Splunk.SPLK-1002.v2026-06-01.q250

試験コード：	SPLK-1002
試験名称：	Splunk Core Certified Power User Exam
認証ベンダー：	Splunk
無料問題の数：	250
バージョン：	v2026-06-01
ページの閲覧量：	102
問題集の閲覧量：	2575

https://www.jpnshiken.com/shiken/Splunk.SPLK-1002.v2026-06-01.q250.html

質問: **1**
セカンダリ検索を実行するワークフロー アクション タイプはどれですか?
A. ポスト
B. ドリルダウン
C. 取得
D. 検索
正解: (正解を表示します)
正解はD.検索です。
ワークフローアクションは、イベント内のフィールドと他のWebリソース間の様々なインタラクションを可能にするナレッジオブジェクトです。ワークフローアクションは、HTMLリンクの作成、HTTP POSTリクエストの生成、フィールド値に基づく二次検索の開始などを行うことができます1。
Splunk Web を使用して設定できるワークフロー アクションには、GET、POST、Search2 の 3 種類があります。
* GET ワークフロー アクションは、特定の値で Google 検索を実行したり、外部の WHOIS データベースに対してドメイン名クエリを実行したりするための一般的な HTML リンクを作成します2。
* POSTワークフローアクションは、指定されたURIへのHTTP POSTリクエストを生成します。このアクションタイプを使用すると、関連するフィールド値のセットを使用して外部の課題管理システムにエントリを作成するなどの操作が可能になります2。
* 検索ワークフロー アクションは、特定の時間範囲2 におけるインデックス内の ipaddress フィールド値と http_status フィールド値の特定の組み合わせの出現を検索する検索など、イベントの特定のフィールド値を使用するセカンダリ検索を開始します。
したがって、二次検索を実行するワークフロー アクション タイプは検索です。
参考文献:
* Splexicon:ワークフローアクション
* Splunk Webのワークフローアクションについて

質問: **2**
検索ではマクロはどのように参照されますか?
A. macroname コマンドを使用します。
B. マクロコマンドを使用します。
C. マクロ名をバッククォート文字 (') で囲みます。
D. マクロ名を一重引用符 (') で囲みます。
正解: (正解を表示します)

説明
正解は C です。マクロ名をバッククォート文字 (`) で囲みます。
マクロは、SPLコードの一部を異なる検索で再利用するための手段です。マクロは引数（変数）を取ることができ、マクロ呼び出し時に異なる値に置き換えることができます。また、マクロ内に別のマクロを含めることも可能で、これはネストされたマクロと呼ばれます1。
検索でマクロを参照するには、マクロ名をバッククォート文字 () で囲む必要があります。例えば、引数を1つ取る「my_macro」というマクロがある場合、次の構文を使用して検索で参照できます。
| my_macro(引数) | ...
これにより、マクロ名と引数が、マクロ定義に含まれるSPLコードに置き換えられます。例えば、マクロ定義が以下の場合：
[my_macro(引数)] ソースタイプを検索=$引数$
そして、検索では次のように参照します。
index=main | my_macro(web) | ホスト別の統計カウント
これによりマクロが展開され、次の SPL コードが実行されます。
index=main | search sourcetype=web | 統計情報（ホスト別）
参考文献:
検索で検索マクロを使用する

質問: **3**
GET ワークフロー アクションを作成するために必要な情報には、次のうちどれが含まれますか? (該当するものをすべて選択してください。)
A. 検索時にユーザーが誘導される URI の名前。
B. 検索時にユーザーが誘導される URI。
C. ワークフローアクションの名前
D. 検索時にイベントアクションメニューに表示されるラベル。
正解: **B,C,D** (コメントを発表する)

質問: **4**
マクロが 3 つの引数を受け入れるには何が必要ですか?
A. マクロの名前は(3)で終わります。
B. マクロの名前は(3)で始まります。
C. マクロの引数数設定が3以上です。
D. 何もなし。すべてのマクロは任意の数の引数を受け入れることができます。
正解: (正解を表示します)
説明
引数を受け入れるマクロを作成するには、マクロ名の末尾に引数の数を括弧で囲んで指定する必要があります1。例えば、my_macro(3) は3つの引数を受け入れるマクロです。マクロ名の引数の数は、定義内の引数の数と一致する必要があります1。したがって、選択肢Aは正解ですが、選択肢B、C、Dは不正解です。

質問: **5**
次の記述のうち、計算フィールドについて説明しているものはどれですか? (該当するものをすべて選択してください)
A. 計算フィールドは検索バーで使用できます。
B. 計算フィールドは抽出されたフィールドに基づいて作成できます。
C. 計算フィールドはホストとソースタイプにのみ適用できます。

D. 計算フィールドは、eval コマンドを使用して計算を実行するためのショートカットです。
正解: (正解を表示します)
参照：
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

質問: **6**
少なくとも 1 つの REJECT イベントを含むトランザクション内のすべての寄与イベントを識別するには、どの構文が正しいですか。
A. インデックスメイン | REJECT トランスセッションID
B. インデックスメイン | トランザクションセッションID | 検索拒否
C. インデックス=メイン | トランザクションセッションID | そのトランザクション=拒否
D. インデックス=メイン | トランザクションセッションID | トランザクション=拒否"
正解: (正解を表示します)
説明
トランザクションコマンドは、1つ以上のフィールドで共通の値を持つイベントをトランザクション2にグループ化するために使用されます。トランザクションコマンドは、各イベントグループにトランザクションIDを割り当て、各トランザクション2に対してduration、eventcount、eventlistなどの新しいフィールドを作成します。少なくとも1つのREJECTイベントを含むトランザクション内のすべての寄与イベントを識別するには、次の構文を使用できます :index=main | transaction sessionid | search REJECT2。この検索は、まずイベントをセッションIDでグループ化し、次にどのイベント2にもREJECTを含まないトランザクションを除外します。したがって、オプションBは正解ですが、オプションA、C、Dはトランザクションコマンドまたは検索コマンドの正しい構文に従っていないため不正解です。

質問: **7**
次の eval ステートメントがあるとします。
... | eval field1 = if(isnotnull(field1),field1,0), field2 = if(isnull(field2), "NO-VALUE", field2) 次のどれが fillnull を使用した場合と同等でしょうか?
A. ... | fillnull values=(0,"NO-VALUE") fields=(field1,field2)
B. fillnull を使用した同等の式はありません
C. ... | fillnull フィールド1 | fillnull 値="NO-VALUE" フィールド2
D. ... | fillnull 値=0 フィールド1 | fillnull フィールド2
正解: (正解を表示します)
fillnull コマンドは、特定のフィールドの null 値を置き換えるために使用できます。与えられた eval ステートメントと同等の正しい式は、fillnull を 2 回使用することです。1 回は field1 で null 値を 0 に置き換え、もう 1 回は field2 で null 値を "NO-VALUE" に置き換えます。
参考文献:
Splunk ドキュメント - fillnull コマンド

質問: **8**
計算フィールドは、次のコマンドのどれを使用して、反復的、長い、または複雑な変換を実行するためのショートカットですか?
A. トランザクション
B. ルックアップ
C. 統計
D. 評価
正解: (正解を表示します)
正解はD.evalです。

計算フィールドとは、検索時にeval式を用いてイベントに追加されるフィールドです。計算フィールドは、イベント内に既に存在する2つ以上のフィールドの値を使用して計算を実行できます。計算フィールドは、Splunk Webまたはprops.confファイルで定義できます。他の抽出フィールドと同様に、検索、レポート、ダッシュボード、データモデルで使用できます1。
計算フィールドは、evalコマンドを用いて、反復的、長大、あるいは複雑な変換を実行するためのショートカットです。evalコマンドは、式を用いてフィールドを作成または変更するために使用されます。evalコマンドは、フィールドまたは値に対して、数学演算、文字列演算、日付と時刻演算、比較演算、論理演算などの演算を実行できます2。
たとえば、price と tax という 2 つのフィールドの合計である total という新しいフィールドを作成する場合は、次のように eval コマンドを使用できます。
| 評価合計=価格+税金
ただし、この新しいフィールドを複数の検索、レポート、またはダッシュボードで使用したい場合は、毎回evalコマンドを記述する代わりに、計算フィールドを作成できます。Splunk Webで計算フィールドを作成するには、「設定」>「フィールド」>「計算フィールド」に移動し、新しいフィールド名（total）、ソースタイプ名（sales）、およびeval式（price+tax）を入力します。これにより、検索時にソースタイプがsalesであるすべてのイベントに追加されるtotalという名前の計算フィールドが作成されます。その後、eval式を記述することなく、他の抽出フィールドと同様にtotalフィールドを使用できます1。
その他のオプションは計算フィールドとは関係がないため、正しくありません。これらのオプションは以下のとおりです。
* A. トランザクション: このコマンドは、共通の値を持つイベントを、トランザクションと呼ばれる単一のレコードにグループ化するために使用されます。トランザクションは複数のイベントと複数のソースにまたがることができ、
* 関連しているが連続していないイベントを相関させるのに役立ちます3。
* B. lookup: このコマンドは、CSVファイルやデータベースなどの外部ソースから取得したフィールドを追加してイベントを拡充するために使用されます。lookupは、ホスト、ソース、ソースタイプ、その他の抽出されたフィールドなど、既存のフィールドの値に基づいてイベントにフィールドを追加できます。
* C. stats: このコマンドは、検索結果のフィールドの要約統計 (カウント、合計、平均など) を計算するために使用されます。1 つ以上のフィールドでデータをグループ化および集計するために使用できます。
参考文献:
* 計算フィールドについて
* evalコマンドの概要
* トランザクションコマンドの概要
* [lookupコマンドの概要]
* [統計コマンドの概要]

質問: **9**
ほとんどの大規模な Splunk 環境で、イベントをフィールド別にグループ化するために使用できる最も効率的なコマンドは何ですか?
A. 参加
B. 統計
C. ストリーム統計
D. トランザクション
正解: **(**正解を表示します**)**
説明/参照: https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html

質問: **10**
Splunk Common Information Model (CIM) アドオンをインストールする利点は何ですか?
A. ユーザーは業界標準に準拠したワークフロー アクションを作成できます。
B. データを正規化するための標準化されたフィールド名とタグのセットをユーザーに提供します。
C. ユーザーはデータの 3D モデルを作成し、これらの視覚化をエクスポートできます。
D. ユーザーは、検索ジョブ インスペクターの結果に基づいてイベントを項目別に分類できます。

正解: **B** (コメントを発表する)
Splunk CIMアドオンは、標準化されたフィールド名とタグのセットを提供し、データを正規化します。Splunk CIMアドオンは、標準化されたフィールド名とデータモデルのセットを提供し、ユーザーはさまざまなソースからのデータを共通の形式に正規化および分類できます。これにより、データの相互運用性が高まり、異なるデータソース間でより高速で一貫性のあるレポート作成と検索が可能になります。参考資料 :Splunkドキュメント - 共通情報モデル（CIM）

質問: **11**
evalcommands の結果はどこに保存されますか?
A. フィールド内。
B. インデックス内。
C. KV ストア内。
D. データベース内。
正解: **A** (コメントを発表する)
説明/リファレンス: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Eval

質問: **12**
タグに関する次の記述のうち正しいものはどれですか? (該当するものをすべて選択してください。)
A. タグは大文字と小文字を区別しません。
B. タグはフィールド/値のペアに基づいています。
C. タグは検索に基づいてイベントを分類します。
D. タグはデータをより理解しやすくするために設計されています。
正解: (正解を表示します)
タグに関する以下の記述は正しい: タグはフィールド/値のペアに基づいており、タグはイベントを分類する。
タグは、フィールドまたはフィールド値に適用できるカスタムラベルで、追加の情報を提供します。
データの文脈や意味をタグで表現できます。タグは、共通の概念や
テーマ。タグは、検索コマンド、設定ファイル、ユーザーアカウントなど、さまざまな方法で作成できます。
インターフェースなど。タグの特徴は次のとおりです。
タグはフィールド/値のペアに基づいています。つまり、タグは特定のフィールド名と
特定のフィールド値。例えば、フィールド名「status」に「alert」というタグを作成し、
フィールド値が「critical」の場合、ステータスが「critical」のイベントにのみ「alert」タグが付きます。
彼らに適用されます。
タグは検索に基づいてイベントを分類します。つまり、タグは検索文字列によって定義され、
タグ付けしたいイベントに一致するタグを作成します。例えば、検索に「web」というタグを作成できます。
文字列sourcetype=access_combined。これは、検索文字列に一致するイベントのみが表示されることを意味します。
sourcetype=access_combined には「web」タグが適用されます。
タグに関する以下の記述は誤りです。タグは大文字と小文字を区別しません。タグはデータを
より理解しやすくなっています。タグは大文字と小文字を区別し、データの検索性を高めるために設計されています。タグは
大文字と小文字を区別します。これは、タグがフィールド名とフィールド値の大文字と小文字を正確に一致させる必要があることを意味します。
関連付けられています。例えば、フィールド名「ステータス」に「アラート」というタグを作成し、フィールド値「
critical」と入力すると、status=CRITICALまたはStatus=criticalのイベントには適用されません。タグは、

データの検索性向上:タグを使用すると、データ内の関連するイベントやパターンを簡単に見つけることができます。
共通の概念やテーマ。例えば、検索文字列に 'web'というタグを作成すると、
sourcetype=access_combined の場合、tag=web を使用して、Web アクティビティに関連するすべてのイベントを見つけることができます。

質問: **13**
検索ワークフロー アクションを作成するときに必須となるフィールドはどれですか?
A. 検索文字列
B. データモデル名
C. 権限設定
D. 評価文
正解: **(**正解を表示します**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction

質問: **14**
フィールド サイドバー内の興味深いフィールドは、過去に要求したフィールドに基づいています。
A. 真
B. 偽
正解: **B (**コメントを発表する**)**

質問: **15**
次のワークフロー アクションのうち、検索結果から実行できるものはどれですか (該当するものをすべて選択してください)。
A. 取得
B. ポスト
C. ルックアップ
D. 検索
正解: **A,B,D (**コメントを発表する**)**
前述の通り、ワークフローアクションにはGETとPOSTの2種類があります1。どちらの種類のワークフローアクションも、ワークフローアクションが設定されているイベントフィールド値をクリックすることで、検索結果から実行できます1。もう1つの種類のワークフローアクションは '検索'で、これはフィールド値に基づいて別の検索を実行します1。したがって、選択肢A、B、Dは正解ですが、選択肢CはLOOKUPがワークフローアクションの種類ではないため不正解です。

質問: **16**
フィールド抽出 (FX)の正規表現モードはいつ使用すればよいですか？（該当するものをすべて選択してください）
A. スペース、カンマ、またはパイプ文字で区切られたデータの場合。
B. CSV (カンマ区切り値) ファイル内のデータの場合。
C. フィールドを区切る複数の異なる文字を含むデータの場合。
D. 非構造化データの場合。
正解: **(**正解を表示します**)**
フィールド抽出器 (FX)の正規表現モードは、複数の異なる文字列を含むデータに使用する必要があります。
フィールドを区切る文字や非構造化データに使用できます。正規表現モードでは、
サンプルイベントを選択し、抽出したいフィールドをハイライトすると、フィールド抽出ツールが通常の

類似のイベントを一致させ、そこからフィールドを抽出する式。参照フィールド抽出の構築を参照
フィールド抽出ツールを使用 - Splunkドキュメントおよびフィールド抽出ツール: メソッドの選択ステップ - Splunk
ドキュメント。

質問: **17**
次の知識オブジェクト/構成はどのような順序で適用されますか?
A. フィールド抽出、フィールドエイリアス、ルックアップ
B. ルックアップ、フィールドエイリアス、フィールド抽出
C. フィールドエイリアス、フィールド抽出、ルックアップ
D. フィールド抽出、ルックアップ、フィールドエイリアス
正解: **A (**コメントを発表する**)**

質問: **18**
ここで示すコマンドは次のいずれかを実行します: コマンド: |outputlookup products.csv
A. products.csv というファイルの内容を返します。
B. 検索結果をproducts.csvというファイルに書き込みます。
正解: **(**正解を表示します**)**

質問: **19**
イベントの種類に関する次の記述のうち正しいものはどれですか? (該当するものをすべて選択してください)
A. イベント タイプにタグを付けることができます。
B. イベント タイプは、検索に基づいてイベントを分類します。
C. イベント タイプは、知識をキャプチャして共有するための便利な方法です。
D. イベントタイプには時間範囲を含める必要があります。
正解: **(**正解を表示します**)**

質問: **20**
トランザクション内のイベントに共通するものは何ですか?
A. トランザクション内のすべてのイベントは同じタイムスタンプを持つ必要があります。
B. トランザクション内のすべてのイベントは同じソースタイプを持つ必要があります。
C. トランザクション内のすべてのイベントは、まったく同じフィールド セットを持つ必要があります。
D. トランザクション内のすべてのイベントは、1 つ以上のフィールドによって関連付けられる必要があります。
正解: **D (**コメントを発表する**)**
参照：

トランザクションとは、フィールド、時間、またはその両方など、いくつかの共通特性を持つイベントのグループです。トランザクションは、transaction コマンドを使用するか、props.conf で transactiontype=true を指定してイベントタイプを定義することで作成できます。トランザクション内のイベントには、互いに関連付ける共通フィールドが 1 つ以上あります。例えば、Web ログ内の各ユーザーセッションの一意の識別子である JSESSIONID に基づいてトランザクションを作成できます。トランザクション内のイベントは、タイムスタンプ、ソースタイプ、または完全に同じフィールドセットを持つ必要はありません。トランザクションを定義する 1 つ以上のフィールドを共有していれば十分です。

質問: **21**
以下に示すマクロ定義に基づいて、検索文字列でマクロを実行する正しい方法は何ですか?
A. Convert_sales (ユーロ, €, 79)"
B. Convert_sales (ユーロ、€、.79)
C. Convert_sales ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)
正解: **(**正解を表示します**)**
参照:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros 検索文字列内でマクロを実行する正しい方法は、macro_name($arg1$, $arg2$, ...) のように記述します。$arg1$、$arg2$ などはマクロの引数です。この場合、マクロ名は convert_sales で、通貨、シンボル、レートの3つの引数を取ります。引数はドル記号で囲み、カンマで区切ります。したがって、マクロを正しく実行するには、convert_sales ($euro$, $€$, .79) と記述します。

質問: **22**
次の検索のうち、マクロの有効な使用法を示しているものはどれですか? (該当するものをすべて選択してください)

A. オプションD
B. オプションC
C. オプションA
D. オプションB
正解: **(**正解を表示します**)**

質問: **23**
eval コマンドの 'if' 関数には、次の 3 つの引数 (順番に) が必要です。
A. ブール式、真の場合は結果、偽の場合は結果
B. 真の場合の結果、偽の場合の結果、ブール式
C. 偽の場合の結果、真の場合の結果、ブール式
D. ブール式、偽の場合の結果、真の場合の結果
正解: **(**正解を表示します**)**
evalコマンドの「if」関数には、次の3つの引数（順番に）が必要です :ブール式、ifの結果
trueの場合、falseの場合は結果を返します。evalコマンドは、新しいフィールドを作成したり、フィールドの値を変更したりできる検索コマンドです。
既存のフィールドに対して計算や変換を実行することで、フィールドの値を変更します。evalコマンドは様々な

フィールドに対してさまざまな操作を実行する関数。ff」関数は、使用できる関数の1つです。
evalコマンドを使用して、フィールドの条件評価を実行します。ff」関数は3つの引数を取ります。
真または偽に評価されるブール式、ブール式が真の場合に返される結果、
ブール式が偽の場合に返される結果。ff」関数は2つのうちの1つを返します。
ブール式の評価に基づく結果。

質問: **24**
次の記述のうち、Filed Extractor (FX) の使用法を説明しているものはどれですか。
A. フィールド抽出機能は、検索時にすべてのフィールドを自動的に抽出します。
B. フィールド抽出機能は、PERL を使用して生のイベントからフィールドを抽出します。
C. 抽出されたフィールドはナレッジ オブジェクトとして保持されます。
D. フィールド抽出を使用して抽出されたフィールドは永続的ではないため、検索ごとに定義する必要があります。
正解: **C** (コメントを発表する)
フィールド抽出 (FX) は、グラフィカル インターフェイスを使用するか、正規表現を手動で編集することで、イベントからフィールドを抽出できるツールです2。FX を使用すると、ナレッジ オブジェクトとして保存されるフィールド抽出を作成できます。ナレッジ オブジェクトは、データに知識を追加して検索や分析を容易にするために作成するエンティティです2。フィールド抽出は、正規表現、区切り文字、キーと値のペアなどのさまざまな手法を使用して生データからフィールドを抽出する方法です2。FX を使用してフィールド抽出を作成すると、検索時にデータに適用されるナレッジ オブジェクトとして保存できます2。また、フィールド抽出を管理して、組織内の他のユーザーと共有することもできます2。したがって、オプション C が正解ですが、オプション A、B、および D は FX の使用方法について説明していないため不正解です。

質問: **25**
次の eval ステートメントで、ステータスが 503 の場合、description の値は何でしょうか? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")
A. 説明フィールドに値が含まれません。
B. 説明フィールドには値 0 が含まれます。
C. 説明フィールドには 内部サーバー エラー」という値が含まれます。
D. このステートメントは不完全であるため、Splunk ではエラーが発生します。
正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.1.1/検索リファレンス/条件関数

質問: **26**
次の検索は何をしますか?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. ユーザーの合計数をコーンドッグごとに分割したテーブルを作成します。
B. ユーザー別に分けられたミステリーミート コーンドッグの合計数のテーブルを作成します。
C. ユーザーごとに分けられた、食べたアメリカン ドッグのすべての種類の数を含むテーブルを作成します。
D. ベジタリアン アメリカン ドッグごとにユーザーの合計数をグループ化するテーブルを作成します。
正解: (正解を表示します)
以下の検索文字列は、ミステリーミート コーンドッグの合計数をユーザー別に分類した表を作成します。

| ユーザー別の統計カウント | corndog=mysterymeat
検索文字列は次のことを行います。
statsコマンドを使用して、userフィールドの各値に対するイベント数を計算します。statsコマンドは、userとcountの2つの列を持つテーブルを作成します。
where コマンドを使用して、corndog フィールドの値で結果をフィルタリングします。where コマンドは、corndog が mysterymeat と等しい行のみを保持します。
したがって、検索文字列により、ミステリーミート コーンドッグの合計数をユーザー別に分割したテーブルが作成されます。

質問: **27**
次の定義のうち、2 つの引数を受け入れる 「samplemacro」という名前のマクロを説明しているものはどれですか。
A. 例マクロ [1,2]
B. サンプルマクロ(1,2)
C. u amp -CJEUCXG (2)
D. サンプルマクロ[2]
正解: **(**正解を表示します**)**
Splunkでは、マクロは引数を受け入れることができます。2つの引数を取るマクロの正しい構文は、macro_name(引数1, 引数2)です。この場合、マクロの名前はsamplemacroで、2つの引数を受け入れるため、正しい形式はsamplemacro(1,2)です。この構文により、マクロに動的な値を渡すことができ、指定された引数に基づいて検索を動的に変更できます。
参考文献:
* Splunk ドキュメント - マクロ

質問: **28**
この検索に当てはまるのは次のうちどれですか? (該当するものをすべて選択してください。) 検索:
sourcetype=access* |フィールド アクション 製品 ステータス
A. 3列のテーブルを返します
B. 抽出されるフィールドを制限します
C. 検索語 「fields AND action AND productId AND status」を含むすべてのイベントを検索します。
D. パフォーマンスを向上させるためにテーブルコマンドを使用します
正解: **B,D (**コメントを発表する**)**

質問: **29**
次のどれが eval コマンドの tostring 関数で使用できますか (該当するものをすべて選択してください)。
A. "16進数"
B. "カンマ"
C. "10進数"
D. "期間"
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X を参照してください。
2CY.29
evalコマンドのtostring関数は、数値を文字列値に変換します。オプションで2番目の引数を指定して、文字列値の形式を指定できます。指定可能な形式は以下のとおりです。
* hex: 数値を 16 進文字列に変換します。
* カンマ: 数値の千の位を区切るためにカンマを追加します。
* duration: 数値を 「2h 3m 4s」などの人間が読める期間文字列に変換します。

したがって、tostring 関数では形式 A、B、および D を使用できます。

質問: **30**
次の検索のうち、Privileged という名前のタグを含むイベントを返すものはどれですか。
A. タグ=特権
B. タグ=プライベート*
C. タグ=priv*
D. タグ=特権
正解: **(**正解を表示します**)**
説明/参照: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

質問: **31**
デフォルトでは、Splunk Common Information Model (CIM) アドオンでアクセラレーションはどのように構成されますか?
A. オフ
B. オン
C. ソースタイプに基づいて自動的に決定されます。
D. データ ソースに基づいて自動的に決定されます。
正解: **(**正解を表示します**)**
説明
デフォルトでは、アクセラレーションはSplunk Common Information Model (CIM)アドオンのデータソースに基づいて自動的に決定されます。Splunk CIMアドオンは、ネットワークトラフィック、Webアクティビティ、認証など、様々なドメインに共通するデータモデルを提供するアプリです。CIMアドオンを使用すると、定義済みのフィールドとタグを使用してデータを正規化および拡充できます。また、CIMアドオンはデータモデルを高速化し、検索やレポートの高速化を図ることもできます。アクセラレーションは、データモデルのサマリーデータを事前に計算し、tsidxファイルに保存する機能です。アクセラレーションにより、データモデルを使用する検索やレポートのパフォーマンスと効率を向上させることができます。
デフォルトでは、CIMアドオンのデータソースに基づいてアクセラレーションが自動的に決定されます。つまり、Splunkはデータ量、データタイプ、データモデルの複雑さなどの要素に基づいて、各データモデルに対してアクセラレーションを有効化または無効化するかどうかを決定します。ただし、 設定」メニューを使用するか、datamodels.confファイルを編集することで、各データモデルに対してアクセラレーションを手動で有効化または無効化することもできます。

質問: **32**
次の記述のうち、Filed Extractor (FX) の使用法を説明しているものはどれですか。
A. フィールド抽出機能は、検索時にすべてのフィールドを自動的に抽出します。
B. フィールド抽出機能は、PERL を使用して生のイベントからフィールドを抽出します。
C. 抽出されたフィールドはナレッジ オブジェクトとして保持されます。
D. フィールド抽出を使用して抽出されたフィールドは永続的ではないため、検索ごとに定義する必要があります。
正解: **C (**コメントを発表する**)**

説明
フィールド抽出 (FX) は、グラフィカル インターフェイスを使用するか、正規表現を手動で編集することで、イベントからフィールドを抽出できるツールです2。FX を使用すると、ナレッジ オブジェクトとして保存されるフィールド抽出を作成できます。ナレッジ オブジェクトは、データに知識を追加して検索や分析を容易にするために作成するエンティティです2。フィールド抽出は、正規表現、区切り文字、キーと値のペアなどのさまざまな手法を使用して生データからフィールドを抽出する方法です2。FX を使用してフィールド抽出を作成すると、検索時にデータに適用されるナレッジ オブジェクトとして保存できます2。また、フィールド抽出を管理して、組織内の他のユーザーと共有することもできます2。したがって、オプション C が正解ですが、オプション A、B、および D は FX の使用方法について説明していないため不正解です。

質問: **33**
次のどの記述が、ユーザーがトランザクション コマンドと統計コマンドのどちらかを選択するのに役立ちますか?
A. statscan は IP アドレスのみを使用してイベントをグループ化します。
B. トランザクション コマンドはより高速かつ効率的です。
C. トランザクション コマンドには 1000 イベントの制限があります。
D. イベントを単一の相関イベントとして表示する必要がある場合は、統計を使用します。
正解: **C (**コメントを発表する**)**
説明/リファレンス: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction

質問: **34**
次の検索で 1 つのトランザクションではなく複数のトランザクションが生成される理由は何でしょうか?

```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

Events (641) Patterns **Statistics (147)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src	num_events	total_events
107.3.146.207	1000 1000 1000 405	3405
108.65.113.83	1000 120	1120
109.169.32.135	1000 1000 79	2079
11.17.160.129	1000 1000 238	2238

maxspan オプションは含まれていません。
トランザクション コマンドには、トランザクションあたり 1000 イベントの制限があります。
トランザクションとコマンドを併用することはできません。
統計リスト()関数が使用されます。
正解:
maxspan オプションは含まれません1。
Splunkでは、transactionコマンドを使用して、共通の特性を持つイベントを単一のtransaction1にグループ化します。デフォルトでは、transactionコマンドは一致するすべてのイベントを単一のtransaction1にグループ化します。
ただし、maxspanオプションを使用してトランザクションの期間を制限することができます1。トランザクション内の最初のイベントと最後のイベントの間の期間がmaxspan値を超える場合、トランザクションコマンドは新しいトランザクションを開始します1。
したがって、検索に maxspan オプションが含まれていない場合、トランザクション内の最初のイベントと最後のイベント間の時間範囲がデフォルトの maxspan 値 1 を超えると、トランザクション コマンドによって 1 つのトランザクションではなく複数のトランザクションが生成されることがあります。
検索で maxspan オプションを使用する方法の例を次に示します。
index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h この検索では、トランザクションコマンドは、同じsomeuniqefield値を持つイベントを単一のトランザクションにグループ化します。ただし、トランザクション内の最初のイベントと最後のイベントの間の時間間隔が1時間を超えない場合に限ります1。時間間隔が1時間を超える場合、トランザクションコマンドは新しいトランザクションを開始します1。
Explanation:
正解は

質問: **35**
フィールド抽出ワークフローの検証ステップ中:
回答を選択してください。
A. 定義したいフィールドと一致しない値を削除できます
B. データの出所を検証できます
C. フィールド抽出を変更することはできません
正解: (正解を表示します)
フィールド抽出ワークフローの検証ステップで、一致しない値を削除できます。
定義したいフィールド2. 検証ステップでは、入力された値を確認および編集できます。
FXによって抽出された値が正しく、一貫性があることを確認します2。
一致するものをクリックしてメニューから 値の削除」を選択することで、一致した値を除外できます。これで、一致した値がリストから除外されます。
フィールド抽出を行い、それに応じて正規表現を更新します2。したがって、オプションAが正解ですが、オプション
BとCは、フィールドの検証ステップで実行できるアクションではないため、不正解です。
抽出ワークフロー。

質問: **36**
次の検索で 1 つのトランザクションではなく複数のトランザクションが生成される理由は何でしょうか?

```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

Events (641) Patterns Statistics (147) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src ◇	num_events ◇	total_events ◇
107.3.146.207	1000	3405
	1000	
	1000	
	405	
108.65.113.83	1000	1120
	120	
109.169.32.135	1000	2079
	1000	
	79	
11.17.160.129	1000	2238
	1000	
	238	

A. maxspan オプションは含まれません。
B. トランザクション コマンドには、トランザクションあたり 1000 イベントの制限があります。
C. トランザクションとコマンドを併用することはできません。
D. 統計リスト()関数が使用されます。
正解: **A** (コメントを発表する)
Splunkでは、transactionコマンドを使用して、共通の特性を持つイベントを単一のtransaction1にグループ化します。デフォルトでは、transactionコマンドは一致するすべてのイベントを単一のtransaction1にグループ化します。
ただし、maxspanオプションを使用してトランザクションの期間を制限することができます1。トランザクション内の最初のイベントと最後のイベントの間の期間がmaxspan値を超える場合、トランザクションコマンドは新しいトランザクションを開始します1。
したがって、検索に maxspan オプションが含まれていない場合、トランザクション内の最初のイベントと最後のイベント間の時間範囲がデフォルトの maxspan 値 1 を超えると、トランザクション コマンドによって 1 つのトランザクションではなく複数のトランザクションが生成されることがあります。
検索で maxspan オプションを使用する方法の例を次に示します。
index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h この検索では、トランザクションコマンドは、同じsomeuniqefield値を持つイベントを単一のトランザクションにグループ化します。ただし、トランザクション内の最初のイベントと最後のイベントの間の時間間隔が1時間を超えない場合に限ります1。時間間隔が1時間を超える場合、トランザクションコマンドは新しいトランザクションを開始します1。

質問: **37**
Splunk 共通情報モデル (CIM) は、どのようなタイプの知識オブジェクトのコレクションですか?
A. KVストア

B. ルックアップ
C. 保存された検索
D. データモデル
正解: **(**正解を表示します**)**
Splunk共通情報モデル（CIM）は、共通の構造を適用するデータモデルの集合体である。
あらゆるソースからのデータに、命名規則とデータモデルを適用します。データモデルとは、データモデルを定義する知識オブジェクトの一種です。
データセット内のフィールドの構造と関係。データモデルは1つ以上のデータセットを持つことができ、それらは
データの異なる側面を表すデータモデルのサブセット。例えば、ネットワークトラフィックデータ
モデルには、すべてのトラフィック、DNS、HTTPなどのデータセットがあります。CIMには、28個の事前構成されたデータモデルが含まれており、
認証、ネットワークトラフィック、ウェブ、電子メールなど、さまざまなドメインをカバーします。CIMは、
データモデル、ドキュメント、一貫性をサポートするツールのJSONファイルを含むアドオン。
検索時の効率を最大化するためのデータの正規化処理23
1: Splunk Core Certified Power User Track、10ページ。2: Splunkドキュメント、Splunkの概要
共通情報モデル 1. 3: Splunkbase、Splunk 共通情報モデル (CIM) 2。

質問: **38**
少なくとも 1 つの REJECT イベントを含むトランザクション内のすべての寄与イベントを識別するには、どの構文が正しいですか。
A. インデックスメイン | REJECT トランスセッションID
B. インデックスメイン | トランザクションセッションID | 検索拒否
C. インデックス=メイン | トランザクションセッションID | そのトランザクション=拒否
D. インデックス=メイン | トランザクションセッションID | トランザクション=拒否"
正解: **B (**コメントを発表する**)**
トランザクションコマンドは、1つ以上のフィールドで共通の値を持つイベントをトランザクション2にグループ化するために使用されます。トランザクションコマンドは、各イベントグループにトランザクションIDを割り当て、各トランザクション2に対してduration、eventcount、eventlistなどの新しいフィールドを作成します。少なくとも1つのREJECTイベントを含むトランザクション内のすべての寄与イベントを識別するには、次の構文を使用できます :index=main | transaction sessionid | search REJECT2。この検索は、まずイベントをセッションIDでグループ化し、次にどのイベント2にもREJECTを含まないトランザクションを除外します。したがって、オプションBは正解ですが、オプションA、C、Dはトランザクションコマンドまたは検索コマンドの正しい構文に従っていないため不正解です。

質問: **39**
次の検索のうち、マクロの有効な使用法を示しているものはどれですか? (該当するものをすべて選択してください)

```
index=main source=mySource oldField=* |`makeMyField(oldField)`| table _time newField

index=main source=mySource oldField=* | stats if(`makeMyField(oldField)`) | table _time
newField

index=main source=mySource oldField=* |eval newField=`makeMyField(oldField)`| table _time
newField

index=main source=mySource oldField=* | "`newField(`makeMyField(oldField)`)`" | table _time
newField
```

A. オプションC
B. オプションA
C. オプションB
D. オプションD

正解: **A,B** (コメントを発表する)

質問: **40**
履歴検索に指定された時間範囲は、_____ を定義します。-------回答に疑問があります
A. 静的結果の時間範囲
B. その時間範囲に一致するインデックスから取得されたデータの量
C. タイムラインに表示されるデータストリームの量のことです。
正解: (正解を表示します)

質問: **41**
なぜ stats コマンドの代わりに transaction コマンドが使用されるのでしょうか?
A. トランザクション コマンドでは、検索時間のパフォーマンスが向上します。
B. トランザクション コマンドは、フィールドに対して計算を実行できます。
C. トランザクション コマンドは、各イベントの生データを保持します。
D. トランザクション コマンドはリソースをあまり消費しません。
正解: (正解を表示します)
トランザクションコマンドは、イベントをグループ化し、生のイベントデータを保持する必要がある場合に使用します。これは、コンテキストが重要であり、各イベントの元の詳細を維持する必要がある場合に不可欠です。
参照：
Splunk ドキュメント - トランザクションコマンド
Splunk の回答 - トランザクションと統計の使い分け

質問: **42**
Splunk Common Information Model (CIM) アドオンに含まれるデータ モデルは次のうちどれですか (該当するものをすべて選択してください)。
A. ユーザー権限
B. アラート
C. データベース
D. メール
正解: (正解を表示します)
Splunk Common Information Model (CIM) アドオンには、さまざまなデータモデルが含まれており、さまざまなソースからのデータを正規化して、クロスソースのレポート作成と分析を可能にします。含まれるデータモデルのうち、アラート（オプション B）とメール（オプション D）はCIMの一部です。アラートデータモデルはアラートやインシデントに関連するデータに使用され、メールデータモデルはメールメッセージやトランザクションに関連するデータに使用されます。ユーザー権限（オプション A）とデータベース（オプション C）はCIMに含まれるデータモデルではなく、それぞれデータアクセス制御の側面と特定の種類のデータソースに関係しており、CIMの定義済みデータモデルの範囲外です。

質問: **43**
どちらの記述が正しいでしょうか?
A. ピボットはデータセットの作成に使用されます。
B. データ モデルはランダムに構造化されたデータセットです。
C. ピボットはレポートとダッシュボードの作成に使用されます。
D. ほとんどの場合、各 Splunk ユーザーは独自のデータ モデルを作成します。

正解: **(**正解を表示します**)**
説明/参考資料: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

質問: **44**
eval コマンドの 'if' 関数には、次の 3 つの引数 (順番に) が必要です。
A. ブール式、真の場合は結果、偽の場合は結果
B. 真の場合の結果、偽の場合の結果、ブール式
C. 偽の場合の結果、真の場合の結果、ブール式
D. ブール式、偽の場合の結果、真の場合の結果
正解: **(**正解を表示します**)**
eval コマンドの 'if' 関数には、次の 3 つの引数（この順序で）が必要です :ブール式、true の場合の結果、false の場合の結果。eval コマンドは、計算や変換を実行して新しいフィールドを作成したり、既存のフィールドを変更したりできる検索コマンドです。eval コマンドは、さまざまな関数を使用して、フィールドに対してさまざまな操作を実行できます。'if' 関数は、eval コマンドでフィールドの条件評価を実行するために使用できる関数の 1 つです。'if' 関数には、true または false に評価されるブール式、ブール式が true の場合に返される結果、ブール式が false の場合に返される結果という 3 つの引数が必要です。'if' 関数は、ブール式の評価に基づいて 2 つの結果のいずれかを返します。

質問: **45**
計算フィールドは次のどれに基づくことができますか?
A. タグ
B. 抽出されたフィールド
C. ルックアップの出力フィールド
D. 検索文字列から生成されたフィールド
正解: **(**正解を表示します**)**
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields
計算フィールドは、別のフィールドの値に基づいて作成されるフィールドです。
計算フィールドを使用して、データに追加情報を加えたり、データをより有用なものに変換したりすることができます。
計算フィールドは、生のフィールドから抽出されたフィールドに基づいて作成できます。
正規表現、区切り文字、キーと値のペアなど、様々な方法でデータを分類します1。したがって、オプションBは
正解ですが、オプションA、C、Dはタグ、ルックアップの出力フィールド、生成されたフィールドが不正解です。
検索文字列から抽出されたフィールドの種類ではありません。

質問: **46**
どの検索が「アラート」タグを「ホスト」フィールドに制限しますか?
A. タグ=アラート
B. ホスト::タグ::アラート
C. タグ==アラート
D. タグ::ホスト=アラート
正解: **D (**コメントを発表する**)**
以下の検索では、「alert」タグが「host」フィールドに制限されます。
タグ::ホスト=アラート
検索では次のことが行われます。

タグ構文を使用して、イベントをタグでフィルタリングします。タグは、フィールドまたはフィールド値に適用できるカスタムラベルであり、データに追加のコンテキストや意味を与えることができます。
タグフィルターとして tag::host=alert を指定します。これは、ホストフィールドまたはホストフィールド値に「alert」タグが適用されたイベントのみを返すことを意味します。
等号 (=) を使用して、タグとフィールドまたはフィールド値が完全に一致することを示します。

質問: **47**
scats コマンドの代わりに transaction コマンドを使用する必要があるのはどのような場合ですか?
A. 複数の値をグループ化する必要がある場合。
B. 検索結果において期間が関係ない場合。
C. 開始制約と終了制約に基づいてグループ化する必要がある場合。
D. トランザクションに 1000 を超えるイベントがある場合。
正解: **D** (コメントを発表する)

質問: **48**
次の検索は何をしますか?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. ユーザーの合計数をコーンドッグごとに分割したテーブルを作成します。
B. ユーザー別に分けられたミステリーミート コーンドッグの合計数のテーブルを作成します。
C. ユーザーごとに分けられた、食べたアメリカン ドッグのすべての種類の数を含むテーブルを作成します。
D. ベジタリアン アメリカン ドッグごとにユーザーの合計数をグループ化するテーブルを作成します。
正解: (正解を表示します)
以下の検索文字列は、ミステリーミート コーンドッグの合計数をユーザー別に分類した表を作成します。
| ユーザー別の統計カウント | corndog=mysterymeat
検索文字列は次のことを行います。
statsコマンドを使用して、userフィールドの各値に対するイベント数を計算します。statsコマンドは、userとcountの2つの列を持つテーブルを作成します。
where コマンドを使用して、corndog フィールドの値で結果をフィルタリングします。where コマンドは、corndog が mysterymeat と等しい行のみを保持します。
したがって、検索文字列により、ミステリーミート コーンドッグの合計数をユーザー別に分割したテーブルが作成されます。

質問: **49**
アクション タイプがリンクに設定されている場合に使用できるワークフロー アクション メソッドはどれですか。
A. 取得
B. 置く
C. 検索

D. 更新
正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETワークフローアクション
GETワークフローアクションを定義する
手順
[設定] > [フィールド] > [ワークフロー アクション] に移動します。
[新規] をクリックして、新しいワークフロー アクション フォームを開きます。
アクションのラベルを定義します。
ラベル フィールドを使用すると、フィールドまたはイベント ワークフロー メニューに表示されるテキストを定義できます。
ラベルは静的にすることも、関連するフィールドの値を含めることもできます。
ワークフロー アクションがデータ内の特定のフィールドまたはイベント タイプに適用されるかどうかを決定します。
「次のフィールドのみに適用」を使用して、1つまたは複数のフィールドを指定します。フィールドを指定すると、ワークフローは
アクションは、イベントメニューまたはフィールドメニューにこれらのフィールドがあるイベントにのみ表示されます。
空白にするかアスタリスクを入力すると、そのアクションがすべてのフィールドのメニューに表示されます。
1つ以上のイベントタイプを識別するには、「次のイベントタイプにのみ適用」を使用します。イベントタイプを識別する場合
タイプを選択すると、ワークフロー アクションは、そのイベント タイプに属するイベントのイベント メニューにのみ表示されます。
「アクションの表示」では、アクションをイベントメニューに表示するかどうかを決定します。フィールド
メニュー、または両方を選択します。
アクションタイプをリンクに設定します。
URI では、フィールド値を送信する外部リソースの場所の URI を指定します。
ラベル設定と同様に、フィールドの値を宣言するときは、フィールド名を
ドル記号。
GETアクションでURI経由で渡される変数は、送信時に自動的にURLエンコードされます。つまり、
単語や句読点の間にスペースがある値を含めることができます。
「リンクを開く」で、ワークフローアクションを現在のウィンドウに表示するか、
リンクを新しいウィンドウで開きます。
Link メソッドを取得に設定します。
[保存] をクリックして、ワークフロー アクション定義を保存します。

質問: **50**
高速、最適化、詳細はすべて選択可能な検索モードです。
A. 偽
B. 真
正解: (正解を表示します)

質問: **51**
ブラッドは「SpecialProjectX」というタグを作成しました。このタグは、team=support、location=Austin、release=Fuji といった複数のフィールド/値のペアに関連付けられています。サポートチームに関連する SpecialProjectX イベントの結果を絞り込むには、ブラッドはどのような検索を実行すればよいでしょうか？
A. タグ=SpecialProjectX

B. タグ::チーム=SpecialProjectX
C. タグ::サポート-SpecialProjectX
D. タグ!=富士、オースティン
正解: **(**正解を表示します**)**
Splunk のタグを使用すると、ユーザーは共通のラベルに複数のフィールドと値のペアを割り当てることができます。
タグでフィルタリングするための正しい構文は tag::<field>=<tag_name> です。
tag::team=SpecialProjectX は、team=support がタグ SpecialProjectX に関連付けられている結果をフィルタリングします。
tag=SpecialProjectX は、サポート チームだけでなく、SpecialProjectX に関連付けられているすべてのイベントを検索します。
tag::Support-SpecialProjectX は構文が正しくありません。
tag!=Fuji,Austin は SpecialProjectX タグを使用してフィルタリングされないため、正しくありません。
参考: Splunk ドキュメント - タグ

質問: **52**
計算フィールドは次のどれに基づくことができますか?
A. タグ
B. 抽出されたフィールド
C. ルックアップの出力フィールド
D. 検索文字列から生成されたフィールド
正解: **B (**コメントを発表する**)**
参照：
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

質問: **53**
Splunk 共通情報モデル (CIM) とは何ですか?
A. CIM は、Splunk で完全にサポートできるアプリのエコシステムを定義します。
B. CIM は、Splunk に正常にオンボードされるためにすべてのデータ ソースが満たす必要がある前提条件です。
C. CIM は、さまざまなソースおよびソース タイプからのデータを正規化する方法を提供します。
D. CIM は、ソフトウェア ベンダー間のデータ交換イニシアチブです。
正解: **C (**コメントを発表する**)**
Splunk Common Information Model (CIM) は、異なるソースやソースタイプからのデータを正規化するための手法を提供します。CIM は、Web、ネットワーク、メールなど、異なるデータタイプに対して共通のフィールドとタグのセットを定義します。これにより、異なるソースからのデータを一貫した方法で検索および分析できます。

質問: **54**
イベント タイプは保存されたレポートとどう違うのでしょうか?
A. イベント タイプを使用してデータをカテゴリに整理することはできません。
B. イベント タイプには、検索結果の書式設定が含まれます。
C. イベント タイプは Splunk ユーザーと共有したり、ダッシュボードに追加したりできます。
D. イベント タイプには時間範囲が含まれません。
正解: **D (**コメントを発表する**)**
こんにちは、Bingです。Splunk Core Power User Technologiesに関するご質問にお答えできます。

正解は D です。イベント タイプには時間範囲は含まれません。
説明は次のとおりです。
* イベントタイプは、同じ検索文字列1に一致するイベントを照合することで、データの意味を理解するのに役立つ分類システムです。イベントタイプは検索時にイベントに適用され、検索語句やフィルターとして使用できます12。
* 保存済みレポートは、検索アクションから保存された結果で、イベントの統計情報や視覚化を表示できます3。保存済みレポートはいつでも実行でき、実行するたびに最新の結果が取得されます34。保存済み
* レポートは他のユーザーと共有したり、ダッシュボードに追加したりできます4。
* イベントタイプと保存済みレポートの主な違いは、イベントタイプには時間範囲が指定されないのに対し、保存済みレポートには時間範囲が指定されることです14。つまり、イベントタイプはどの期間のイベントにも一致しますが、保存済みレポートは作成時または実行時に指定された時間範囲に限定されます14。

質問: **55**
データ モデルは、どのような 3 種類のデータセットで構成できますか?
A. ピボット、検索、およびイベント。
B. ピボット、イベント、トランザクション。
C. 検索、トランザクション、ピボット。
D. イベント、検索、トランザクション。
正解: **D (**コメントを発表する**)**
説明/参照: https://docs.splunk.com/Splexicon:Datamodeldataset

質問: **56**
Splunk Common Information Model (CIM) アドオンに含まれるデータ モデルは次のうちどれですか (該当するものをすべて選択してください)。
A. アラート
B. メール
C. データベース
D. ユーザー権限
正解: **(**正解を表示します**)**
参照：
Splunk Common Information Model (CIM) アドオンは、事前に構築されたデータモデルとナレッジオブジェクトのコレクションであり、さまざまなソースからのデータを正規化し、分析とレポート作成を容易にします3。CIM アドオンには、アラート、メール、データベース、ネットワークトラフィック、Web など、さまざまなドメインをカバーする複数のデータモデルが含まれています3。したがって、選択肢 A、B、C は CIM アドオンに含まれるデータモデルの名前であるため正解です。選択肢 D は不正解です。ユーザー権限は CIM アドオンのデータモデルの名前ではないためです。

質問: **57**
timechart コマンドを使用する場合、_time の間隔を指定するためにどのオプション引数が使用されますか?
A. ビン
B. によって
C. スパン
D. オーバー
正解: **(**正解を表示します**)**
包括的かつ詳細なステップバイステップ

Splunk の timechart コマンドは、データの時系列視覚化を生成するために使用されます。
span 引数は、_time フィールドの間隔 (またはビン サイズ) を指定するために使用されます。
使用例:
CSS
コピー編集
インデックス=_internal | タイムチャート スパン=1時間カウント
このコマンドは、_time が 1 時間間隔にグループ化されたタイムチャートを作成します。
bin は、bin コマンドで数値または時間ベースのフィールドをグループ化するために使用されますが、timechart に固有のものではありません。
by は、特定のフィールドで結果を分割するために使用されますが、間隔は定義しません。
over は timechart の有効な引数ではありません。
参考: Splunk ドキュメント - timechart コマンド

質問**: 58**
次の変換コマンドのうち、トランザクションで使用できるものはどれですか?
A. チャート、タイムチャート、統計、イベント統計
B. チャート、タイムチャート、統計、差分
C. チャート、タイムライン、データモデル、ピボット
D. チャート、timecha:t、統計、ピボット
正解**: (**正解を表示します**)**
正解は A. chart、timechart、stats、eventstats です。
変換コマンドは、検索結果の形式を表やグラフに変更するコマンドです。
統計計算を実行したり、視覚化を作成したり、さまざまな方法でデータを操作したりするために使用できます1。
トランザクションとは、共通の値を共有し、何らかの形で関連しているイベントのグループです。トランザクションは、transactionコマンドを使用するか、transactiontypes.confファイル2でトランザクションタイプを作成することで定義できます。
いくつかの変換コマンドをトランザクションで使用すると、トランザクションフィールドに基づいて表やグラフを作成できます。これらのコマンドには以下が含まれます。
* chart: このコマンドは、2つ以上のフィールド間の関係を示す表またはグラフを作成します。
* 値の集計、発生回数のカウント、統計の計算に使用できます3。
* timechart: このコマンドは、フィールドの経時的な変化を示す表またはグラフを作成します。傾向、パターン、外れ値をプロットするのに使用できます4。
* stats: このコマンドは、検索結果のフィールドの要約統計 (カウント、合計、平均など) を計算します。1 つ以上のフィールドでデータをグループ化および集計するために使用できます5。
* eventstats: このコマンドは、statsコマンドと同様に検索結果のフィールドの要約統計を計算しますが、各イベントに新しいフィールドとして結果を追加します。イベントと全体の統計を比較するのに使用できます。
これらのコマンドは、トランザクションフィールドを引数として指定することで、トランザクションに適用できます。例えば、「ログイン」というトランザクションタイプがあり、userフィールドに基づいてイベントをグループ化し、durationやeventcountなどのフィールドがある場合、以下のコマンドをトランザクションに適用できます。
* | chart count by user: このコマンドは、各ユーザーのトランザクション数を示す表またはグラフを作成します。
* | timechart span=1h avg(duration) by user : このコマンドは、各ユーザーの 1 時間あたりのトランザクションの平均期間を示す表またはグラフを作成します。
* | stats sum(eventcount) as total_events by user : このコマンドは、すべてのトランザクションにわたる各ユーザーのイベントの合計数を示すテーブルを作成します。
* | eventstats avg(duration) as avg_duration : このコマンドは、すべてのトランザクションの平均期間を示す avg_duration という新しいフィールドを各トランザクションに追加します。

その他のオプションは、変換コマンドではないコマンド、またはトランザクションで使用できないコマンドが含まれているため無効です。これらのコマンドは次のとおりです。
* diff: このコマンドは2つの検索結果を比較し、それらの差異を表示します。これは変換コマンドではなく、トランザクションでは機能しません。
* datamodel: このコマンドは、Splunk でデータを整理および分類する方法であるデータモデルからデータを取得します。これは変換コマンドではなく、トランザクションでは機能しません。
* pivot: このコマンドはピボットレポートを作成します。ピボットレポートは、グラフィカルインターフェースを使用してデータモデルのデータを分析する方法です。これは変換コマンドではなく、トランザクションでは機能しません。
参考文献:
* 変換コマンドについて
* 取引について
* チャートコマンドの概要
* タイムチャートコマンドの概要
* 統計コマンドの概要
* [eventstatsコマンドの概要]
* [diffコマンドの概要]
* [データモデルコマンドの概要]
* [ピボットコマンドの概要]

質問: **59**
レポートに関して正しいのは次のうちどれですか?
A. レポートをスケジュールできます。
B. レポートはナレッジ オブジェクトです。
C. レポートはスクリプトを実行できます。
D. 上記のすべて。
正解: **(**正解を表示します**)**

質問: **60**
データ モデルのルート データセットについて正しい記述は次のうちどれですか。
A. ルート トランザクション データセットの場合は、トランザクション コマンドを含める必要があります。
B. ルート検索データセットである限り、変換コマンドを含めることができます。
C. ベース検索に関連付けられたナレッジ オブジェクトが自動的に含まれます。
D. 変換コマンドのない基本検索のみを含めることができます。
正解: **C (**コメントを発表する**)**
Splunk では、データモデルのルートデータセットは、データモデルの残りの部分を構築する基盤要素です。ルートデータセットには、検索、トランザクション、イベントベースのデータセットなど、さまざまなタイプがあります。ルートデータセットの重要な機能の一つは、ベース検索に関連付けられたナレッジオブジェクトを自動的に継承することです。これらのナレッジオブジェクトには、ベース検索用に定義されたフィールド抽出、ルックアップ、エイリアス、計算フィールドなどが含まれており、ルートデータセットには最初から必要なコンテキスト情報がすべて含まれています。これにより、ユーザーはベース検索のナレッジオブジェクトを再定義することなく、このデータセット上に子データセットやオブジェクトを追加して構築できます。

質問: **61**
eval はどのようなタイプのコマンドですか?

A. 一部のモードでのストリーミング
B. レポート生成
C. 分散ストリーミング
D. 集中型ストリーミング
正解: (正解を表示します)
正解はC. 分散ストリーミングです。これは、evalコマンドが次のような種類のコマンドであるためです。
結果が検索ヘッドに送られる前に、インデクサー上で実行できます。これにより、検索ヘッドに送られるデータの量が削減されます。
転送する必要のあるデータが少なくなり、検索パフォーマンスが向上します。分散ストリーミングコマンドは、
各イベントまたは結果を個別に評価し、他のイベントや結果に依存せずに評価します。
Splunk ドキュメント1 から、コマンドの種類とそれが検索パフォーマンスに与える影響について説明します。

質問: **62**
以下の検索を説明する記述はどれですか？（該当するものをすべて選択してください）Index=main I transaction clientip host maxspan=30s maxpause=5s
A. 最初のイベントと最後のイベントの間隔は 30 秒以内です。
B. 最初のイベントと最後のイベントの間隔は 5 秒以内です。
C. トランザクション内のイベントが 5 秒以内に発生しました。
D. 同じクライアント IP とホストを共有するイベントをグループ化します。
正解: (正解を表示します)

質問: **63**
フィールド抽出ツール（FX）は、カスタムフィールドを抽出するために使用されます。このカスタムフィールドを使用してレポートを作成できます。作成したレポートは、組織内の他のユーザーと共有できます。
組織内の別のユーザーが共有レポートを実行しても結果が返されない場合、その理由は何でしょうか?
(該当するものをすべて選択してください。)
A. 高速モードが有効です。
B. ダッシュボードは非公開です。
C. 抽出はプライベートです。
D. レポートを実行している組織内のユーザーには、インデックスへのアクセス権がありません。
正解: (正解を表示します)
説明/参照:

質問: **64**
元のフィールドに基づいてフィールドエイリアスが作成されました。その後、変換コマンドを使用せずにスマートモードで検索を実行します。結果にはどのフィールド名が表示されますか？

A. 両方とも 興味深いフィールド」リストに表示されますが、イベントの少なくとも 20% に表示される場合のみです。
B. 検索でエイリアスが指定されている場合のみ、両方が [すべてのフィールド] リストに表示されます。
C. 元のフィールドは [すべてのフィールド] リストにのみ表示され、エイリアスは [関心のあるフィールド] リストにのみ表示されます。
D. エイリアスは [すべてのフィールド] リストにのみ表示され、元のフィールドは [興味深いフィールド] リストにのみ表示されます。
正解: (正解を表示します)

質問: **65**
トランザクションの最初のイベントを定義するオプションは次のどれですか?
A. で始まる
B. と
C. 開始
D. 最初のイベント
正解: (正解を表示します)
正解はA. startswithです。
説明は次のとおりです。
トランザクション コマンドは、さまざまな制約を満たすイベントに基づいてトランザクションを検索するために使用されます12。
トランザクションは、各メンバーの生のテキスト (_raw フィールド)、最も古いメンバーの時刻と日付のフィールド、および各メンバーのその他のすべてのフィールドの結合で構成されます1。
startswith オプションは、検索用語またはイベントに一致する式を指定して、トランザクションの最初のイベントを定義するために使用されます13。
たとえば、| transaction clientip JSESSIONID startswith="view" は、clientip フィールドと JSESSIONID フィールドに基づいてトランザクションを作成し、各トランザクションの最初のイベントの _raw フィールドに 「view」という用語が含まれます2。

質問: **66**
次の検索で 1 つのトランザクションではなく複数のトランザクションが生成される理由は何でしょうか?

```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

Events (641) Patterns **Statistics (147)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src	num_events	total_events
107.3.146.207	1000	3405
	1000	
	1000	
	405	
108.65.113.83	1000	1120
	120	
109.169.32.135	1000	2079
	1000	
	79	
11.17.160.129	1000	2238
	1000	
	238	

A. maxspan オプションは含まれません。
B. トランザクション コマンドには、トランザクションあたり 1000 イベントの制限があります。
C. トランザクションとコマンドを併用することはできません。
D. 統計リスト()関数が使用されます。
正解: **A** (コメントを発表する)
Splunkでは、transactionコマンドを使用して、共通の特性を持つイベントを単一のtransaction1にグループ化します。デフォルトでは、transactionコマンドは一致するすべてのイベントを単一のtransaction1にグループ化します。
ただし、maxspanオプションを使用してトランザクションの期間を制限することができます1。トランザクション内の最初のイベントと最後のイベントの間の期間がmaxspan値を超える場合、トランザクションコマンドは新しいトランザクションを開始します1。
したがって、検索に maxspan オプションが含まれていない場合、トランザクション内の最初のイベントと最後のイベント間の時間範囲がデフォルトの maxspan 値 1 を超えると、トランザクション コマンドによって 1 つのトランザクションではなく複数のトランザクションが生成されることがあります。
検索で maxspan オプションを使用する方法の例を次に示します。

index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h この検索では、トランザクションコマンドは、同じsomeuniqefield値を持つイベントを単一のトランザクションにグループ化します。ただし、トランザクション内の最初のイベントと最後のイベントの間の時間間隔が1時間を超えない場合に限ります1。時間間隔が1時間を超える場合、トランザクションコマンドは新しいトランザクションを開始します1。

質問: **67**
アクション タイプがリンクに設定されている場合に使用できるワークフロー アクション メソッドはどれですか。
A. 取得
B. 置く
C. 検索
D. 更新
正解: **A (**コメントを発表する**)**
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction GET ワークフロー アクションを定義する手順 [設定] > [フィールド] > [ワークフロー アクション] に移動します。
[新規] をクリックして、新しいワークフロー アクション フォームを開きます。
アクションのラベルを定義します。
ラベル フィールドを使用すると、フィールドまたはイベント ワークフロー メニューに表示されるテキストを定義できます。
ラベルは静的にすることも、関連するフィールドの値を含めることもできます。
ワークフロー アクションがデータ内の特定のフィールドまたはイベント タイプに適用されるかどうかを決定します。
「次のフィールドのみに適用」を使用して、1つまたは複数のフィールドを指定します。フィールドを指定すると、そのフィールドを含むイベントのイベントメニューまたはフィールドメニューにのみ、ワークフローアクションが表示されます。空白のままにするかアスタリスクを入力すると、すべてのフィールドのメニューにアクションが表示されます。
「次のイベントタイプにのみ適用」を使用して、1つ以上のイベントタイプを指定します。イベントタイプを指定すると、そのイベントタイプに属するイベントのイベントメニューにのみワークフローアクションが表示されます。
[アクションの表示場所] では、アクションを [イベント] メニュー、[フィールド] メニュー、またはその両方のいずれに表示するかを決定します。
アクションタイプをリンクに設定します。
URI では、フィールド値を送信する外部リソースの場所の URI を指定します。
ラベル設定と同様に、フィールドの値を宣言するときは、ドル記号で囲まれたフィールドの名前を使用します。
GETアクションでURI経由で渡される変数は、送信時に自動的にURLエンコードされます。つまり、単語間にスペースや句読点を含む値を含めることができます。
[リンクを開く場所] で、ワークフロー アクションを現在のウィンドウに表示するか、新しいウィンドウでリンクを開くかを決定します。
Link メソッドを取得に設定します。
[保存] をクリックして、ワークフロー アクション定義を保存します。

質問: **68**
ピボットを使用する可能性が高いのはどのユーザー グループですか?
A. 建築家
B. ユーザー
C. 管理者
D. ナレッジマネージャー
正解: **(**正解を表示します**)**

質問: **69**

Splunk の計算フィールドに関する次の記述のうち正しいものはどれですか?
A. 計算フィールドを連結してより複雑なフィールドを作成することはできません
B. 計算フィールドを連結して、より複雑なフィールドを作成できます。
C. 計算フィールドはダッシュボードでのみ使用できます。
D. 計算フィールドは保存されたレポートでのみ使用できます。
正解: (正解を表示します)
説明
正解は B です。計算フィールドを連結して、より複雑なフィールドを作成できます。
計算フィールドは、検索時にeval式を使用してイベントに追加されるフィールドです。イベントに既に存在する2つ以上のフィールドの値を使って計算を実行するために使用できます。
計算フィールドは、Splunk Webまたはprops.confファイルで定義できます。他の抽出フィールドと同様に、検索、レポート、ダッシュボード、データモデルで使用できます1。
計算フィールドを連結して、より複雑なフィールドを作成することもできます。つまり、計算フィールドを別の計算フィールドの入力として使用できます。例えば、 合計」という名前の計算フィールドがあり、 価格」と 税金」という2つのフィールドの値を合計するとします。この合計フィールドを使用して、 割引」という名前の別の計算フィールドを作成し、合計フィールドに割引率を適用することができます。これを行うには、次のように、合計フィールドを参照するeval式を使用して割引フィールドを定義する必要があります。
割引 = 合計 * 0.9
これにより、各イベント 2 の合計フィールド値の 90% に等しい、discount という名前の新しいフィールドが作成されます。
参考文献:
計算フィールドについて
計算フィールドの連鎖

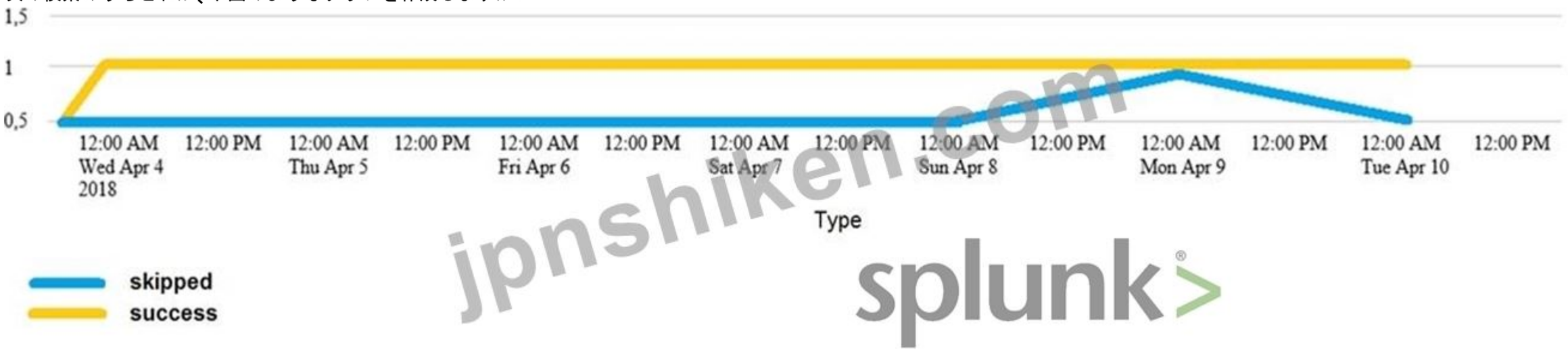
質問: **70**
検索結果が生成されるたびにアラートをトリガーする必要はありません。
A. 偽
B. 真
正解: (正解を表示します)

質問: **71**
次のナレッジ オブジェクト/構成はどのような順序で適用されますか?
A. フィールドエイリアス、フィールド抽出、ルックアップ
B. フィールド抽出、フィールドエイリアス、ルックアップ
C. フィールド抽出、ルックアップ、フィールドエイリアス
D. ルックアップ、フィールドエイリアス、フィールド抽出
正解: (正解を表示します)
説明/参考資料: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge

質問: **72**
Splunk 共通情報モデル (CIM) とは何ですか?
A. CIM は、Splunk に正常にオンボードされるためにすべてのデータ ソースが満たす必要がある前提条件です。
B. CIM は、さまざまなソースおよびソース タイプからのデータを正規化する方法を提供します。
C. CIM は、Splunk で完全にサポートできるアプリのエコシステムを定義します。
D. CIM は、ソフトウェア ベンダー間のデータ交換イニシアチブです。

正解: (正解を表示します)
Splunk共通情報モデル（CIM）は、異なるデータソースからデータを正規化する手法を提供します。
ソースとソースタイプ。CIMは、例えば以下のような様々なデータタイプに対して共通のフィールドとタグのセットを定義します。
ウェブ、ネットワーク、メールなど、さまざまなソースから一貫した方法でデータを検索・分析できます。
方法。

質問: **73**
次の検索のうちどれが、下図のようなグラフを作成しますか?



A. index_internal seourcetype=Savesplunker | フィールド ソースタイプ、ステータス | トランザクション ステータス maxspan-id | 開始カウント 状態
B. index_internal seourcetype=Savesplunker | フィールド sourcetype、status | トランザクション ステータス maxspan-id | チャート count states by -time
C. index_internal seourcetype=Savesplunker | フィールド sourcetype、status | トランザクション ステータス maxspan-id | タイムチャート ステータス別カウント
D. これらの検索のいずれも、類似のグラフを生成しません。
正解: **C** (コメントを発表する)
次の検索を実行すると、次のようなグラフが作成されます。
index_internal sourcetype=Savesplunker | fields sourcetype、status | transaction status maxspan=1d | timechart count by status 検索では次のことが行われます。
index_internal を使用して、Splunk ログとメトリックを含む内部インデックスを指定します。
sourcetype=Savesplunker を使用して、Splunk Enterprise Security アプリを示すソースタイプでイベントをフィルターします。
イベント内のソースタイプとステータスのフィールドのみを保持するために、ソースタイプとステータスのフィールドを使用します。
トランザクション ステータス maxspan=1d を使用して、トランザクション内の最初のイベントと最後のイベント間の最大期間が 1 日であるステータス フィールドに基づいて、イベントをトランザクションにグループ化します。
タイムチャート カウント バイ ステータスを使用して、時間の経過に伴う各ステータス値のトランザクション数を示す時間ベースのチャートを作成します。
グラフには次の内容が示されています。
黄色と青色の 2 本の線がある折れ線グラフです。
x 軸には、2018 年 4 月 4 日水曜日から 2018 年 4 月 10 日火曜日までの日付がラベル付けされています。
Y軸には0から15までの数字が付けられます。
黄色の線は「発送済み」、青い線は「成功」を表します。
黄色の線は 0 から 15 まで着実に増加していますが、青い線は 0 から 5 まで急激に増加し、その後 0 まで減少し、その後 10 まで急激に増加しています。
グラフのタイトルは「タイプ」です。

したがって、選択肢Cが正解です。

質問: **74**
Splunk 共通情報モデル (CIM) について正しいのは次のうちどれですか?
正解:
DSplunk Common Information Model (CIM)は、定義済みのデータモデル
のセットを含むアプリです。
あらゆるソースからのデータに共通の構造と命名規則を適用します。CIMを使用すると、データを
異なる情報源から一貫性と整合性のある方法でデータを取得します。CIMには、28個の事前設定されたデータセットが含まれており、
認証、ネットワークトラフィック、ウェブ、電子メールなど、さまざまなドメインをカバーしています。
CIMはデフォルトでデータモデルアクセラレーションがオンに設定されており、最適化されていることを意味します。
より高速な検索と分析を実現します。データモデルアクセラレーションは、データの要約データを作成し、維持します。
モデル化することで、データモデルを使用して検索を実行するときにスキャンする必要がある生データの量を削減できます。
モデル。
Splunk Core Certified Power User Track、10ページ。: Splunkドキュメント、Splunk Commonについて
情報モデル。

質問: **75**
次のどれがイベント タイプとして保存できますか?
A. index-server_472 sourcetype-BETA_494 code-488 I 統計はコードごとにカウントされます
B. index=server_472 sourcetype=BETA_494 code=488 [I inputlookup append=t servercode.csv]
C. index=server_472 sourcetype=BETA_494 code=488 コード > 200 の I 統計
D. インデックス=server_472 ソースタイプ=BETA_494 コード-488
正解: **D (**コメントを発表する**)**
Splunkのイベントタイプは、データを分類して保存された検索であり、データ内の特定のパターンや条件を簡単に検索できます。イベントタイプを保存する際、検索は基本的に、データの変換や集計などの操作を実行せずに、条件に基づいてイベントをフィルタリングする必要があります。オプションの詳細は次のとおりです。
A: 検索インデックスサーバー472 ソースタイプBETA_494 コード488 | コード別の統計カウントは集計操作 ロード別の統計カウント）を実行するため、イベントタイプとして保存するには適していません。イベントタイプは、データを集計または変換することなく分類することを目的としています。
B: 検索インデックス=server_472 sourcetype=BETA_494 code=488 [| inputlookup append=t servercode.csv] にはサブ検索と入力ルックアップが含まれており、通常は外部データに基づいてイベントを拡充またはフィルター処理するために使用されます。
この複雑さは、単純なイベントの分類を超えています。
C: 検索 index=server_472 sourcetype=BETA_494 code=488 | stats where code > 200 には、変換コマンド (stats) 内にフィルタリング条件が含まれていますが、これもデータの変換のため、イベント タイプの定義には適していません。
D: 検索 index=server_472 sourcetype=BETA_494 code-488 は、データを変換または集約せずに、インデックス、ソースタイプ、およびコード フィールド条件に基づいてイベントをフィルター処理するだけなので、正解です。
イベントの構造や内容を変更せずに、特定の基準に基づいてデータを分類するため、イベント タイプとして保存するのに適しています。

質問: **76**
次の eval ステートメントがあるとします。
...| eval fieldl - if(isnotnull(fieldl),fieldl,0), field2 = if(isnull<field2>, "NO-VALUE", fieid2) 次のどれが f ilinull を使用した場合と同等でしょうか?

A. f ilinull を使った同等の式はありません
B. ... t filinull 値=(0,"NO-VALUE") フィールド=(fieldl,field2)
C. ... l filinull value=0 fieldl l fillnull fields
D. ... フィールド1にnullを記入 フィールド2に値="NO-VALUE"を記入
正解: **(**正解を表示します**)**
fillnullコマンドは、1つ以上のフィールドのnull値を指定された値に置き換えます。valuesオプションを使用すると、対応するフィールドのnull値を埋める値をカンマ区切りで指定できます。fieldsオプションを使用すると、fillnullコマンドを適用するフィールドをカンマ区切りで指定できます。質問のeval文では、if関数とisnull関数を使用して、field1とfield2にnull値があるかどうかを確認し、それぞれ0と 「NO-VALUE」に置き換えています。fillnullを使用した同等の式は、valuesオプションで0と 「NO-VALUE」を指定し、fieldsオプションでfield1とfield2を指定します。
1: Splunk Core Certified Power User Track、9 ページ。2: Splunk ドキュメント、fillnull コマンド。

質問: **77**
POST ワークフロー アクションを作成するには、次のうちどれが必要ですか?
A. ラベル、URI、検索文字列。
B. XMI 属性、URI、名前。
C. ラベル、URI、投稿引数。
D. URI、検索文字列、時間範囲ピッカー。
正解: **C (**コメントを発表する**)**
説明
POSTワークフローアクションは、検索結果のフィールド値をクリックしたときに、WebサーバーにPOSTリクエストを送信するカスタムアクションです。POSTワークフローアクションは、ラベル名、ベースURL、URIパラメータ、投稿引数、アプリコンテキストなど、さまざまなオプションで設定できます。POSTワークフローアクションを作成するために必要なオプションの1つが投稿引数です。投稿引数は、Webサーバーに追加情報を提供するためにPOSTリクエストの本文で送信されるキーと値のペアです。フィールド名をドル記号で囲むことで、データからフィールド値を含めることができます。

質問: **78**
検索コマンドに関する次の記述のうち正しいものはどれですか?
A. ワイルドカードは使用できません。
B. フィールド値は大文字と小文字を区別して扱われます。
C. 検索パイプラインの先頭でのみ使用できます。
D. 最初のパイプの前の検索文字列とまったく同じように動作します。
正解: **(**正解を表示します**)**
参考: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand searchコマンドは、イベント2に一致する検索文字列に基づいて検索結果をフィルタリングまたは絞り込むために使用されます。searchコマンドは最初のパイプの前の文字列と全く同じように動作します。つまり、search2の最初の部分で使用するのと同じ構文と演算子を使用できます。したがって、選択肢Dは正解ですが、選択肢A、B、Cは不正解です。これらはsearchコマンドに関する記述が誤っているためです。

質問: **79**
Splunk Common Information Model (CIM) アドオンについて説明しているのは次のうちどれですか?
A. CIM アドオンは Splunk 環境に自動的にインストールされます。
B. CIM アドオンには、データの正規化に役立つデータ モデルが含まれています。
C. CIM アドオンには、データをマップする方法を示すダッシュボードが含まれています。
D. CIM アドオンは機械学習を使用してデータを正規化します。
正解: **B (**コメントを発表する**)**

質問: **80**
次のワークフロー アクションのうち、検索結果から実行できるものはどれですか (該当するものをすべて選択してください)。
A. 取得
B. ポスト
C. ルックアップ
D. 検索
正解: **(**正解を表示します**)**

質問: **81**
マクロweekly_sales ⑵には検索文字列が含まれています。
インデックスゲーム I eval 製品売上 = $price$ $AmountS01d$
次のどれが結果を返しますか?
A. 'weekly_sales(3.99, 10)'
B. 'weekly_sales(3.99, 10)
C. 'weekly_sales (3.99, 10)
D. 'weekly_sales(3)
正解: **C (**コメントを発表する**)**
正解はCです。「weekly_sales (3.99, 10)」です。これは、検索マクロは引用符やドル記号なしで引数を受け入れ、引数の数はマクロで定義されたパラメータの数と一致する必要があるためです。その他の選択肢は、引数を引用符またはドル記号で囲んでいるか、マクロが想定する引数の数と異なる数を指定しているため、正しくありません。検索マクロの検索での使用方法の詳細については、Splunkのドキュメント1をご覧ください。

質問: **82**
この検索では、_____がy軸に表示されます。検索: sourcetype=access_combined status!=200 | chart count over host
A. ステータス
B. ホスト
C. カウント
正解: **(**正解を表示します**)**
説明
この検索では、count は y 軸に表示されます2。この検索では、chart コマンドを使用して、ステータスが 2002 以外のイベントについて、ホスト上のイベント数のグラフを作成します。chart コマンドは、over 句の後のフィールドの値ごとに 1 列、by 句 (存在する場合) の後のフィールドの値ごとに 1 行を含むテーブルを作成します2。テーブルの値は、over 句の前の関数を各グループのイベントに適用することで計算されます2。この場合、chart コマンドは、ホストごとに 1 列、ホストごとのイベント数を 1 行含むテーブルを作成します。グラフの

y 軸には、各ホストに適用された count 関数の値が表示されます。したがって、オプション C は正解ですが、オプション A と B は x 軸またはグラフのラベルとして表示されるため不正解です。

質問: **83**
検索用語では大文字と小文字は区別されません。
A. 偽
B. 真
正解: **(**正解を表示します**)**

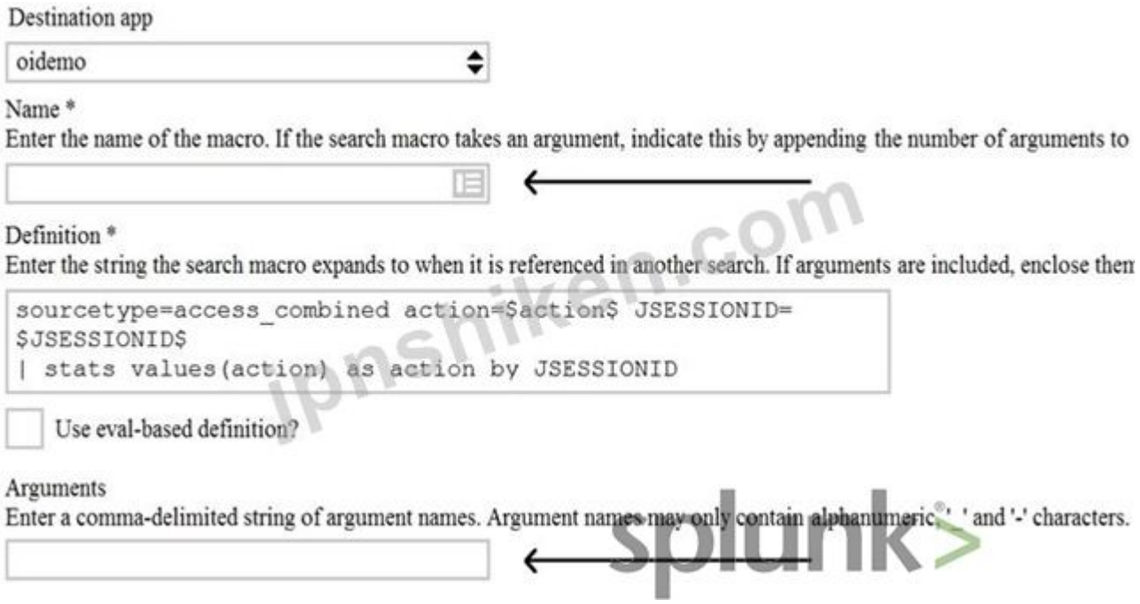
質問: **84**
SPL を使用せずにデータ モデルを使用してレポートとダッシュボード パネルを生成するツールはどれですか。
A. 視覚化タブ
B. ピボット
C. データセット
D. スプランクCIM
正解: **(**正解を表示します**)**
正解はB.ピボット1です。
Splunkでは、ピボットはデータモデルを使用してレポートやダッシュボードパネルを生成するツールです。
ユーザーがSplunkの検索処理言語 $PL）を記述または理解できるようにします1.データモデルにより、Pivotのユーザーは
魅力的なレポートやダッシュボードを作成する1.ピボットユーザーがピボットレポートをデザインする際、データを選択します
作業したいイベントデータのカテゴリを表すモデルを作成します1。次に、データセットを選択します
報告したい特定のデータセットを表すデータモデルです1。これにより、Pivotは強力な
視覚化を作成する必要があるが、SPL1 を深く理解していないユーザー向けのツール。

質問: **85**
次の SPL コマンドを実行した場合、どのような検索結果が期待されますか?
インデックス=ネットワーク NOT ステータスコード=200
A. このフィールドに値がないネットワーク インデックス内のすべてのイベント。
B. ネットワーク インデックス内の StatusCode が 200 を含まないすべてのイベント。ただし、このフィールドに値がないイベントは除きます。
C. ネットワーク インデックス内の StatusCode が 200 を含まないすべてのイベント (このフィールドに値がないイベントを含む)。
D. 構文が正しくないため結果はありません。NOT 演算子の代わりに != フィールド式を使用する必要があります。
正解: **(**正解を表示します**)**
Splunkでは、NOT演算子を使用して検索結果からイベントを除外します。「index=network NOT StatusCode=200」という検索は、「network」インデックス内のStatusCodeが200以外のすべてのイベントを返します。これには、StatusCodeフィールドが存在し、その値が200以外のイベントだけでなく、StatusCodeフィールドが全く存在しないイベントも含まれます。
参照：
SPL（検索処理言語）におけるNOT演算子の使用は、効率的な検索を生成し、Splunkの機能を最大限に活用する方法を説明したSplunkのドキュメントとリソースに記載されている情報と一致しています。

質問: **86**
次の検索では、どのフィールドが x 軸に入力されますか?

index=security sourcetype=linux secure | タイムチャート アクション別カウント
A. アクション
B. ソースタイプ
C. _time
D. 時間
正解: **(**正解を表示します**)**
正解はC._timeです。
timechartコマンドは、時間をX軸として、対応する統計表を含む時系列チャートを作成します1。分割フィールドを指定すると、分割フィールドの各値がチャート内の系列になります1。この場合、分割フィールドはactionです。つまり、チャートには承認、拒否、失敗などの異なるアクションごとに異なる線が表示されます2。count関数は、各時間ビンにおける各アクションのイベント数を計算します1。
たとえば、次の画像は、類似検索3 のアクション別のカウントのタイムチャートを示しています。
ご覧のとおり、x軸には検索の時間範囲を表す_timeフィールドが設定されています。y軸にはcount関数が設定されており、これは各アクションのイベント数を表しています。凡例にはactionフィールドの異なる値が表示されており、これに基づいてチャートが複数の系列に分割されています。
参照：
2: Splunk のタイムチャートコマンドと例 - Mindmajix 1: timechart - Splunk ドキュメント 3:
timechart コマンドの例 - Splunk ドキュメント

質問: **87**
以下のマクロ定義では、マクロを正しく構成するために、名前と引数のフィールドに何を入力する必要がありますか?

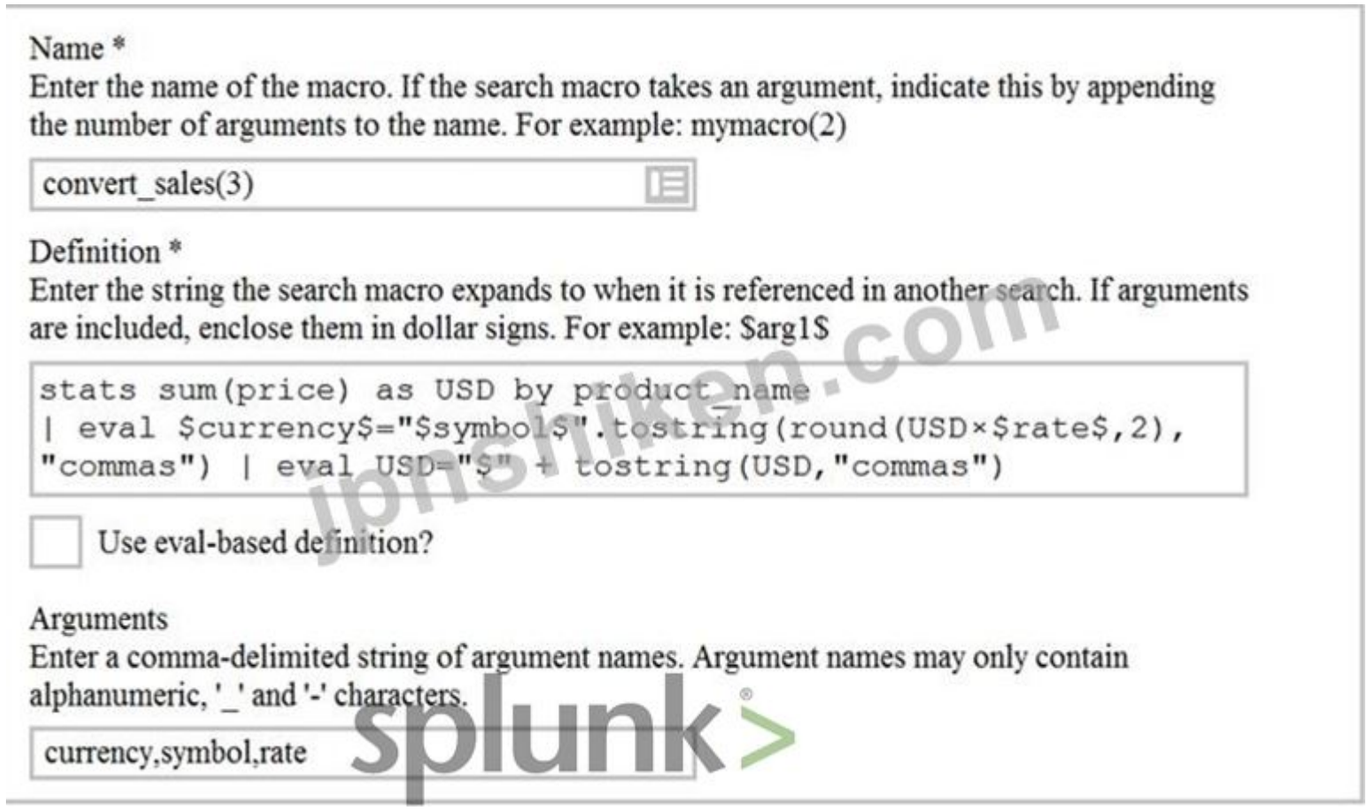


A. マクロ名はsessiontracker(2)で、引数はaction、JESSIONIDです。
B. マクロ名は sessiontracker で、引数は $action$、$JESSIONID$ です。
C. マクロ名はsessiontracker(2)で、引数は$action$、$JESSIONID$で　す。
D. マクロ名は sessiontracker で、引数は action、JESSIONID です。
正解: **(**正解を表示します**)**

質問: **88**

次の変換コマンドのうち、トランザクションで使用できるものはどれですか?
A. チャート、タイムチャート、統計、イベント統計
B. チャート、タイムチャート、統計、差分
C. チャート、タイムライン、データモデル、ピボット
D. チャート、timecha:t、統計、ピボット
正解**: (**正解を表示します**)**
変換コマンドは、検索結果の形式を表やグラフに変換するコマンドです。統計計算、視覚化の作成、さまざまな方法でのデータ操作などに使用できます1。
トランザクションとは、共通の値を共有し、何らかの形で関連しているイベントのグループです。トランザクションは、transactionコマンドを使用するか、transactiontypes.confファイル2でトランザクションタイプを作成することで定義できます。
いくつかの変換コマンドをトランザクションで使用すると、トランザクションフィールドに基づいて表やグラフを作成できます。これらのコマンドには以下が含まれます。
chart: このコマンドは、2つ以上のフィールド間の関係を示す表またはグラフを作成します。値の集計、出現回数のカウント、統計の計算などに使用できます3。
timechart: このコマンドは、フィールドの経時的な変化を示す表またはグラフを作成します。傾向、パターン、外れ値をプロットするのに使用できます4。
stats: このコマンドは、検索結果のフィールドの要約統計 (カウント、合計、平均など) を計算します。1 つ以上のフィールドでデータをグループ化および集計するために使用できます5。
eventstats: このコマンドは、statsと同様に検索結果のフィールドの要約統計を計算しますが、各イベントに新しいフィールドとして結果を追加します。イベントと全体の統計を比較するのに使用できます。
これらのコマンドは、トランザクションフィールドを引数として指定することで、トランザクションに適用できます。例えば、「ログイン」というトランザクションタイプがあり、userフィールドに基づいてイベントをグループ化し、durationやeventcountなどのフィールドがある場合、以下のコマンドをトランザクションに適用できます。
| ユーザー別のチャートカウント: このコマンドは、各ユーザーのトランザクション数を示す表またはチャートを作成します。
| timechart span=1h avg(duration) by user : このコマンドは、各ユーザーの 1 時間あたりのトランザクションの平均期間を示す表またはグラフを作成します。
| stats sum(eventcount) as total_events by user : このコマンドは、すべてのトランザクションにわたる各ユーザーのイベントの合計数を示すテーブルを作成します。
| eventstats avg(duration) as avg_duration : このコマンドは、すべてのトランザクションの平均期間を示す avg_duration という新しいフィールドを各トランザクションに追加します。
その他のオプションは、変換コマンドではないコマンド、またはトランザクションで使用できないコマンドが含まれているため無効です。これらのコマンドは次のとおりです。
diff: このコマンドは2つの検索結果を比較し、それらの差異を表示します。これは変換コマンドではなく、トランザクションでは機能しません。
datamodel: このコマンドは、Splunk でデータを整理および分類する方法であるデータモデルからデータを取得します。これは変換コマンドではなく、トランザクションでは機能しません。
pivot: このコマンドはピボットレポートを作成します。ピボットレポートは、グラフィカルインターフェースを使用してデータモデルのデータを分析する方法です。これは変換コマンドではなく、トランザクションでは機能しません。
Explanation:
正解は
参照：
変換コマンドについて
取引について
チャートコマンドの概要
タイムチャートコマンドの概要
統計コマンドの概要
[eventstats コマンドの概要]
[diffコマンドの概要]
[データ モデル コマンドの概要]
[ピボットコマンドの概要]

質問: **89**
以下に示すマクロ定義に基づいて、検索文字列でマクロを実行する正しい方法は何ですか?



A. Convert_sales (ユーロ, €, 79)"
B. Convert_sales (ユーロ、€、.79)
C. Convert_sales ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)
正解: **B (**コメントを発表する**)**
参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros 検索文字列内でマクロを実行する正しい方法は、macro_name($arg1$, $arg2$, ...) で、$arg1$、$arg2$ などはマクロの引数です。この場合、マクロ名は convert_sales で、通貨、シンボル、レートの3つの引数を取ります。引数はドル記号で囲み、カンマで区切ります。したがって、マクロを実行する正しい方法は convert_sales($euro$, $€$, .79）。

質問: **90**
データ モデル コマンドを使用してデータ モデル内のフィールドを検索する正しい方法はどれですか。
Web データセット内ですか?
A. | データモデル Web 検索 | ファイルされた Web *
B. | 検索データモデル Web Web | ファイルされた Web*
C. | データモデル ウェブ ウェブフィールド | 検索ウェブ*
D. データモデル = web | 検索 web | ファイルされた web*
正解: **(**正解を表示します**)**

データモデルコマンドを使用すると、高速化されたデータモデルに対して検索を実行できます1。構文は
データ モデル コマンドを使用するには、| datamodel <model_name> <dataset_name> [search <search_string>]1 を使用します。
したがって、オプションAは、データモデルコマンドを使用してデータモデル内のフィールドを検索する正しい方法です。
ウェブデータセット内。選択肢BとCはデータモデルの構文に従っていないため不正解です。
コマンド。オプション D は、データ モデル コマンドをまったく使用していないため、不正解です。

質問: **91**
次の検索は何をしますか?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. ユーザーの合計数をコーンドッグごとに分割したテーブルを作成します。
B. ユーザー別に分けられたミステリーミート コーンドッグの合計数のテーブルを作成します。
C. ユーザーごとに分けられた、食べたアメリカン ドッグのすべての種類の数を含むテーブルを作成します。
D. ベジタリアン アメリカン ドッグごとにユーザーの合計数をグループ化するテーブルを作成します。
正解: **(**正解を表示します**)**
以下の検索文字列は、ミステリーミート コーンドッグの合計数をユーザー別に分類した表を作成します。
| ユーザー別の統計カウント | corndog=mysterymeat
検索文字列は次のことを行います。
* statsコマンドを使用して、userフィールドの各値に対するイベント数を計算します。statsコマンドは、userとcountの2つの列を持つテーブルを作成します。
* where コマンドを使用して、corndog フィールドの値で結果をフィルタリングします。where コマンドは、corndog が mysterymeat と等しい行のみを保持します。
したがって、検索文字列により、ミステリーミート コーンドッグの合計数をユーザー別に分割したテーブルが作成されます。

質問: **92**
Splunk Common Information Model (CIM) に付属するデータ モデルの説明はどこにありますか?
アドオンは文書化されていますか?
A. データモデル コマンド リファレンス ガイド。
B. Pivot ユーザー マニュアル。
C. 検索およびレポートのユーザー マニュアル。
D. CIM アドオン マニュアル。
正解: **(**正解を表示します**)**
CIMアドオンマニュアルには、Splunk Commonに付属するデータモデルの説明が含まれています。
情報モデル (CIM) アドオンと、アドオンの設定、使用、カスタマイズの方法について説明します。
参考文献
CIMアドオンマニュアル

Splunk 共通情報モデル (CIM) | Splunkbase
共通情報モデルアドオンの理解と使用 - Splunk

質問: **93**
Splunk Common Information Model (CIM) アドオンについて説明しているのは次のうちどれですか?
A. CIM アドオンは機械学習を使用してデータを正規化します。
B. CIM アドオンには、データをマップする方法を示すダッシュボードが含まれています。
C. CIM アドオンには、データの正規化に役立つデータ モデルが含まれています。
D. CIM アドオンは Splunk 環境に自動的にインストールされます。
正解: **(**正解を表示します**)**
Splunk Common Information Model (CIM) アドオンは、さまざまなソースや形式のデータの正規化を支援するデータモデルを含む Splunk アプリケーションです。CIM アドオンは、Splunk のフィールドとイベントの命名と分類に関する共通かつ一貫した方法を定義します。これにより、ネットワーク、セキュリティ、Web など、さまざまなドメインにまたがるデータの相関分析が容易になります。CIM アドオンは、データの正規化に機械学習を使用するのではなく、定義済みのフィールド名と値を使用します。CIM アドオンには、データのマッピング方法を示すダッシュボードは含まれていませんが、データモデルの使用方法に関するドキュメントと例が提供されています。CIM アドオンは Splunk 環境に自動的にインストールされず、Splunkbase からダウンロードしてインストールする必要があります。

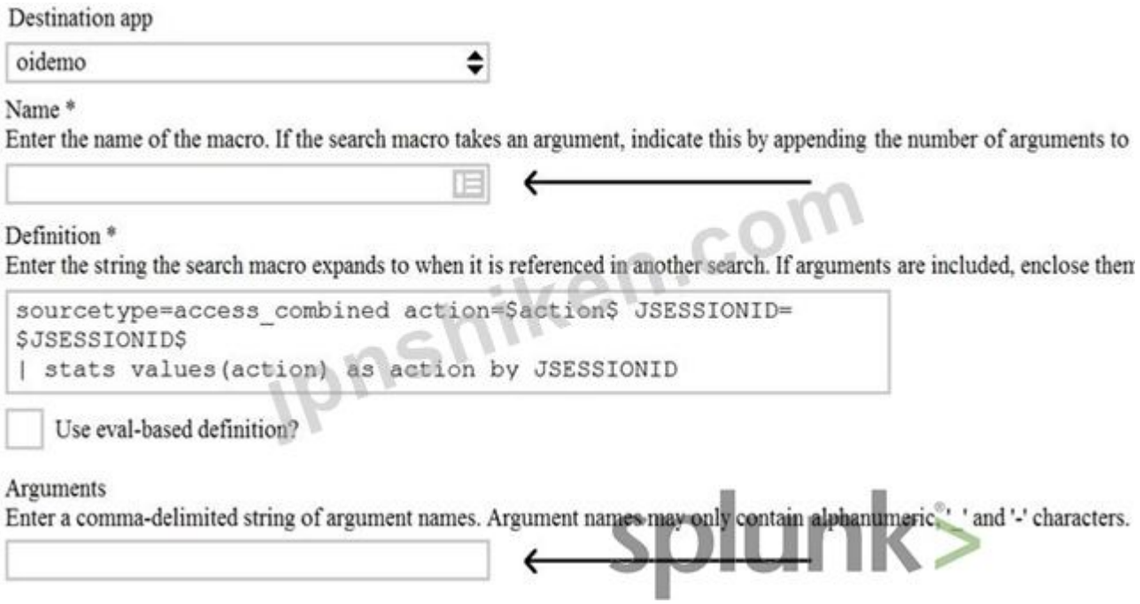
質問: **94**
次のどの記述が、ユーザーがトランザクション コマンドと統計コマンドのどちらかを選択するのに役立ちますか?
A. イベントを単一のイベントとして表示する必要がある場合に状態を使用します。
B. トランザクション コマンドがより高速かつ効率的になります。
C. トランザクション コマンドには 1000 イベントの制限があります。
D. 状態は IP アドレスを使用してのみイベントをグループ化できます。
正解: **(**正解を表示します**)**

質問: **95**
計算フィールドについて説明しているのは次のうちどれですか? (該当するものをすべて選択してください。)
A. 計算フィールドは検索バーで使用できます。
B. 計算フィールドは抽出されたフィールドに基づいて作成できます。
C. 計算フィールドはホストとソースタイプにのみ適用できます。
D. 計算フィールドは、eval コマンドを使用して計算を実行するためのショートカットです。
正解: **(**正解を表示します**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

質問: **96**
イベント タイプを作成するときに、検索文字列で許可されるのはどれですか?
A. タグ
B. 結合
C. サブ検索
D. パイプ
正解: **(**正解を表示します**)**

Splunkでイベントタイプを作成する際、検索文字列にサブ検索を使用できます。サブ検索を使用すると、メイン検索の入力として使用される二次検索を実行できます。この機能は、追加のフィルタリングや別の検索に基づく条件を必要とする、より複雑なイベントタイプ定義に役立ちます。
参照：
Splunkドキュメント: サブ検索について
Splunkドキュメント: イベントタイプの作成
Splunk Answers: イベントタイプでのサブ検索の使用

質問: **97**
以下のマクロ定義では、マクロを正しく構成するために、名前と引数のフィールドに何を入力する必要がありますか?



A. マクロ名は sessiontracker で、引数は action、JESSIONID です。
B. マクロ名はsessiontracker(2)、引数はaction、JESSIONIDです。
C. マクロ名は sessiontracker で、引数は $action$、$JESSIONID$ です。
D. マクロ名はsessiontracker(2)で、引数は$action$、$JESSIONID$で す。
正解: (正解を表示します)
参照：
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/検索マクロの定義

質問: **98**
Splunk Common Information Model (CIM) アドオンに含まれるデータ モデルは次のどれですか。
（該当するものをすべて選択してください）
A. ユーザー権限
B. アラート
C. データベース
D. メール
正解: (正解を表示します)
Splunk Common Information Model (CIM)アドオンには、事前設定されたデータモデルのコレクションが含まれています。

検索時にデータに適用できるもの。CIMの各データモデルは、フィールド名と
関心領域の最小公分母を定義するタグ。CIMには現在、データモデルが存在する。
アラート、データベース、メールなど22のカテゴリーが定義されています。ユーザー権限は定義されていません。
CIMのカテゴリ。参考資料Splunk共通情報モデルの概要とSplunk
共通情報モデル - ご質問にお答えします。

質問: **99**
これらの種類のチャートは、複数のセクションを持つ単一のバーでシリーズを表します。
A. マルチシリーズ
B. 分割シリーズ
C. nullを省略する
D. 積み重ね
正解: **(**正解を表示します**)**
積み上げグラフは、複数のセクションを持つ1本の棒グラフで系列を表します。グラフとは、
傾向、パターン、比較を示すデータ。グラフには、縦棒グラフ、横棒グラフ、折れ線グラフなど、さまざまな種類があります。
面グラフ、円グラフなど。また、分割系列、複数系列、積み上げなど、さまざまなモードを持つグラフもあります。積み上げ
チャートは、複数のシリーズを 1 つのバーまたは領域に表示し、各シリーズごとに異なるセクションを持つチャートの一種です。

質問: **100**
次の検索文字列のうち、有効でないものはどれですか。
A. index=web status=50* | ホスト、ステータス別のチャート数
B. インデックス=ウェブ ステータス=50* | ホストごとのステータス別チャート数
C. インデックス=ウェブ ステータス=50* | ホスト上のチャート数、ステータス
正解: **C (**コメントを発表する**)**

質問: **101**
次の検索コントロールのうち、検索を再実行しないものはどれですか? (該当するものをすべて選択してください。)
A. ズームアウト
B. タイムライン上のバーを選択する
C. 選択解除
D. タイムライン上のバーの範囲を選択する
正解: **(**正解を表示します**)**
タイムラインは、検索結果を時間経過に伴うイベントの分布を示すグラフィカルな表現です2。タイムラインを使用して、特定の時間範囲を拡大または縮小したり、タイムライン上の1つまたは複数のバーを選択して、その時間範囲で結果を絞り込んだりすることができます2。ただし、これらの操作では検索が再実行されるのではなく、選択した時間範囲に基づいて既存の結果が絞り込まれます2。したがって、オプションB、C、Dは正解です。オプションAは不正解です。ズームアウトすると、より広い時間範囲で検索が再実行されるためです。

質問: **102**
マクロが 3 つの引数を受け入れるには何が必要ですか?
A. マクロの名前は(3)で終わります。
B. マクロの名前は(3)で始まります。

C. マクロの引数数設定が3以上です。
D. 何もなし。すべてのマクロは任意の数の引数を受け入れることができます。
正解: (正解を表示します)
引数を受け入れるマクロを作成するには、マクロ名の末尾に引数の数を括弧で囲んで指定する必要があります1。例えば、my_macro(3) は3つの引数を受け入れるマクロです。マクロ名の引数の数は、定義内の引数の数と一致する必要があります1。したがって、選択肢Aは正解ですが、選択肢B、C、Dは不正解です。

質問: **103**
次のどれが統計関数ではありませんか?
A. 合計
B. 合計を追加
C. カウント
D. 平均
正解: (正解を表示します)
統計コマンドは、検索結果の集計統計（count、sum、avgなど）を計算するために使用されます。
min、maxなど2。statsコマンドは計算を実行するために使用できるさまざまな関数をサポートしています。
フィールド2に。ただし、addtotalsは統計関数ではなく、行または列を追加する別のコマンドです。
各グループ2の値の合計です。したがって、選択肢Bが正解ですが、選択肢A、C、Dは
これらは有効な統計関数であるため、誤りです。

質問: **104**
次の検索のうちどれが、下図のようなグラフを作成しますか?


A. index_internal seourcetype=Savesplunker | フィールド sourcetype、status | トランザクション ステータス maxspan-id | タイムチャート ステータス別カウント
B. index_internal seourcetype=Savesplunker | フィールド ソースタイプ、ステータス | トランザクション ステータス maxspan-id | 開始カウント 状態
C. index_internal seourcetype=Savesplunker | フィールド sourcetype、status | トランザクション ステータス maxspan-id | チャート count states by -time
D. これらの検索のいずれも、類似のグラフを生成しません。
正解: (正解を表示します)

質問: **105**
GET ワークフロー アクションを作成するために必要な情報には、次のうちどれが含まれますか? (該当するものをすべて選択してください。)
A. ワークフローアクションの名前
B. 検索時にユーザーが誘導される URI。
C. 検索時にイベントアクションメニューに表示されるラベル。
D. 検索時にユーザーが誘導される URI の名前。
正解: (正解を表示します)
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction

質問: **106**
次の記述のうち、フィールド エクストラクター (FX) の使用法を説明しているものはどれですか。
A. フィールド抽出機能は、検索時にすべてのフィールドを自動的に抽出します。
B. フィールド抽出機能は、PERL を使用して生のイベントからフィールドを抽出します。
C. フィールド抽出を使用して抽出されたフィールドは永続的ではないため、検索ごとに定義する必要があります。
D. フィールド抽出を使用して抽出されたフィールドは、ナレッジ オブジェクトとして保存されます。
正解: **D** (コメントを発表する)

質問: **107**
次のどれがイベント タイプの作成方法を説明していないでしょうか。
A. 検索文字列を実行し、[名前を付けて保存] ボタンを使用します。
B. [設定] メニューの [新しいイベント タイプ] ボタンを使用します。
C. フィールド抽出機能を使用して分析し、[名前を付けて保存] ボタンを使用します。
D. イベント タイプ ビルダー内で検索条件を選択します。
正解: **C** (コメントを発表する)
イベント タイプは、フィールド抽出ではなく検索から作成されます。
抽出: 「イベントタイプを作成するには、検索を実行してイベントタイプとして保存するか、「設定」> 「イベントタイプ」> 「新しいイベントタイプ」を使用します。」フィールド抽出機能はフィールド抽出に使用され、イベントタイプの作成には使用されません。したがって、選択肢Cが正解です。

質問: **108**
次の検索のうち、マクロの有効な使用法を示しているものはどれですか? (該当するものをすべて選択してください)
A. インデックス=メイン ソース=mySource oldField=* |'makeMyField(oldField)'| テーブル _time newField
B. インデックス=メイン ソース=mySource oldField=* | 統計 if('makeMyField(oldField)') | テーブル _time newField
C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
D. インデックス=メイン ソース=mySource oldField=* | "'newField('makeMyField(oldField)')'" | テーブル _time newField
正解: (正解を表示します)
参考:https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1。
html
検索でマクロを使用するには、マクロ名と引数を一重引用符で囲む必要があります1。
例えば、「my_macro(arg1,arg2)」は、2つの引数を持つマクロを使用する有効な方法です。検索文字列内で、通常検索コマンドまたは式1を使用する場所であればどこでもマクロを使用できます。したがって、オプションAとCはマクロを使用した有効な検索ですが、オプションBとDはマクロを一重引用符で囲んでいないため無効です。

質問: **109**

次の文のうち、検索ワークフローのアクションについて説明しているものはどれですか。
A. デフォルト。検索ワークフローアクションはリアルタイム検索として実行されます。
B. 検索ワークフローアクションはスケジュールされた検索として設定できます。
C. ユーザーは、ワークフロー アクションを作成するときに、検索の時間範囲を定義できます。
D. 検索ワークフローアクションは、トランザクションコマンドを含む検索文字列では設定できません。
正解: **C** (コメントを発表する)
説明
検索ワークフロー アクションは、検索結果のフィールド値をクリックしたときに検索を実行するカスタム アクションです。検索ワークフロー アクションは、ラベル名、検索文字列、時間範囲、アプリ コンテキストなど、さまざまなオプションを使用して構成できます。オプションの 1 つは、ワークフロー アクションの作成時に検索の時間範囲を定義することです。過去 24 時間、過去 7 日間などの定義済み時間範囲から選択することも、相対または絶対時間修飾子を使用してカスタムの時間範囲を指定することもできます。検索ワークフロー アクションは、デフォルトではリアルタイム検索として実行されず、特に指定がない限り、元の検索と同じ時間範囲が使用されます。検索ワークフロー アクションは、ユーザー操作によってのみトリガーされるため、スケジュールされた検索として構成することはできません。検索ワークフロー アクションは、transaction などの検索コマンドを含む有効な検索文字列を使用して構成できます。

質問: **110**
マクロに関する次の記述のうち正しいものはどれですか? (該当するものをすべて選択してください)
A. 引数値は、マクロの作成時に検索文字列を解決するために使用されます。
B. 引数値は実行時に検索文字列を解決するために使用されます。
C. 引数は実行時に定義されます。
D. 引数はマクロの作成時に定義されます。
正解: (正解を表示します)

質問: **111**
次の記述のうち、データ モデルの加速について説明しているものはどれですか (該当するものをすべて選択してください)。
A. 高速化されたデータ モデルは編集できません。
B. プライベート データ モデルは高速化できません。
C. ルート イベントは高速化できません。
D. データ モデルを高速化するには、管理者権限または accelerate_dacamodel 機能が必要です。
正解: (正解を表示します)

質問: **112**
検索ワークフロー アクションを元の検索と同じ時間範囲で実行するように構成するにはどうすればよいですか?
A. 元の検索に一致する最も早い時刻を設定します。
B. 時間範囲ピッカーから同じ時間範囲を選択します。
C. ワィールド リストを作成した検索と同じ時間範囲を使用する」チェックボックスをオンにします。
D. 元の検索で時間範囲を上書きする」チェックボックスを選択します。
正解: **C** (コメントを発表する)
説明

検索ワークフローアクションを元の検索と同じ時間範囲で実行するように設定するには、「フィールドリストを作成した検索と同じ時間範囲を使用する」チェックボックスをオンにする必要があります。これにより、ワークフローアクションの検索で元の検索と同じ最古および最新の時間パラメータが使用されるようになります。

質問: **113**
eval コマンドの結果はどこに保存されますか?
A. フィールド内。
B. インデックス内。
C. KV ストア内。
D. データベース内。
正解: **A (**コメントを発表する**)**
https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval eval コマンドは式を計算し、結果の値を検索結果フィールドに格納します。
指定したフィールド名が出力内のフィールドと一致しない場合は、新しいフィールドが検索結果に追加されます。
指定したフィールド名が検索結果に既に存在するフィールド名と一致する場合、eval 式の結果によってそのフィールドの値が上書きされます。

質問: **114**
Splunk Common Information Model (CIM)アドオンを使用する場合、どのようなアプローチが推奨されますか？
データを正規化しますか?
A. CIM データ モデル参照テーブルを参照してください。
B. 認証コマンドを使用して検索を実行します。
C. CIM イベント タイプ参照テーブルを参照してください。
D. 相関コマンドを使用して検索を実行します。
正解: **(**正解を表示します**)**
Splunk Common Information Model (CIM)アドオンを使用して正規化する場合の推奨アプローチ
データはAです。CIMデータモデル参照テーブルを参照してください。これは、CIMデータモデル参照テーブルが
データモデル内の各データセットに期待されるフィールドとタグに関する詳細な情報を提供します。
参照テーブルを参照することで、どのデータモデルがデータソースに関連しているかを判断し、
データフィールドをCIMフィールドにマッピングする方法。また、参照テーブルを使用してデータを検証することもできます。
正規化に関する問題のトラブルシューティングを行います。CIMデータモデル参照テーブルはSplunk
ドキュメント1またはSplunk Web2のデータモデルエディタページで確認できます。その他のオプションは、
これらはCIMアドオンやデータ正規化とは関係ありません。認証コマンドはカスタムです。
認証データモデルに対してイベントを検証するコマンドですが、正規化には役立ちません。
他の種類のデータ。相関コマンドは、イベントの統計分析を実行する検索コマンドです。
フィールドはありますが、データフィールドをCIMフィールドにマッピングするのには役立ちません。CIMイベントタイプ参照テーブル
イベント タイプは CIM アドオンの一部ではないため、存在しません。

質問: **115**
ユーザーは、イベントから特定のフィールド値を取得し、ユーザーのSplunkインスタンスの新しいブラウザウィンドウで検索を実行するワークフローアクションを作成したいと考えています。どのようなワークフローアクションを作成すればよいでしょうか？
A. ワークフロー実行アクション。ユーザーの検索で返されたイベントの特定のフィールド値を使用して、ユーザーが新しい検索を実行しているためです。

B. 検索ワークフロー アクション。ユーザーは、ユーザーの検索で返されたイベントの特定のフィールド値を使用して新しい検索を実行しているためです。
C. 検索はユーザーの現在の Splunk インスタンスに送信されるため、POST ワークフロー アクションです。
D. ユーザーの検索で返されたイベントからフィールド値を取得する必要があるため、GET ワークフロー アクションです。
正解: (正解を表示します)
検索ワークフローアクションは、イベントから特定のフィールド値を取得し、Splunkインスタンス内の新しいブラウザウィンドウで検索を実行したい場合（オプションB）に適しています。このタイプのワークフローアクションを使用すると、選択したイベントのフィールド値をパラメータとして利用する検索を定義できるため、元の検索結果に基づいてより詳細な調査やコンテキスト固有の分析を行うことができます。

質問: **116**
データ モデルを作成するときに、どのルート データセットに少なくとも 1 つの制約が必要ですか?
A. ルートトランザクションデータセット
B. ルートイベントデータセット
C. ルート子データセット
D. ルート検索データセット
正解: (正解を表示します)
正解はB. ルートイベントデータセットです。これは、ルートイベントデータセットが、データセットに関連しないイベントを除外する制約によって定義されているためです。ルートイベントデータセットの制約は、sourcetype=access_combinedなど、かなり広範囲のデータを返す単純な検索です。制約がない場合、ルートイベントデータセットにはインデックス内のすべてのイベントが含まれるため、データモデリングには役立ちません。データモデルの設計方法とルートイベントデータセットの追加方法の詳細については、Splunkドキュメント1を参照してください。その他の選択肢は不正解です。ルートトランザクションデータセットとルート検索データセットでは、トランザクション定義や複雑な検索など、データセットの定義方法が異なり、ルート子データセットは有効なルートデータセットの種類ではないためです。

質問: **117**
トランザクション内のイベントに共通するものは何ですか?
A. トランザクション内のすべてのイベントは同じタイムスタンプを持つ必要があります。
B. トランザクション内のすべてのイベントは同じソースタイプを持つ必要があります。
C. トランザクション内のすべてのイベントは、まったく同じフィールド セットを持つ必要があります。
D. トランザクション内のすべてのイベントは、1 つ以上のフィールドによって関連付けられる必要があります。
正解: (正解を表示します)

質問: **118**
ユーザーはどのようにしてスタック モードでチャートを表示するのでしょうか?
A. stack コマンドを使用します。
B. トレリス レイアウトの使用オプションをオンにします。
C. フォーマットメニューでスタックモードを変更します。
D. スタック モードではチャートを表示できません。タイム チャートのみ表示できます。
正解: **C** (コメントを発表する)
チャートは、検索結果を2つ以上のフィールド間の関係性を示すグラフィカルな表現です2。「書式」メニューの「スタックモード」オプションを変更すると、チャートをスタックモードで表示できます2。スタックモードでは、複数の系列をチャート内で積み重ねて、各系列の累積値を表示できます2。したがって、選択肢Cが正解です。選択肢A、B、Dはチャートをスタックモードで表示する方法ではないため、不正解です。

質問: **119**
データモデルフィールドは自動抽出方式で追加できます。次の記述のうち、
自動抽出されたフィールドですか? (該当するものをすべて選択してください)
A. 自動抽出フィールドはピボットで非表示にすることができます。
B. 自動抽出フィールドのデータ型を変更できます。
C. 自動抽出フィールドには、ピボットで使用するためのわかりやすい名前を付けることができます。
D. 自動抽出フィールドは、制約付きのデータセット内に既に存在する場合に追加できます。
正解: **(**正解を表示します**)**
データモデルフィールドは、データモデル2内のデータセットの属性を記述するフィールドです。データモデルフィールドは、
自動抽出、評価、ルックアップ2などのさまざまな方法で追加されます。自動抽出フィールドは、
正規表現などのさまざまな技術を使用して生データから自動的に抽出されます。
区切り文字またはキーと値のペア2. 自動抽出されたフィールドはピボットで非表示にすることができます。つまり、
ピボットインターフェース2に表示するかどうか。したがって、選択肢Aが正解です。自動抽出フィールド
データ型を変更できるため、文字列、数値、
ブール値またはタイムスタンプ2。したがって、選択肢Bが正解です。自動抽出されたフィールドにはわかりやすい名前を付けることができます。
ピボットで使用するために、より説明的な代替名を割り当てることができることを意味します。
元のフィールド名2よりもユーザーフレンドリーです。したがって、選択肢Cが正解です。自動抽出されたフィールドは追加できます。
制約付きのデータセットに既に存在する場合、データモデルに含めることができます。
フィルターや制約を適用して生データから既に抽出されている場合でも、
データセット2。したがって、選択肢Dが正解です。

質問: **120**
次の文のうち、POST ワークフロー アクションについて説明しているものはどれですか。
A. POST ワークフロー アクションでは、同じウィンドウまたは新しいウィンドウで Web ページを開くことができます。
B. POST ワークフロー アクションは常に暗号化されます。
C. カスタム ソースタイプでは POST ワークフロー アクションを作成できません。
D. POST ワークフロー アクションでは、URI 内のフィールド値を使用できません。
正解: **A (**コメントを発表する**)**

質問: **121**
stats コマンドのこの機能を使用すると、フィールドに含まれる値の数を識別できます。
A. フィールド
B. カウント
C. 最大
D. 個別カウント
正解: **B (**コメントを発表する**)**

質問: **122**
フィールドエイリアスを適用できるのは次のどれですか?
A. インデックス
B. タグ
C. イベントの種類
D. ソースタイプ
正解: **(**正解を表示します**)**
フィールド エイリアスは、ホスト、ソース、またはソースタイプに基づいて適用されます。
抜粋:　エイリアスが適用されるホスト、ソース、またはソースタイプを指定して、フィールド エイリアスを作成します。」したがって、正解は Sourcetypes です。

質問: **123**
次の検索のうち、商品名別の売上レポートを返すものはどれですか?
A. 商品名別の売上合計(価格)をグラフ化する
B. product_name 別に売上をグラフ化する
C. 統計合計(価格)をproduct_nameの売上として計算します
D. タイムチャートリスト(売上), 値(製品名)
正解: **(**正解を表示します**)**

質問: **124**
次の知識オブジェクト/構成はどのような順序で適用されますか?
A. フィールドエイリアス、フィールド抽出、ルックアップ
B. フィールド抽出、フィールドエイリアス、ルックアップ
C. フィールド抽出、ルックアップ、フィールドエイリアス
D. ルックアップ、フィールドエイリアス、フィールド抽出
正解: **B (**コメントを発表する**)**
参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge ナレッジ オブジェクトは、データに知識を追加し、検索と分析を容易にするために作成するエンティティです2。ナレッジ オブジェクトの例としては、フィールド抽出、フィールド エイリアス、ルックアップなどがあります2。フィールド抽出は、正規表現、区切り文字、キーと値のペアなどのさまざまな手法を使用して、生データからフィールドを抽出する方法です2。フィールド エイリアスは、元のフィールド名や値を変更せずに、既存のフィールドに別の名前を割り当てる方法です2。ルックアップは、CSV ファイルやデータベースなどの外部ソースからの追加情報を使用してデータを拡充する方法です2。これらのナレッジ オブジェクト/設定が適用される順序は、フィールド抽出、フィールド エイリアス、ルックアップの順です2。つまり、Splunk は最初に生データからフィールドを抽出し、次に抽出されたフィールドにエイリアスを適用し、最後にエイリアスが付けられたフィールドに対してルックアップを実行します2。したがって、オプション B は正解ですが、オプション A、C、D は不正解です。

質問: **125**
イベント タイプは保存されたレポートとどう違うのでしょうか?

A. イベント タイプを使用してデータをカテゴリに整理することはできません。
B. イベント タイプには、検索結果の書式設定が含まれます。
C. イベント タイプは Splunk ユーザーと共有したり、ダッシュボードに追加したりできます。
D. イベント タイプには時間範囲が含まれません。
正解: **D** (コメントを発表する)
こんにちは、Bingです。Splunk Core Power User Technologiesに関するご質問にお答えできます。
正解は D です。イベント タイプには時間範囲は含まれません。
説明は次のとおりです。
* イベントタイプは、同じ検索文字列1に一致するイベントを照合することで、データの意味を理解するのに役立つ分類システムです。イベントタイプは検索時にイベントに適用され、検索語句やフィルターとして使用できます12。
* 保存されたレポートは、検索アクションから保存された結果であり、統計情報や視覚化を表示できます。
* イベント3. 保存したレポートはいつでも実行でき、実行するたびに最新の結果が取得されます34. 保存したレポートは他のユーザーと共有したり、ダッシュボードに追加したりできます4.
* イベントタイプと保存済みレポートの主な違いは、イベントタイプには時間範囲が指定されないのに対し、保存済みレポートには時間範囲が指定されることです14。つまり、イベントタイプはどの期間のイベントにも一致しますが、保存済みレポートは作成時または実行時に指定された時間範囲に限定されます14。

質問: **126**
1 フィールドの値が Renewal-MonthYear フィールドの値と一致するイベントを検索する構文はどれですか。
A. | 10yearAnnerversary=更新月年
B. | where '10yearAnnerversary=Renewal-MonthYear
C. | 10yearAnnerversary='Renewal-MonthYear'
D. | '10yearAnnerversary' = 'Renewal-MonthYear'
正解: **A** (コメントを発表する)
説明
正解は A です。| ここで、10yearAnnerversary=Renewal-MonthYear です。
where コマンドは、true または false に評価される式に基づいて検索結果をフィルターするために使用されます。
whereコマンドは、2つのフィールド、2つの値、またはフィールドと値を比較できます。また、関数、演算子、ワイルドカードを使用して複雑な式を作成することもできます1。
where コマンドの構文は次のとおりです。
| where <式>
式は比較、計算、論理演算、またはこれらの組み合わせで表すことができます。式は各イベントに対してtrueまたはfalseに評価される必要があります。
whereコマンドで2つのフィールドを比較するには、フィールド名を引用符なしで指定する必要があります。例えば、10yearAnnerversaryフィールドの値がRenewal-MonthYearフィールドの値と一致するイベントを検索する場合は、次の構文を使用します。
| 10yearAnnerversary=更新月年
これにより、2 つのフィールドの値が同じであるイベントのみが返されます。
その他のオプションは、フィールド名を引用符で囲んでいるため正しくありません。そのため、whereコマンドはフィールド名を引用符で囲み、文字列値として解釈してしまいます。例えば、次のように記述すると、
| ここで '10yearAnnerversary' = 'Renewal-MonthYear'
文字列値 '10yearAnnerversary' が文字列値 'Renewal-MonthYear' と等しいイベントがないため、イベントは返されません。
参考文献:
コマンドの使用法

質問: **127**
フィールド抽出 (FX)の正規表現モードはいつ使用すればよいですか？（該当するものをすべて選択してください）
A. スペース、カンマ、またはパイプ文字で区切られたデータの場合。
B. CSV (カンマ区切り値) ファイル内のデータの場合。
C. フィールドを区切る複数の異なる文字を含むデータの場合。
D. 非構造化データの場合。
正解: **(**正解を表示します**)**
フィールドエクストラクター (FX)の正規表現モードは、複数の異なる文字で区切られたフィールドを持つデータや非構造化データに使用する必要があります。正規表現モードでは、サンプルイベントを選択し、抽出するフィールドをハイライト表示できます。フィールドエクストラクターは、類似のイベントに一致する正規表現を生成し、そこからフィールドを抽出します。参考資料 :フィールドエクストラクターを使用したフィールド抽出の構築 - Splunkドキュメントおよびフィールドエクストラクター :メソッド選択ステップ - Splunkドキュメントをご覧ください。

質問: **128**
データ モデル属性について正しいのは次のうちどれですか。
A. データ モデル内では作成できません。
B. ルート検索データセットにのみ追加できます。
C. 親データセットから継承された場合は編集できません。
D. 検索時間フィールドの抽出からデータセットに追加できます。
正解: **(**正解を表示します**)**
データモデル属性は、検索時のフィールド抽出、計算フィールド、ルックアップ、またはエイリアスによってデータセットに追加されるフィールドです。データモデルエディタ内で作成することも、親データセットから継承することもできます。データモデルで必要な場合を除き、編集または削除できます。ルート検索データセットだけでなく、あらゆるタイプのデータセットに追加できます。参考資料 :データモデルについて、[データモデル属性の定義]、および
Splunk ドキュメントの [データ モデル データセットの編集]。

質問: **129**
データ モデルとピボットの関係は何ですか?
A. データ モデルはピボットのデータセットを提供します。
B. ピボットとデータ モデルには関係がありません。
C. ピボットとデータ モデルは同じものです。
D. ピボットはデータ モデルのデータセットを提供します。
正解: **A (**コメントを発表する**)**
データモデルとピボットの関係は、データモデルがピボットのデータセットを提供するという点です。データ
モデルは、データを構造化され階層的に表現するデータセットの集合です。データモデル
データがオブジェクトとフィールドにどのように整理されるかを定義します。ピボットは、
データモデルのさまざまな側面を示すデータ視覚化。ピボットを使用すると、メニューからオプションを選択して
SPLコードを書かずに、グラフ、表、地図などを作成するためのフォーム。ピボットはデータモデルのデータセットを使用する。
ピボットとデータモデルは同じものではありません。ピボットはデータを視覚化するツールです。
モデル。ピボットはデータ モデルにデータセットを提供するのではなく、それを入力として使用します。

したがって、データ モデルとピボットの関係については、ステートメント A のみが正しいことになります。

質問: **130**
計算フィールドがソースとして使用できるオブジェクトは次のどれですか?
A. フィールドのエイリアス。
B. 自動ルックアップによって追加されたフィールド。
C. タグ フィールド。
D. イベントタイプ フィールド。
正解: **B** (コメントを発表する)
正解は B です。自動ルックアップによって追加されたフィールドです。
計算フィールドは、検索時にeval式を使用してイベントに追加されるフィールドです。計算フィールドは
フィールドは、イベントにすでに存在する2つ以上のフィールドの値を使用して計算を実行できます。
計算フィールドは、計算フィールドが作成される前にフィールドが抽出されている限り、任意のフィールドをソースとして使用できます。
定義済み1。
自動ルックアップは、CSVなどの外部ソースからの追加フィールドを使用してイベントを充実させる方法です。
ファイルまたはデータベース。自動ルックアップでは、既存のフィールドの値に基づいてイベントにフィールドを追加できます。
ホスト、ソース、ソースタイプ、またはその他の抽出フィールド2.計算される前に自動ルックアップが実行されます
フィールドが定義されているため、ルックアップによって追加されたフィールドを計算フィールド3のソースとして使用できます。
したがって、計算フィールドは、自動ルックアップによって追加されたフィールドをソースとして使用できます。
参考文献:
計算フィールドについて
ルックアップについて
検索時間処理

質問: **131**
次の文のうち、GET ワークフロー アクションを説明しているものはどれですか。
A. GET ワークフロー アクションは、POST 引数を使用して構成する必要があります。
B. GET ワークフロー アクションの構成には、ソース タイプを選択することが含まれます。
C. GET ワークフロー アクションのラベル名には、ドル記号で囲まれたフィールド名を含める必要があります。
D. GETワークフローアクションは、URTリンクを現在のウィンドウまたは新しいウィンドウで開くように設定できます。
正解: (正解を表示します)
GET ワークフローアクションは、検索結果のフィールド値をクリックしたときに URL リンクを開くカスタムアクションです。GET ワークフローアクションは、ラベル名、ベース URL、URI パラメータ、アプリケーションコンテキストなど、さまざまなオプションで設定できます。オプションの 1 つは、URL リンクを現在のウィンドウで開くか、新しいウィンドウで開くかを選択することです。GET ワークフローアクションは、GET メソッドを使用して Web サーバーにリクエストを送信するため、POST 引数で設定する必要はありません。GET ワークフローアクションは Splunk でデータを生成しないため、設定にソースタイプの選択は含まれません。GET ワークフローアクションのラベル名には、URL リンク内の変数を置き換えるために使用されるフィールド値を示すため、ドル記号で囲まれたフィールド名を含める必要があります。

質問: **132**
次のどの記述が、ユーザーがトランザクション コマンドと統計コマンドのどちらかを選択するのに役立ちますか?

A. 状態は IP アドレスを使用してのみイベントをグループ化できます。
B. トランザクション コマンドがより高速かつ効率的になります。
C. トランザクション コマンドには 1000 イベントの制限があります。
D. イベントを単一のイベントとして表示する必要がある場合に状態を使用します。
正解: **C** (コメントを発表する)
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction
トランザクションコマンドと統計コマンドのどちらを選択するかを決める際に役立つステートメントの1つは、
トランザクションコマンド3では、イベントの数が1000に制限されます。トランザクションコマンドは、イベントをグループ化するために使用されます。
1つ以上のフィールドで共通の値を共有するものをトランザクション3にインポートします。トランザクションコマンドにはデフォルトの
1トランザクションあたり1000イベントの制限があり、1000を超えるイベントを1つのトランザクションにグループ化することはできません。
この制限はmaxeventsパラメータを使用して変更できますが、パフォーマンスに影響を与える可能性があります。
Splunk3のメモリ使用量。したがって、選択肢Cは正解ですが、選択肢A、B、Dは誤りです。
これらは、ユーザーがトランザクション コマンドと統計コマンドのどちらかを選択するのに役立つステートメントではありません。

質問: **133**
3 次元内の離散値間の関係を示す視覚化のタイプはどれですか?
A. 円グラフ
B. 折れ線グラフ
C. バブルチャート
D. 散布図
正解: **C** (コメントを発表する)
https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub

質問: **134**
次の検索のうち、マクロの有効な使用法を示しているものはどれですか? (該当するものをすべて選択してください。)
A. インデックス=メイン ソース=mySource oldField=* |'makeMyField(oldField)'| テーブル _time newField
B. インデックス=メイン ソース=mySource oldField=* | 統計 if('makeMyField(oldField)') | テーブル _time newField
C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
D. インデックス=メイン ソース=mySource oldField=* | "'newField('makeMyField(oldField)')"' | テーブル _time newField
正解: (正解を表示します)
検索AとCは、マクロの有効な使用例を示しています。マクロとは、一重引用符 '() を使用して呼び出すことができる再利用可能なSPLコードです。マクロは引数を取ることができ、引数はマクロ名の後に括弧で囲んで渡されます。例えば、 fmakeMyField(oldField)」は、引数oldFieldを指定してmakeMyFieldという名前のマクロを呼び出します。検索BとDは、一重引用符 '() ではなく二重引用符 "(") を使用しているため、有効ではありません。

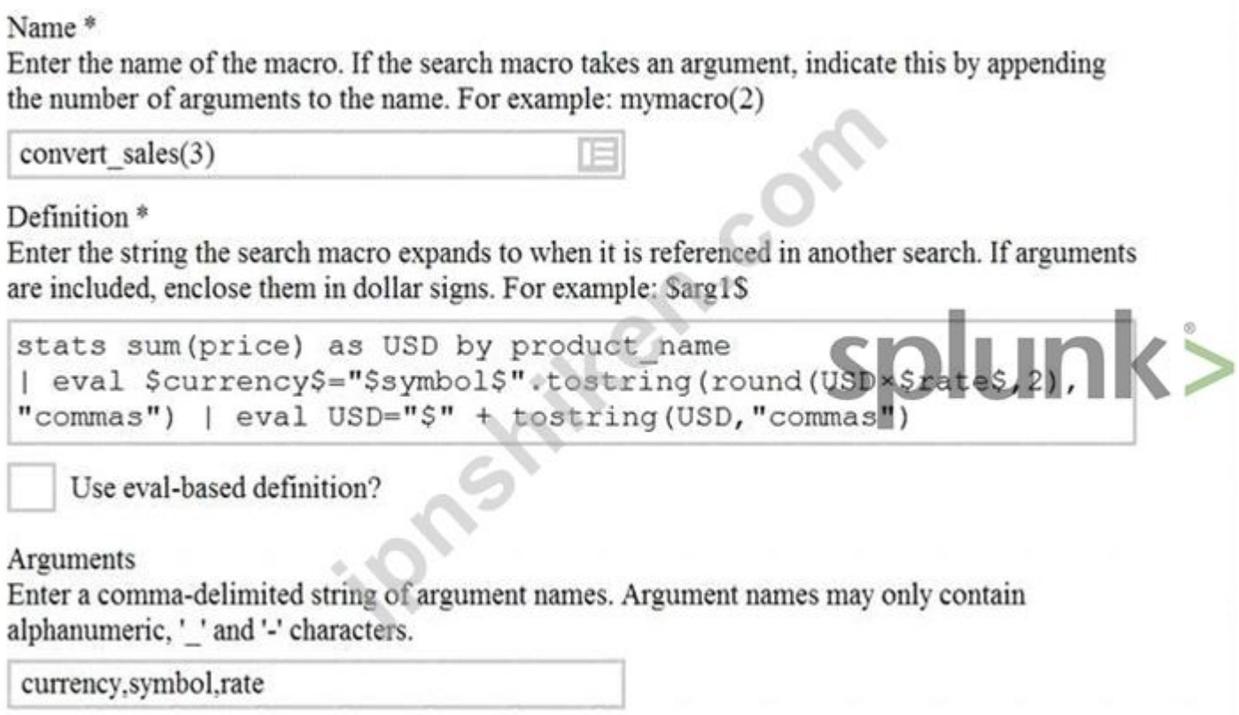
質問: **135**
次の検索のうち、マクロの有効な使用法を示しているものはどれですか? (該当するものをすべて選択してください)
A. インデックス=メイン ソース=mySource oldField=* |'makeMyField(oldField)'| テーブル _time newField
B. インデックス=メイン ソース=mySource oldField=* | 統計 if('makeMyField(oldField)') | テーブル _time newField
C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
D. インデックス=メイン ソース=mySource oldField=* | "'newField('makeMyField(oldField)')"' | テーブル _time newField

正解: (正解を表示します)
参照：
https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html

質問: **136**
フィールド抽出 (FX) はどの区切り文字を検出できますか? (該当するものをすべて選択してください)
A. タブ
B. パイプ
C. スペース
D. カンマ
正解: (正解を表示します)
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep
フィールド抽出ツール（FX）は、区切り文字や通常の文字列を使用してデータからフィールドを抽出するツールです。
式。区切り文字は、データ内のフィールドを区切る文字または文字列です。FXはいくつかの
パイプ（|）、スペース（ ）、カンマ（,）、セミコロン（;）などの一般的な区切り文字を自動的に認識します。FXは
タブ (\t) は区切り文字として自動的に検出されます。ただし、FX インターフェイスで手動で指定することもできます。

質問: **137**
検索で _____ が返された場合は、グラフとして表示できます。
A. タイムスタンプ
B. 統計
C. イベント
D. キーワード
正解: (正解を表示します)
検索で統計情報が返された場合、それをグラフとして表示できます2。統計情報とは、2つ以上のフィールド間の関係を示す表形式のデータです2。統計情報は、stats、chart、timechartなどのコマンドを使用して作成できます2。検索アプリの「視覚化」タブを選択し、縦棒グラフ、折れ線グラフ、円グラフなどのグラフの種類を選択すると、統計情報をグラフとして表示できます2。したがって、選択肢Bが正解です。選択肢A、C、Dはグラフとして表示できるデータの種類ではないため、不正解です。

質問: **138**
以下に示すマクロ定義に基づいて、検索文字列でマクロを実行する正しい方法は何ですか?



A. Convert_sales (ユーロ, €, 79)"
B. Convert_sales (ユーロ、€、.79)
C. Convert_sales ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)
正解: (正解を表示します)
参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros 検索文字列内でマクロを実行する正しい方法は、macro_name($arg1$, $arg2$, ...) で、$arg1$、$arg2$ などはマクロの引数です。この場合、マクロ名は convert_sales で、通貨、シンボル、レートの3つの引数を取ります。引数はドル記号で囲み、カンマで区切ります。したがって、マクロを実行する正しい方法は convert_sales($euro$, $€$, .79)。

質問: **139**
Splunk 共通情報モデル (CIM) は、フィールド エイリアス、イベント タイプ、タグに加えて、どのナレッジ オブジェクトを使用してデータを正規化しますか。
A. マクロ
B. ルックアップ
C. ワークフローアクション
D. フィールド抽出
正解: (正解を表示します)
フィールド エイリアス、フィールド抽出、およびルックアップを組み合わせて、これらの各フィールドのデータを正規化します。
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeddataatsearchtime

質問: **140**
次の検索のうち、商品名別の売上レポートを返すものはどれですか?
A. product_name 別に売上をグラフ化する

B. 商品名別の売上合計(価格)をグラフ化する
C. 統計sum(price)をproduct_nameの売上として計算します
D. タイムチャートリスト(売上)、値(製品名)
正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.1.0/検索リファレンス/チャート
https://docs.splunk.com/Documentation/Splunk/8.1.0/検索リファレンス/統計

質問: **141**
次の記述のうち、データ モデルの加速化について説明しているものはどれですか (該当するものをすべて選択してください)。
A. ルート イベントは高速化できません。
B. 高速化されたデータ モデルは編集できません。
C. プライベート データ モデルは高速化できません。
D. データ モデルを高速化するには、管理者権限または accelerate_datamodel 機能が必要です。
正解: (正解を表示します)
説明/参照:

質問: **142**
|join コマンドを使用して、2つの別々の結果テーブルを結合します。外部テーブルには以下の値があります。
以下の表を参照してください

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

テーブルを結合するために使用される SPL の行は次のとおりです: | join employeeNumber type=outer 新しいテーブルに返される行数はいくつですか?
A. ゼロ
B. 5
C. 8
D. 3

正解: (正解を表示します)
Splunkで|join employeeNumber type=outerコマンドを使用して外部結合を実行すると、employeeNumberフィールドに基づいて両方のテーブルの行が結合されます。外部結合は、両方のテーブルのすべての行を返します。一致する行がある場合は、両方のテーブルから一致する行も返します。一致する行がない場合、一致しない側の結合結果はNULLになります。
提供されたテーブルでは、最初のテーブルには5行、2番目のテーブルには3行あります。これは外部結合なので、両方のテーブルのすべての行が返されます。つまり、新しいテーブルには、両方のテーブルの一致する行と一致しない行を合わせた合計8行が含まれます。
参考文献:
* join コマンドに関する Splunk ドキュメント。
* 結合の使用方法と結合の種類に関する Splunk コミュニティのディスカッション。

質問: **143**
データ モデルは、次のデータセットの 1 つ以上で構成されていますか (該当するものをすべて選択してください)。
A. トランザクションデータセット
B. イベントデータセット
C. データセットを検索する
D. イベント、トランザクション、検索データセットの任意の子
正解: (正解を表示します)
データモデルのデータセットは互いに階層的な関係を持ち、親子関係を持つ。
関係。データモデルには複数のデータセット階層を含めることができます。データセットには3つの種類があります。
階層: イベント、検索、トランザクション。
https://docs.splunk.com/Splexicon:データモデルデータセット

質問: **144**
フィールド値を使用して二次検索を実行するワークフローはどれですか?
A. ポスト
B. アクション
C. 検索
D. サブ検索
正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SplunkWeb でのワークフローアクションの作成

質問: **145**
フィールド抽出ツールにアクセスする方法はいくつかあります。データ型、ソースタイプ、サンプルイベントを自動的に識別するオプションはどれですか？
A. イベントアクション > フィールドの抽出
B. フィールドサイドバー > 新しいフィールドの抽出
C. 設定 > フィールド抽出 > 新しいフィールド抽出
D. 設定 > フィールド抽出 > フィールド抽出を開く
正解: (正解を表示します)
説明

フィールド抽出ツールにアクセスするには、いくつかの方法があります。データ型、ソースタイプ、サンプルイベントを自動的に識別するオプションは、「フィールド」サイドバー > 「新しいフィールドを抽出」です。フィールド抽出ツールは、区切り文字または正規表現を使用してデータからフィールドを抽出するのに役立つツールです。フィールド抽出ツールは、選択したサンプル値に基づいて正規表現を生成することも、独自の正規表現を入力することもできます。フィールド抽出ツールには、以下のような様々な方法でアクセスできます。
フィールドサイドバー > 新しいフィールドの抽出 :これはフィールド抽出ツールにアクセスする最も簡単な方法です。フィールドサイドバーは、データに使用可能なすべてのフィールドとその値を表示するパネルです。フィールドサイドバーで 「新しいフィールドの抽出」をクリックすると、Splunkは現在の検索条件に基づいて、データのデータ型、ソースタイプ、サンプルイベントを自動的に識別します。その後、フィールド抽出ツールを使用してサンプル値を選択し、新しいフィールドの正規表現を生成できます。
イベントアクション > フィールドの抽出 :これもフィールド抽出ツールにアクセスする方法です。イベントアクションとは、検索結果内の個々のイベントに対して実行できるアクションで、イベントの詳細の表示、レポートへの追加、ダッシュボードへの追加などが含まれます。イベントアクションメニューの 「フィールドの抽出」をクリックすると、Splunk は現在のイベントをデータのサンプルイベントとして使用し、データのソースタイプとデータ型を選択するように要求します。その後、フィールド抽出ツールを使用してサンプル値を選択し、新しいフィールドの正規表現を生成できます。
「設定」> 「フィールド抽出」> 「新規フィールド抽出」 :これは、フィールド抽出ツールへのより高度なアクセス方法です。 「設定」は、インデックス、入力、出力、ユーザー、ロール、アプリケーションなど、Splunkのさまざまな側面を設定できるメニューです。 「設定」メニューで 「新規フィールド抽出」をクリックすると、アプリケーションのコンテキスト、名前、ソースタイプ、データ型、サンプルイベント、正規表現など、新しいフィールド抽出に必要なすべての詳細を手動で入力するよう求められます。その後、フィールド抽出ツールを使用して、新しいフィールドの正規表現を検証または変更できます。

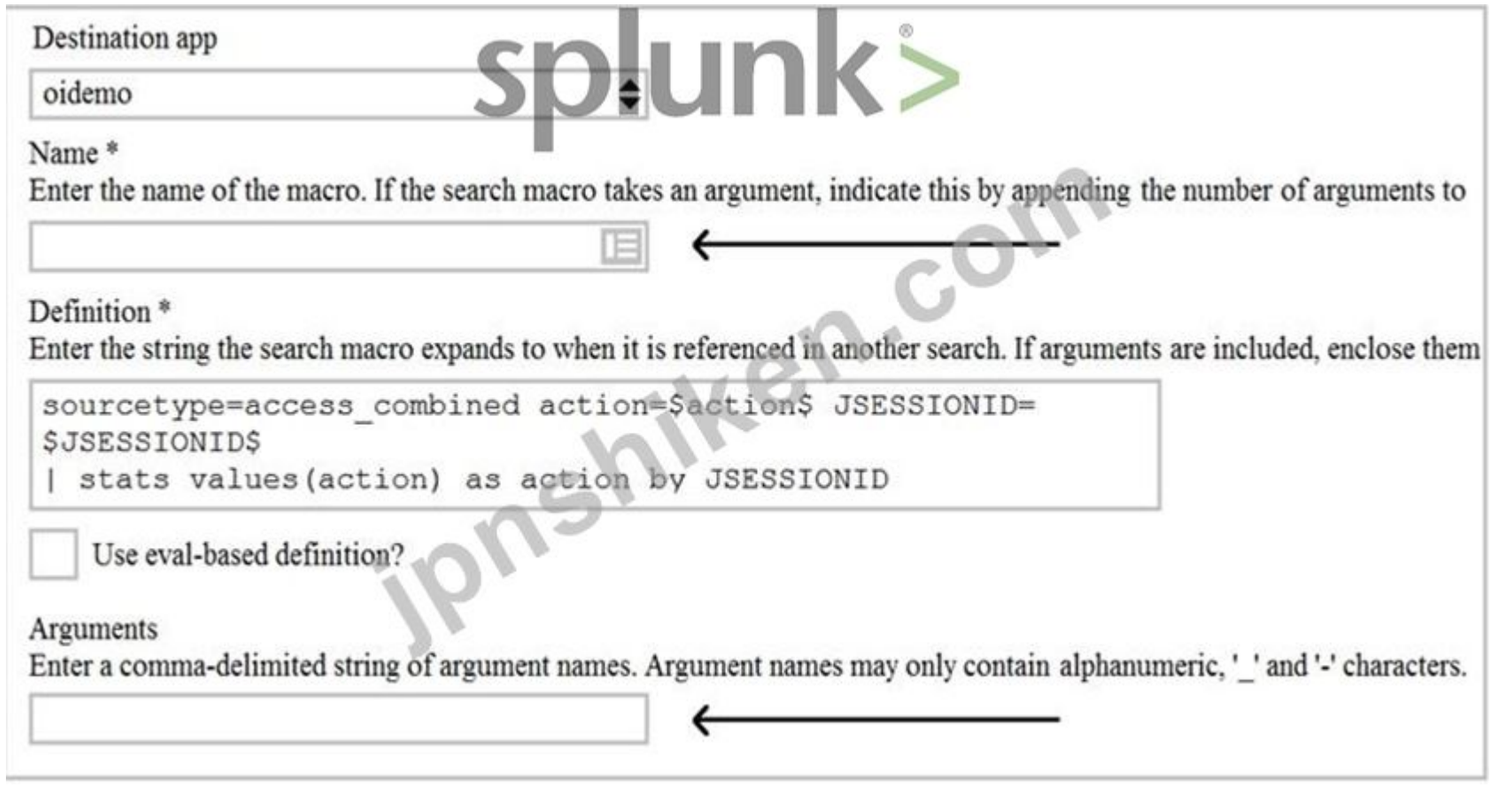
質問: **146**
eval はどのようなタイプのコマンドですか?
A. 一部のモードでのストリーミング
B. レポート生成
C. 分散ストリーミング
D. 集中型ストリーミング
正解: **C** (コメントを発表する)
説明
正解はCです。分散ストリーミングです。evalコマンドは、結果が検索ヘッドに送信される前にインデクサー上で実行できるコマンドの一種であるためです。これにより、転送する必要があるデータの量が削減され、検索パフォーマンスが向上します。分散ストリーミングコマンドは、他のイベントや結果に依存することなく、各イベントまたは結果を個別に処理できます。コマンドの種類と検索パフォーマンスへの影響の詳細については、Splunkのドキュメント1をご覧ください。

質問: **147**
次の検索モードのうち、抽出されたすべてのフィールドをフィールド サイドバーに自動的に返すものはどれですか。
A. C. 詳細
B. 速い
C. 賢い
正解: **A** (コメントを発表する)

質問: **148**
次のどれがイベント タイプとして保存できますか?
A. index-server_472 sourcetype-BETA_494 code-488 I 統計はコードごとにカウントされます
B. index=server_472 sourcetype=BETA_494 code=488 [I inputlookup append=t servercode.csv]
C. index=server_472 sourcetype=BETA_494 code=488 コード > 200 の I 統計

D. インデックス=server_472 ソースタイプ=BETA_494 コード-488
正解: **D** (コメントを発表する)
Splunkのイベントタイプは、データを分類して保存された検索であり、データ内の特定のパターンや条件を簡単に検索できます。イベントタイプを保存する際、検索は基本的に、データの変換や集計などの操作を実行せずに、条件に基づいてイベントをフィルタリングする必要があります。オプションの詳細は次のとおりです。
A: 検索インデックスサーバー472 ソースタイプBETA_494 コード488 | コード別の統計カウントは集計操作（コード別の統計カウント）を実行するため、イベントタイプとして保存するには適していません。イベントタイプは、データを集計または変換することなく分類することを目的としています。
B: 検索インデックス=server_472 sourcetype=BETA_494 code=488 [| inputlookup append=t servercode.csv] には、サブ検索と入力ルックアップが含まれています。これらは通常、外部データに基づいてイベントを拡充またはフィルタリングするために使用されます。この複雑さは、単純なイベント分類の範疇を超えています。
C: 検索 index=server_472 sourcetype=BETA_494 code=488 | stats where code > 200 には、変換コマンド (stats) 内にフィルタリング条件が含まれていますが、これもデータの変換のため、イベント タイプの定義には適していません。
D: 検索 index=server_472 sourcetype=BETA_494 code-488 は、データを変換または集約せずに、インデックス、ソースタイプ、およびコード フィールド条件に基づいてイベントをフィルター処理するだけなので、正解です。
イベントの構造や内容を変更せずに、特定の基準に基づいてデータを分類するため、イベント タイプとして保存するのに適しています。

質問: **149**
以下のマクロ定義では、マクロを正しく構成するために、名前と引数のフィールドに何を入力する必要がありますか?



A. マクロ名は sessiontracker で、引数は action、JESSIONID です。
B. マクロ名はsessiontracker(2)、引数はaction、JESSIONIDです。
C. マクロ名は sessiontracker で、引数は $action$、$JESSIONID$ です。
D. マクロ名はsessiontracker(2)で、引数は$action$、$JESSIONID$で す。
正解: (正解を表示します)

参考: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros 以下のマクロ定義は、action と JSESSIONID の 2 つの引数に基づいてユーザー セッションを追跡するマクロを示しています。
セッショントラッカー(2)
マクロ定義は次のことを行います。
マクロ名をsessiontrackerとして指定します。これは、検索文字列内でマクロを実行する際に使用される名前です。
マクロの引数の数を 2 に指定します。これは、マクロが実行時に 2 つの引数を取ることを示します。
マクロのコードを、index=main、sourcetype=access_combined_wcookie、action=$action$、JSESSIONID=$JSESSIONID$、| stats count by JSESSIONID のように指定します。これは、マクロ実行時に実行される検索文字列です。検索文字列には、検索語、コマンド、引数など、検索の任意の部分を含めることができます。また、ドル記号で囲んだ引数の変数も検索文字列に含めることができます。
この場合、action と JSESSIONID は、マクロの実行時にその値に置き換えられる引数の変数です。
したがって、マクロを正しく設定するには、名前にsessiontracker、引数にアクションとJSESSIONIDを入力する必要があります。あるいは、名前にsessiontracker(2)を使用し、引数を空白のままにすることもできます。

質問: **150**
視覚化を作成するときに使用する次のコマンドのどれですか (該当するものをすべて選択してください)。
A. コロプレス
B. iplocation
C. ジオメトリ
D. ジオスタッツ
正解: **B,C,D** (コメントを発表する)

質問: **151**
次のどれが eval コマンドの tostring 関数で使用できますか (該当するものをすべて選択してください)。
A. "カンマ"
B. "10進数"
C. "16進数"
D. "期間"
正解: **(**正解を表示します**)**

質問: **152**
正規表現 (regex) を手動で編集した後、次の文のうち正しいものはどれですか。
A. 手動で行われた変更は、フィールド抽出 (FX) UI で元に戻すことができます。
B. フィールド抽出 (FX) UI でフィールド抽出を編集することはできなくなりました。
C. フィールド抽出機能を使用して作成された正規表現 (regex) を手動で編集することはできません。

(FX) UI。
D. フィールド抽出 (FX) UI は、手動で編集されたものに加えて、独自のバージョンのフィールド抽出を保持します。
正解: **(**正解を表示します**)**
フィールド抽出 FX)UIを使用して作成された正規表現 egex)を手動で編集した後、
FX UIでフィールド抽出を編集できなくなりました。FX UIは、フィールド抽出を支援するツールです。
区切り文字または正規表現を使用してデータを入力できます。FX UIは、入力したデータに基づいて正規表現を生成します。
サンプル値を選択するか、FX UIで独自の正規表現を入力することができます。ただし、正規表現を編集すると
props.confファイルに手動で変更を加えると、FX UIは変更を認識できず、編集できなくなります。
FX UIでのフィールド抽出はもう機能しません。さらに詳細を設定するには、props.confファイルを使用する必要があります。
フィールド抽出の変更。手動で行った変更は、FX UIでは元に戻すことができません。FX UIでは元に戻すことができません。
props.confファイルに加えられた変更は追跡されません。手動で正規表現を編集することは可能です。
props.conf ファイルで行う限り、FX UI を使用して作成されます。
したがって、正規表現を手動で編集することに関しては、ステートメント B のみが当てはまります。

質問: **153**
タグに関する次の記述のうち正しいものはどれですか? (該当するものをすべて選択してください。)
A. タグはデータをより理解しやすくするために設計されています。
B. タグは検索に基づいてイベントを分類します。
C. タグはフィールド/値のペアに基づいています。
D. タグは大文字と小文字を区別しません。
正解: **A,C (**コメントを発表する**)**
タグに関する以下の記述は正しいです。タグはフィールドと値のペアに基づいており、検索に基づいてイベントを分類します。タグは、フィールドまたはフィールド値に適用できるカスタムラベルであり、データに追加のコンテキストや意味を与えることができます。タグは、共通の概念やテーマに基づいてデータをフィルタリングまたは分析するために使用できます。タグは、検索コマンド、設定ファイル、ユーザーインターフェースなど、さまざまな方法で作成できます。タグの特徴は次のとおりです。
タグはフィールドと値のペアに基づいています。つまり、タグは特定のフィールド名と特定のフィールド値に関連付けられます。例えば、フィールド名が tatus」でフィールド値が ritical」の場合、 lert」というタグを作成できます。この場合、status=critical のイベントにのみ lert」タグが適用されます。
タグは検索に基づいてイベントを分類します。つまり、タグは、タグ付けしたいイベントに一致する検索文字列によって定義されます。例えば、検索文字列 sourcetype=access_combined に対して eb」というタグを作成できます。つまり、検索文字列 sourcetype=access_combined に一致するイベントにのみ eb」タグが適用されます。
タグに関する以下の記述は誤りです。タグは大文字と小文字を区別せず、データの理解を容易にするように設計されています。タグは大文字と小文字を区別し、データの検索を容易にするように設計されています。タグは大文字と小文字を区別します。つまり、タグは、関連付けられているフィールド名とフィールド値の大文字と小文字が完全に一致している必要があります。例えば、フィールド名 tatus」とフィールド値 ritical」に対して lert」というタグを作成した場合、status=CRITICAL または Status=critical のイベントには適用されません。
タグはデータの検索を容易にするように設計されています。つまり、タグは、共通の概念やテーマを使用して、データ内の関連するイベントやパターンを見つけるのに役立ちます。例えば、検索文字列 sourcetype=access_combined に対して eb」というタグを作成した場合、tag=web を使用して、Web アクティビティに関連するすべてのイベントを検索できます。

質問: **154**
次の検索は何をしますか?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. ユーザーの合計数をコーンドッグごとに分割したテーブルを作成します。

B. ユーザー別に分けられたミステリーミート コーンドッグの合計数のテーブルを作成します。
C. ユーザーごとに分けられた、食べたアメリカン ドッグのすべての種類の数を含むテーブルを作成します。
D. ベジタリアン アメリカン ドッグごとにユーザーの合計数をグループ化するテーブルを作成します。
正解: **B (**コメントを発表する**)**
以下の検索文字列は、ミステリーミート コーンドッグの合計数をユーザー別に分類した表を作成します。
| ユーザー別の統計カウント | corndog=mysterymeat
検索文字列は次のことを行います。
* statsコマンドを使用して、userフィールドの各値に対するイベント数を計算します。statsコマンドは、userとcountの2つの列を持つテーブルを作成します。
* where コマンドを使用して、corndog フィールドの値で結果をフィルタリングします。where コマンドは、corndog が mysterymeat と等しい行のみを保持します。
したがって、検索文字列により、ミステリーミート コーンドッグの合計数をユーザー別に分割したテーブルが作成されます。

質問: **155**
レポートに関して正しいのは次のうちどれですか?
A. レポートはナレッジ オブジェクトです。
B. レポートをスケジュールできます。
C. レポートはスクリプトを実行できます。
D. 上記のすべて。
正解: **(**正解を表示します**)**
レポートは、検索とその結果を保存し、再利用したり他のユーザーと共有したりできる方法です2。レポートはナレッジ オブジェクトの一種でもあり、データに知識を追加して検索や分析を容易にするために作成するエンティティです2。したがって、オプション A が正解です。レポートはスケジュール設定できます。つまり、定期的に実行するように設定し、結果を電子メールやその他の方法で自分や他のユーザーに送信できます2。したがって、オプション B が正解です。レポートはスクリプトを実行できます。つまり、レポートの実行時に実行するスクリプト ファイルを指定し、それを使用してカスタム アクションや統合を実行できます2。したがって、オプション C が正解です。上記のすべての記述がレポートに当てはまるため、オプション D が正解です。

質問: **156**
次の eval コマンド関数のうち有効なものはどれですか?
A. int()
B. カウント()
C. 印刷()
D. tostring()
正解: **(**正解を表示します**)**
説明
https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions evalコマンド関数tostring()は有効です。tostring()関数は数値を文字列値に変換します。例えば、tostring(3.14)は 「3.14」を返します。その他の関数は有効なevalコマンド関数ではありません。

質問: **157**
自動ルックアップが機能するには、ルックアップ ファイルにこれが含まれていることが必須です。
A. タイムスタンプ
B. 入力フィールド
C. 少なくとも5列

D. ソースタイプ
正解: **(**正解を表示します**)**

質問: **158**
次のどれが eval コマンドの tostring 関数で使用できますか (該当するものをすべて選択してください)。
A. "16進数"
B. "カンマ"
C. "10進数"
D. "期間"
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY。
evalコマンドのtostring関数は数値を文字列に変換します。オプションで
2番目の引数は文字列値の形式を指定します。指定可能な形式は次のとおりです。
hex: 数値を 16 進文字列に変換します。
カンマ: 数値の千の位を区切るためにカンマを追加します。
duration: 数値を「2h 3m 4s」などの人間が読める期間文字列に変換します。
したがって、tostring 関数では形式 A、B、および D を使用できます。

質問: **159**
次の記述のうち、計算フィールドについて説明しているものはどれですか? (該当するものをすべて選択してください)
A. 計算フィールドは検索バーで使用できます。
B. 計算フィールドは抽出されたフィールドに基づいて作成できます。
C. 計算フィールドはホストとソースタイプにのみ適用できます。
D. 計算フィールドは、eval コマンドを使用して計算を実行するためのショートカットです。
正解: **(**正解を表示します**)**
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

質問: **160**
どのタイプのワークフロー アクションがフィールド値を外部リソース (チケット システムなど) に送信しますか?
A. ポスト
B. 検索
C. 取得
D. フォーマット
正解: **A (**コメントを発表する**)**
フィールド値を外部リソース (チケット システムなど) に送信するワークフロー アクションのタイプは POST です。
POSTワークフローアクションを使用すると、フィールド値または静的な文字列を含むPOSTリクエストをURIの場所に送ることができます。
値を引数として渡すことができます。例えば、POSTワークフローアクションを使用して外部のチケットを作成できます。
イベントからの情報を備えたシステム。

質問: **161**

次の検索は何をしますか?
index=condlog type=mysterymeat action=eaten 私たちによるスキャットのカウントは cornlog_count です:
A. ユーザーごとに分けられた、食べたアメリカン ドッグのすべての種類の数を含むテーブルを作成します。
B. ユーザー別に分けられたミステリーミート コーンドッグの合計数のテーブルを作成します。
C. ユーザーの合計数をコーンドッグごとに分割したテーブルを作成します。
D. ベジタリアン アメリカン ドッグごとにユーザーの合計数をグループ化するテーブルを作成します。
正解: **(**正解を表示します**)**

質問: **162**
timechart コマンドは、次の条件に応じてデータを時間間隔でバケット化します。
A. 返されるイベントの数
B. 選択された時間範囲
C. 選択された視覚化の種類
正解: **(**正解を表示します**)**
timechartコマンドは、選択した時間範囲2に応じて、時間間隔でデータをバケット化します。timechartコマンドはchartコマンドに似ていますが、_timeフィールド2に基づいてイベントを自動的に時間バケットにグループ化します。時間バケットのサイズは、検索で選択した時間範囲によって異なります。たとえば、時間範囲として 過去24時間」を選択した場合、Splunkはタイムチャートに30分単位のバケットを使用します。時間範囲として 過去7日間」を選択した場合、Splunkはタイムチャートに4時間単位のバケットを使用します。したがって、オプションBは正解ですが、オプションAとCはタイムバケットのサイズに影響を与える要因ではないため、不正解です。

質問: **163**
次の知識オブジェクト/構成はどのような順序で適用されますか?
A. フィールドエイリアス、フィールド抽出、ルックアップ
B. フィールド抽出、フィールドエイリアス、ルックアップ
C. フィールド抽出、ルックアップ、フィールドエイリアス
D. ルックアップ、フィールドエイリアス、フィールド抽出
正解: **B (**コメントを発表する**)**
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge

質問: **164**
次の記述のうち、イベントの種類を説明しているものはどれですか?
A. ログ レベルの測定: 情報、警告、エラー。
B. フィールドが抽出される前に適用されるナレッジ オブジェクト。
C. 検索文字列に基づいてイベントを分類するためのフィールド。
D. ログ、メトリック、またはトレースのいずれか。
正解: **(**正解を表示します**)**
説明
これは、イベント タイプが、特定の検索条件に一致する一連のイベントにユーザー定義の名前を割り当てるナレッジ オブジェクトであるためです。たとえば、sourcetype=access_combined、status=200、action=purchase のイベントに対して successful_purchase という名前のイベント タイプを作成できます。次に、eventtype=successful_purchase を検索語として使用して、それらのイベントを見つけることができます。また、イベント タイプを使用して、アラート、レポート、ダッシュボードを

作成することもできます。イベント タイプの詳細については、Splunk のドキュメント1を参照してください。その他のオプションは、イベント タイプが何であるかを説明していないため、正しくありません。ログ レベルの測定は、情報、警告、エラーなど、イベントの重大度を示すフィールドです。フィールドが抽出される前に適用されるナレッジ オブジェクトはソース タイプであり、データの形式と構造を識別します。ログ、メトリック、トレースはいずれも、Splunk が取り込んで分析できるデータ タイプですが、イベント タイプではありません。

質問: **165**
次の eval ステートメントがあるとします。
... | eval field1 = if(isnotnull(field1),field1,0), field2 = if(isnull(field2), "NO-VALUE", field2) 次のどれが fillnull を使用した場合と同等でしょうか?
A. ... | fillnull values=(0,"NO-VALUE") fields=(field1,field2)
B. fillnull を使用した同等の式はありません
C. ... | fillnull フィールド1 | fillnull 値="NO-VALUE" フィールド2
D. ... | fillnull 値=0 フィールド1 | fillnull フィールド2
正解: **D (**コメントを発表する**)**
fillnull コマンドは、特定のフィールドの null 値を置き換えるために使用できます。与えられた eval ステートメントと同等の正しい式は、fillnull を 2 回使用することです。1 回は field1 で null 値を 0 に置き換え、もう 1 回は field2 で null 値を "NO-VALUE" に置き換えます。
参照：
Splunk ドキュメント - fillnull コマンド

質問: **166**
次の文のうち、フィールド エイリアスについて説明しているものはどれですか。
A. フィールドエイリアス名が元のフィールド名に置き換えられます。
B. フィールドエイリアスは、ルックアップファイル定義で使用できます。
C. フィールド エイリアスは、ソースとソースタイプ間でのみデータを正規化します。
D. フィールドエイリアス名は、検索の一部として使用される場合、大文字と小文字は区別されません。
正解: (正解を表示します)
フィールド エイリアスは、Splunk のフィールドの別名です。フィールド エイリアスを使用すると、同じ概念に対して異なるフィールド名を持つ異なるソースおよびソースタイプ間でデータを正規化できます。たとえば、src_ip のフィールド エイリアスを作成して、clientip、source_address、または異なるソースタイプのソース IP アドレスを表すその他のフィールド名にマップできます。フィールド エイリアスは、ルックアップ ファイル定義でも使用して、データ内のフィールドをルックアップ ファイルのフィールドにマップできます。たとえば、src_ip のフィールド エイリアスを使用して、IP アドレスの位置情報を含むルックアップ ファイルで ip_address にマップできます。フィールド エイリアス名は元のフィールド名を置き換えず、異なる名前でフィールドのコピーを作成します。フィールド エイリアス名は、検索の一部として使用する場合、大文字と小文字が区別されます。つまり、src_ip と SRC_IP は異なるフィールドです。

質問: **167**
カンマ区切りデータの場合、どのフィールド抽出方法を選択する必要がありますか?
A. 正規表現

B. 区切り文字
C. eval式
D. テーブル抽出
正解: (正解を表示します)
正解はB. 区切り文字です。区切り文字方式は、ヘッダー付きファイルのデータなど、イベント内のすべてのフィールドがコンマやスペースなどの共通の区切り文字で区切られている構造化イベントデータ向けに設計されているためです。サンプルイベントを選択し、区切り文字を特定してから、フィールド抽出機能が検出したフィールドの名前を変更できます。区切り文字方式の詳細については、Splunkのドキュメント1を参照してください。その他の選択肢は、コンマ区切りデータには適していないため、正しくありません。正規表現方式は、非構造化イベントデータに最適です。サンプルイベントから抽出する1つ以上のフィールドを選択して強調表示すると、フィールド抽出機能が類似イベントに一致する正規表現を生成し、そこからフィールドを抽出します。eval式は、算術演算、文字列演算、論理演算を使用して新しいフィールドを計算したり、既存のフィールドを変更したりできるコマンドです。表抽出は、PDFファイルやWebページから表形式のデータを抽出できる機能です。これらの方法の詳細については、Splunkのドキュメント23を参照してください。

質問: **168**
コロプレスマップの場合、Splunk には次の KMZ ファイルが付属しています (該当するものをすべて選択してください)。
A. アメリカ合衆国の州
B. アメリカ合衆国とカナダの州と州
C. 欧州連合諸国
D. 世界の国々
正解: (正解を表示します)
Splunk には、コロプレスマップ用の以下の KMZ ファイルが付属しています：米国の州と世界の国々。KMZ ファイルは、KML ファイルやその他のリソースを含む圧縮ファイルです。KML ファイルは、地理的特徴とそのプロパティを定義する XML ファイルです。KMZ ファイルを使用して、Splunk で geom コマンドを使用してコロプレスマップを作成できます。コロプレスマップとは、ある基準に基づいて地理的領域を異なる色で表示するマップの一種です。Splunk には、コロプレスマップの地理的領域を定義する 2 つの KMZ ファイルが付属しています。
* アメリカ合衆国の州 :このKMZファイルは、アメリカ合衆国の50州とその境界を定義しています。このKMZファイルの名前はus_states.kmzで、以下の場所にあります。$SPLUNK_HOME/etc/apps/maps/appserver/static/geo ディレクトリ。
* 世界の国々: このKMZファイルは、世界の国々とその国境を定義しています。このKMZファイルの名前はworld_countries.kmzで、以下の場所にあります。$SPLUNK_HOME/etc/apps/maps/appserver/static/geo ディレクトリ。
Splunkには、米国およびカナダの州や県、または欧州連合加盟国のKMZファイルは付属していません。ただし、独自のKMZファイルを作成したり、外部ソースからダウンロードしてSplunkで使用することは可能です。

質問: **169**
次のどれが eval コマンドの tostring 関数で使用できますか (該当するものをすべて選択してください)。
A. "16進数"
B. "カンマ"
C. "10進数"
D. "期間"
正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.29

質問: **170**
Splunkの比較演算子ではないもの

A. <
B.
C. !
D. >
E. ?
正解: **E** (コメントを発表する)
比較演算子は、2つの値を比較してブール値（真または偽）を返す記号です。
Splunkは、<、>、=、!=、<=、>=、IN、LIKE2などのさまざまな比較演算子をサポートしています。ただし、
?= は Splunk では有効な比較演算子ではないため、検索文字列で使用すると構文エラーが発生します2。
したがって、選択肢Eは正解であり、選択肢A、B、C、Dは有効な比較であるため不正解である。
Splunkの演算子

質問: **171**
フィールドサイドバーに_____が表示されません。（該当するものをすべて選択してください。）
A. 興味深い分野
B. 選択されたフィールド
C. 抽出されたすべてのフィールド
正解: **C** (コメントを発表する)
フィールド サイドバーは、検索結果に存在するフィールドを表示するパネルです2。フィールド サイドバーには、正規表現、区切り文字、キーと値のペアなどのさまざまな方法を使用して生データから抽出されたフィールドである抽出フィールドがすべて表示されるわけではありません2。フィールド サイドバーには、選択されたフィールドと興味深いフィールドだけが表示されます2。選択されたフィールドとは、フィールド サイドバーでクリックするか、フィールド コマンドを使用して、検索結果に表示するように選択したフィールドです2。興味深いフィールドとは、イベントの少なくとも 20% に出現するフィールド、または値に大きなばらつきがあるフィールドです2。したがって、オプション C は正解ですが、オプション A と B はフィールド サイドバーに表示されるフィールドの種類であるため不正解です。

質問: **172**
これらの種類のチャートは、複数のセクションを持つ単一のバーでシリーズを表します。
A. nullを省略する
B. 積み重ね
C. マルチシリーズ
D. 分割シリーズ
正解: (正解を表示します)
積み上げグラフは、複数のセクションを持つ1本の棒グラフで系列を表します。グラフとは、
傾向、パターン、比較を示すデータ。グラフには、縦棒グラフ、横棒グラフ、折れ線グラフなど、さまざまな種類があります。
面グラフ、円グラフなど。また、分割系列、複数系列、積み上げなど、さまざまなモードを持つグラフもあります。積み上げ
チャートは、複数のシリーズを 1 つのバーまたは領域に表示し、各シリーズごとに異なるセクションを持つチャートの一種です。

質問: **173**
1 フィールドの値が Renewal-MonthYear フィールドの値と一致するイベントを検索する構文はどれですか。
A. | 10yearAnnerversary=更新月年
B. | where '10yearAnnerversary=Renewal-MonthYear

C. | 10yearAnnerversary='Renewal-MonthYear'
D. | '10yearAnnerversary' = 'Renewal-MonthYear'
正解: (正解を表示します)
whereコマンドは、真偽値を返す式に基づいて検索結果をフィルタリングするために使用されます。whereコマンドは、2つのフィールド、2つの値、またはフィールドと値を比較できます。また、関数、演算子、ワイルドカードを使用して複雑な式を作成することもできます1。
where コマンドの構文は次のとおりです。
| where <式>
式は比較、計算、論理演算、またはこれらの組み合わせで表すことができます。式は各イベントに対してtrueまたはfalseに評価される必要があります。
whereコマンドで2つのフィールドを比較するには、フィールド名を引用符なしで指定する必要があります。例えば、10yearAnnerversaryフィールドの値がRenewal-MonthYearフィールドの値と一致するイベントを検索する場合は、次の構文を使用します。
| 10yearAnnerversary=更新月年
これにより、2 つのフィールドの値が同じであるイベントのみが返されます。
その他のオプションは、フィールド名を引用符で囲んでいるため正しくありません。そのため、whereコマンドはフィールド名を引用符で囲み、文字列値として解釈してしまいます。例えば、次のように記述すると、
| ここで '10yearAnnerversary' = 'Renewal-MonthYear'
文字列値 '10yearAnnerversary' が文字列値 'Renewal-MonthYear' と等しいイベントがないため、イベントは返されません。
Explanation:
正解は
参照：
コマンドの使用法

質問: **174**
次の検索コントロールのうち、検索を再実行しないものはどれですか? (該当するものをすべて選択してください。)
A. ズームアウト
B. タイムライン上のバーを選択する
C. 選択解除
D. タイムライン上のバーの範囲を選択する
正解: (正解を表示します)
説明
タイムラインは、検索結果を時間経過に伴うイベントの分布を示すグラフィカルな表現です2。タイムラインを使用して、特定の時間範囲を拡大または縮小したり、タイムライン上の1つまたは複数のバーを選択して、その時間範囲で結果を絞り込んだりすることができます2。ただし、これらの操作では検索が再実行されるのではなく、選択した時間範囲に基づいて既存の結果が絞り込まれます2。したがって、オプションB、C、Dは正解です。オプションAは不正解です。ズームアウトすると、より広い時間範囲で検索が再実行されるためです。

質問: **175**
ユーザーは次のような検索を実行します。
index-X sourcetype=YI chart count (domain) as count、sum (price) as sum by product、action usenull=f useother-f このコマンドが作成する順序と一致するテーブル ヘッダーは次のどれですか。
A. チャート コマンドでは複数の統計関数は使用できません。
B. 商品、合計: カートに追加、合計: 削除、合計: 購入、カウント: カートに追加、カウント: 削除、カウント: 購入
C. 商品、count: addtocart、count: remove、count: purchase、sum: addtocart、sum: remove、sum: purchase

D. カウント: 製品、合計: 製品、カウント: アクション、合計: アクション
正解**: C (**コメントを発表する**)**
正解は C です。Product、count: addtocart、count: remove、count: purchase、sum: addtocart、sum:
削除、合計：購入。
Splunkでは、chartコマンドを使用してデータから表またはグラフの視覚化を作成します2。chartコマンドは、少なくとも1つの関数と1つのフィールド、そしてオプションでグループ化する別のフィールドを指定します2。
この検索では、chartコマンドに2つの関数（countとsum）、2つのフィールド（domainとprice）、そして2つのグループ化フィールド（productとaction）が指定されています。usenull=fおよびuseother=fオプションは、chart2からnull値やその他の値を除外するために使用されています。
chartコマンドは、command1内のフィールドと関数の順序に一致するヘッダーを持つテーブルを作成します。count関数のヘッダーにはcount:というプレフィックスが、sum関数のヘッダーにはsum:1というプレフィックスが付きます。productフィールドとactionフィールドの値は、headers1のサフィックスとして使用されます。
したがって、このコマンドによって作成されるテーブル ヘッダーは、Product、count: addtocart、count: remove、count: となります。
purchase、sum: addtocart、sum: remove、sum: purchase1。

質問**: 176**
イベント タイプを作成する有効な方法はどれですか? (該当するものをすべて選択してください)
A. [設定] メニューに移動し、[イベント タイプ] > [新規] をクリックします。
B. 検索結果でイベントを選択し、[イベント アクション] > [イベント タイプのビルド] をクリックします。
C. props.conf ファイルの event_type スタンザを編集します。
D. 検索バーで searchtypes コマンドを使用します。
正解**: (**正解を表示します**)**

質問**: 177**
アクション タイプがリンクに設定されている場合に使用できるワークフロー アクション メソッドはどれですか。
A. 取得
B. 置く
C. 検索
D. 更新
正解**: (**正解を表示します**)**
Contoso では、次の技術要件を特定しています。
* データ サイエンティストは、ASDK を使用して Butler をテストする必要があります。
* 可能な限り、ソリューションではコストを最小限に抑える必要があります。
* バトラーは、ユーザーが初めて接続するときに、名前で挨拶する必要があります。
* Butler は 1 日に最大 10,000 件のメッセージを処理できる必要があります。
* Butler は、基本的な発話に基づいてユーザーの意図を認識する必要があります。
* Azure Bot Service のすべての構成は、一元的にログに記録する必要があります。
* 可能な限り、ソリューションでは最小権限の原則を使用する必要があります。
* 内部ユーザーは、Microsoft Skype for Business を使用して Butler にアクセスできる必要があります。
* 新しい Bookings アプリは、ユーザーが Butler と対話できるユーザー インターフェイスを提供する必要があります。
* KeyManagers という名前の Azure AD グループ内のユーザーは、すべての Azure Cognitive Services のキーを管理できる必要があります。

* Butler は、ユーザーに部屋の予約、予約のキャンセル、既存の予約の表示機能を提供する必要があります。
* 単一のデータ センターまたは Azure リージョンに障害が発生した場合でも、新しい Bookings アプリは北米とヨーロッパのユーザーが利用できる必要があります。
* 継続的な改善のためには、サンプル発話を送信し、チャットボットの応答を実際の意図と比較することで Butler をテストできる必要があります。
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction GETワークフローアクションを定義する手順
* [設定] > [フィールド] > [ワークフロー アクション] に移動します。
* [新規] をクリックして、新しいワークフロー アクション フォームを開きます。
* アクションのラベルを定義します。
ラベルフィールドでは、フィールドまたはイベントワークフローメニューに表示されるテキストを定義できます。ラベルは静的にすることも、関連フィールドの値を含めることもできます。
* ワークフロー アクションがデータ内の特定のフィールドまたはイベント タイプに適用されるかどうかを決定します。
「次のフィールドのみに適用」を使用して、1つまたは複数のフィールドを指定します。フィールドを指定すると、そのフィールドを含むイベントのイベントメニューまたはフィールドメニューにのみ、ワークフローアクションが表示されます。空白のままにするかアスタリスクを入力すると、すべてのフィールドのメニューにアクションが表示されます。
「次のイベントタイプにのみ適用」を使用して、1つ以上のイベントタイプを指定します。イベントタイプを指定すると、そのイベントタイプに属するイベントのイベントメニューにのみワークフローアクションが表示されます。
* [アクションの表示場所] では、アクションを [イベント] メニュー、[フィールド] メニュー、またはその両方のいずれに表示するかを決定します。
* アクションタイプをリンクに設定します。
* URI には、フィールド値を送信する外部リソースの場所の URI を指定します。
ラベル設定と同様に、フィールドの値を宣言するときは、ドル記号で囲まれたフィールドの名前を使用します。
GETアクションでURI経由で渡される変数は、送信時に自動的にURLエンコードされます。つまり、単語間にスペースや句読点を含む値を含めることができます。
* [リンクを開く場所] で、ワークフロー アクションを現在のウィンドウに表示するか、新しいウィンドウでリンクを開くかを決定します。
* 取得するLinkメソッドを設定します。
* [保存] をクリックして、ワークフロー アクション定義を保存します。

質問: **178**
次の文のうち、マクロについて説明しているものはどれですか?
A. マクロは完全な検索を含む必要がある再利用可能な検索文字列です。
B. マクロは、固定の時間範囲を持つ必要がある再利用可能な検索文字列です。
C. マクロは、柔軟な時間範囲を持つことができる再利用可能な検索文字列です。
D. マクロは、検索の一部のみを含む再利用可能な検索文字列です。
正解: **D** (コメントを発表する)
説明
説明/参考資料: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros

質問: **179**
次の検索では、5 回以上存在する IP アドレスのみをさらにフィルターするコマンドはどれですか。
A. index=ゲームIの統計はIP BごとにIP_countとしてカウントされます。| IP_count > 5
B. インデックス=ゲーム | 検索 IP_Count > 5
C. index=games | IP > 5
D. インデックス=ゲーム I 検索 IP > 5

正解: (正解を表示します)
index=games の検索結果に5回以上出現するIPアドレスのみをフィルタリングするには、statsコマンドとwhereコマンドを組み合わせて使用できます。statsコマンドは各IPアドレスの出現回数をカウントし、その回数をIP_countに代入します。whereコマンドは、出現回数が5回を超えるIPアドレスのみを結果に含めます。
完全な検索は次のようになります。
index=ゲーム | 統計は IP_count として IP ごとにカウントされます | IP_count > 5
参照：
Splunk ドキュメント: stats コマンド
Splunk ドキュメント: where コマンド
Splunk Answers: 統計とwhereコマンドを使った結果のフィルタリング

質問: **180**
timechart コマンドは、次の条件に応じてデータを時間間隔でバケット化します。
A. 返されるイベントの数
B. 選択された時間範囲
C. 選択された視覚化の種類
正解: (正解を表示します)
timechartコマンドは、選択された時間範囲2に応じて、データを時間間隔でグループ化します。timechartコマンドはchartコマンドに似ていますが、イベントを時間間隔に基づいて自動的にグループ化します。
_timeフィールド2。タイムバケットのサイズは、検索で選択した時間範囲によって異なります。例えば、時間範囲として「過去24時間」を選択した場合、Splunkはタイムチャートに30分単位のバケットを使用します。時間範囲として「過去7日間」を選択した場合、Splunkはタイムチャート2に4時間単位のバケットを使用します。
したがって、オプション B は正解ですが、オプション A と C はタイムバケットのサイズに影響を与える要因ではないため不正解です。

質問: **181**
| ホスト別のタイムチャートを使用する場合、x 軸にはどのフィールドが表示されますか?
A. 日付
B. ホスト
C. 時間
D. _time
正解: (正解を表示します)
説明/リファレンス: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart

質問: **182**
次の文のうち、以下の検索文字列を説明しているものはどれですか?
| データモデル Application_State All_Application_State 検索

A. Evenrches は州別の売上レポートを返します。
B. Application_State という名前のデータ モデルからイベントが返されます。
C. All_Application_state という名前のデータ モデルからイベントが返されます。
D. パイプはデータモデルコマンドの後に実行されるため、イベントは返されません。
正解: **B** (コメントを発表する)
以下の検索文字列は、Application_State という名前のデータ モデルからイベントを返します。
| データモデル Application_State All_Application_State 検索
検索文字列は次のことを行います。
* Splunk のデータモデルにアクセスするには、datamodel コマンドを使用します。datamodel コマンドは、データモデルの名前と、データモデル内のデータセットの名前という 2 つの引数を取ります。
* データモデルの名前をApplication_Stateとして指定します。これは、Webアプリケーションに関する情報を含む、Splunkの定義済みデータモデルです。
* データセットの名前を 「All_Application_State」と指定します。これはデータモデルのルートデータセットであり、すべての子データセットのすべてのイベントが含まれます。
* 検索コマンドを使用して、データセットからイベントをフィルタリングおよび変換します。検索コマンドは
* 結果を変更するには、任意の検索条件またはコマンドを使用します。
したがって、検索文字列は、Application_State という名前のデータ モデルからイベントを返します。

質問: **183**
検索コマンドに関する次の記述のうち正しいものはどれですか?
A. フィールド値は大文字と小文字を区別して扱われます。
B. 最初のパイプの前の検索文字列とまったく同じように動作します。
C. 検索パイプラインの先頭でのみ使用できます。
D. ワイルドカードは使用できません。
正解: **B** (コメントを発表する)

質問: **184**
Common Information Model (CIM) アドオンに含まれるものは次のどれですか?
A. マクロを検索
B. イベントカテゴリタグ
C. ワークフローアクション
D. tsidx ファイル
正解: (正解を表示します)
正解はBです。イベントカテゴリタグ。これは、CIMアドオンにイベントカテゴリタグのコレクションが含まれているためです。
検索時にデータに適用できる、事前設定されたデータモデルです。CIM内の各データモデルは、
関心領域の最小公分母を定義するフィールド名とタグのセット。イベント
カテゴリタグは、認証、ネットワークトラフィック、または
ウェブアクティビティ。これらのタグを使用して、イベントをカテゴリ別にフィルタリングして分析できます。詳細はこちらをご覧ください。
Splunkドキュメント12のイベントカテゴリタグについて。他のオプションは正しくありません。
CIMアドオンには含まれていません。検索マクロは、再利用可能な検索構文の一部であり、
他の検索から取得できます。CIMアドオンに固有のものではありませんが、一部のSplunkアプリでは独自の検索機能を提供している場合があります。

独自の検索マクロを作成できます。ワークフローアクションは、特定のフィールドまたはイベントで実行できるカスタムリンクまたはスクリプトです。
これらはCIMアドオンに固有のものではありませんが、一部のSplunkアプリは独自のワークフローを提供する場合があります。
アクション。tsidxファイルは、Splunkバケット内の生データへの用語とポインタを保存するインデックスファイルです。
これは Splunk のインデックス作成プロセスの一部であり、CIM アドオンとは関係ありません。

質問: **185**
ユーザーはどのようにしてスタック モードでチャートを表示するのでしょうか?
A. stack コマンドを使用します。
B. トレリス レイアウトの使用オプションをオンにします。
C. フォーマットメニューでスタックモードを変更します。
D. スタック モードではチャートを表示できません。タイム チャートのみ表示できます。
正解: **(**正解を表示します**)**
説明
チャートは、検索結果を2つ以上のフィールド間の関係性を示すグラフィカルな表現です2。 書式」メニューの 区タックモード」オプションを変更すると、チャートをスタックモードで表示できます2。スタックモードでは、複数の系列をチャート内で積み重ねて、各系列の累積値を表示できます2。したがって、選択肢Cが正解です。選択肢A、B、Dはチャートをスタックモードで表示する方法ではないため、不正解です。

質問: **186**
次の文のうち、以下の検索文字列を説明しているものはどれですか?
| データモデル Application_State All_Application_State 検索
A. All_Application_state という名前のデータ モデルからイベントが返されます。
B. パイプはデータモデルコマンドの後に実行されるため、イベントは返されません。
C. Evenrches は州別の売上レポートを返します。
D. Application_State という名前のデータ モデルからイベントが返されます。
正解: **(**正解を表示します**)**

質問: **187**
これら 2 つの検索では同じ結果が返されません。検索 1: ログイン失敗、検索 2: 口グイン失敗」。
A. 真
B. 偽
正解: **(**正解を表示します**)**

質問: **188**
次の検索文字列のうち、有効でないものはどれですか。
A. インデックス=ウェブ ステータス=50* | ホスト上のチャート数、ステータス
B. インデックス=ウェブ ステータス=50* | ホストごとのステータス別チャート数
C. index=web status=50* | ホスト、ステータス別のチャート数
正解: **A (**コメントを発表する**)**

この検索文字列は無効です :index=web status=50* | chart count over host,status2。この検索文字列は、chartコマンドの構文として正しくありません。chartコマンドでは、over句の後に1つのフィールドが必要であり、by句の後にオプションで1つのフィールドが必要です。しかし、この検索文字列では、over句の後にカンマで区切られた2つのフィールドがあります。これにより構文エラーが発生し、検索を実行できません。したがって、オプションAは正しいですが、オプションBとCはchartコマンドを正しく使用した有効な検索文字列であるため、正しくありません。

質問: **189**
セカンダリ検索を実行するワークフロー アクション タイプはどれですか?
A. ポスト
B. ドリルダウン
C. 取得
D. 検索
正解: **(**正解を表示します**)**
正解はD.検索です。
ワークフローアクションは、イベント内のフィールドと
ワークフローアクションはHTMLリンクを作成したり、HTTP POSTリクエストを生成したり、
フィールド値に基づく二次検索1。
Splunk Web を使用して設定できるワークフロー アクションには、GET、POST、Search2 の 3 種類があります。
GETワークフローアクションは、特定の条件でGoogle検索を実行するなどの一般的なHTMLリンクを作成します。
値を取得したり、外部の WHOIS データベースに対してドメイン名のクエリを実行したりします2。
POSTワークフローアクションは、指定されたURIへのHTTP POSTリクエストを生成します。このアクションタイプでは、
関連するフィールドセットを使用して外部の問題管理システムにエントリを作成するなどの操作を実行できます。
値2。
検索ワークフローアクションは、イベントの特定のフィールド値を使用する二次検索を開始します。
ipaddress と http_status フィールド値の特定の組み合わせの出現を探す検索
特定の期間にわたるインデックス2。
したがって、二次検索を実行するワークフロー アクション タイプは検索です。
参考文献:
Splexicon:ワークフローアクション
Splunk Webのワークフローアクションについて

質問: **190**
フィールド抽出 (FX) を使用する場合、次の区切り文字のうちどれが機能しますか? (該当するものをすべて選択してください)
A. タブ
B. パイプ
C. 入植者
D. スペース
正解: **A,B,D (**コメントを発表する**)**
参考: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep
https://community.splunk.com/t5/Splunk-Search/フィールド抽出セパレートオンコロン/mp/29751

質問: **191**
トランザクション コマンドは生のイベントにどのようなフィールドを追加しますか? (該当するものをすべて選択してください)
A. カウント
B. 持続時間
C. イベント数
D. トランザクションID
正解: **(**正解を表示します**)**
こんにちは、Bingです。Splunk Core Power User Technologiesに関するご質問にお答えできます。
正解は、B. 期間と D. トランザクション ID です。
説明は次のとおりです。
トランザクション コマンドは、さまざまな制約を満たすイベントに基づいてトランザクションを検索する Splunk コマンドです12。
トランザクションは、各メンバーの生のテキスト (_raw フィールド)、最も古いメンバーの時刻と日付のフィールド、および各メンバーのその他のすべてのフィールドの結合で構成されます12。
トランザクションコマンドは、トランザクション123の一部である生のイベントにいくつかのフィールドを追加します。これらのフィールドは次のとおりです。
期間: トランザクション123 の最初のイベントと最後のイベントのタイムスタンプ間の差 (秒単位)。
eventcount: トランザクション内のイベントの数123。
transaction_id: 各トランザクション3の一意の識別子。このフィールドは、トランザクション3のフィルタリングや結合に役立ちます。
したがって、トランザクション コマンドが生のイベントに追加するフィールドは duration と transaction_id であり、これらは質問のオプション B と D です。

質問: **192**
次の記述のうち、計算フィールドについて説明しているものはどれですか? (該当するものをすべて選択してください)
A. 計算フィールドは検索バーで使用できます。
B. 計算フィールドは抽出されたフィールドに基づいて作成できます。
C. 計算フィールドはホストとソースタイプにのみ適用できます。
D. 計算フィールドは、eval コマンドを使用して計算を実行するためのショートカットです。
正解: **A,B,D (**コメントを発表する**)**
参照：
計算フィールドは、eval コマンドを使用して既存のフィールドに対して計算を実行することで作成されるフィールドです。計算フィールドは検索バーで使用でき、計算値に基づいてイベントをフィルタリングおよび変換できます。また、計算フィールドは、正規表現、区切り文字、ルックアップなど、さまざまな方法を使用して生データから抽出されたフィールドである抽出フィールドに基づいて作成することもできます。計算フィールドは、eval コマンドを使用して計算を実行するためのショートカットではなく、eval コマンドを使用して計算を実行した結果です。計算フィールドは、ホストやソースタイプだけでなく、Splunk の任意のフィールドに適用できます。
したがって、計算フィールドについては、ステートメント A、B、および D が当てはまります。

質問: **193**
フィールド抽出 (FX) を使用して正規表現 (regex) フィールド抽出を実行するときに、requireoption を使用するとどうなるでしょうか?
A. 正規表現は編集できなくなりました。
B. 抽出されるフィールドは、今後のすべてのイベントに必要になります。
C. 必須フィールドがないイベントは検索に表示されません。
D. 必要な文字列を含むイベントのみが抽出に含まれます。

正解: (正解を表示します)

質問: **194**
特定のイベントの productName フィールドと product:d フィールドに値がある場合、どのフィールドがフィールドに入力されるでしょうか。
| eval productINFO=coalesco(productName,productid)
A. 両方のフィールド値が使用され、製品 INFO フィールドは指定されたイベントの複数値フィールドになります。
B. 最初に表示されるため、productName フィールドの値になります。
C. どちらのフィールド値も使用されず、指定されたイベントのフィールドには NULL 値が割り当てられます。
D. 2 番目に表示されるフィールドの値。
正解: **B** (コメントを発表する)
正解は B です。productName フィールドの値が最初に表示されるためです。
coalesce 関数は、任意の数の引数を受け取り、null ではない最初の値を返す eval 関数です。null 値はフィールドに値が全くないことを意味し、空の値はフィールドに値があるものの、""または長さ 0 であることを意味します。
coalesce関数は、IPアドレスやユーザー名など、名前は異なるが同じデータを表すフィールドを結合するために使用できます。また、coalesce関数は、わかりやすくするためにフィールド名を変更したり、利便性を高めたりするためにも使用できます2。
coalesce 関数の構文は次のとおりです。
coalesce(<フィールド1>,<フィールド2>,...)
coalesce関数は、引数リストの中でnullではない最初のフィールドの値を返します。すべてのフィールドがnullの場合、coalesce関数はnullを返します。
たとえば、IP アドレスが clientip または ipaddress のいずれかに抽出されるイベント セットがある場合、coalesce 関数を使用して、null でないかどうかに応じて clientip または ipaddress のいずれかの値を取得する、ip という新しいフィールドを定義できます。
| eval ip=coalesce(クライアントIP、IPアドレス)
この例では、製品名が productName または productid のいずれかに抽出される一連のイベントがあり、coalesce 関数を使用して、null でない場合に応じて productName または productid のいずれかの値を取得する productINFO という新しいフィールドを定義します。
| eval productINFO=coalesce(productName,productid)
特定のイベントにおいて、productNameフィールドとproductidフィールドの両方に値がある場合、coalesce関数は引数リストの先頭にあるproductNameフィールドの値を返します。productidフィールドはcoalesce関数によって無視されます。
したがって、特定のイベントに対して両方のフィールドに値がある場合、productName フィールドの値が productINFO フィールドの値として入力されます。
参考文献:
* 検索コマンド > 結合
* SPLUNK EVAL 関数の使用: COALESCE

質問: **195**
既存の高速データ モデルを編集するにはどうすればよいですか?
A. 高速化されたデータ モデルは、.tsidx ファイルの有効期限が切れた後でも編集できます。
B. 高速化されたデータ モデルは、ピボット ツールから編集できます。
C. データ モデルの構造を編集する前に、データ モデルをデアクセラレーションする必要があります。
D. 編集できません。新しいデータモデルを作成する必要があります。
正解: (正解を表示します)

既存の高速化データモデルは編集可能ですが、構造的な編集を行う前にデータモデルの高速化を解除する必要があります（オプションC）。これは、高速化プロセスにはデータの事前計算と保存が含まれるため、データモデルの構造を変更すると、事前計算されたデータが無効になったり、競合したりする可能性があるためです。
データ モデルの高速化が解除され、編集が完了したら、パフォーマンスを最適化するために再度高速化できます。

質問: **196**
Splunk Common Information Model (CIM) アドオンには何が含まれていますか? (該当するものをすべて選択してください)
A. カスタム視覚化
B. 事前設定されたデータモデル
C. フィールドとイベントカテゴリタグ
D. 自動データモデルアクセラレーション
正解: **(**正解を表示します**)**
Splunk Common Information Model (CIM) アドオンは、事前に構築されたデータモデルとナレッジオブジェクトのコレクションであり、さまざまなソースからのデータを正規化し、分析とレポート作成を容易にします3。CIM アドオンには、アラート、メール、データベース、ネットワークトラフィック、Web など、さまざまなドメインをカバーする事前構成済みのデータモデルが含まれています3。したがって、選択肢 B が正解です。CIM アドオンには、データモデルの共通属性とラベルを定義するフィールドとイベントカテゴリタグも含まれています3。したがって、選択肢 C が正解です。CIM アドオンには、カスタム視覚化機能や自動データモデルアクセラレーション機能は含まれていません。したがって、選択肢 A と D は不正解です。

質問: **197**
次の検索は何をしますか?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. ユーザー別に分けられたミステリーミート コーンドッグの合計数のテーブルを作成します。
B. ユーザーの合計数をコーンドッグごとに分割したテーブルを作成します。
C. ユーザーごとに分けられた、食べたアメリカン ドッグのすべての種類の数を含むテーブルを作成します。
D. ベジタリアン アメリカン ドッグごとにユーザーの合計数をグループ化するテーブルを作成します。
正解: **(**正解を表示します**)**

質問: **198**
特定のフィールドの値に関連付けられたタグを検索するための正しい構文は何ですか?
A. タグ=<フィールド>
B. タグ=<フィールド>(<タグ名>)
C. tag=<フィールド>::<タグ名>
D. tag::<フィールド>=<タグ名>
正解: **D (**コメントを発表する**)**

説明/参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/ TagandaliasfieldvaluesinSplunkWeb

質問: **199**
Splunk Common Information Model (CIM) アドオンに含まれるものは次のどれですか?
A. 最も人気のあるテクノロジー ベンダーからのソースタイプ定義。
B. 事前に構成されたデータ モデルのセット。
C. データを CIM に事前に合わせるためのスクリプト入力。
D. データ品質を検証するためのダッシュボード。
正解: (正解を表示します)
Splunk Common Information Model (CIM) アドオンは、多くの Splunk アプリの基盤コンポーネントであり、データの正規化とフィールド抽出のための共通フレームワークを提供します。このアドオンには、様々なデータタイプにわたる一貫したレポート、検索、相関分析に不可欠な、事前設定済みのデータモデルセットが含まれています。これらのデータモデルは、フィールド名とイベント構造の標準化に役立ち、異なるソースからのデータを統一された方法でクエリできるようにします。CIM アドオンは標準化されたソースタイプの使用を容易にし、データ検証をサポートしますが、その主な機能は、異なるデータセット間での一貫性を維持するために不可欠な、事前設定済みのデータモデルセットです。

質問: **200**
以下の検索文字列を最もよく表す記述は次のどれですか?
| データモデル Application_State 検索
A. イベントはデータセット Application_State から返されます。
B. Application_State という名前のデータ モデルからイベントが返されます。
C. イベントは返されません。パイプはデータ モデル コマンドの後に出現する必要があります。
D. イベントは、Application_State (フラット モード) という名前のデータ モデルから返されます。
正解: (正解を表示します)
datamodel コマンドは、データ モデルを検索する生成コマンドです。
抜粋: 「datamodel コマンドを使用すると、データ モデル データセットを検索できます。検索キーワードと一緒に使用すると、データ モデルからイベントが返されます。」つまり、検索ではデータ モデル Application_State からイベントが返されます。

質問: **201**
Splunk Common Information Model (CIM) アドオンについて説明しているのは次のうちどれですか?
A. CIM アドオンは機械学習を使用してデータを正規化します。
B. CIM アドオンには、データをマップする方法を示すダッシュボードが含まれています。
C. CIM アドオンには、データの正規化に役立つデータ モデルが含まれています。
D. CIM アドオンは Splunk 環境に自動的にインストールされます。
正解: (正解を表示します)
Splunk Common Information Model (CIM)アドオンは、次のようなデータモデルを含むSplunkアプリです。
異なるソースやフォーマットからのデータを正規化します。CIMアドオンは、共通かつ一貫した方法を定義します。
Splunkのフィールドとイベントに名前を付けて分類します。これにより、複数のデータを簡単に相関分析できます。
ネットワーク、セキュリティ、ウェブなど、さまざまなドメインに対応しています。CIMアドオンは機械学習を使用して
データの正規化ではなく、事前定義されたフィールド名と値に依存します。CIMアドオンには
ダッシュボードはデータのマッピング方法を示すものではなく、ダッシュボードの使い方に関するドキュメントや例を提供するものです。

データモデル。CIMアドオンはSplunk環境に自動的にインストールされず、
Splunkbase からダウンロードしてインストールしました。

質問: **202**
特に大規模な環境において、次の記述のうち正しいものはどれですか?
A. 2 つ以上のフィールドでイベントをグループ化する場合は、scats コマンドを使用します。
B. statsコマンドはtransactionコマンドよりも高速かつ効率的です
C. トランザクション コマンドは、統計コマンドよりも高速かつ効率的です。
D. 計算の結果を確認する場合は、トランザクション コマンドを使用します。
正解: **(**正解を表示します**)**
参照：
stats コマンドは、特に大規模環境では、transaction コマンドよりも高速で効率的です。stats コマンドは、カウント、合計、平均など、イベントの要約統計を計算するために使用されます。stats コマンドは、1 つ以上のフィールドまたは時間バケットによってイベントをグループ化できます。stats コマンドは、イベントのグループから新しいイベントを作成するのではなく、統計値を持つ新しいフィールドを作成します。transaction コマンドは、フィールド、時間、またはその両方などの共通の特性に基づいて、イベントをトランザクションにグループ化するために使用されます。transaction コマンドは、1 つ以上のフィールドを共有するイベントのグループから新しいイベントを作成します。transaction コマンドは、duration、eventcount、starttime など、各トランザクションの追加フィールドも作成します。transaction コマンドは、処理するデータが多く、作成するイベントとフィールドが多いため、stats コマンドよりも遅く、多くのリソースを消費します。

質問: **203**
値引数が指定されていない場合、fillnull コマンドは null 値を何に置き換えますか?
A. 0
B. 該当なし
C. NaN
D. NULL
正解: **(**正解を表示します**)**
参照：
fillnull コマンドは、null 値を指定された値に置き換える検索コマンドです。値が指定されていない場合は 0 に置き換えます。null 値とは、Splunk で欠落している、空である、または未定義の値です。fillnull コマンドは、すべてのフィールドまたは特定のフィールドの null 値を置き換えることができます。fillnull コマンドは、null 値を置き換える値を指定するためのオプション引数 value を取ることができます。value 引数が指定されていない場合、fillnull コマンドはデフォルトで null 値を 0 に置き換えます。

質問: **204**
どちらの記述が正しいでしょうか?
A. ピボットはデータセットの作成に使用されます。
B. データ モデルはランダムに構造化されたデータセットです。
C. ピボットはレポートとダッシュボードの作成に使用されます。
D. ほとんどの場合、各 Splunk ユーザーは独自のデータ モデルを作成します。
正解: **C (**コメントを発表する**)**
参照：

ピボットは、レポートやダッシュボードの作成に使用されます。ピボットは、SPLコマンドを記述することなく、データモデルからレポートやダッシュボードを作成できるツールです。フィルター、行、列、セル、グラフ、表、マップなど、さまざまなオプションを使用してデータを視覚化および分析できます。また、高速化されたデータモデルのサマリーデータを使用することで、レポートやダッシュボードの作成を高速化することもできます。
Pivotはデータセットやデータモデルの作成には使用されません。データセットは、データを構造化かつ階層的に表現するイベントの集合です。データモデルは、ネットワークトラフィック、Webアクティビティ、認証など、様々なドメイン向けに事前定義されたデータセットです。データセットとデータモデルは、datamodelやpivotなどのコマンドを使用して作成できます。

質問: **205**
特定のイベントの productName フィールドと product:d フィールドに値がある場合、どのフィールドがフィールドに入力されるでしょうか。
A. | eval productINFO=coalesco(productName,productid)
B. 両方のフィールド値が使用され、製品 INFO フィールドは指定されたイベントの複数値フィールドになります。
C. 最初に表示されるため、productName フィールドの値になります。
D. どちらのフィールド値も使用されず、指定されたイベントに対してフィールドに NULL 値が割り当てられます。
E. 2 番目に表示されるフィールドの値。
正解: **(**正解を表示します**)**
正解は B です。productName フィールドの値が最初に表示されるためです。
coalesce 関数は、任意の数の引数を受け取り、null ではない最初の値を返す eval 関数です。null 値はフィールドに値が全くないことを意味し、空の値はフィールドに値があるものの、""または長さ 0 であることを意味します。
coalesce関数は、IPアドレスやユーザー名など、名前は異なるが同じデータを表すフィールドを結合するために使用できます。また、coalesce関数は、わかりやすくするためにフィールド名を変更したり、利便性を高めたりするためにも使用できます2。
coalesce 関数の構文は次のとおりです。
coalesce(<フィールド1>,<フィールド2>,...)
coalesce関数は、引数リストの中でnullではない最初のフィールドの値を返します。すべてのフィールドがnullの場合、coalesce関数はnullを返します。
たとえば、IP アドレスが clientip または ipaddress のいずれかに抽出されるイベント セットがある場合、coalesce 関数を使用して、null でないかどうかに応じて clientip または ipaddress のいずれかの値を取得する、ip という新しいフィールドを定義できます。
| eval ip=coalesce(クライアントIP、IPアドレス)
この例では、製品名が productName または productid のいずれかに抽出される一連のイベントがあり、coalesce 関数を使用して、null でない場合に応じて productName または productid のいずれかの値を取得する productINFO という新しいフィールドを定義します。
| eval productINFO=coalesce(productName,productid)
特定のイベントにおいて、productNameフィールドとproductidフィールドの両方に値がある場合、coalesce関数は引数リストの先頭にあるproductNameフィールドの値を返します。productidフィールドはcoalesce関数によって無視されます。
したがって、特定のイベントに対して両方のフィールドに値がある場合、productName フィールドの値が productINFO フィールドの値として入力されます。
参照：
検索コマンド > 結合
Splunk EVAL関数の使用法 :COALESCE

質問: **206**
マクロweekly_sales (2)には検索文字列が含まれています。
index=games | eval ProductSales = $Price$ * $AmountSold$

次のどれが結果を返しますか?
A. '週間売上(3)'
B. 'weekly_sales($3.995, $108)'
C. 'weekly_sales (3.99, 10)'
D. '週間売上 (3.99, 10)'
正解: **(**正解を表示します**)**
検索文字列で検索マクロを使用するには、マクロの前後にバッククォート文字 ` を配置する必要があります。
name1。また、macro2で定義されているのと同じ数の引数を使用する必要があります。マクロweekly sales
(2) には2つの引数、PriceとAmountSoldがあります。したがって、これらの引数には2つの値を指定する必要があります。
マクロを呼び出すとき。
オプションAは、マクロ名をバッククォートではなく括弧で囲んでいるため、誤りです。オプション
Bはマクロ名にスペースではなくアンダースコアを使用しているため不正解です。Dは不正解です。
引数値を区切るのにコンマではなくスペースを使用するためです。
参考資料:1検索での検索マクロの使用 - Splunkドキュメント2設定で検索マクロを定義する - Splunk
ドキュメント

質問: **207**
|join コマンドを使用して、2つの別々の結果テーブルを結合します。外部テーブルには以下の値があります。
以下の表を参照してください

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

テーブルを結合するために使用される SPL の行は次のとおりです: | join employeeNumber type=outer 新しいテーブルに返される行数はいくつですか?

A. ゼロ
B. 5
C. 8
D. 3
正解: **C** (コメントを発表する)
Splunkで|join employeeNumber type=outerコマンドを使用して外部結合を実行すると、employeeNumberフィールドに基づいて両方のテーブルの行が結合されます。外部結合は、両方のテーブルのすべての行を返します。一致する行がある場合は、両方のテーブルから一致する行も返します。一致する行がない場合、一致しない側の結合結果はNULLになります。
提供されたテーブルでは、最初のテーブルには5行、2番目のテーブルには3行あります。これは外部結合なので、両方のテーブルのすべての行が返されます。つまり、新しいテーブルには、両方のテーブルの一致する行と一致しない行を合わせた合計8行が含まれます。
参考文献:
* join コマンドに関する Splunk ドキュメント。
* 結合の使用方法と結合の種類に関する Splunk コミュニティのディスカッション。

質問: **208**
|join コマンドを使用して、2つの別々の結果テーブルを結合します。外部テーブルには以下の値があります。
以下の表を参照してください

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

テーブルを結合するために使用される SPL の行は次のとおりです: | join employeeNumber type=outer 新しいテーブルに返される行数はいくつですか?
A. ゼロ
B. 5
C. 8
D. 3
正解: **C** (コメントを発表する)
Splunkで|join employeeNumber type=outerコマンドを使用して外部結合を実行すると、employeeNumberフィールドに基づいて両方のテーブルの行が結合されます。外部結合は、両方のテーブルのすべての行を返します。一致する行がある場合は、両方のテーブルから一致する行も返します。一致する行がない場合、一致しない側の結合結果はNULLになります。

提供されたテーブルでは、最初のテーブルには5行、2番目のテーブルには3行あります。これは外部結合なので、両方のテーブルのすべての行が返されます。つまり、新しいテーブルには、両方のテーブルの一致する行と一致しない行を合わせた合計8行が含まれます。
参考文献:
join コマンドに関する Splunk ドキュメント。
結合の使用方法と結合の種類に関する Splunk コミュニティのディスカッション。

質問: **209**
次のどれが eval コマンドの tostring 関数で使用できますか (該当するものをすべて選択してください)。
A. "16進数"
B. "カンマ"
C. "10進数"
D. "期間"
正解: **(**正解を表示します**)**
説明
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY。

質問: **210**
以下のコマンドを説明する記述はどれですか（該当するものをすべて選択してください）Sourcetype=access_combined | transaction JSESSIONID
A. eventcount という名前の追加フィールドが作成されます。
B. 同じ JSESSIONID を持つイベントは 1 つのイベントにグループ化されます。
C. maxspan という名前の追加フィールドが作成されます。
D. duration という名前の追加フィールドが作成されます。
正解: **(**正解を表示します**)**

質問: **211**
これらを使用すると、検索用語に基づいてイベントを分類できます。
回答を選択してください。
A. タグ
B. マクロ
C. イベントタイプ
D. グループ
正解: **(**正解を表示します**)**

質問: **212**

新しいルックアップを作成するための正しい手順は何ですか?
1. ルックアップを自動的に実行するように設定する
2. ルックアップテーブルを作成する
3. ルックアップを定義する
A. 2, 3, 1
B. 1、2、3
C. 2, 1, 3
D. 3, 2, 1
正解: **A** (コメントを発表する)

質問: **213**
|join コマンドを使用して、2つの別々の結果テーブルを結合します。外部テーブルには以下の値があります。
以下の表を参照してください

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

テーブルを結合するために使用される SPL の行は次のとおりです: | join employeeNumber type=outer 新しいテーブルに返される行数はいくつですか?
A. ゼロ
B. 5
C. 8
D. 3
正解: (正解を表示します)

Splunkで|join employeeNumber type=outerコマンドを使用して外部結合を実行すると、employeeNumberフィールドに基づいて両方のテーブルの行が結合されます。外部結合は、両方のテーブルのすべての行を返します。一致する行がある場合は、両方のテーブルから一致する行も返します。一致する行がない場合、一致しない側の結合結果はNULLになります。
提供されたテーブルでは、最初のテーブルには5行、2番目のテーブルには3行あります。これは外部結合なので、両方のテーブルのすべての行が返されます。つまり、新しいテーブルには、両方のテーブルの一致する行と一致しない行を合わせた合計8行が含まれます。
参考文献:
join コマンドに関する Splunk ドキュメント。
結合の使用方法と結合の種類に関する Splunk コミュニティのディスカッション。

質問: **214**
ピボットを使用する可能性が高いのはどのユーザー グループですか?
A. ユーザー
B. 建築家
C. 管理者
D. ナレッジマネージャー
正解: **D (**コメントを発表する**)**
説明/参考資料: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

質問: **215**
Splunk Common Information Model (CIM) アドオンに含まれるデータ モデルは次のうちどれですか。
（該当するものをすべて選択してください）
A. アラート
B. メール
C. データベース
D. ユーザー権限
正解: **(**正解を表示します**)**
参考 :https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview Splunk Common Information Model（CIM）アドオンは、さまざまなソースからのデータを正規化し、分析とレポート作成を容易にする、事前に構築されたデータモデルとナレッジオブジェクトのコレクションです3。CIMアドオンには、アラート、メール、データベース、ネットワークトラフィック、Webなど、さまざまなドメインをカバーする複数のデータモデルが含まれています3。したがって、オプションA、B、CはCIMアドオンに含まれるデータモデルの名前であるため、正解です。オプションDは、ユーザー権限はCIMアドオンのデータモデルの名前ではないため、不正解です。

質問: **216**
どちらの記述が正しいでしょうか?
A. ピボットはデータセットの作成に使用されます。
B. データ モデルはランダムに構造化されたデータセットです。
C. ピボットはレポートとダッシュボードの作成に使用されます。
D. ほとんどの場合、各 Splunk ユーザーは独自のデータ モデルを作成します。
正解: **C (**コメントを発表する**)**
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

質問: **217**

計算フィールドを定義するには何が必要ですか?
A. 式の評価
B. データモデル
C. イベントタイプ
D. 正規表現
正解: **(**正解を表示します**)**
Splunk の計算フィールドは eval 式を使用して作成され、ユーザーは検索時にフィールド値に対して計算や変換を実行できます。
参考文献:
Splunk ドキュメント - 計算フィールド

質問: **218**
次の文のうち、フィールド エイリアスについて説明しているものはどれですか。
A. フィールドエイリアス名が元のフィールド名に置き換えられます。
B. フィールドエイリアスは、ルックアップファイル定義で使用できます。
C. フィールド エイリアスは、ソースとソースタイプ間でのみデータを正規化します。
D. フィールドエイリアス名は、検索の一部として使用される場合、大文字と小文字は区別されません。
正解: **B (**コメントを発表する**)**
説明
フィールド エイリアスは、Splunk のフィールドの別名です。フィールド エイリアスを使用すると、同じ概念に対して異なるフィールド名を持つ異なるソースおよびソースタイプ間でデータを正規化できます。たとえば、src_ip のフィールド エイリアスを作成して、clientip、source_address、または異なるソースタイプのソース IP アドレスを表すその他のフィールド名にマップできます。フィールド エイリアスは、ルックアップ ファイル定義でも使用して、データ内のフィールドをルックアップ ファイルのフィールドにマップできます。たとえば、src_ip のフィールド エイリアスを使用して、IP アドレスの位置情報を含むルックアップ ファイルで ip_address にマップできます。フィールド エイリアス名は元のフィールド名を置き換えず、異なる名前でフィールドのコピーを作成します。フィールド エイリアス名は、検索の一部として使用する場合、大文字と小文字が区別されます。つまり、src_ip と SRC_IP は異なるフィールドです。

質問: **219**
ピボットを使用する可能性が高いのはどのユーザー グループですか?
A. ユーザー
B. 建築家
C. 管理者
D. ナレッジマネージャー
正解: **(**正解を表示します**)**
参考:https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

質問: **220**
検索に「example(100,200)」が含まれています。マクロの名前は何ですか？
A. 例(2)
B. 例(var1,var2)
C. 例($,$)
D. 例[2]

正解: **B** (コメントを発表する)
Splunkでは、引数を受け入れるマクロは、引数のプレースホルダをexample(var1, var2)という形式で定義します。検索example(100,200)では、var1とvar2にそれぞれ「100」と「200」が渡されます。
参考文献:
Splunk ドキュメント - マクロ

質問: **221**
次の記述のうち、Filed Extractor (FX) の使用法を説明しているものはどれですか。
A. 抽出されたフィールドはナレッジ オブジェクトとして保持されます。
B. フィールド抽出を使用して抽出されたフィールドは永続的ではないため、検索ごとに定義する必要があります。
C. フィールド抽出機能は、PERL を使用して生のイベントからフィールドを抽出します。
D. フィールド抽出機能は、検索時にすべてのフィールドを自動的に抽出します。
正解: (正解を表示します)

質問: **222**
次のシナリオのうち、保存した検索よりもイベント タイプの方が効果的なのはどれですか。
A. 検索に常に同じ時間範囲を含める必要がある場合。
B. 検索を他のユーザーのダッシュボードに追加する必要がある場合。
C. 検索文字列を将来の検索で使用する必要があるとき。
D. 検索文字列にフォーマットを含める必要がある場合。
正解: **C** (コメントを発表する)
参照：
イベントタイプとは、イベントに一致する検索文字列に基づいてイベントを分類する方法です2。イベントタイプを使用すると、長く複雑な検索文字列を短くシンプルなイベントタイプ名に置き換えることで、検索を簡素化できます2。イベントタイプを使用すると、検索文字列を記憶したり再度入力したりする必要がなく、保存済みの検索文字列を再利用できるため、将来の検索で同じ検索文字列を使用する必要がある場合、保存済みの検索文字列よりも効果的です2。したがって、オプションCが正解です。オプションA、B、Dは不正解です。これらのシナリオでは、イベントタイプが保存済みの検索文字列よりも効果的ではありません。

質問: **223**
フィールド抽出ツール（FX）は、カスタムフィールドを抽出するために使用されます。このカスタムフィールドを使用してレポートを作成できます。作成したレポートは、組織内の他のユーザーと共有できます。組織内の他のユーザーが共有レポートを実行しても結果が返されない場合は、なぜでしょうか？（該当するものをすべて選択してください）
A. 高速モードが有効です。
B. ダッシュボードは非公開です。
C. 抽出は非公開です
D. レポートを実行している組織内のユーザーには、インデックスへのアクセス権がありません。
正解: (正解を表示します)
フィールド抽出ツール（FX）は、グラフィカルインターフェース2を使用してイベントからフィールドを抽出できるツールです。FXで抽出したカスタムフィールドを使用してレポートを作成し、組織内の他のユーザーと共有できます2。ただし、他のユーザーが共有レポートを実行しても結果が返されない場合は、2つの理由が考えられます。1つは、抽出がプライベート設定になっていることです。つまり、抽出されたフィールドは自分だけが表示および使用できます2。抽出を他のユーザーが利用できるようにするには、抽出をグローバルまたはアプリレベルに設定する必要があります2。

したがって、選択肢Cが正解です。もう一つの理由は、他のユーザーがイベントが保存されているインデックス2へのアクセス権を持っていないことです。この問題を解決するには、他のユーザーにインデックス2に対する適切な権限を付与する必要があります。したがって、選択肢Dが正解です。選択肢AとBはフィールド抽出やレポートとは関係がないため、不正解です。

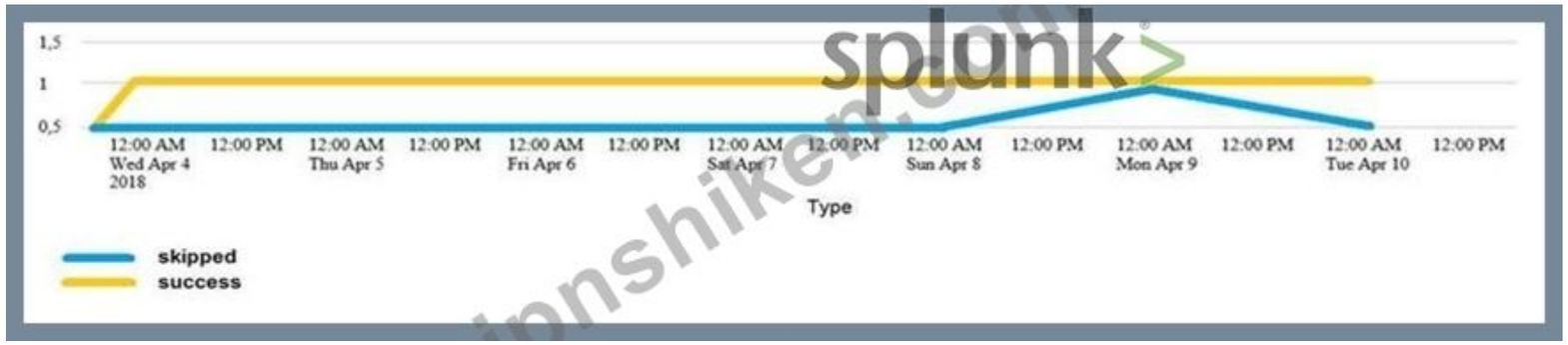
質問: **224**
フィールド抽出（FX）を使用して正規表現フィールド抽出を実行する場合、サンプルイベントを選択する前にデータ型を選択する必要があります。サポートされているデータ型は次のうちどれですか？
A. インデックスまたはソース
B. ソースタイプまたはホスト
C. インデックスまたはソースタイプ
D. ソースタイプまたはソース
正解: (正解を表示します)
Splunkのフィールド抽出機能（FX）を使用して正規表現フィールドを抽出する場合、抽出を実行するコンテキストを選択することが重要です。コンテキストとは、基本的に、フィールド抽出タスクで対象とするデータのサブセットのことです。
D: ソースタイプまたはソース: これが正しい選択肢です。フィールド抽出ツールを使用する最初のステップでは、フィールド抽出のデータ型を選択するように求められます。利用可能なオプションは通常、データの性質とSplunk内でのデータの整理方法に基づいています。「ソースタイプ」は処理対象のデータの種類、つまりSplunkが特定の処理ルールを適用するのに役立つ分類を指します。「ソース」は、特定のログファイルやデータ入力など、データの取得元を指します。ソースタイプまたはソースのいずれかを選択することで、正規表現抽出を実行するデータセットを絞り込み、より管理しやすく、関連性の高いデータセットを作成できます。

質問: **225**
次のどれが eval コマンドの tostring 関数で使用できますか (該当するものをすべて選択してください)。
A. "16進数"
B. "カンマ"
C. "10進数"
D. "期間"
正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.29 evalコマンドのtostring関数は、数値を文字列値に変換します。オプションで、文字列値の形式を指定する2番目の引数を取ることができます。指定可能な形式は以下のとおりです。
hex: 数値を 16 進文字列に変換します。
カンマ: 数値の千の位を区切るためにカンマを追加します。
duration: 数値を「2h 3m 4s」などの人間が読める期間文字列に変換します。
したがって、tostring 関数では形式 A、B、および D を使用できます。

質問: **226**
計算フィールドは次のどれに基づくのでしょうか?
A. ルックアップテーブル
B. 検索文字列内で生成されたフィールド
C. 抽出されたフィールド
D. 正規表現
正解: (正解を表示します)

説明
前述の通り、計算フィールドとは、別のフィールド（複数可の値に基づいて作成されるフィールドです2。計算フィールドは、正規表現、区切り文字、キーと値のペアなど、様々な方法を用いて生データから抽出されたフィールド（抽出フィールド）に基づいて作成できます2。したがって、選択肢Bが正解です。選択肢A、C、Dは不正解です。これらのフィールドは、計算フィールドの基になるフィールドの種類ではないためです。

質問: **227**
次の検索のうちどれが、下図のようなグラフを作成しますか?



index=_internal sourcetype=SavedSplunker | フィールド sourcetype、status |
A. トランザクション ステータス maxspan=1d | ステータス別の統計カウント
index=_internal sourcetype=SavedSplunker | フィールド sourcetype、status |
B. トランザクション ステータス maxspan=1d | チャート カウント OVER ステータス by _time
index=_internal sourcetype=SavedSplunker | フィールド sourcetype、status |
C. トランザクション ステータス maxspan=1d | ステータス別のタイムチャート カウント
D. これらの検索のいずれも、同様のグラフを生成しません。
正解: (正解を表示します)
これらの関数はいずれも、図のグラフとは関連がありません。これらの関数はすべて、有効な引数ではないmaxspan=ldを持っています。

質問: **228**
データ モデルを作成するときに、どのルート データセットに少なくとも 1 つの制約が必要ですか?
A. ルートトランザクションデータセット
B. ルートイベントデータセット
C. ルート子データセット
D. ルート検索データセット
正解: (正解を表示します)
正解はB. ルートイベントデータセットです。これは、ルートイベントデータセットが制約によって定義されるためです。
データセットに関連しないイベントを除外します。ルートイベントデータセットの制約は、次のような単純な検索です。

かなり広範囲のデータを返します（sourcetype=access_combinedなど）。制約がない場合、ルートイベントは
データセットにはインデックス内のすべてのイベントが含まれるため、データモデリングには役立ちません。詳細については、
Splunkのドキュメント1からデータモデルの設計方法とルートイベントデータセットの追加方法について学びます。
ルートトランザクションデータセットとルート検索データセットでは定義方法が異なるため、オプションは正しくありません。
トランザクション定義や複雑な検索などのデータセットやルート子データセットは有効なタイプではありません
ルート データセットの。

質問: **229**
次の統計コマンドのうち、ページとサーバーの一意の組み合わせごとに合計バイト数を表示するものはどれですか?
A. index=web | ページ別、サーバー別の統計合計（バイト）
B. index=web | ページサーバー別の統計合計（バイト）
C. index=web | ページとサーバーの統計合計(バイト)
D. index=web | stats sum(bytes) BY values (page) values (server)
正解: **B (**コメントを発表する**)**
ページとサーバーの一意の組み合わせごとに合計バイト数を表示する正しいコマンドは、index=web | stats sum (bytes) BY page serverです。Splunkでは、statsコマンドはデータセット全体の集計統計（count、sum、avgなど）を計算するために使用されます。BY句を使用すると、指定されたフィールドごとに結果がグループ化されます。正しい構文では、フィールド名の間にカンマや「AND」は使用しません。代わりに、BY句内でフィールド名をスペースで区切って列挙します。
参照：
BY 句を指定した stats コマンドの使用法は、Splunk コミュニティの例によって確認されており、by foo bar を指定した stats では、by フィールド 1 の一意の組み合わせごとに 1 行が出力されることが説明されています。

質問: **230**
この検索に当てはまるのは次のうちどれですか？（該当するものをすべて選択してください。）検索sourcetype=access* |fields action productId status
A. 抽出されるフィールドを制限します
B. パフォーマンスを向上させるためにテーブルコマンドを使用します
C. 3列のテーブルを返します
D. 検索語「fields AND action AND productId AND status」を含むすべてのイベントを検索します。
正解: **(**正解を表示します**)**

質問: **231**
検索ワークフロー アクションを作成するときに必須となるフィールドはどれですか?
A. データモデル名
B. 権限設定
C. eval文
D. 検索文字列
正解: **(**正解を表示します**)**

質問: **232**
検索ワークフロー アクションを作成するときに必須となるフィールドはどれですか?
A. 権限設定

B. データモデル名
C. eval文
D. 検索文字列
正解: (正解を表示します)

質問: **233**
POST ワークフロー アクションを作成するには、次のうちどれが必要ですか?
A. ラベル、URI、検索文字列。
B. XML 属性、URI、名前。
C. ラベル、URI、投稿引数。
D. URI、検索文字列、時間範囲ピッカー。
正解: (正解を表示します)
説明/参照: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaPOSTworkflowaction

質問: **234**
次の文のうち、マクロについて説明しているものはどれですか?
A. マクロは完全な検索を含む必要がある再利用可能な検索文字列です。
B. マクロは、柔軟な時間範囲を持つことができる再利用可能な検索文字列です。
C. マクロは、固定の時間範囲を持つ必要がある再利用可能な検索文字列です。
D. マクロは、検索の一部のみを含む再利用可能な検索文字列です。
正解: (正解を表示します)
参照：
マクロは、検索用語、コマンド、引数など、検索の任意の部分を含めることができる再利用可能な検索文字列です。マクロには、マクロの実行時に指定できる柔軟な時間範囲を設定できます。また、マクロの実行時にマクロに渡すことができる引数も設定できます。マクロは、[設定] メニューを使用するか、macros.conf ファイルを編集することで作成できます。マクロには完全な検索を含める必要はなく、再利用する必要がある部分のみを含めることができます。マクロには固定の時間範囲を設定する必要はありませんが、相対的または絶対的な時間範囲修飾子を使用できます。マクロには検索の一部のみを含める必要はなく、検索の複数の部分を含めることができます。

質問: **235**
過去 7 日間の範囲で実行された次の検索について考えてみましょう。
index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane 結果が 12 時間間隔でグループ化されるようにデフォルトの時間範囲を変更するには、どのオプションを使用しますか?
A. スパン=12時間
B. 時間範囲=12時間
C. スパン=12
D. タイムスパン=12
正解: (正解を表示します)
spanオプションは、timechartコマンドの時間範囲を指定するために使用されます。span値は、数値に時間単位（hは時間、dは日、wは週など）を続けて指定できます。span値は、データがどのように時間バケットにグループ化されるかを決定します。例えば、span=12hは、データが12時間間隔にグループ化されることを意味します。timespanオプションは、timechartコマンドでは有効なオプションではありません。
1: Splunk Core Certified Power User Track、9 ページ。2: Splunk ドキュメント、timechart コマンド。

質問: **236**
Splunk の単一インスタンスでマシンの入力、解析、インデックスを管理することはできません。
A. 偽
B. 真
正解: **(**正解を表示します**)**

質問: **237**
少なくとも 1 つの REJECT イベントを含むトランザクション内のすべての寄与イベントを識別するには、どの構文が正しいですか。
A. インデックス=メイン | トランザクションセッションID | そのトランザクション=拒否
B. インデックスメイン | REJECT トランスセッションID
C. インデックス=メイン | トランザクションセッションID | トランザクション=拒否"
D. インデックスメイン | トランザクションセッションID | 検索拒否
正解: **(**正解を表示します**)**

質問: **238**
正規表現 (regex) を手動で編集した後、次の文のうち正しいものはどれですか。
A. 手動で行われた変更は、フィールド抽出 (FX) UI で元に戻すことができます。
B. フィールド抽出 (FX) UI でフィールド抽出を編集することはできなくなりました。
C. フィールド抽出 (FX) UI を使用して作成された正規表現 (regex) を手動で編集することはできません。
D. フィールド抽出 (FX) UI は、手動で編集されたものに加えて、独自のバージョンのフィールド抽出を保持します。
正解: **(**正解を表示します**)**
説明
フィールド抽出 (FX) UI を使用して作成された正規表現 (regex) を手動で編集した後は、FX UI でフィールド抽出を編集できなくなります。FX UI は、区切り文字または正規表現を使用してデータからフィールドを抽出するのに役立つツールです。FX UI は、選択したサンプル値に基づいて正規表現を生成することも、FX UI に独自の正規表現を入力することもできます。ただし、props.conf ファイルで正規表現を手動で編集すると、FX UI は変更を認識できなくなり、FX UI でフィールド抽出を編集できなくなります。フィールド抽出をさらに変更するには、props.conf ファイルを使用する必要があります。FX UI は props.conf ファイルで行われた変更を追跡しないため、手動で行われた変更を FX UI で元に戻すことはできません。props.conf ファイルで行う限り、FX UI を使用して作成された正規表現を手動で編集することは可能です。
したがって、正規表現を手動で編集することに関しては、ステートメント B のみが当てはまります。

質問: **239**
ピボット エディターを使用すると、ユーザーはすぐにレポートを作成できますが、ピボット コマンドを使用する必要があります。'
A. 偽
B. 真
正解: **(**正解を表示します**)**

質問: **240**
トランザクション内のイベントに共通するものは何ですか?
A. トランザクション内のすべてのイベントは同じタイムスタンプを持つ必要があります。
B. トランザクション内のすべてのイベントは同じソースタイプを持つ必要があります。

C. トランザクション内のすべてのイベントは、まったく同じフィールド セットを持つ必要があります。
D. トランザクション内のすべてのイベントは、1 つ以上のフィールドによって関連付けられる必要があります。
正解: **(**正解を表示します**)**
参照: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions トランザクションとは、フィールド、時間、またはその両方など、いくつかの共通特性を持つイベントのグループです。トランザクションは、transaction コマンドを使用するか、props.conf で transactiontype=true を指定してイベントタイプを定義することで作成できます。トランザクション内のイベントには、互いに関連付ける共通フィールドが 1 つ以上あります。たとえば、Web ログ内の各ユーザーセッションの一意の識別子である JSESSIONID に基づいてトランザクションを作成できます。トランザクション内のイベントは、タイムスタンプ、ソースタイプ、またはまったく同じフィールドセットを持つ必要はありません。トランザクションを定義する 1 つ以上のフィールドを共有しているだけで十分です。

質問: **241**
計算フィールドの名前が抽出フィールドと同じ場合、抽出フィールドはどうなりますか?
A. 計算フィールドは抽出されたフィールドを上書きします。
B. 計算されたフィールドと抽出されたフィールドが結合されます。
C. 計算フィールドは抽出されたフィールドを複製します。
D. エラーが返され、検索は失敗します。
正解: **A (**コメントを発表する**)**
計算フィールドを定義するときは、eval式で作成されるフィールドの名前を指定できます。
変更します。計算フィールドの名前が既存の抽出フィールドの名前と一致する場合、計算フィールドは
抽出されたフィールドを上書きし、その値をeval式の結果で置き換えます。つまり、
抽出されたフィールドの元の値は検索や分析に使用できなくなります。これを避けるには、
計算フィールドには一意の名前を使用するか、抽出フィールドには別の名前を使用します2
1: Splunk Core Certified Power User Track、9ページ。2: Splunkドキュメント、計算フィールドの設定
props.conf を使用します。

質問: **242**
計算フィールドの名前が抽出フィールドと同じ場合、抽出フィールドはどうなりますか?
A. 計算フィールドは抽出されたフィールドを上書きします。
B. 計算されたフィールドと抽出されたフィールドが結合されます。
C. 計算フィールドは抽出されたフィールドを複製します。
D. エラーが返され、検索は失敗します。
正解: **A (**コメントを発表する**)**

計算フィールドを定義する際に、eval式によって作成または変更されるフィールドの名前を指定できます。計算フィールドの名前が既存の抽出フィールドの名前と一致する場合、計算フィールドは抽出フィールドを上書きし、その値をeval式の結果に置き換えます。つまり、抽出フィールドの元の値は検索や分析に使用できなくなります。これを避けるには、計算フィールドに一意の名前を使用するか、抽出フィールドに別の名前を使用する必要があります2。
1: Splunk Core Certified Power User Track、9 ページ。2: Splunk ドキュメント、props.conf を使用して計算フィールドを構成する。

質問: **243**
where コマンドのブール値の正しい評価順序は最初から最後までどれですか?
A. NOT、括弧、OR、AND
B. AND、括弧、NOT、OR
C. 括弧、NOT、AND、OR
D. 括弧、NOT、OR、AND
正解: **C (**コメントを発表する**)**
Splunk では、where コマンド内のブール論理の演算順序は次のようになります。
* 括弧: 括弧内の演算が最初に評価されます。
* NOT: NOT 演算子は括弧の後で評価されます。
* AND: 次に AND 演算子が評価されます。
* OR: 最後に、OR 演算子が評価されます。
この順序により、括弧内の式が優先され、次に否定 (NOT)、接続詞 (AND)、最後に論理和 (OR) が優先されます。
参考文献:
* Splunk ドキュメント - where コマンド

質問: **244**
scats コマンドの代わりに transaction コマンドを使用する必要があるのはどのような場合ですか?
A. 複数の値をグループ化する必要がある場合。
B. 検索結果において期間が関係ない場合。
C. トランザクションに 1000 を超えるイベントがある場合。
D. 開始制約と終了制約に基づいてグループ化する必要がある場合。
正解: **D (**コメントを発表する**)**
説明
transactionコマンドは、フィールド、時間、またはその両方などの共通の特性に基づいて、イベントをトランザクションにグループ化するために使用されます。また、transactionコマンドでは、トランザクションの開始または終了を示すフィールド値など、トランザクションの開始および終了制約を指定することもできます。statsコマンドは、イベントの集計統計（カウント、合計、平均など）を計算するために使用されます。statsコマンドは、開始および終了制約に基づいてイベントをグループ化することはできません。フィールドまたは時間バケットに基づいてのみグループ化できます。したがって、開始および終了制約に基づいてイベントをグループ化する必要がある場合は、statsコマンドではなくtransactionコマンドを使用する必要があります。

質問: **245**
データ モデル コマンドを使用して、Web データセット内のデータ モデル内のフィールドを検索する正しい方法はどれですか。
A. | データモデル Web 検索 | ファイルされた Web *
B. | 検索データモデル Web Web | ファイルされた Web*
C. | データモデル ウェブ ウェブフィールド | 検索ウェブ*

D. データモデル = web | 検索 web | ファイルされた web*
正解: (正解を表示します)
データモデルコマンドを使用すると、高速化されたデータモデル1に対して検索を実行できます。データモデルコマンドの構文は、| datamodel <model_name> <dataset_name> [search <search_string>]1です。
したがって、オプションAは、Webデータセット内のデータモデル内のフィールドを検索するためにデータモデルコマンドを使用する正しい方法です。オプションBとCは、データモデルコマンドの構文に従っていないため、誤りです。オプションDは、データモデルコマンドを全く使用していないため、誤りです。

質問: **246**
ユーザーは、数値フィールドの値を文字列に変換し、それらの値で並べ替えたいと考えています。
theeva と thesort のどちらのコマンドを最初に使用すべきでしょうか?
A. eval と sort のどちらを先に使用しても問題ありません。
B. まず eval を使用して数値を文字列に変換し、次にソートします。
C. 最初に sort を使用し、次に eval を使用して数値を文字列に変換します。
D. 同じフィールドで sort コマンドと eval コマンドを使用することはできません。
正解: (正解を表示します)
evalコマンドは、式2に基づいて新しいフィールドを作成したり、既存のフィールドを変更したりするために使用されます。
コマンドは、1つ以上のフィールドで結果を昇順または降順に並べ替えるために使用されます2。
数値フィールドの値を文字列に変換し、それらの値で並べ替えるには、まず sort コマンドを使用する必要があります。
次にevalコマンドを使って値を文字列2に変換します。こうすることで、sortコマンドは元の文字列を使用します。
正しく並べ替えられない可能性のある文字列値ではなく、数値を並べ替えに使用します。したがって、
オプション C は正解ですが、オプション A、B、D は不正解です。

質問: **247**
レポートはデフォルトでドリルダウンを許可します。
A. ない
B. です
正解: (正解を表示します)

質問: **248**
ユーザーは、数値フィールドの値を文字列に変換し、それらの値で並べ替えたいと考えています。
最初に eval コマンドと sort コマンドのどちらのコマンドを使用する必要がありますか?
A. 最初に sort を使用し、次に eval を使用して数値を文字列に変換します。
B. まず eval を使用して数値を文字列に変換し、次にソートします。
C. 同じフィールドで sort コマンドと eval コマンドを使用することはできません。
D. eval と sort のどちらを先に使用しても問題ありません。
正解: (正解を表示します)

質問: **249**
共通情報モデル（CIM）を説明する記述は次のどれですか？（該当するものをすべて選択してください）
A. CIM は、単一の Splunk デプロイメント上で他のアプリと共存できる ^n アプリです。

B. CIM はさまざまなソースからのデータを相関させることができます。
C. ナレッジ マネージャーは CIM を使用してナレッジ オブジェクトを作成します。
D. CIM はデータを正規化するための方法論です。
正解: (正解を表示します)

質問: **250**
次の記述のうち、共通情報モデル (CIM) について説明しているものはどれですか (該当するものをすべて選択してください)。
A. CIM はデータを正規化するための方法論です。
B. CIM はさまざまなソースからのデータを相関させることができます。
C. Knowledge Manager は CIM を使用してナレッジ オブジェクトを作成します。
D. CIM は、単一の Splunk デプロイメント上で他のアプリと共存できるアプリです。
正解: (正解を表示します)
参考 :https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview Common Information Model (CIM) は、さまざまなソースからのデータを正規化し、分析やレポート作成を容易にする方法です3。CIM は、アラート、電子メール、データベース、ネットワーク トラフィック、Web などのさまざまなドメインに共通のフィールドとタグのセットを定義します3。CIM について説明する記述の 1 つは、CIM はデータを正規化するための方法であるということです。つまり、さまざまなソースからのデータの命名と構造化を行う標準的な方法を提供し、それらのデータを比較して相関関係を示せるということです3。したがって、オプション A が正解です。CIM について説明するもう 1 つの記述は、CIM はさまざまなソースからのデータを相関関係に置けるということです。つまり、共通のフィールドとタグを共有するさまざまなソースのデータ全体にわたって検索とレポートを実行できるということです3。したがって、オプション B が正解です。 CIMを説明する別の記述として、 ナレッジマネージャーはCIMを使用してナレッジオブジェクトを作成する」というものがあります。これは、データモデル、フィールドエイリアス、タグ、イベントタイプなどのナレッジオブジェクトの作成と管理を担当する担当者が、CIMをガイドとして使用することで、ナレッジオブジェクトの一貫性と他のアプリやアドオンとの互換性を確保できることを意味します3。したがって、選択肢Cが正解です。選択肢Dは不正解です。これはCIMそのものについてではなく、その構成要素の1つについて説明しているからです。