Fortinet.NSE5_FSM-6.3.v2025-01-31.q40

試験コード:	NSE5_FSM-6.3
試験名称:	Fortinet NSE 5 - FortiSIEM 6.3
認定資格:	Fortinet
無料問題数:	40
バージョン:	v2025-01-31
アクセス数:	340
ページビュー数:	400
https://www.jpnpdf.com/Fortinet.NSE5_FSM-6.3.v2025-01-31.q40-mondaishu.html	

最新問題: **1**
FortiSIEM管理者は、Microsoft WindowsサーバーからSIEMイベントログとパフォーマンスおよび可用性メトリック (PAM) イベントの両方を収集したいと考えています。
FortiSIEM が SIEM イベントと PAM イベントの両方を収集できるように、管理者は AccessProtocol ドロップダウン リストでどのプロトコルを選択する必要がありますか?
A. LDAPS
B. LDAP 開始 TLS
C. TELNET
D. WMI
Answer: D (メーッセージを残す**)**

最新問題: **2**
エージェントレス方式で Windows イベント ログを収集するにはどのプロトコルを使用できますか?
A. SSH
B. SNMP
C. WMI
D. SMTP
Answer: (解答を表示する**)**

最新問題: **3**
ルールのサブパートはどのように定義されますか?
A. フィルターの集計。定義によるグループ化
B. 定義に基づいてグループ化をフィルターします。しきい値
C. しきい値時間ウィンドウの定義をフィルターします
D. フィルター集計時間ウィンドウの定義
Answer: D (メーッセージを残す**)**

ルール サブパターンの定義: FortiSIEM では、ルール内のサブパターンを使用して、ルールがインシデントまたはアラートをトリガーするために満たす必要がある特定の条件と基準を定義します。
サブパターンのコンポーネント: サブパターンには次の要素が含まれます。
* フィルター: ルールが評価するイベントをフィルターするための基準。
* 集約: 分析のためにイベントを集約またはグループ化する方法を定義する条件。
* 時間ウィンドウの定義: ルール条件が満たされているかどうかを判断するためにイベントを評価する時間枠を指定します。
説明: これらのコンポーネントを組み合わせることで、システムはイベント データ内の関心のあるパターンを効率的かつ正確に検出できるようになります。
参考資料: FortiSIEM 6.3 ユーザー ガイドの 「ルールとパターン」セクションでは、フィルター、集約、時間ウィンドウの定義の使用など、ルール サブパターンの構造と構成について説明しています。

最新問題**: 4**
展示品を参照してください。

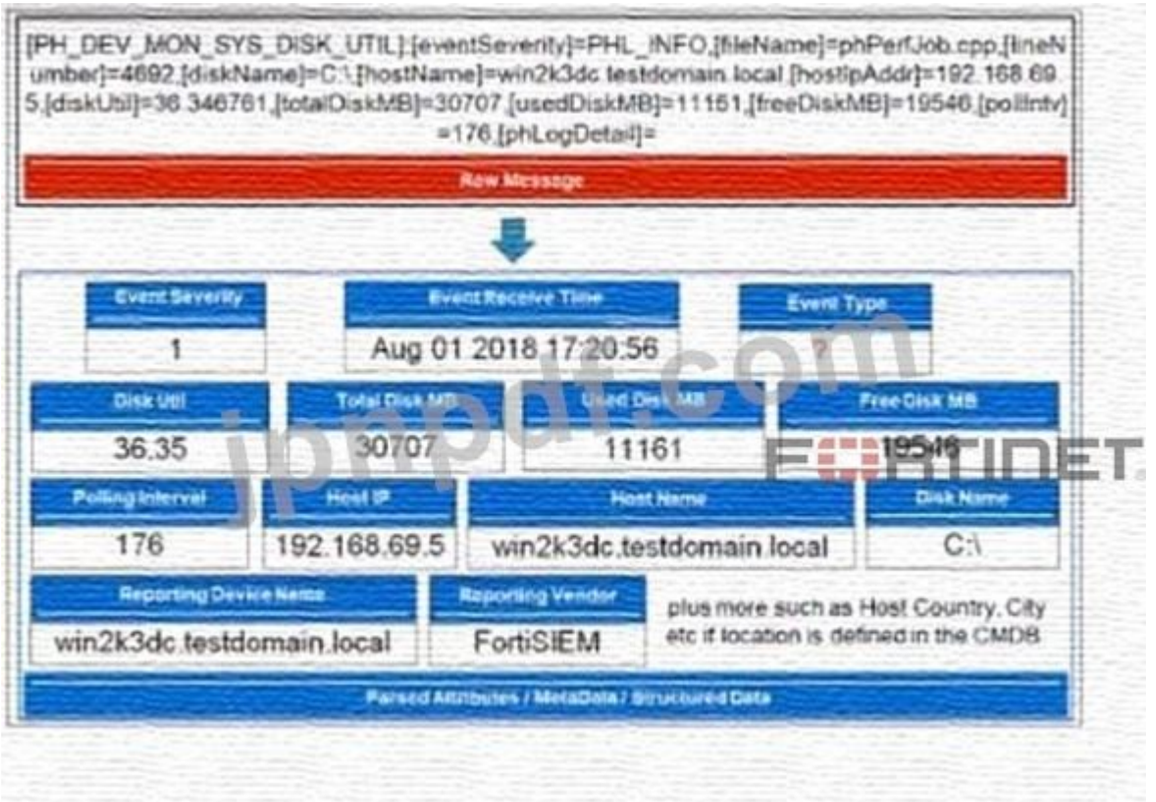
Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

FortiSIEM でイベントがレポート IP、イベント タイプ、ユーザー属性別にグループ化されている場合、いくつの結果が表示されますか?
A. 7件の結果が表示されます。
B. 結果が表示されます。
C. 一意の属性をグループ化できません。
D. 5件の結果が表示されます。
Answer: (解答を表示する**)**
イベントのグループ化: 特定の属性でイベントをグループ化すると、類似のイベントを集約できます。
グループ化基準: この質問では、イベントは 「レポート IP」、「イベント タイプ」、および 「ユーザー」別にグループ化されます。一意の組み合わせ分析:
* 10.10.10.10、ログオン失敗、Ryan、1.1.1.1、Web アプリ
* 10.10.10.11、ログオン失敗、ジョン、5.5.5.5、DB

* 10.10.10.10、ログオン失敗、Ryan、1.1.1.1、Web アプリ (重複、1 つの一意の結果としてカウント)
* 10.10.10.10、ログオン失敗、ポール、3.3.2.1、Web アプリ
* 10.10.10.11、ログオン失敗、Ryan、1.1.1.15、DB
* 10.10.10.11、ログオン失敗、ウェンディ、1.1.1.6、DB
* 10.10.10.10、ログオン失敗、Ryan、1.1.1.15、DB
結果の計算: 指定されたグループ化属性に基づいて、7 つの一意の組み合わせが存在します。
参考資料: FortiSIEM 6.3 ユーザー ガイドのイベント管理とレポートのセクションでは、選択した属性に基づいてイベントをグループ化してレポートする方法について説明します。

最新問題**: 5**
FortiSIEM でルール通知と自動修復を構成する場所はどこですか?
A. 通知ポリシー
B. 修復ポリシー
C. 通知エンジン
D. 修復エンジン
Answer: A (メーッセージを残す**)**
ルール通知と自動修復: FortiSIEM では、ルールによって生成された特定のインシデントやアラートに対応するように通知と自動修復アクションを構成できます。
通知ポリシー: これは、管理者が通知の設定を構成し、ルールによってアラートがトリガーされたときに実行されるアクションを指定するセクションです。
* 構成オプション: 通知の受信者、通知の種類 (電子メール、SMS など)、および実行する必要がある自動修復アクションの定義が含まれます。
重要性: 通知ポリシーを適切に構成すると、タイムリーなアラートとインシデントへの自動応答が保証され、SIEM システムの有効性が向上します。
参考資料: FortiSIEM 6.3 ユーザー ガイドの通知と自動修復のセクションでは、ルールによってトリガーされるアクションと応答の通知ポリシーを構成する方法について詳しく説明しています。

最新問題**: 6**
展示品を参照してください。



FortiSIEM はイベント タイプ フィールドに入力するためにどの値を使用しますか?

A. PHL_INFO

B. phPerfJob

C. PH_DSV_MON_SYS_DISK_UTIL

D. ディスク使用率

Answer: (解答を表示する**)**

イベント タイプの入力: FortiSIEM では、イベント タイプ フィールドは、生のメッセージまたはイベント ログ内の特定の識別子に基づいて入力されます。

生のメッセージ分析: この展示では、PH_DEV_MON_SYS_DISK_UTIL、PHL_INFO、phPerfJob、diskUtil などのさまざまなコンポーネントを含む生のメッセージが表示されます。

プライマリ イベント識別子: 生のメッセージの先頭にある PH_DEV_MON_SYS_DISK_UTIL は、イベント タイプのプライマリ識別子です。これは、イベントのタイプ (この場合は、システム ディスク使用率監視イベント) を分類します。

イベント タイプ フィールド: FortiSIEM はこのプライマリ識別子を使用してイベント タイプ フィールドに入力し、イベントを明確に分類します。

参考資料: FortiSIEM 6.3 ユーザー ガイドのイベント処理とイベント タイプのセクションでは、システム内でイベント タイプがどのように識別され、入力されるかについて詳しく説明しています。

最新問題**: 7**

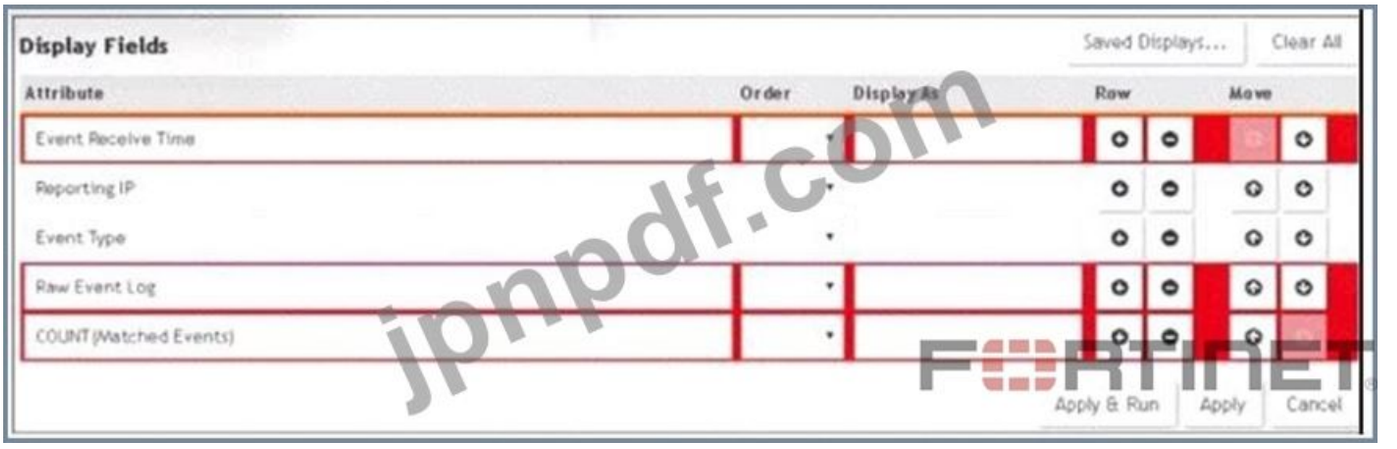
展示品を参照してください。

管理者は、図に示す式ビルダー設定に基づいた式を使用して問題を特定しようとしていますが、図に示すエラー メッセージは、式が無効であることを示しています。
正しい表現はどれでしょうか？
A. 一致したイベント COUNT()
B. 一致したイベント(COUNT)
C. COUNT(一致したイベント)
D. (COUNT) 一致したイベント
Answer: C (メーッセージを残す**)**
FortiSIEM の式ビルダー: 式ビルダーは、イベント データを分析するための式を作成するために使用されます。
正しい構文: 一致したイベントをカウントするための正しい構文は、COUNT(Matched Events) です。
* 関数:COUNT は、パラメータ (この場合は 「一致したイベント」) を受け取り、発生回数をカウントする関数です。
一般的なエラー: 順序を逆にしたり、括弧を不適切に使用したりするなど、構文が正しくない場合、無効な式が発生する可能性があります。
参考資料: FortiSIEM 6.3 ユーザー ガイドの式ビルダー セクションでは、イベント分析用の有効な式を作成するための正しい構文と使用法について説明しています。

最新問題**: 8**
環境内のどの FortiGate デバイスがどのファームウェア バージョンを実行しているかに関するレポートを生成するには、どの FortiSIEM 機能を使用する必要がありますか?
A. 分析検索を実行します。
B. [インベントリ] タブを使用してクエリを実行します。
C. ベースライン レポートを実行します。
D. CMDBレポートを実行する
Answer: B (メーッセージを残す**)**
機能の概要: FortiSIEM は、環境内のデバイス情報を照会およびレポートするためのツールをいくつか提供します。
インベントリ タブ: インベントリ タブは、ファームウェア バージョンなど、デバイスに関する詳細情報を表示するために特別に設計されています。
クエリ機能: [インベントリ] タブでは、クエリを実行して、FortiGate デバイスのファームウェア バージョンなどの特定の属性に基づいてデバイスをフィルタリングおよび表示できます。

レポート生成: [インベントリ] タブでクエリを実行すると、FortiGate デバイスと対応するファームウェア バージョンを一覧表示するレポートを生成できます。
参考資料: FortiSIEM 6.3 ユーザー ガイドのインベントリ管理セクションでは、インベントリ タブを使用してデバイス属性を照会およびレポートする方法について説明しています。

最新問題: **9**
展示品を参照してください。



FortiSIEM 管理者はレポートのいくつかの属性をグループ化したいと考えていますが、うまくできません。
図に示されているように、一部のフィールドが赤で強調表示されているのはなぜですか?
A. 一意の属性はグループ化できません。
B. イベント受信時間属性はログでは使用できません。
C. 属性 COUNT(一致したイベント) は無効な式です。
D. デバイスでは RAW イベント ログ属性は使用できません。
Answer: A (メーッセージを残す**)**
レポート内の属性のグループ化: FortiSIEM でレポートを作成するときに、特定の属性をグループ化してデータを要約および整理できます。
一意の属性: 各イベントに固有の属性は、意味のある集計や要約を提供しないため、グループ化できません。
赤色のハイライトの説明: 図の赤色のハイライトは、その固有の性質のためグループ化できない属性を示します。これらの固有の属性には、イベント受信時間、レポート IP、イベント タイプ、生のイベント ログ、および COUNT(一致したイベント) が含まれます。
属性特性:
* イベント受信時間はイベントごとに異なります。
* レポート IP とイベント タイプは大きく異なる可能性があるため、このコンテキストではグループ化するのは実用的ではありません。
* 生のイベント ログは、未処理のログ データを表します。これも一意です。
* COUNT(一致したイベント)は計算フィールドであり、グループ化には適していません。
参考資料: FortiSIEM 6.3 ユーザー ガイドのレポート セクションでは、レポート内の属性のグループ化に関する制約について説明しています。

最新問題: **10**
FortiSIEM はどのオペレーティング システムに基づいていますか?
A. レッドハット
B. セントOS
C. マイクロソフトウィンドウズ
D. ウブントゥ
Answer: B (メーッセージを残す**)**

最新問題: **11**
展示品を参照してください。

```
[root@FSM_NSE5 bin]#./phLicenseTool --collect license_req.dat
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phMiscUtils.cpp,
[lineNumber]=992,[phLogDetail]=Interface eth0 IP = 192.168.69.109
License information collected to the output file: license_req.dat
```

管理者は FortiSIEM ライセンスの問題を調査しています。
この手順はどのオフライン ライセンス条件用ですか?
A. この手順はオフライン ライセンスのデバッグ用です。
B. オフラインライセンス登録の手順です。
C. この手順はオフラインでのライセンス検証用です。
D. この手順はオフラインでのライセンス検証用です。
Answer: B (メーッセージを残す**)**
FortiSIEM のオフライン ライセンス: FortiSIEM は、直接インターネットにアクセスできない環境に対応するために、オフライン ライセンスのメカニズムを提供します。
ライセンス ツール コマンド: コマンド ./phLicenseTool --collect license_req.dat は、オフライン登録に必要なライセンス情報を収集するために使用されます。
手順の分析: この図はこのコマンドの出力を示しており、license_req.dat という名前のファイルにライセンス情報が収集されていることを示しています。
オフライン ライセンス登録: 収集されたデータ ファイルは通常、FortiSIEM サポート ポータルにアップロードされるか、ライセンス ファイルの処理と生成のために FortiSIEM サポート チームに提供されます。
参考資料: FortiSIEM 6.3 管理ガイドのライセンス セクションでは、オフライン シナリオでの phLicenseTool の使用を含む、オンラインとオフラインの両方のライセンス登録の手順について詳しく説明しています。

最新問題: **12**
パフォーマンスの可用性とパフォーマンスの監視を実行できる FortiSIEM コンポーネントはどれですか?
A. 監督者、作業者、収集者
B. 監督者と作業者のみ

C. スーパーバイザーのみ
D. コレクターのみ
Answer: (解答を表示する**)**
パフォーマンスと可用性の監視: FortiSIEM のさまざまなコンポーネントが、デバイスとサービスのパフォーマンスと可用性を監視します。
コンポーネント:
* スーパーバイザー: FortiSIEM インフラストラクチャ全体を監督し、他のコンポーネントのアクティビティを調整します。
* ワーカー: パフォーマンスや可用性のメトリックなど、収集されたデータを処理および分析します。
* コレクター: ネットワーク内のデバイスからパフォーマンスと可用性のデータを収集します。
共同機能: これらのコンポーネントは連携して動作し、ネットワークのパフォーマンスと可用性を包括的に監視します。
参考資料: FortiSIEM 6.3 ユーザー ガイドのパフォーマンスと可用性の監視セクションでは、監視タスクにおけるスーパーバイザー、ワーカー、コレクターの役割について説明しています。

最新問題**: 13**
FortiSIEM は、FortiGate ファイアウォールから syslog イベントを継続的に受信しています。FortiSIEM 管理者は、キーワード tcp を含む過去 2 時間の生のイベント ログを検索しようとしています。しかし、管理者は検索結果を取得できません。
展示に表示されている選択したフィルターに基づいて、検索結果が表示されないのはなぜですか?
A. 管理者が [次へ] ドロップダウン リストで [AND] を選択しました。これは間違ったブール演算子です。
B. キーワードは大文字と小文字が区別されます。管理者は、値フィールドに TCP と入力する代わりに、tcp と入力する必要があります。
C. 管理者が演算子列で - を選択しましたが、これは間違った演算子です。
D. 時間セクションで、管理者は相対的な最終オプションを選択し、ドロップダウン リストで期間として 2 と時間を選択しました。期間は 24 時間である必要があります。
Answer: (解答を表示する**)**

最新問題**: 14**
さまざまなパラメータに対して計算された異常ベースラインデータの保存を検討します。このデータの保存にはどのデータベースが使用されますか?
A. イベントDB
B. プロファイルDB
C. SVNDB
D. CMDB
Answer: D (メーッセージを残す**)**

異常ベースライン データ: 異常ベースライン データとは、潜在的なセキュリティ インシデントを示す逸脱を検出するために、さまざまなパラメータに対して計算された統計プロファイルとベースラインを指します。
プロファイル DB: プロファイル DB は、FortiSIEM にこのようなベースライン データを保存するために特別に設計されています。
* 目的: 異常検出を容易にするために、さまざまな監視パラメータの統計プロファイルを維持します。
* 使用方法: このデータは、FortiSIEM によって、リアルタイム メトリックと確立されたベースラインを比較して異常を識別するために使用されます。
参考資料: FortiSIEM 6.3 ユーザー ガイドのデータベース アーキテクチャ セクションでは、異常ベースライン データを格納するためのプロファイル DB など、FortiSIEM で使用されるさまざまなデータベースとその目的について説明しています。

最新問題**: 15**
展示品を参照してください。

FortiSIEM は、FortiGate ファイアウォールから syslog イベントを継続的に受信しています。FortiSIfcM 管理者は、キーワード tcp を含む過去 2 時間の生のイベント ログを検索しようとしています。ただし、管理者は検索結果を取得できません。
展示に表示されている選択したフィルターに基づいて、検索結果が表示されないのはなぜですか?
A. キーワードは大文字と小文字が区別されます。管理者は、値フィールドに TCP と入力する代わりに、tcp と入力する必要があります。
B. 時間セクションで、管理者は相対的な最終オプションを選択し、ドロップダウン リストで、時間間隔として 2 と時間を選択しました。時間は 24 時間である必要があります。
C. 管理者が演算子列で - を選択しましたが、これは間違った演算子です。
D. 管理者が [次へ] ドロップダウン リストで [AND] を選択しました。これは間違ったブール演算子です。
Answer: (解答を表示する**)**

検索における大文字と小文字の区別: FortiSIEM では、生のイベント ログの検索クエリも含め、検索クエリで大文字と小文字が区別されます。つまり、キーワードはログに表示されるとおりに正確に入力する必要があります。
キーワードの不一致: 展示では、値フィールドにキーワード 『TCP」が表示されます。実際のイベントで 『cp」(小文字) が使用されている場合、大文字と小文字が一致しないため、検索では結果が返されません。
正しいキーワード: キーワードを正しく一致させるには、管理者は値フィールドに 『cp」と入力する必要があります。
参考資料: FortiSIEM 6.3 ユーザー ガイドの検索とフィルタリングのセクションでは、検索クエリにおける大文字と小文字の区別の重要性について説明しています。

最新問題: **16**
本社の FortiSIEM スーパーバイザーは、企業全体で報告されている EPS (1 秒あたりのイベント数) の増加に対応するのに苦労しています。
管理者は、スーパーバイザーのデータ処理を支援するために、どのようなコンポーネントの導入を検討する必要がありますか?
A. ワーカー
B. コレクター
C. 監督者
D. エージェント
Answer: A (メーッセージを残す**)**

最新問題: **17**
展示品を参照してください。

作成されるインシデントの数を決定するソートはどのセクションに含まれていますか?

A. アクション

B. グループ化

C. 集計

D. フィルター

Answer: B (メーッセージを残す**)**

FortiSIEM でのインシデント作成: FortiSIEM でのインシデントは、システム内で定義された特定のパターンと条件に基づいて作成されます。

グループ化機能: 『サブパターンの編集』ウィンドウの 『グループ化』セクションでは、分析とインシデントの作成のためにデータをグループ化する方法を指定します。

グループ化の影響: データのグループ化方法は、生成されるインシデントの数に影響します。グループ化された属性の一意の組み合わせごとに、個別のインシデントが生成されます。

展示分析: 提供された展示の 『グループ化』セクションには、『レポート デバイス』、『レポート IP』、および 『ユーザー』がリストされています。これは、これらの属性の一意の組み合わせごとにインシデントが作成されることを意味します。

参考資料: FortiSIEM 6.3 ユーザー ガイドのルールとパターンの作成セクションでは、グループ化がインシデント生成にどのように影響するかについて詳しく説明しています。

最新問題**: 18**

管理者は、SNMP と WMI の資格情報を使用して Windows デバイスを検出しています。WMI メソッドはこれをどのように処理しますか?

A. WMI メソッドはトラフィックと IIS ログのみを収集します。

B. WMI メソッドは DNS ログのみを収集します。

C. WMI メソッドは DHCP ログのみを収集します。

D. WMI メソッドは、セキュリティ、アプリケーション、およびシステム イベント ログを収集します。

Answer: D (メーッセージを残す)
WMI メソッド: Windows Management Instrumentation (WMI) は、ネットワーク内のデバイスとアプリケーションの管理を統合するための Microsoft の仕様セットです。
ログ収集: WMI は、Windows デバイスからさまざまな種類のログを収集するために使用されます。
* セキュリティ ログ: ログイン試行やリソース アクセスなどのセキュリティ関連イベントの記録が含まれます。
* アプリケーション ログ: システム上で実行されているアプリケーションによって生成されたログが含まれます。
* システム ログ: オペレーティング システムとそのコンポーネントに関連するログが含まれます。
包括的なデータ収集: WMI を使用することで、FortiSIEM は Windows デバイスのセキュリティとパフォーマンスの監視と分析に不可欠な幅広いイベント ログを収集できます。
参考資料: FortiSIEM 6.3 ユーザー ガイドのデータ収集方法のセクションでは、Windows デバイスからイベント ログを収集するための WMI の使用について詳しく説明しています。

最新問題**: 19**
FortiSIEM でイベントがレポート IP、イベント タイプ、ユーザー属性別にグループ化されている場合、いくつの結果が表示されますか?
A. 一意の属性をグループ化できません。
B. 7件の結果が表示されます。
C. 結果が表示されます。
D. 5件の結果が表示されます。
Answer: D (メーッセージを残す)

最新問題**: 20**
展示品を参照してください。

管理者は、図に示す式ビルダー設定に基づいた式を使用して問題を特定しようとしていますが、図に示すエラー メッセージは、式が無効であることを示しています。
正しい表現はどれでしょうか？
A. 一致したイベント COUNT()
B. 一致したイベント(COUNT)

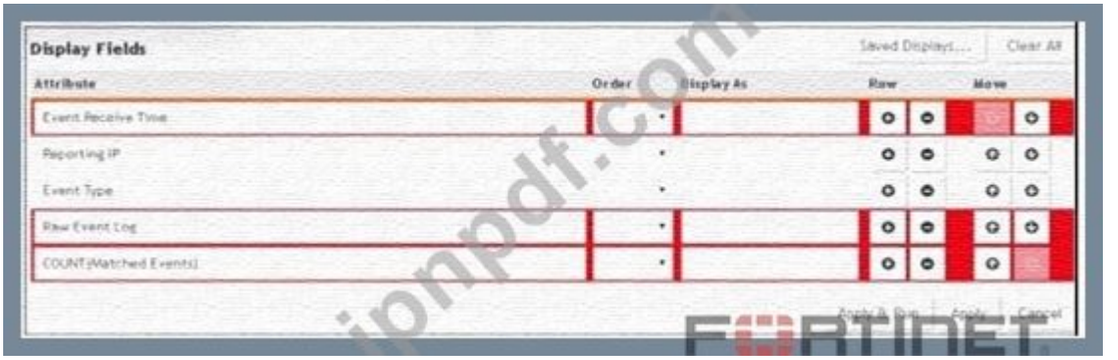
C. COUNT(一致したイベント)
D. (COUNT) 一致したイベント
Answer: (解答を表示する**)**
FortiSIEM の式ビルダー: 式ビルダーは、イベント データを分析するための式を作成するために使用されます。
正しい構文: 一致したイベントをカウントするための正しい構文は、COUNT(Matched Events) です。
* 関数:COUNT は、パラメータ (この場合は 「一致したイベント」) を受け取り、発生回数をカウントする関数です。
一般的なエラー: 順序を逆にしたり、括弧を不適切に使用したりするなど、構文が正しくない場合、無効な式が発生する可能性があります。
参考資料: FortiSIEM 6.3 ユーザー ガイドの式ビルダー セクションでは、イベント分析用の有効な式を作成するための正しい構文と使用法について説明しています。

最新問題**: 21**
ルールの頻度フィールドは何を決定しますか?
A. ルールがサブパターンを評価する頻度。
B. 同じ条件でルールがトリガーされる頻度。
C. ルールがトリガーされる頻度。
D. ルールが明確なアクションを実行する頻度。
Answer: A (メーッセージを残す**)**
FortiSIEM でのルール評価: FortiSIEM のルールは定期的に評価され、定義された条件またはサブパターンが満たされているかどうかが確認されます。
頻度フィールド: ルールの頻度フィールドは、ルールのサブパターンが評価される間隔を決定します。
* 評価間隔: システムがルールのサブパターンに対して受信イベントをチェックし、インシデントをトリガーする必要があるかどうかを判断する頻度を定義します。
* パフォーマンスへの影響: インシデントのタイムリーな検出とシステム パフォーマンスのバランスをとるには、適切な頻度を設定することが重要です。
例:
* 頻度が 5 分に設定されている場合、ルールは 5 分ごとにサブパターンを評価します。
* これは、システムが 5 分ごとに、サブパターンで定義された条件が受信イベントによって満たされているかどうかをチェックすることを意味します。
参考資料: FortiSIEM 6.3 ユーザー ガイドの 「ルールとインシデント」セクションでは、頻度フィールドと、それがルール内のサブパターンの評価にどのように影響するかについて説明しています。

最新問題**: 22**
どのプロセスが生のログデータを構造化データに変換しますか?

A. データの拡充
B. データ解析
C. データ分類
D. データの検証
Answer: B (メーッセージを残す**)**

最新問題**: 23**
展示品を参照してください。



FortiSIEM 管理者はレポートのいくつかの属性をグループ化したいと考えていますが、うまくできません。
図に示されているように、一部のフィールドが赤で強調表示されているのはなぜですか?
A. 一意の属性はグループ化できません。
B. イベント受信時間属性はログでは使用できません。
C. 属性 COUNT(一致したイベント) は無効な式です。
D. デバイスでは RAW イベント ログ属性は使用できません。
Answer: A (メーッセージを残す**)**
レポート内の属性のグループ化: FortiSIEM でレポートを作成するときに、特定の属性をグループ化してデータを要約および整理できます。
一意の属性: 各イベントに固有の属性は、意味のある集計や要約を提供しないため、グループ化できません。
赤色のハイライトの説明: 図中の赤色のハイライトは、その固有の性質のためグループ化できない属性を示しています。これらの固有の属性には、イベント受信時間、レポート IP、イベント タイプ、生のイベント ログ、および COUNT(一致したイベント) が含まれます。
属性特性:
* イベント受信時間はイベントごとに異なります。
* レポート IP とイベント タイプは大きく異なる可能性があるため、このコンテキストではグループ化するのは実用的ではありません。
* 生のイベント ログは、未処理のログ データを表します。これも一意です。
* COUNT(一致したイベント)は計算フィールドであり、グループ化には適していません。
参考資料: FortiSIEM 6.3 ユーザー ガイドのレポート セクションでは、レポート内の属性のグループ化に関する制約について説明しています。

最新問題: **24**
すべてのネットワーク デバイスで ping が無効になっているネットワーク環境に最適な検出スキャン オプションは何ですか?
A. スマートスキャン
B. CMDBスキャン
C. L2スキャン
D. 範囲スキャン
Answer: A (メーッセージを残す**)**

最新問題: **25**
展示品を参照してください。

```
[root@FSM_NSE5 bin]#./phLicenseTool --collect license_req.dat
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phMiscUtils.cpp,
[lineNumber]=992,[phLogDetail]=Interface eth0 IP = 192.168.69.109
License information collected to the output file: license_req.dat
```

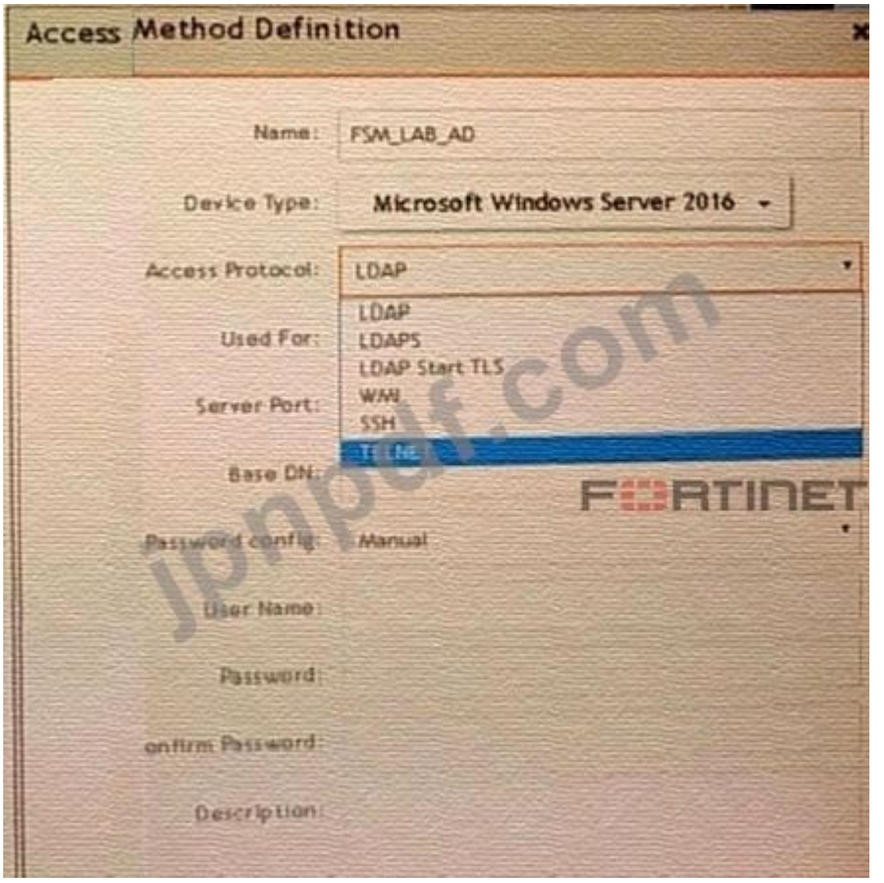
管理者は FortiSIEM ライセンスの問題を調査しています。
この手順はどのオフライン ライセンス条件用ですか?
A. この手順はオフライン ライセンスのデバッグ用です。
B. オフラインライセンス登録の手順です。
C. この手順はオフラインでのライセンス検証用です。
D. この手順はオフラインでのライセンス検証用です。
Answer: B (メーッセージを残す**)**
FortiSIEM のオフライン ライセンス: FortiSIEM は、直接インターネットにアクセスできない環境に対応するために、オフライン ライセンスのメカニズムを提供します。
ライセンス ツール コマンド: コマンド ./phLicenseTool --collect license_req.dat は、オフライン登録に必要なライセンス情報を収集するために使用されます。
手順の分析: この図はこのコマンドの出力を示しており、license_req.dat という名前のファイルにライセンス情報が収集されていることを示しています。
オフライン ライセンス登録: 収集されたデータ ファイルは通常、FortiSIEM サポート ポータルにアップロードされるか、ライセンス ファイルの処理と生成のために FortiSIEM サポート チームに提供されます。
参考資料: FortiSIEM 6.3 管理ガイドのライセンス セクションでは、オフライン シナリオでの phLicenseTool の使用を含む、オンラインとオフラインの両方のライセンス登録の手順について詳しく説明しています。

最新問題: **26**
どの FortiSIEM コンポーネントがデバイス検出を実行できますか?
A. FortiSIEM Linuxエージェント
B. コレクター
C. FortiSIEM Windowsエージェント

D. 労働者
Answer: (解答を表示する**)**

最新問題**: 27**
インシデントの 4 つのカテゴリとは何ですか?
A. パフォーマンス、デバイス、高リスク、低リスク
B. デバイス、ユーザー、高リスク、低リスク
C. パフォーマンス、可用性、セキュリティ、変更
D. セキュリティ、変更、高リスク、低リスク
Answer: C (メーッセージを残す**)**

最新問題**: 28**
展示品を参照してください。



FortiSIEM 管理者は、Microsoft Windows サーバーから SIEM イベント ログとパフォーマンスおよび可用性メトリック (PAM) イベントの両方を収集したいと考えています。FortiSIEM が SIEM イベントと PAM イベントの両方を収集するには、管理者はアクセス プロトコル ドロップダウン リストでどのプロトコルを選択する必要がありますか?
A. TELNET
B. WMI
C. LDAPS
D. LDAP 開始 TLS
Answer: B (メーッセージを残す**)**

SIEM および PAM イベントの収集: Microsoft Windows サーバーから SIEM イベント ログとパフォーマンスおよび可用性監視 (PAM) イベントの両方を収集するには、適切なプロトコルを選択する必要があります。
WMI プロトコル: Windows Management Instrumentation (WMI) は、このタスクに適したプロトコルです。
* SIEM イベント ログ: WMI は、Windows デバイスからセキュリティ、アプリケーション、およびシステム ログを収集できます。
* PAM イベント: WMI は、CPU 使用率、メモリ使用率、ディスク アクティビティなどのパフォーマンス メトリックも収集できます。
包括的なデータ収集: WMI を使用すると、両方の種類のデータが Windows サーバーから効率的に収集されます。
参考資料: FortiSIEM 6.3 ユーザー ガイドのデータ収集方法のセクションでは、さまざまな種類のログとパフォーマンス メトリックを収集するための WMI の使用について詳しく説明しています。

最新問題**: 29**
FortiSIEM は災害復旧モードで展開されます。
災害が発生した場合、災害復旧操作を成功させるために手動で実行する必要がある 2 つのタスクはどれですか? (2 つ選択してください。)
A. phSecworker2priworker コマンドを使用して、セカンダリ ワーカーをプライマリ ワーカーに昇格します。
B. phSecondary2primary コマンドを使用して、セカンダリ スーパーバイザーをプライマリ ロールに昇格します。
C. DNS 構成を変更して、ユーザー、デバイス、コレクターがセカンダリ FortiSIEM にログインできるようにします。
D. EventDB 用に構成された共有ストレージ NFS の構成をセカンダリ FortiSIEM に変更します。
Answer: A,C (メーッセージを残す**)**
災害復旧モード: FortiSIEM の災害復旧 (DR) モードでは、プライマリ システムに障害が発生した場合に引き継ぐバックアップ システムが確保されます。
DR 操作の手動タスク: 災害が発生した場合、セカンダリ システムへのスムーズな移行を確実にするために、特定のタスクを手動で実行する必要があります。
副監督者の昇進:
* セカンダリ スーパーバイザをプライマリ ロールに昇格するには、コマンド phSecondary2primary を使用します。このコマンドは、セカンダリ スーパーバイザがプライマリ スーパーバイザとして引き継ぐように再構成し、管理と調整の継続性を確保します。
DNS 構成の変更:
* DNS 構成を更新して、すべてのユーザー、デバイス、コレクターをセカンダリ FortiSIEM インスタンスに誘導します。これにより、環境内のすべてのコンポーネントが、個々のデバイスを手動で再構成することなく、新しく昇格したプライマリ スーパーバイザと通信できるようになります。

参考資料: FortiSIEM 6.3 管理ガイドの災害復旧セクションでは、災害復旧操作中にセカンダリスーパーバイザを昇格し、DNS 構成を更新する詳細な手順が説明されています。

最新問題: **30**
リアルタイムのイベント相関を提供するために連携する FortiSIEM コンポーネントはどれですか?
A. 監督者と作業者
B. コレクターとWindowsエージェント
C. ワーカーとコレクター
D. 監督者とコレクター
Answer: A (メーッセージを残す**)**
FortiSIEM アーキテクチャ: FortiSIEM アーキテクチャには、スーパーバイザー、ワーカー、コレクター、エージェントなどの複数のコンポーネントが含まれており、それぞれが SIEM エコシステムで異なる役割を果たします。
リアルタイム イベント相関: リアルタイム イベント相関は、受信イベントを分析および相関させて、セキュリティ インシデントや運用上の問題を示すパターンを検出する重要な機能です。
監督者と労働者の役割:
* スーパーバイザー: スーパーバイザーは、FortiSIEM システム全体を監視して、イベントの処理と分析を調整します。
* ワーカー: ワーカーは、コレクターとエージェントから受信したイベントの処理と相関を担当します。
相関関係のコラボレーション: スーパーバイザー コンポーネントとワーカー コンポーネントが連携して、負荷を分散し、イベントの効率的な処理を確保することで、リアルタイムのイベント相関関係を実行し、インシデントをリアルタイムで識別します。
参考資料: FortiSIEM 6.3 ユーザー ガイドのイベント相関と処理のセクションでは、スーパーバイザー コンポーネントとワーカー コンポーネントが連携してリアルタイムのイベント相関を実現する方法について詳しく説明しています。

最新問題: **31**
生のログデータを構造化データに変換するプロセスはどれですか?
A. データ分類
B. データの検証
C. データ解析
D. データの拡充
Answer: C (メーッセージを残す**)**
生のログ データ: デバイスが FortiSIEM にログを送信すると、データは生の非構造化形式で届きます。
データ解析プロセス: この生のログ データを構造化された形式に変換するプロセスは、データ解析と呼ばれます。
* データ解析: 生のログエントリから関連フィールドを抽出し、整理します。

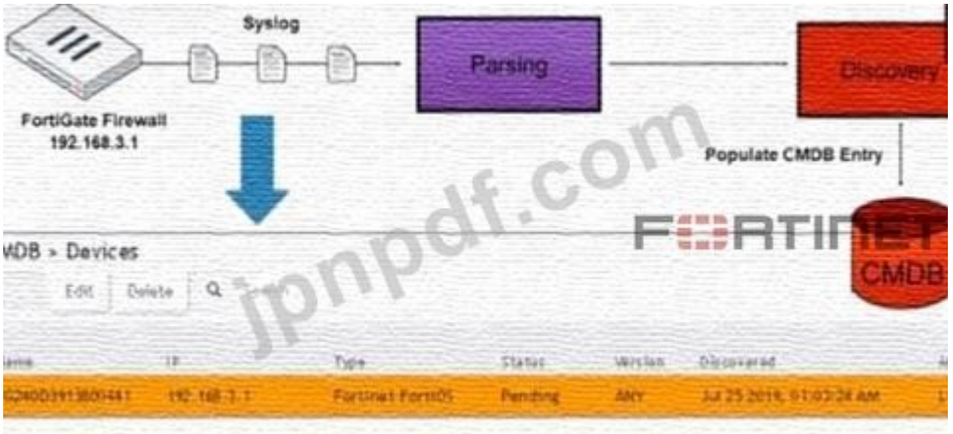
* 構造化された形式により、データを分析、レポート、相関に使用できるようになります。
構造化データの重要性: 構造化データは、効果的なイベント相関、アラート、および意味のあるレポートの生成に不可欠です。
参考資料: FortiSIEM 6.3 ユーザー ガイドのデータ解析セクションでは、解析によって生のログデータが構造化データに変換される仕組みについて詳しく説明しています。

最新問題: **32**
ルールの頻度フィールドは何を決定しますか?
A. ルールがサブパターンを評価する頻度。
B. 同じ条件でルールがトリガーされる頻度。
C. ルールがトリガーされる頻度。
D. ルールが明確なアクションを実行する頻度。
Answer: B (メーッセージを残す**)**
FortiSIEM でのルール評価: FortiSIEM のルールは定期的に評価され、定義された条件またはサブパターンが満たされているかどうかが確認されます。
頻度フィールド: ルールの頻度フィールドは、ルールのサブパターンが評価される間隔を決定します。
* 評価間隔: システムがルールのサブパターンに対して受信イベントをチェックし、インシデントをトリガーする必要があるかどうかを判断する頻度を定義します。
* パフォーマンスへの影響: インシデントのタイムリーな検出とシステム パフォーマンスのバランスをとるには、適切な頻度を設定することが重要です。
例:
* 頻度が 5 分に設定されている場合、ルールは 5 分ごとにサブパターンを評価します。
* これは、システムが 5 分ごとに、サブパターンで定義された条件が受信イベントによって満たされているかどうかをチェックすることを意味します。
参考資料: FortiSIEM 6.3 ユーザー ガイドの 「ルールとインシデント」セクションでは、頻度フィールドと、それがルール内のサブパターンの評価にどのように影響するかについて説明しています。

最新問題: **33**

ルール エンジンでは、どの条件が FortiSIEM に一致する評価済みデータを要約してカウントするように指示しますか。
A. グループ化
B. 集約
C. 時間枠
D. フィルター
Answer: (解答を表示する**)**

最新問題**: 34**
展示品を参照してください。



FortiSIEM によって FortiGate デバイスがどのように検出されたのでしょうか?
A. GUIログ検出
B. Syslog 検出
C. プルイベント検出
D. 自動ログ検出
Answer: B (メーッセージを残す**)**
FortiSIEM の検出方法: FortiSIEM は、syslog、SNMP などのさまざまな方法を使用してデバイスを検出できます。
Syslog 検出: この図は、FortiGate デバイスが syslog を使用して FortiSIEM によって検出されたことを示しています。
* Syslog 解析: FortiGate デバイスから送信された Syslog メッセージは、FortiSIEM によって解析され、関連情報が抽出されます。
* CMDB エントリ: 解析された情報に基づいて、デバイスの構成管理データベース (CMDB) にエントリが入力されます。
展示の証拠: この展示では、FortiGate ファイアウォールから解析および検出プロセスまでの syslog フローが示されており、その結果、デバイスが CMDB に 「保留中」のステータスでリストされます。参考資料: FortiSIEM 6.3 ユーザー ガイドのデバイス検出セクションでは、syslog 検出の仕組みと、syslog データに基づいてデバイスが CMDB に追加される仕組みについて説明しています。

最新問題**: 35**

リアルタイムのイベント相関を提供するために連携する FortiSIEM コンポーネントはどれですか?
A. 監督者と作業者
B. コレクターとWindowsエージェント
C. 労働者と収集者
D. 監督者とコレクター
Answer: A (メーッセージを残す**)**

最新問題**: 36**
ルール エンジンでは、どの条件が FortiSIEM に一致する評価済みデータを要約してカウントするように指示しますか。
A. 時間枠
B. 集約
C. グループ化
D. フィルター
Answer: (解答を表示する**)**
FortiSIEM のルール エンジン: ルール エンジンは、定義された条件に基づいて受信イベントを評価し、インシデントや異常を検出します。
集計条件: 集計条件は、一致する評価済みデータを集計してカウントするように FortiSIEM に指示します。
* 機能: 集計は、指定された基準に基づいてイベントをグループ化し、定義された時間枠内での発生回数をカウントするなどの操作を実行するために使用されます。
目的: これにより、短期間内に多数のログイン試行が失敗するなどのパターンや異常を検出できます。
参考資料: FortiSIEM 6.3 ユーザー ガイドのルール エンジン セクションでは、集計を使用して一致するデータを要約およびカウントする方法について説明しています。

最新問題**: 37**
さまざまなパラメータに対して計算された異常ベースライン データの保存について考えてみましょう。このデータの保存にはどのデータベースが使用されますか?
A. イベントDB
B. プロファイルDB
C. SVNDB
D. CMDB
Answer: B (メーッセージを残す**)**
異常ベースライン データ: 異常ベースライン データとは、潜在的なセキュリティ インシデントを示す逸脱を検出するために、さまざまなパラメータに対して計算された統計プロファイルとベースラインを指します。
プロファイル DB: プロファイル DB は、FortiSIEM にこのようなベースライン データを保存するために特別に設計されています。

* 目的: 異常検出を容易にするために、さまざまな監視パラメータの統計プロファイルを維持します。
* 使用方法: このデータは、FortiSIEM によって、リアルタイム メトリックと確立されたベースラインを比較して異常を識別するために使用されます。
参考資料: FortiSIEM 6.3 ユーザー ガイドのデータベース アーキテクチャ セクションでは、異常ベースライン データを格納するためのプロファイル DB など、FortiSIEM で使用されるさまざまなデータベースとその目的について説明しています。

最新問題**: 38**
FortiSIEM の高度な分析ルール エンジンでは、どの 3 つの操作を使用して複数のサブパターンを参照できますか?(3 つ選択してください。)
A. それ以外の場合
B. いいえ
C. フォローされている
D. または
E. かつ
Answer: (解答を表示する**)**
高度な分析ルール エンジン: FortiSIEM のルール エンジンでは、複数のサブパターンを使用して複雑なイベントの相関関係を分析できます。
サブパターンを参照するための操作:
* FOLLOWED_BY: この操作は、指定された時間枠内で 1 つのイベントが別のイベントに続くことを示すために使用されます。
* OR: この論理演算では、複数のサブパターンを含めることができ、いずれかのサブパターンが一致するとルールがトリガーされます。
* AND: この論理演算では、ルールをトリガーするために、参照されているすべてのサブパターンが一致する必要があります。
使用方法: これらの操作により、詳細かつ正確なイベント相関が可能になり、複雑なパターンやインシデントの検出に役立ちます。
参考資料: FortiSIEM 6.3 ユーザー ガイドの 「Advanced Analytics Rules Engine」セクションでは、ルール内のサブパターンを参照するためのさまざまな操作の使用について説明しています。

最新問題**: 39**
リアルタイムのイベント相関を提供するために連携する FortiSIEM コンポーネントはどれですか?
A. 監督者と作業者
B. コレクターとWindowsエージェント
C. ワーカーとコレクター
D. 監督者とコレクター
Answer: C (メーッセージを残す**)**

FortiSIEM アーキテクチャ: FortiSIEM アーキテクチャには、スーパーバイザー、ワーカー、コレクター、エージェントなどの複数のコンポーネントが含まれており、それぞれが SIEM エコシステムで異なる役割を果たします。
リアルタイム イベント相関: リアルタイム イベント相関は、受信イベントを分析および相関させて、セキュリティ インシデントや運用上の問題を示すパターンを検出する重要な機能です。
監督者と労働者の役割:
* スーパーバイザー: スーパーバイザーは、FortiSIEM システム全体を監視して、イベントの処理と分析を調整します。
* ワーカー: ワーカーは、コレクターとエージェントから受信したイベントの処理と相関を担当します。
相関関係のコラボレーション: スーパーバイザー コンポーネントとワーカー コンポーネントが連携して、負荷を分散し、イベントの効率的な処理を保証してリアルタイムでイベントの相関関係を実行し、インシデントをリアルタイムで識別します。
参考資料: FortiSIEM 6.3 ユーザー ガイドのイベント相関と処理のセクションでは、スーパーバイザー コンポーネントとワーカー コンポーネントが連携してリアルタイムのイベント相関を実現する方法について詳しく説明しています。

最新問題**: 40**
FortiSIEM 管理者は、問題を調査するために 2 つのデバイスのイベントを調べていますが、管理者は検索から結果を取得できません。
展示品に表示されている選択されたフィラーに基づいて、検索で結果が返されないのはなぜですか?
A. 演算子列で間違ったオプションが選択されています
B. 次の列で間違ったブール演算子が選択されています
C. 括弧がありません
D. 値列に無効なIPサブネットが入力されています
Answer: B (メーッセージを残す**)**