありません。
* オプション C: SELECT DEVID WHERE 'user' - 'USER1' FROM $log GROUP BY DEVID
* SELECT キーワードが SELCT と誤って入力されており、WHERE 条件の構文が無効であるため、これは誤りです。
参考資料: FortiAnalyzer の SQL クエリに関するドキュメントでは、FortiAnalyzer でログをクエリするときに標準の SQL 順序に従う必要があることが示されています。クエリは SELECT ... FROM ... という形式に従う必要があります。
オプション D に示されているように、WHERE ... GROUP BY ... を使用します。

最新問題**: 25**
FortiAnalyzer は、どのような目的で SSL 経由の最適化ファブリック転送プロトコル (OFTP) を使用しますか?
A. ログをSFTPサーバーにアップロードする
B. デバイス間のログ通信を暗号化する
C. 同一のログセットを2番目のログサーバーに送信する
D. バックアップ中にログが変更されないようにする
Answer: B (メーッセージを残す**)**

最新問題**: 26**
不正な管理者が許可なく FortiAnalyzer にアクセスしており、その不正な管理者が FortiAnalyzer でどのようなアクティビティを実行したかを確認することが求められています。
これを実現するために FortiAnalyzer で何ができるでしょうか?
A. FortiView をクリックして、その管理者のレポートを生成します。

B. タスク モニターをクリックし、その管理者が実行したタスクを表示します。
C. [ログ表示] をクリックして、その管理者のレポートを生成します。
D. [ファブリック ビュー] をクリックし、不正な管理者によって実行されたタスクを表示します。
Answer: (解答を表示する**)**

最新問題**: 27**
フィルタリングされた検索結果に基づいてデータセットとグラフを自動的に構築するために使用できる FortiView ツールは何ですか?
A. データセットライブラリ
B. カスタムビュー
C. チャートビルダー
D. レポートチャートにエクスポート
Answer: D (メーッセージを残す**)**

最新問題**: 28**
FortiAnalyzer のオフライン ログとは何ですか?
A. FortiAnalyzer を再起動すると、保存されているすべてのログはオフライン ログと見なされます。
B. インデックスが作成され、SQL データベースに保存されるログ。
C. 圧縮ログ (アーカイブ ログとも呼ばれます) は、オフライン ログと見なされます。
D. 起動後にオフラインデバイスから収集されたログ。
Answer: (解答を表示する**)**

最新問題**: 29**
FortiAnalyzer のアーカイブ ログについて説明している文はどれですか。
A. FortiAnalyzer管理者がFortiViewでアクセスできるログ
B. ログは圧縮され、.gz拡張子のファイルに保存されます
C. SQLデータベースにインデックス付けされ保存されるログ
D. オフラインのデバイスから以前に収集されたログ
Answer: (解答を表示する**)**

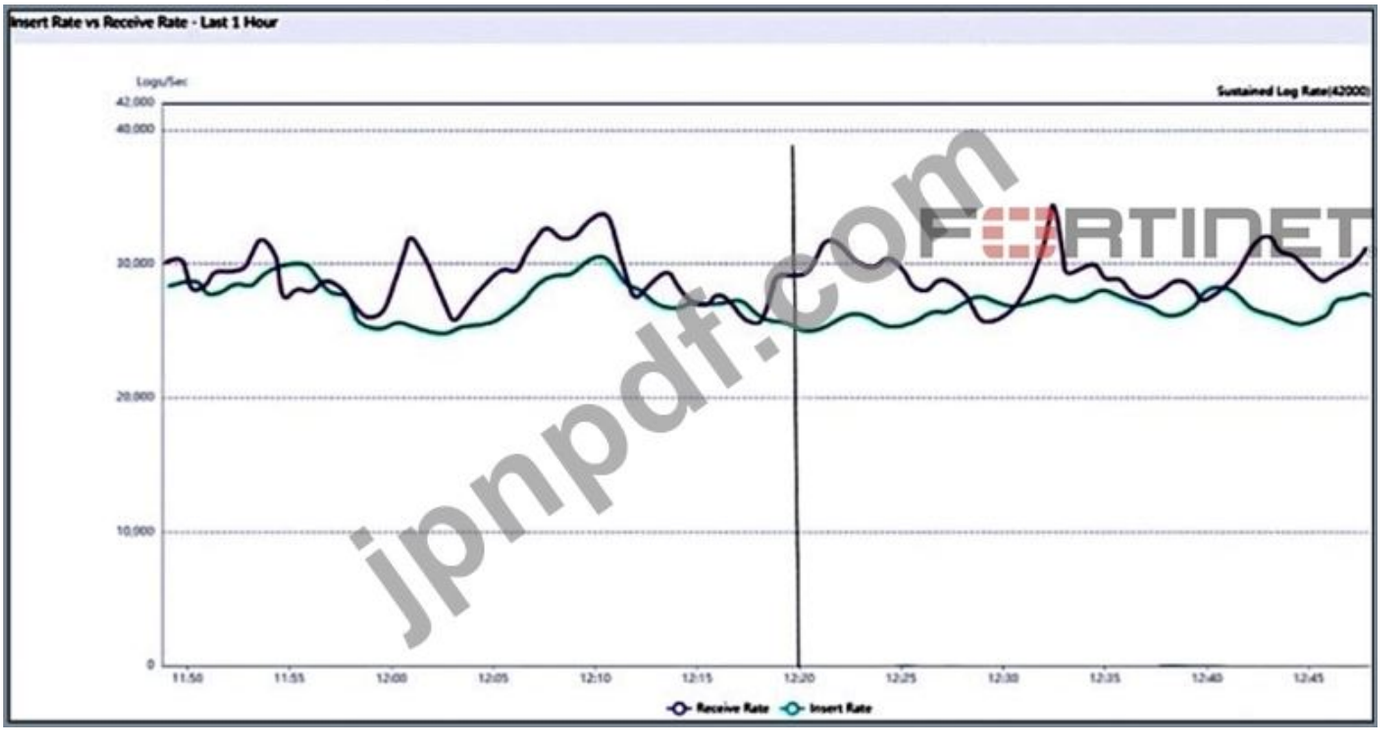
最新問題**: 30**
FortiAnlyzer でインシデントを管理する場合、アナリストは何に注意する必要がありますか?
A. 生成されたレポートを手動でインシデントに添付できます。
B. インシデントのステータスは常にアタッチ イベントのステータスにリンクされます。
C. 重大度レベルが 高」と評価されたインシデントの初期サービス レベル アグリーメント (SLA) 応答時間は 1 時間です。
D. インシデントを分析する前に確認する必要があります。
Answer: A (メーッセージを残す**)**

FortiAnalyzer のインシデント管理システムでは、アナリストは手動でインシデントを管理するオプションがあり、これには、さらなる調査と文書化のためにインシデントに関連レポートを添付することが含まれます。この機能により、アナリストは疑わしいアクティビティに関する詳細なレポートなどの情報をインシデント レコードに統合し、インシデント対応のための包括的なビューを提供できます。
他のオプションを確認して、なぜ間違っているのかを明らかにしましょう。
* オプションA: 生成されたレポートを手動でインシデントに添付できます
* 正解です。FortiAnalyzer を使用すると、アナリストは手動でレポートをインシデントに添付できます。これは、インシデントに関連する追加のコンテキスト、証拠、または分析を提供するのに役立ちます。この機能はインシデント管理プロセスの一部であり、追跡と解決のための情報を合理化するのに役立ちます。
* オプションB: インシデントのステータスは常に添付イベントのステータスにリンクされます
* これは誤りです。FortiAnalyzer 上のインシデントのステータスは、添付されたイベントのステータスとは独立して管理されます。インシデントには、それぞれステータスが異なる複数のイベントを含めることができますが、インシデント自体は個別に追跡されます。
* オプションC: 重大度レベルが 「高」と評価されたインシデントの初期サービスレベル契約 (SLA) 応答時間は 1 時間です。
* これは誤りです。インシデントには重大度レベルがありますが、特定の SLA 応答時間は通常、組織のインシデント対応ポリシーに従って設定され、FortiAnalyzer は重大度の高いインシデントに対して 1 時間のデフォルトの SLA 応答時間を課しません。
* オプションD: インシデントを分析する前に認識する必要がある
* これは誤りです。FortiAnalyzer のインシデントは、まだ確認されていない場合でも分析できます。インシデントを確認することは、アクティブに対処されているものとしてマークするためのワークフローの一部であることがよくありますが、分析の前提条件ではありません。
参考資料: FortiAnalyzer のドキュメントによると、アナリストはインシデントにレポートを手動で添付できるため、オプション A が正解です。この機能により、FortiAnalyzer のインシデント管理システム内での追跡と文書化が向上します。

最新問題**: 31**
2 つの ADOM 間でレポートを移動する必要があります。
正しい記述はどれですか? (2 つ選択してください。)
A. レポートに関連付けられているすべてのグラフとデータセットが一緒にインポートされます。
B. 最初にレポートをテンプレートに変換する必要があります。
C. 競合を避けるために、データと時刻は元のレポート名に割り当てられます。
D. ADOM は互換性のある型である必要があります。
Answer: A,D (メーッセージを残す**)**

最新問題: **32**
FortiAnalyzer の HA の初期ログ同期とログ データ同期に関係なく、正しい 2 つのステートメントはどれですか。
A. デフォルトでは、ログ データ同期はすべてのバックアップ デバイスで無効になっています。
B. ログ データ同期がオンになっている場合、バックアップ デバイスは再起動し、同期されたログを使用してログ データベースを再構築します。
C. ログ データ 同期は、すべてのバックアップ デバイスへのリアルタイムのログ同期を提供します。
D. 初期ログ同期では、ユニットを HA クラスターに追加すると、プライマリ デバイスはログをバックアップ デバイスと同期します。
Answer: (解答を表示する)

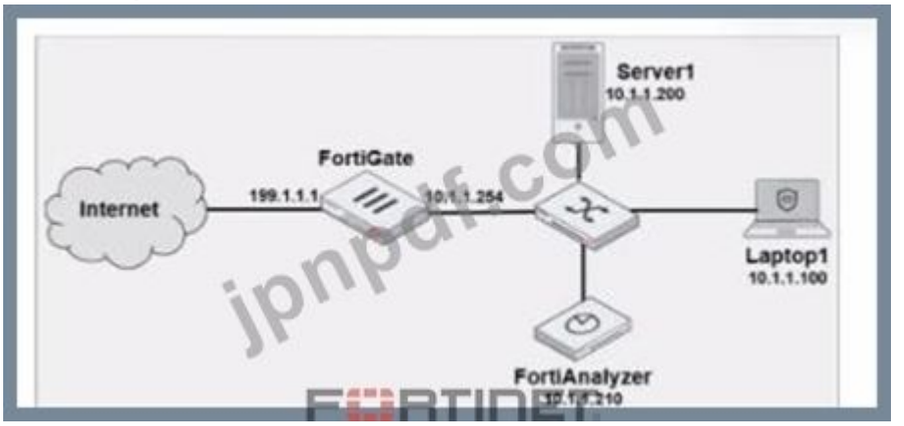
最新問題: **33**
展示品を参照してください。



12:20 のデータポイントは何を示していますか?
A. sqlplugind サービスが新しいログに追いつきました。
B. FortiAnalyzer のパフォーマンスがベースラインを下回っています。

C. ログ挿入の遅延時間が増加しています。
D. FortiAnalyzer はログの削除を回避するためにキャッシュを使用しています。
Answer: C (メーッセージを残す**)**

最新問題**: 34**
展示する。



Laptop1 は、複数の管理者が FotiAnalyzer を管理するために使用します。管理者以外のユーザーによって生成され、Laptop1 から送信される Web インターフェイスへのすべてのログイン試行に一致する汎用テキスト フィルターを構成する必要があります。
どのフィルターが望ましい結果を達成しますか?
A. 操作 - ログイン、実行先 == "GUI(10.1.1.100)'、ユーザー = admin
B. 操作ログイン、実行先=="GU(10.1.1.120)'、ユーザー!=admin
C. 操作ログイン、srcip== 10.1.1.100、dstip==10.1.1.1.210、user==admin
D. 操作-ログイン、dstip==10.1.1.210、ユーザー!-admin
Answer: A (メーッセージを残す**)**
目的は、Laptop1 (IP 10.1.1.100) からの FortiAnalyzer Web インターフェイス (GUI) へのすべてのログイン試行を識別し、管理者ユーザーを除外するフィルターを作成することです。このフィルターは、管理者以外のすべてのユーザーに一致する必要があります。
* フィルターコンポーネント分析:
* Operation-login: フィルターのこの部分はログイン アクションを具体的にターゲットとし、ログイン試行のフィルター処理に適しています。
* performed_on=="GUI(10.1.1.100)': これは、ログイン試行が GUI インターフェイス上で行われ、ラップトップ 1 の IP アドレス (10.1.1.100) と一致する指定された IP から発信される必要があることを示します。これにより、フィルターはこの特定のデバイスからの GUI ログインのみに一致するようになります。
* user!=admin: この部分では、管理者ユーザーによるログインが除外され、管理者以外のユーザーのみをキャプチャするという要件が満たされます。
* オプション分析:
* オプション A: Operation-login、performed_on=="GUI(10.1.1.100)'、および user!=admin を正しく指定します。この設定により、管理者ユーザーを除いて、Laptop1 からの GUI へのログイン試行が効果的にフィルタリングされます。

* オプション B: performed_on フィルターで誤った IP 10.1.1.120 を使用しますが、これは Laptop1 の IP (10.1.1.100) と一致しません。
* オプション C: このオプションには srcip==10.1.1.100 と dstip==10.1.1.210 が含まれますが、user!=admin ではなく user==admin が誤って指定されているため、管理者ユーザーを除外するという要件に一致しません。
* オプション D: このオプションでは、GUI に制限するために、performed_onfield を指定せず、srcip なしの dstip(宛先 IP) のみが含まれます。また、正しい構文 user!=admin の代わりに、誤って user!-admin を使用します。
結論：
* 正解:A. 操作ログイン、実行先=="GUI(10.1.1.100)'、ユーザー!=admin
* このフィルターは、必要な条件（管理者以外のユーザーによるラップトップ 1 から GUI インターフェイスへのログイン試行）を正確にキャプチャします。
参考文献:
* ログ フィルター、ログイン操作の構文、GUI ログイン追跡に関する FortiAnalyzer 7.4.1 のドキュメント。

最新問題: **35**
FortiAnalyzer とそのすべての登録済みデバイスで NTP サーバーを使用する主な目的は何ですか?
A. リアルタイム転送
B. ログ相関
C. ホスト名解決
D. ログ収集
Answer: B (メーッセージを残す**)**

最新問題: **36**
コマンド diagnose sql status sqlreportd を実行する目的は何ですか?
A. スケジュールされたレポートのリストを表示するには
B. 現在実行中のSQLプロセスを一覧表示する
C. SQLクエリ接続とhcacheステータスを表示する
D. データベースログの挿入ステータスを識別する
Answer: (解答を表示する**)**
FortiAnalyzer では、コマンド diagnose sql status sqlreportd を使用して、SQL レポート プロセスとキャッシュ ステータスに関する特定の情報を取得します。このコマンドの実行内容と各オプションの分析は次のとおりです。
コマンド機能:
sqlreportd は、SQL ベースのレポート プロセスの管理を担当する FortiAnalyzer デーモンです。diagnose sql status sqlreportd コマンドは、アクティブな SQL クエリ接続と hcache (履歴キャッシュ) ステータスに関する情報を提供します。これは、SQL レポート生成の監視とトラブルシューティングに役立ちます。

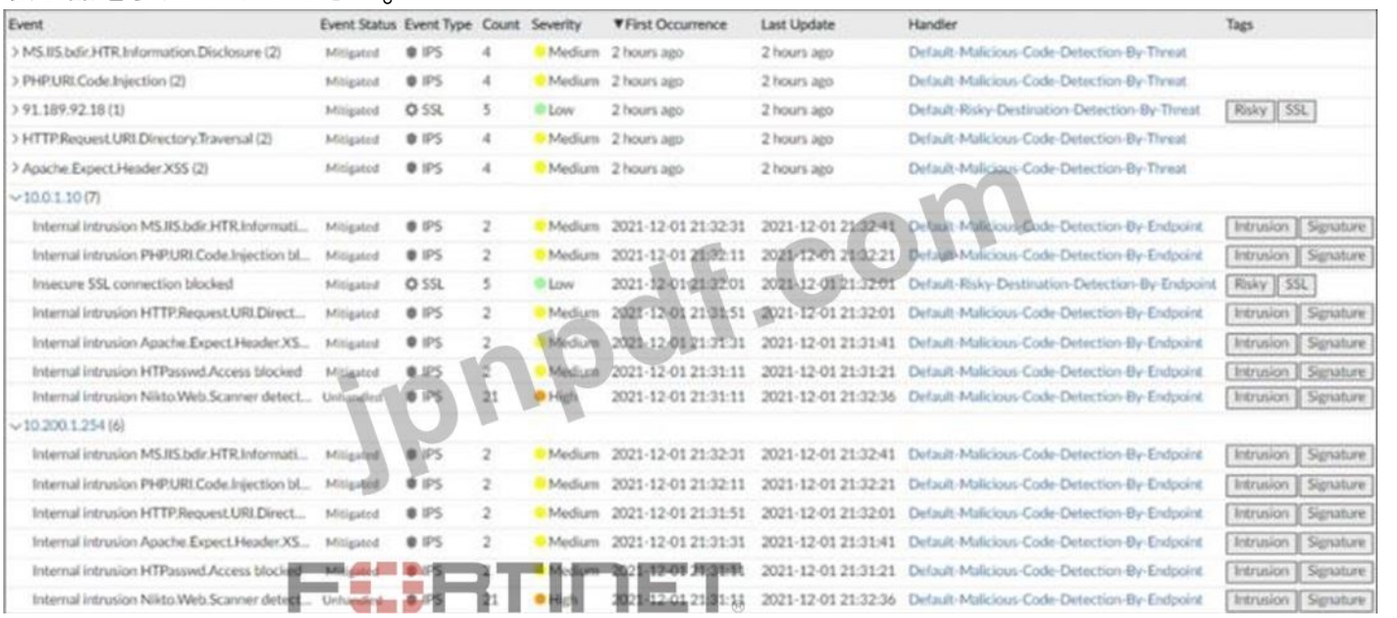
オプション分析:
オプション A - スケジュールされたレポートのリストを表示するには:
このオプションは、スケジュールされたレポートをリストしないため、正しくありません。代わりに、SQL レポート プロセスとキャッシュの詳細に重点が置かれます。
オプション B - 現在実行中の SQL プロセスを一覧表示するには:
このコマンドはアクティブな SQL 接続を表示することがありますが、主な焦点はすべての SQL プロセスの詳細なリストではなく、レポート用の接続とキャッシュ ステータスです。
オプション C - SQL クエリ接続と hcache ステータスを表示するには:
これは正解です。このコマンドは、レポート プロセス (sqlreportd) に関連する SQL クエリ接続に関する情報を具体的に提供し、hcache ステータスを表示します。
オプション D - データベース ログ挿入ステータスを識別するには:
これは正しくありません。このコマンドは、ログ挿入ステータスの詳細を提供しません。ログ挿入ステータスは通常、データベース プロセスとログ処理に重点を置いたさまざまな診断コマンドを通じて監視されます。
結論：
正解: C. SQL クエリ接続と hcache ステータスを表示します。このコマンドは、SQL レポート アクティビティとキャッシュ ステータスを監視するために使用され、レポート生成パフォーマンスと接続の健全性の分析に役立ちます。
参照：
FortiAnalyzer 7.4.1 の SQL 診断コマンドに関するドキュメント。特に、レポート (sqlreportd) とキャッシュ メカニズムに関連するコマンドです。

最新問題**: 37**
レポートの自動キャッシュ設定の目的はどれですか? (2 つ選択してください。)
A. レポート生成時間を短縮します。
B. ログ挿入の遅延率を削減します。
C. 新しいログが到着すると、hcache が自動的に更新されます。
D. レポート生成時間に関する診断を提供します。
Answer: A,C (メーッセージを残す**)**

最新問題**: 38**
ログ取得を使用する場合、何を考慮する必要がありますか? (2 つ選択してください。)
A. フェッチ クライアントは、ローカル デバイス マネージャーに追加されていないデバイスからログを取得できます。
B. 取得プロファイルには、Super_User プロファイルを持つユーザーが含まれている必要があります。
C. サーバーから取得されたアーカイブ ログは、クライアントのアーカイブ ログになります。
D. フィルターを使用して、単一のデバイスからのログのみを含めることができます。
Answer: A,D (メーッセージを残す**)**

最新問題: **39**

展示品を参照してください。



Event	Event Status	Event Type	Count	Severity	▼First Occurrence	Last Update	Handler	Tags
> MS.IIS.bdir.HTR.Information.Disclosure (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> PHP.URI.Code.Injection (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> 91.189.92.18 (1)	Mitigated	SSL	5	Low	2 hours ago	2 hours ago	Default-Risky-Destination-Detection-By-Threat	Risky SSL
> HTTP.Request.URI.Directory.Traversal (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> Apache.Expect.Header.XSS (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
10.0.1.10 (7)								
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Insecure SSL connection blocked	Mitigated	SSL	5	Low	2021-12-01 21:32:01	2021-12-01 21:32:01	Default-Risky-Destination-Detection-By-Endpoint	Risky SSL
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTPasswd.Access blocked	Mitigated	IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner detect...	Unhandled	IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
10.200.1.254 (6)								
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTPasswd.Access blocked	Mitigated	IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner detect...	Unhandled	IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature

このプレイブックを実行した後に作成されたインシデントに追加されるイベントの数はいくつですか?

A. 5つのイベントが追加されます。

B. イベントが 10 件追加されます。

C. イベントは追加されません。

D. 13 個のイベントが追加されます。

Answer: (解答を表示する**)**

最新問題: **40**

FortiAnalyzer と FortiGate 間の 保存とアップロード」ログ転送オプションに関して正しい記述はどれですか? (3 つ選択してください。)

A. すべての FortiGate は、保存およびアップロード オプションを使用して FortiAnalyzer にログを送信できます。

B. ハードディスクを搭載した FortiGate モデルのみが、保存およびアップロード オプションを使用して FortiAnalyzer にログを送信できます。

C. FortiGate では、ディスク ログ記録がデフォルトで有効になっています。

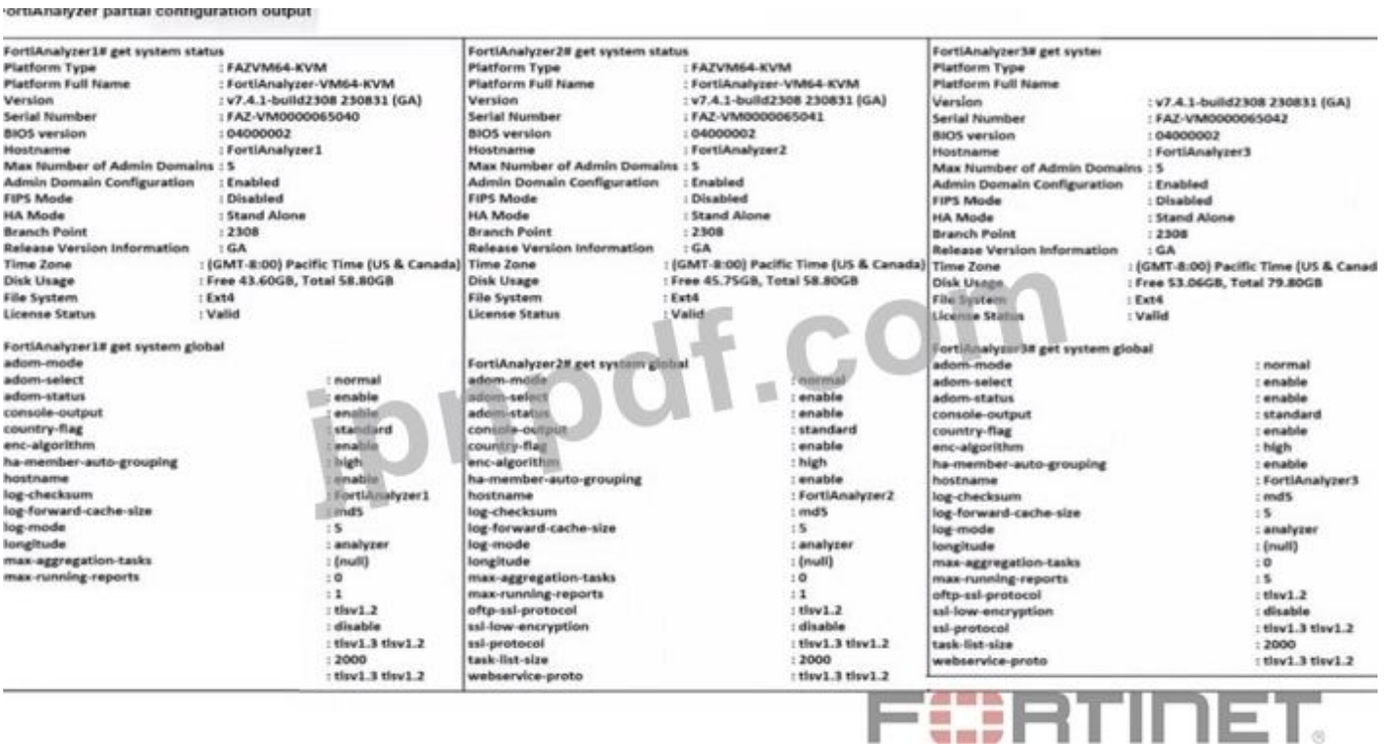
D. ディスク ログは、FortiGate で CLI 経由でのみ有効になります。

E. 両方の安全な通信方法 (SSL と IPsec) で、保存およびアップロード オプションが許可されます。

Answer: B,D,E (メーッセージを残す**)**

最新問題: **41**

展示する。


FortiAnalyzer partial configuration output

FortiAnalyzer1# get system status
Platform Type : FAZVM64-KVM
Platform Full Name : FortiAnalyzer-VM64-KVM
Version : v7.4.1-build2308 230831 (GA)
Serial Number : FAZ-VM0000065040
BIOS version : 04000002
Hostname : FortiAnalyzer1
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Time Zone : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage : Free 43.60GB, Total 58.80GB
File System : Ext4
License Status : Valid

FortiAnalyzer1# get system global
adom-mode : normal
adom-select : enable
adom-status : enable
console-output : standard
country-flag : enable
enc-algorithm : high
ha-member-auto-grouping : enable
hostname : FortiAnalyzer1
log-checksum : md5
log-forward-cache-size : 5
log-mode : analyzer
longitude : (null)
max-aggregation-tasks : 0
max-running-reports : 1
oftp-ssl-protocol : tlsv1.2
ssl-low-encryption : disable
ssl-protocol : tlsv1.3 tlsv1.2
task-list-size : 2000
webservice-proto : tlsv1.3 tlsv1.2

FortiAnalyzer2# get system status
Platform Type : FAZVM64-KVM
Platform Full Name : FortiAnalyzer-VM64-KVM
Version : v7.4.1-build2308 230831 (GA)
Serial Number : FAZ-VM0000065041
BIOS version : 04000002
Hostname : FortiAnalyzer2
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Time Zone : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage : Free 45.75GB, Total 58.80GB
File System : Ext4
License Status : Valid

FortiAnalyzer2# get system global
adom-mode : normal
adom-select : enable
adom-status : enable
console-output : standard
country-flag : enable
enc-algorithm : high
ha-member-auto-grouping : enable
hostname : FortiAnalyzer2
log-checksum : md5
log-forward-cache-size : 5
log-mode : analyzer
longitude : (null)
max-aggregation-tasks : 0
max-running-reports : 1
oftp-ssl-protocol : tlsv1.2
ssl-low-encryption : disable
ssl-protocol : tlsv1.3 tlsv1.2
task-list-size : 2000
webservice-proto : tlsv1.3 tlsv1.2

FortiAnalyzer3# get system
Platform Type
Platform Full Name
Version : v7.4.1-build2308 230831 (GA)
Serial Number : FAZ-VM0000065042
BIOS version : 04000002
Hostname : FortiAnalyzer3
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Time Zone : (GMT-8:00) Pacific Time (US & Canad
Disk Usage : Free 53.06GB, Total 79.80GB
File System : Ext4
License Status : Valid

FortiAnalyzer3# get system global
adom-mode : normal
adom-select : enable
adom-status : enable
console-output : standard
country-flag : enable
enc-algorithm : high
ha-member-auto-grouping : enable
hostname : FortiAnalyzer3
log-checksum : md5
log-forward-cache-size : 5
log-mode : analyzer
longitude : (null)
max-aggregation-tasks : 0
max-running-reports : 5
oftp-ssl-protocol : tlsv1.2
ssl-low-encryption : disable
ssl-protocol : tlsv1.3 tlsv1.2
task-list-size : 2000
webservice-proto : tlsv1.3 tlsv1.2

表示された部分的な出力に基づいて、どのデバイスが FotiAnalyzer Fabric のメンバーになることができますか?

A. FortiAnalayzer1 および FortiAnalyzer3

B. FortiAnalyzer1 および FortiAnalyzer2

C. FortiAnalyzer2 および FortiAnalyzer3

D. リストされているすべてのデバイスがメンバーになることができます。

Answer: D (メーッセージを残す)

FortiAnalyzer Fabric では、デバイスが特定の互換性基準を満たしていれば、クラスターまたはグループに参加できます。提供された出力に基づいて、これらの基準を評価してみましょう。

FortiAnalyzer1、FortiAnalyzer2、FortiAnalyzer3 の 3 つのデバイスはすべてバージョン v7.4.1-build0238 を実行しており、これは全体的に同じです。FortiAnalyzer Fabric では、シームレスな通信と管理のためにデバイスが互換性のあるファームウェア バージョンを実行する必要があるため、このバージョンの調整は非常に重要です。

プラットフォームの種類と構成:

3 つのデバイスはすべて HA モードでスタンドアロンとして構成されており、独立して動作できますが、FortiAnalyzer ファブリックへの参加は制限されません。各デバイスは FAZVM64-KVM プラットフォーム タイプ上にあり、ハードウェアの互換性が確保されています。

グローバル設定:

adm-mode、adm-status、adom-mode などの主要な設定はすべてのデバイス間で一貫しており (adm-mode: normal、adm-status: enable、adom-mode: normal)、ファブリック統合とロール割り当ての柔軟性の要件と一致しています。

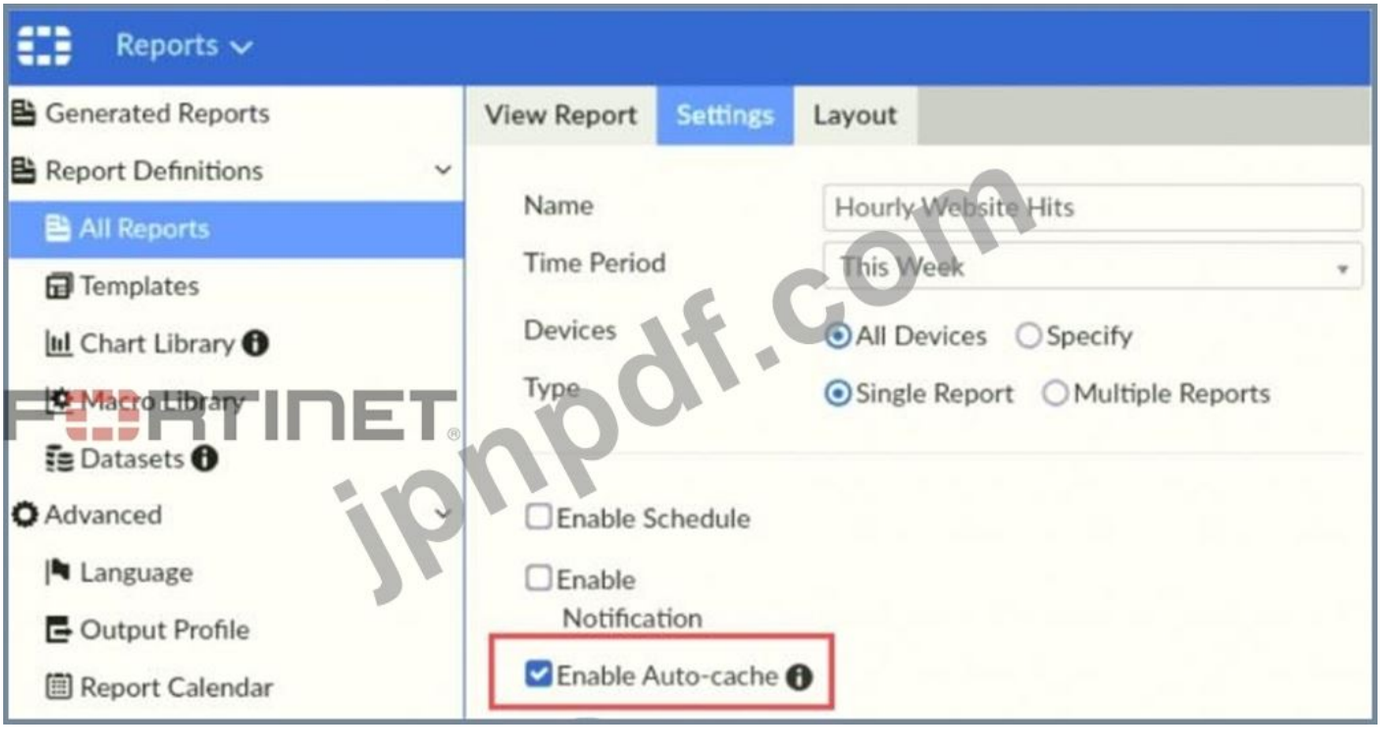
各デバイスには、ファブリック環境内でログを転送するのに関連する log-forward-cache-size セットもあります。

上記の分析に基づくと、すべてのデバイス (FortiAnalyzer1、FortiAnalyzer2、および FortiAnalyzer3) は、FortiAnalyzer ファブリックの一部となるための要件を満たしています。

最新問題: **42**
特定の期間に一致するアーカイブ ログを別の FortiAnalyzer デバイスから取得できる FortiAnalyzer 機能はどれですか。
A. ログ転送集約モード
B. ログアップロード
C. ログ取得
D. 侵害の兆候
Answer: C (メーッセージを残す**)**

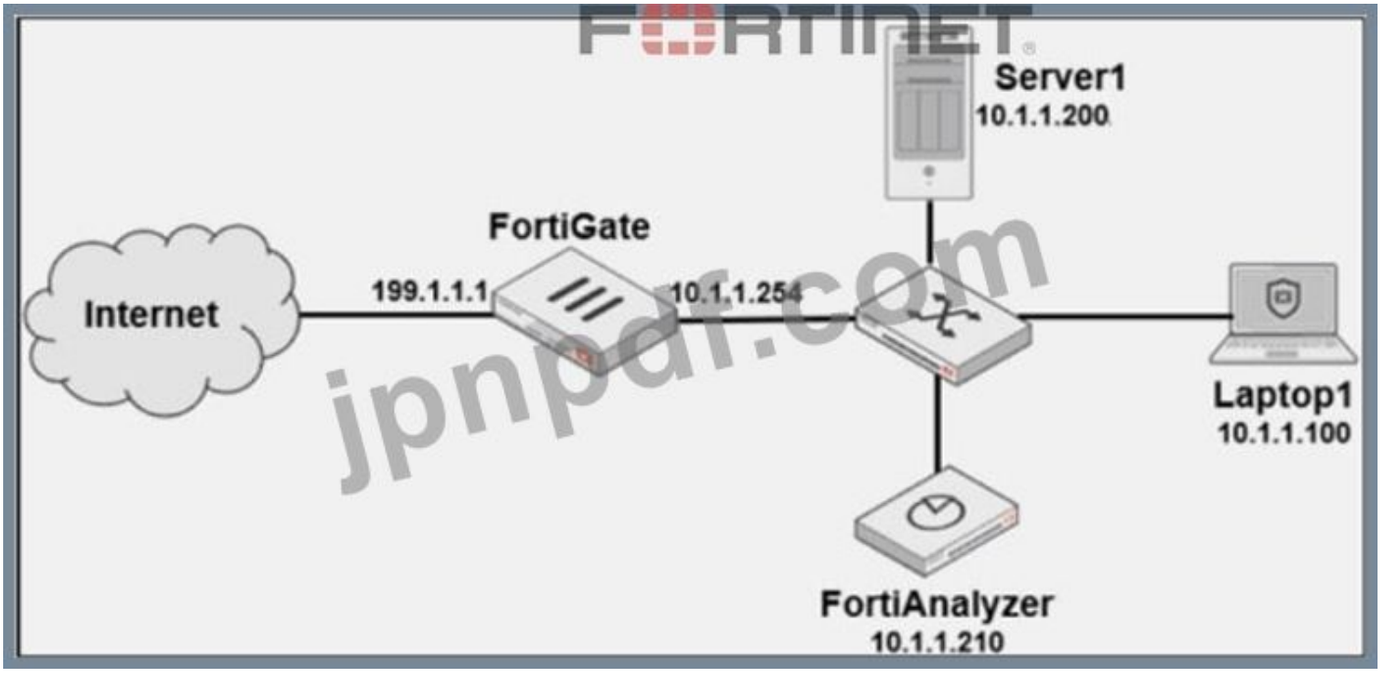
最新問題: **43**
FortiAnalyzer VM のディスク領域を拡張するための推奨方法は何ですか?
A. VMホストマネージャから、既存の仮想ディスクのサイズを拡張します
B. VMホストマネージャから追加の仮想ディスクを追加し、#execute lvm extend <ディスク番号> コマンドを使用してストレージを拡張します。
C. VMホストマネージャから、既存の仮想ディスクのサイズを拡張し、# execute format diskコマンドを使用してディスクを再フォーマットします。
D. VMホストマネージャから、追加の仮想ディスクを追加し、RAIDアレイを再構築します。
Answer: B (メーッセージを残す**)**

最新問題: **44**
展示品を参照してください。



FortiAnalyzer で自動キャッシュを有効にすることに関して正しい記述はどれですか? (2 つ選択してください。)
A. FortiAnalyzer のディスク領域を節約するためにレポート サイズが最適化されます。
B. 自動キャッシュを有効にすると、データセットの組み立てに長い時間を要するレポートの生成時間が短縮されます。
C. レポートはメモリにキャッシュされます。
D. この機能は、スケジュールされたレポートに対して自動的に有効になります。
Answer: (解答を表示する)

最新問題: **45**
展示品を参照してください。



Laptop1 は、FortiAnalyzer を管理するために複数の管理者によって使用されます。「admin」以外のユーザーによって生成され、Laptop1 から送信される Web インターフェイスへのすべてのログイン試行に一致する汎用テキスト フィルターを構成する必要があります。
どのフィルターが望ましい結果を達成しますか?
A. 操作ログイン & 実行先=="GUI(10.1.1.100)" & ユーザー!=admin
B. オペレーションログイン & srcip==10.1.1.100 & dstip==10.1.1.210 & ユーザー==admin
C. 操作ログイン & 実行先=="GUI(10.1.1.210)' & ユーザー!=admin
D. オペレーションログイン & dstip==10.1.1.210 & ユーザーl-admin
Answer: (解答を表示する)

最新問題: **46**
FortiAnalyzer でデータベースをクエリする場合、どの SQL クエリが正しい順序ですか?
A. $log から devid を選択し、GROUP BY devid で 'user'='USER1' を指定します。
B. $log から devid を選択し、'user'='USER1' を GROUP BY devid でグループ化します。
C. $log から 'user'='USER1' を選択し、devid で GROUP BY devid を実行します。

D. SELECT devid WHERE 'user'='USER1' FROM $log GROUP BY devid
Answer: B (メーッセージを残す**)**

最新問題**: 47**
IPsec を使用して FortiAnalyzer と FortiGate 間の通信を保護することに関して正しい記述はどれですか? (2 つ選択してください。)
A. IPsec は FortiAnalyzer の CLI を通じてのみ有効化されます。
B. SSL も有効になっている場合は、IPsec を有効にできません。
C. IPsec トンネル ID と事前共有キーを確立する必要があります。
D. トンネルの FortiAnalyzer 側のみを設定する必要があります。FortiGate 側は自動的にネゴシエートされます。
Answer: C,D (メーッセージを残す**)**

最新問題**: 48**
管理者が FortiAnalyzer デバイスに FortiClient EMS を登録できません。
この失敗の原因は何でしょうか?
A. FortiClient EMS デバイスを登録するには、ADOM モードを詳細に設定する必要があります。
B. FortiClient EMS デバイスを登録するには、FortiAnalyzer に別のライセンスが必要です。
C. FortiAnalyzer では ADOM が有効になっていません。
D. FortiAnalyzer は HA クラスター内にあります。
Answer: C (メーッセージを残す**)**

最新問題**: 49**
FortiAnalyzer のローカル ログをリモート サーバーにアップロードするのがベスト プラクティスです。
アップロードにサポートされているリモート サーバーは 3 つありますか? (3 つ選択してください。)
A. SFTP
B. FTP
C. SCP
D. TCP

E. UDP
Answer: A,B,C (メーッセージを残す**)**

最新問題**: 50**
FortiAnalyzer はどのようにしてデータベースから特定のログ データを取得しますか?
A. SQL EXTRACT ステートメント
B. SQL FROM ステートメント
C. SQL GET ステートメント
D. SQL SELECT ステートメント
Answer: D (メーッセージを残す**)**

最新問題**: 51**
アナリストとしての役割の一環として、同じパラメータを使用してログ ビューを頻繁に検索していることがわかります。
検索フィルターを繰り返し定義する代わりに、時間を節約するにはどうすればよいでしょうか?
Answer:
B. カスタムビューを構成します。
カスタム ビューを使用すると、特定の検索フィルターを保存して、ログ ビューで頻繁に使用するパラメーターにすばやくアクセスできます。
参照：
ログ検索用のカスタム ビューの作成と使用に関する FortiAnalyzer 7.4.1 ドキュメント。

最新問題**: 52**
FortiAnalyzer ファームウェアをアップグレードする必要があります。
FortiAnalyzer が一時的に利用できない間、FortiGate から FortiAnalyzer に送信されるログはどうなりますか?
A. FortiGateはmiglogdプロセスを使用してログをキャッシュします
B. ログがドロップされます
C. ログファイルプロセスはオフラインモードでログを保存します
D. FortiAnalyzerはオンラインに戻ったときにログフェッチを使用してログを取得します
Answer: A (メーッセージを残す**)**

最新問題**: 53**
FortiAnalyzer 管理者のログオンを検証するために設定できるリモート認証サーバーはどれですか? (3 つ選択してください)
A. LDAP
B. 半径
C. ローカル
D. TACACS+
E. PKI

Answer: (解答を表示する**)**