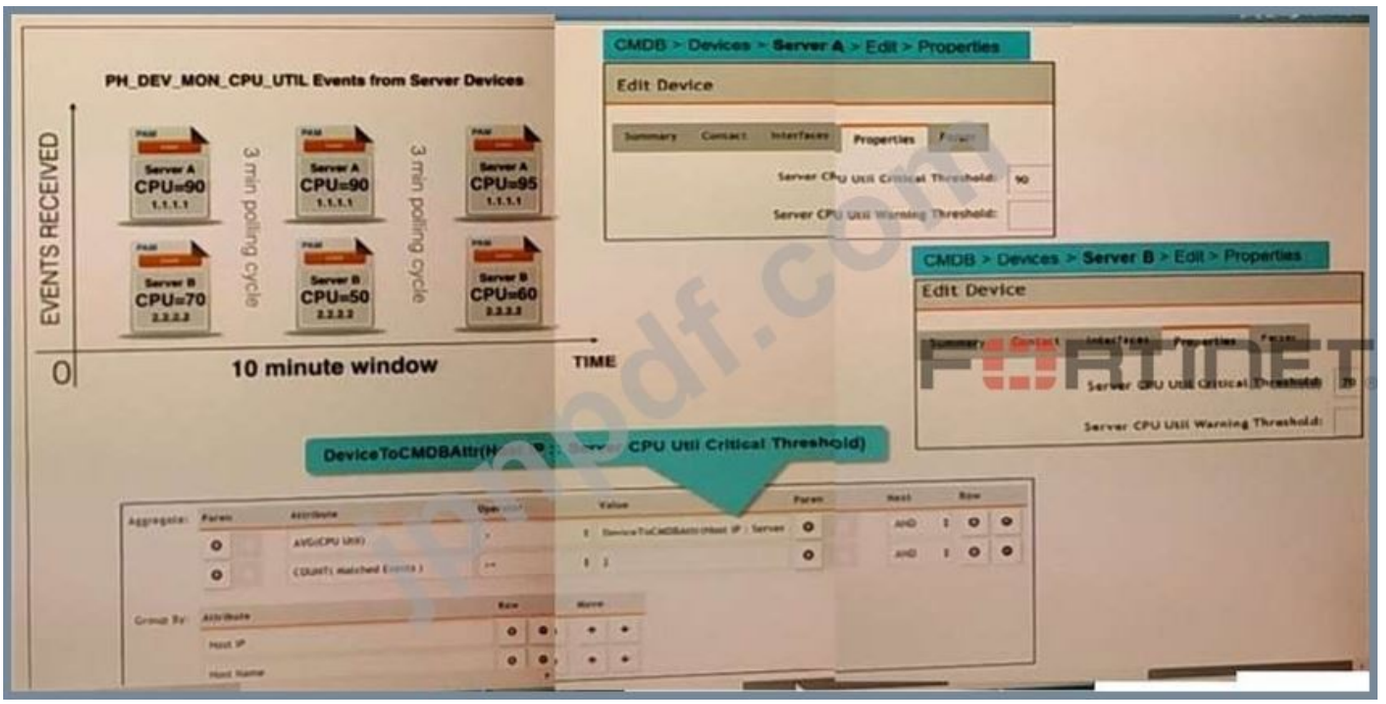
Fortinet.NSE5_FSM-5.2.v2022-11-25.q20

試験コード:	NSE5_FSM-5.2
試験名称:	Fortinet NSE 5 - FortiSIEM 5.2
認定資格:	Fortinet
無料問題数:	20
バージョン:	v2022-11-25
アクセス数:	518
ページビュー数:	200
https://www.jpnpdf.com/Fortinet.NSE5_FSM-5.2.v2022-11-25.q20-mondaishu.html	

最新問題: **1**
報告されたパケット損失が50%から98%の間の場合。サマリーダッシュボードの[可用性]列でデバイスに割り当てられているステータスはどれですか。
A. 受信パケット数が減少したため、クリティカルステータスが割り当てられました
B. パケット損失のためにダウンステータスが割り当てられます。
C. 受信したパケットのためにアップステータスが割り当てられます
D. パケット損失のために劣化ステータスが割り当てられます
Answer: D (メーッセージを残す**)**

最新問題: **2**
生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. データ解析
B. データ検証
C. データの強化
D. データ分類
Answer: B (メーッセージを残す**)**

最新問題: **3**
展示を参照してください。



サーバーAとサーバーBの2つのサーバーから、10分間に3つのイベントが収集されます。
ルールサブパターンに使用されている設定に基づきます。サーバーはいくつのインシデントを生成しますか？

A. サーバーBは1つのインシデントを生成し、サーバーAはインシデントを生成しません
B. サーバーAは1つのインシデントを生成し、サーバーBwiflは1つのインシデントを生成します
C. サーバーAは1つのインシデントを生成し、サーバーBはインシデントを生成しません
D. サーバーAはインシデントを生成せず、サーバーBはインシデントを生成しません
Answer: (解答を表示する**)**

最新問題: **4**
インシデントのステータスがクリアされた場合、これはどういう意味ですか？
A. インシデントはオペレーターによってクリアされました。
B. インシデントが発生してから2時間経過し、インシデントは再発していません。
C. ルールに設定された明確な条件が満たされました。
D. セキュリティルールの問題が解決されました。
Answer: (解答を表示する**)**

最新問題: **5**
展示を参照してください。

管理者は、展示に示されている式ビルダーの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、展示に表示されている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すか？

A. COUNT（一致したイベント）
B. （COUNT）一致したイベント
C. 一致したイベント（COUNT）
D. 一致したイベントCOUNT（）

Answer: (解答を表示する**)**

最新問題**: 6**
FortiSIEM分析結果に使用できる2つのエクスポート方法はどれですか？（2つ選択してください。）

A. PNG
B. CSV
C. PDF
D. HTML

Answer: B,C (メーッセージを残す**)**

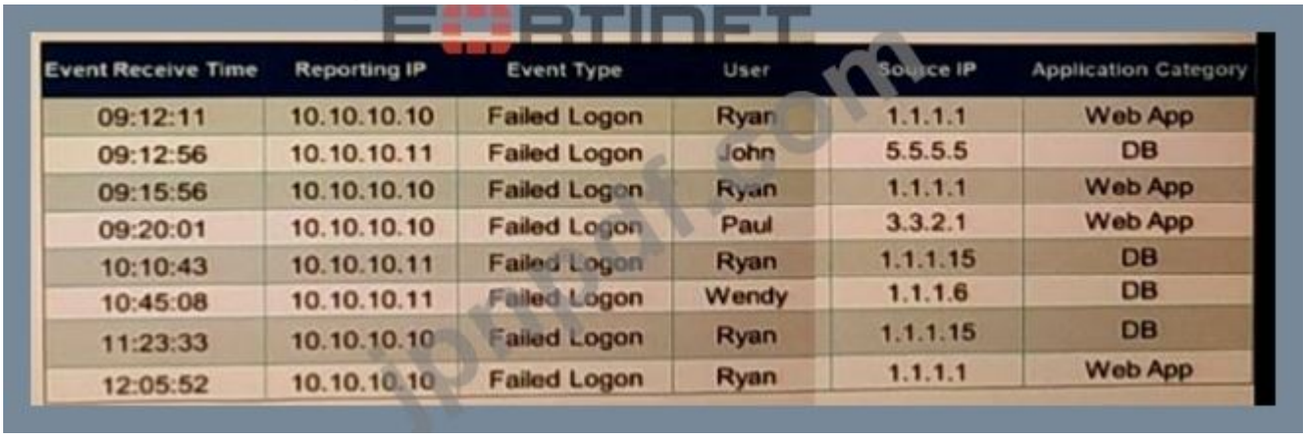
最新問題**: 7**
展示を参照してください。

[モニター]列に表示されている黄色い星は何を示していますか？

A. 黄色の星は、検出中にメトリックが適用されたが、データ収集が開始されていないことを示します
B. 黄色の星は、検出中にメトリックが適用され、データが正常に収集されたことを示します
C. 黄色の星は、検出中にメトリックが適用されたことを示しますが、FortiSIEMはデータを収集できません。

D. 黄色の星は、検出中にメトリックが適用されなかったため、FortiSEIMがデータを収集できなかったことを示します。
Answer: A (メーッセージを残す**)**

最新問題**: 8**
展示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

イベントがFortiSIEMのイベント受信時間、レポートIP、およびユーザー属性によって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. 2つの結果が表示されます
B. 8つの結果が表示されます
C. 4つの結果が表示されます
D. 一意の属性をグループ化できません
Answer: (解答を表示する**)**

最新問題**: 9**
独自のフラットファイルデータベースを使用する場合、FortiSIEMスーパーバイザ仮想アプライアンスの最小メモリ要件はどれくらいですか？
A. 64GB RAM
B. 16GB RAM
C. 24GB RAM
D. 32GB RAM
Answer: (解答を表示する**)**

最新問題**: 10**
展示を参照してください。

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、管理者は検索結果を取得していません。

展示に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. 次の列で間違ったブール演算子が選択されています

B. 無効なIPサブネットが[値]列に入力されています

C. 括弧がありません

D. [演算子]列で間違ったオプションが選択されています

Answer: B (メーッセージを残す**)**

最新問題**: 11**

展示を参照してください。

[モニター]列に表示されている黄色い星は何を示していますか？

A. 黄色の星は、検出中にメトリックが適用され、データが正常に収集されたことを示します

B. 黄色の星は、検出中にメトリックが適用されなかったため、FortiSEIMがデータを収集できなかったことを示します。

C. 黄色の星は、検出中にメトリックが適用されたことを示しますが、FortiSIEMはデータを収集できません。

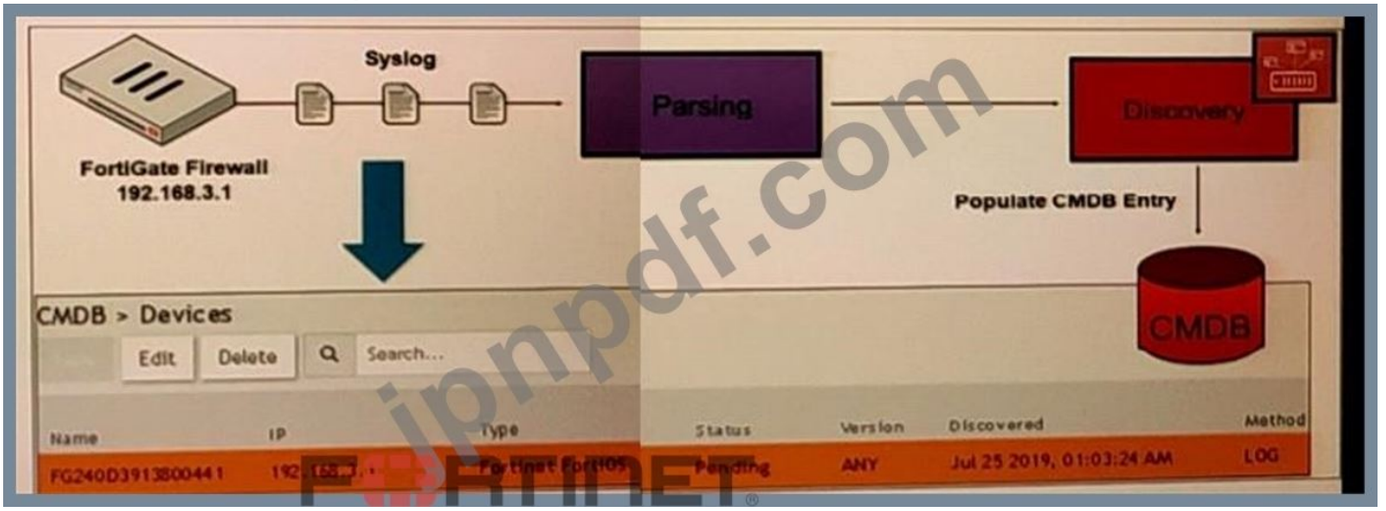
D. 黄色の星は、検出中にメトリックが適用されたが、データ収集が開始されていないことを示します

Answer: (解答を表示する**)**

最新問題: **12**
SyslogをFortiSIEMに送信するために使用できる3つのポートはどれですか？ 3つ選択してください。）
A. UDP 514
B. TCP 514
C. UDP9999
D. TCP 1470
E. UDP 162
Answer: A,D,E (メーッセージを残す**)**

最新問題: **13**
デバイス検出を実行できるFortiSIEMコンポーネントはどれですか？
A. 労働者
B. コレクター
C. FortiSIEMLinuxエージェント
D. FortiSIEMWindowsエージェント
Answer: B (メーッセージを残す**)**

最新問題: **14**
展示を参照してください。



FortiSIEMはFortiGateデバイスをどのように発見しましたか？
A. プルイベントメソッドを使用する
B. syslogディスカバリーを介して
C. GUIログ検出を介して
D. 自動ログ検出による
Answer: C (メーッセージを残す**)**

最新問題: **15**
展示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、管理者は検索から結果を取得していません。
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. 管理者は[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. 管理者が[演算子]列で間違った演算子を選択しました。

C. [時間]セクションで、管理者は[相対最後]オプションを選択し、ドロップダウンリストで[2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。

D. キーワードは、[値]フィールドにTCPと入力する代わりに、大文字と小文字を区別します。管理者はtcpと入力する必要があります。

Answer: B (メーッセージを残す**)**

最新問題**: 16**
FortiSIEM GUI検出プロセスには、ほとんどの場合、どのプロトコルが必要ですか？

A. WMI

B. Syslog

C. Telnet

D. SNMP

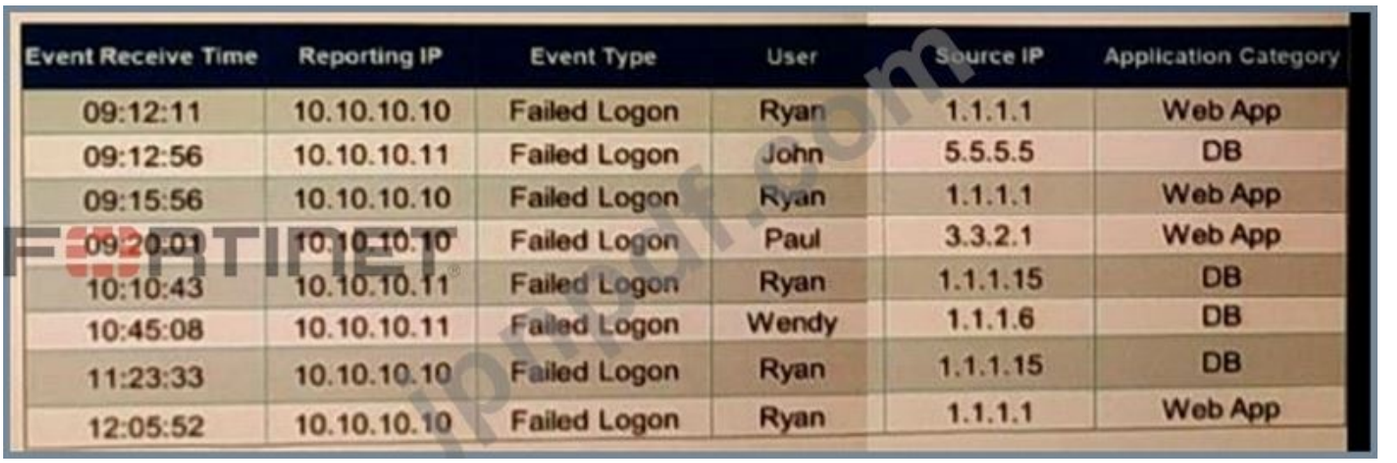
Answer: D (メーッセージを残す**)**

最新問題: 17
どのFortiSIEMコンポーネントが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ますか？
A. スーパーバイザー、ワーカー、コレクター
B. スーパーバイザーのみ
C. スーパーバイザーとワーカーのみ
D. コレクターのみ
Answer: (解答を表示する)

最新問題: 18
FotiSIEMエンタープライズライセンスモードで、コレクターとデータセンターFortiSIEMクラスター間のリンクがダウンした場合はどうなりますか？
A. コレクタープロセスが停止し、イベントがドロップされます
B. コレクターはデバイスのパフォーマンス収集を続行しますが、syslogの受信を停止します
C. コレクターはsyslogなどの着信イベントをドロップします。しかし、パフォーマンスコレクションを傾斜させる
D. コレクターはイベントをバッファリングします
Answer: (解答を表示する)

最新問題: 19
管理者は、SMTPをLinuxサーバー上の重要なプロセスとして定義します。SMTPプロセスが停止した場合、FortiSIEMはどのイベントタイプでクリティカルイベントを生成しますか？
A. PH_DEV_MON_SMTP_STOP
B. Postfix-Mail-Slop
C. PH_DEV_MON_PROC_STOP
D. Generic_SMTP_Process_Exit
Answer: A (メーッセージを残す)

最新問題: 20
展示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

イベントがFortiSIEMのイベント受信時間、レポートIP、およびユーザー属性によって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. 8つの結果が表示されます

B. 4つの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. 2つの結果が表示されます

Answer: C (メーッセージを残す**)**