Splunk.SPLK-3002.v2026-05-29.q73

試験コード:	SPLK-3002
試験名称:	Splunk IT Service Intelligence Certified Admin
認定資格:	Splunk
無料問題数:	73
バージョン:	v2026-05-29
アクセス数:	127
ページビュー数:	730
https://www.jpnpdf.com/Splunk.SPLK-3002.v2026-05-29.q73-mondaishu.html	

最新問題: **1**
ITSI を使用するために Splunk で設定する必要があるデフォルト ポートは次のどれですか。
A. SplunkWeb (8088)、SplunkD (8089)、HTTP Collector (8000)
B. SplunkWeb (8000)、SplunkD (8089)、HTTP Collector (8088)
C. SplunkWeb (8405)、SplunkD (8519)、HTTP Collector (8628)
D. SplunkWeb (8089)、SplunkD (8088)、HTTP Collector (8000)
Answer: B (メーッセージを残す**)**

最新問題: **2**
単一の検索ヘッドに ITSI をインストールするにはどの手順が必要ですか?
A. <splunk home>/etc/apps にある ITSI パッケージを解凍します。
B. splunk_apply shcluster-bundle を実行します。
C. Splunk -> Manage Apps ダッシュボードを使用してダウンロードおよびインストールします。
D. 上記のすべて。
Answer: C (メーッセージを残す**)**
単一の検索ヘッドに Splunk IT Service Intelligence (ITSI) をインストールする最も簡単な方法の 1 つは、Splunk Web インターフェース、具体的には 「アプリの管理」ダッシュボードを使用して ITSI をダウンロードしてインストールすることです。
この方法はユーザーフレンドリーで、手動によるファイル操作やコマンドライン操作は必要ありません。Splunk Webインターフェースの 「アプリの管理」に移動すると、アプリリポジトリでITSIを見つけるか、以前にダウンロード済みのITSIインストールパッケージをアップロードできます。そこからSplunk Webインターフェースを介してインストールプロセスが開始され、セットアッププロセスが簡素化されます。このアプローチにより、インス

トールはSplunkの標準アプリインストール手順に従って行われるため、一般的なインストールエラーを回避し、ITSIがSplunk環境に正しく統合されます。

最新問題: **3**
次の項目のうち、ITSI Deep Dive 機能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. 一定期間にわたるサービスの注目すべきイベントを比較します。
B. 1 つ以上のサービス KPI 値を時間別に視覚化します。
C. 時間の経過に伴うサービス内の KPI のアラート レベルを調べて比較します。
D. 一定時間内のスイムレーンの値を比較します。
Answer: B,C,D (メーッセージを残す**)**
参考 :https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/DeepDives ディープダイブは、ITSIにおけるKPIと指標の過去の傾向や異常を分析できるダッシュボードです。ディープダイブでは、イベントのタイムラインとデータのスイムレーンが表示され、カスタマイズやフィルタリングを行うことで、問題の調査や根本原因分析を行うことができます。
ディープダイブの機能には、以下のものがあります。
B) 1つまたは複数のサービスKPI値を時間経過とともに可視化する。これは、KPIスイムレーンをディープダイブに追加することで、1つまたは複数のKPIの値と重大度を時間経過とともに表示できるため、非常に有効です。また、サービススワッピングやエンティティ分割を使用して、異なるサービスやエンティティのKPIを比較することもできます。
C) サービスにおけるKPIのアラートレベルを時系列で調査 ·比較する。これは、ディープダイブにアラートスイムレーンを追加することで、1つまたは複数のKPIのアラートレベルとカウントを時系列で表示できるため、非常に有効です。また、アラートの詳細にドリルダウンして、各アラートに関連する重要なイベントを確認することもできます。
D) 特定の時間範囲におけるスイムレーンの値を比較する。これは、時間範囲セレクターを使用して、詳細な分析で特定の時間範囲を拡大または縮小できるためです。また、タイムブラシを使用して特定の時間範囲を選択し、その期間のスイムレーンの値を比較することもできます。
他のオプションは、次の理由により、詳細に調査する機能ではありません。
A) 一定期間におけるサービスの注目すべきイベントを比較する。これは正しくありません。ディープダイブでは、ITSIが特定の条件や相関関係に基づいて生成するアラートである注目すべきイベントは表示されないためです。注目すべきイベントは、エピソードレビューやグラステーブルなどの他のダッシュボードに表示されます。
参考資料: [ITSI のディープ ダイブの概要]、[ITSI のディープ ダイブにスイム レーンを追加する]

最新問題: **4**
ITSI で修正が必要な問題は次のうちどれですか?
A. 同じサービス ID を持つ 2 つ以上のエンティティ。

B. 同じエンティティ ID を持つ 2 つ以上のエンティティ。
C. 1 つのエイリアス フィールドに同じ値を持つ 2 つ以上のエンティティ。
D. 任意の情報フィールドに同じエンティティ キー値を持つ 2 つ以上のエンティティ。
Answer: C (メッセージを残す**)**
Splunk IT Service Intelligence (ITSI) では、エンティティは監視対象のインフラストラクチャ コンポーネント、アプリケーション、またはその他の要素を表します。各エンティティはエンティティ ID によって一意に識別され、エイリアスの概念を通じて 1 つ以上のサービスに関連付けることができます。エイリアスは ITSI 内のイベントとエンティティの一致に使用されるため、1 つのエイリアス フィールドに 2 つ以上のエンティティが同じ値を持つと問題が発生します。複数のエンティティが同じエイリアス値を共有している場合、ITSI はデータを間違ったエンティティに誤って関連付ける可能性があり、監視と分析の精度が損なわれる可能性があります。このシナリオでは、各エイリアスが単一のエンティティを一意に識別するように修正する必要があり、それによって ITSI 内の監視および分析プロセスの整合性が維持されます。情報フィールドのサービス ID、エンティティ ID、およびエンティティ キー値の一意性も重要ですが、通常、エイリアス フィールドの重複値と同じレベルの問題は発生しません。

最新問題**: 5**
適応時間しきい値の利点は次のどれですか?
A. KPI 値のパターンが時間の経過とともに変化した場合に自動的にアラートを出します。
B. 通常の KPI 値が時間の経過とともに変化するため、しきい値を自動的に調整します。
C. 休日のスケジュールに合わせて自動的に調整します。
D. 時間の経過に伴う KPI 値の将来の低下を自動的に予測します。
Answer: B (メッセージを残す**)**
Splunk IT Service Intelligence (ITSI) における適応型時間しきい値とは、履歴データの傾向とパターンに基づいて主要業績評価指標 (KPI) のしきい値を動的に調整する機能を指します。この機能により、KPI の 「通常の」動作が時間の経過とともに変化するのに合わせてしきい値を調整できるため、アラートの関連性が維持され、誤検知や誤検出の可能性が低減します。このアプローチの利点は、業務の変化、季節性、その他の要因によって発生する可能性のある KPI 値の自然な変動に、手動でしきい値を調整する必要がなくなることです。これにより、監視システムの回復力と実際の状況への対応力が向上し、IT 運用管理の全体的な有効性が向上します。

最新問題**: 6**
次のどれがマルチ KPI アラートの有効なタイプですか?
A. 複合スコアを超えます。
B. 時間の経過に伴う価値。
C. 時間の経過に伴うステータス。
D. 上昇が走行を超えます。

Answer: B (メーッセージを残す)
参照：
正解はBです。ITSIでは、経時変化はマルチKPIアラートの有効な種類であるためです。マルチKPIアラートとは、1つ以上のサービスの複数のKPIが指定された時間範囲内で特定の条件を満たした場合にトリガーされるアラートの一種です。経時変化は、指定された時間範囲内におけるKPIの現在の値と過去の値を比較する条件です。例えば、サービスのCPU使用率とメモリ使用量の両方が過去24時間の平均値を超えた場合にトリガーされるマルチKPIアラートを作成できます。参考：「ITSIでマルチKPIアラートを作成する」、「ITSIでマルチKPIアラートの条件を設定する」

最新問題: **7**
ITSI における現実的なトラブルシューティング ワークフローを説明するものはどれですか。
A. 相関関係の検索 -> 詳細調査 -> 注目すべきイベント
B. サービス アナライザー -> 注目イベントのレビュー -> 詳細分析
C. サービス アナライザー -> 集約ポリシー -> 詳細分析
D. 相関検索 -> KPI -> 集計ポリシー
Answer: B (メーッセージを残す)
ITSI における現実的なトラブルシューティング ワークフローは次のとおりです。
* B. サービスアナライザー -> 注目イベントレビュー -> 詳細分析
このワークフローには、サービス アナライザー ダッシュボードを使用してサービスと KPI の健全性とパフォーマンスを監視し、重要なイベント レビュー ダッシュボードを使用して ITSI によって生成された重要なイベントを調査および管理し、詳細ダイブ ダッシュボードを使用して KPI とメトリックの履歴傾向と異常を分析します。
その他のワークフローは、相関検索、集約ポリシー、KPIなど、トラブルシューティングプロセスに含まれないコンポーネントが含まれているため、現実的ではありません。これらのコンポーネントは、ITSIが生成するアラートやエピソードの作成と設定に使用され、調査や解決には使用されません。参考資料：
[ITSI のサービス アナライザー ダッシュボード]、ITSI のエピソード レビューの概要、[ITSI の詳細分析の概要]

最新問題: **8**
15～30 分の時間バッファを使用するのがベストプラクティスである ITSI 機能は何ですか?
A. 相関検索。
B. 適応しきい値設定。
C. メンテナンスウィンドウ
D. 異常検出。
Answer: C (メーッセージを残す)
説明

メンテナンス作業の開始と終了の前後に15〜30分のバッファを設けてメンテナンスウィンドウをスケジュールするのがベストプラクティスです。これにより、システムがメンテナンス状態に追いつく時間を確保し、メンテナンス作業中にITSIが誤検知を生成する可能性を低減できます。

最新問題: **9**
「チーム」を通じて有効になる機能はどれですか?
A. チームは itsi_summary インデックスに対する検索を許可します。
B. チームは注目すべきイベントアラートアクションを制限します。
C. チームは itsi_notable_audit インデックスに対する検索を制限します。
D. チームは UI ビュー内のサービス コンテンツへの制限を許可します。
Answer: A (メーッセージを残す**)**
説明
Teams はプレゼンテーション層のセキュリティのみを提供し、データレベルのセキュリティは提供しません。Splunk 検索バーにアクセスできるユーザーは、ITSI サマリーインデックスデータを参照できます。

最新問題: **10**
フィールドがグループ化にどのように影響するかを制御するスマートモード設定が2つあります。正しいのはどちらですか？
A. テキスト偏差とカテゴリ偏差。
B. テキストの類似性とカテゴリの偏差。
C. テキストの類似度とカテゴリの類似度。
D. テキストの偏差とカテゴリの類似性。
Answer: (解答を表示する**)**
Splunk IT Service Intelligence (ITSI) のスマートモード設定において、フィールドがグループ化に与える影響を制御する2つの設定は、「テキスト類似度」と「カテゴリ類似度」です。スマートモードは、機械学習を活用して関連イベントを自動的にグループ化するイベントグループ化機能です。「テキスト類似度」とは、イベントフィールドのテキスト内容が、イベントデータ内の文字列や説明の共通性を考慮して、イベントをグループ化するためにどの程度一致する必要があるかを指します。一方、「カテゴリ類似度」は、イベントタイプやソースタイプなど、イベントのカテゴリ属性の類似度に関連し、性質や発生源が類似するイベントをクラスタリングするのに役立ちます。これらの設定はどちらも、ITSI におけるイベントのグループ化方法を決定する上で非常に重要であり、テキストとカテゴリの類似性に基づくイベントグループ化の粒度と関連性に影響を与えます。

最新問題: **11**
ITSI で修正が必要な問題は次のうちどれですか?
A. 同じサービス ID を持つ 2 つ以上のエンティティ。

B. 同じエンティティ ID を持つ 2 つ以上のエンティティ。
C. 1 つのエイリアス フィールドに同じ値を持つ 2 つ以上のエンティティ。
D. 任意の情報フィールドに同じエンティティ キー値を持つ 2 つ以上のエンティティ。
Answer: C (メーッセージを残す)
Splunk IT Service Intelligence (ITSI) では、エンティティは監視対象となるインフラストラクチャコンポーネント、アプリケーション、その他の要素を表します。各エンティティはエンティティIDによって一意に識別され、エイリアスの概念を通じて1つ以上のサービスに関連付けることができます。ITSIでは、イベントとエンティティを一致させるためにエイリアスが使用されるため、1つのエイリアスフィールドに複数のエンティティが同じ値を持つと問題が発生します。複数のエンティティが同じエイリアス値を共有すると、ITSIはデータを誤ったエンティティに誤って関連付け、監視と分析の精度が低下する可能性があります。このような状況では、各エイリアスが単一のエンティティを一意に識別するように修正する必要があり、それによってITSI内の監視および分析プロセスの整合性が維持されます。
情報フィールド内のサービス ID、エンティティ ID、およびエンティティ キー値の一意性も重要ですが、通常、エイリアス フィールド内の重複した値と同じレベルの問題は発生しません。

最新問題**: 12**
KPI 検索結果はどこに保存されますか?
A. デフォルトのインデックス。
B. KVストア。
C. CSV ルックアップに出力します。
D. itsi_summary インデックス。
Answer: D (メーッセージを残す)
検索結果は、アラート アクションによって処理、作成され、itsi_summary インデックスに書き込まれます。
参考: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch 正解はDです。KPI検索結果はITSIのitsi_summaryインデックスに保存されます。このインデックスは、スケジュールされたKPI検索の結果を保存するイベントインデックスです。サマリーインデックスを使用すると、計算コストの高いレポートのコストを時間的に分散させることで、大規模なデータセットを高速に検索できます。
参考資料: ITSIインデックスの概要

最新問題**: 13**
エピソードレビューで、エピソードの 承認」ボタンをクリックすると、どのような結果になりますか?
A. 現在のユーザーを所有者として割り当てます。
B. ステータスを 新規」から 確認済み」に変更します。

C. ステータスを 新規」から 進行中」に変更し、現在のユーザーを所有者として割り当てます。
D. ステータスを 新規」から 確認済み」に変更し、現在のユーザーを所有者として割り当てます。
Answer: D (メーッセージを残す**)**
エピソードを調査する必要がある場合、アナリストはエピソードを確認し、ステータスを 新規」から 進行中」に変更します。
参照：
エピソードとは、業務運営に影響を与えるサービス運用の中断を指します。これは、大規模なシーケンスの一部として発生する重要なイベントの重複を除いたグループ、または個別に検討されるインシデントや期間を指します。エピソードレビューでは、さまざまなアクションを使用してエピソードとそのステータスを管理できます。アクションの1つに 確認」があります。これは、エピソードのステータスを 新規」から 確認済み」に変更し、現在のユーザーを所有者として割り当てます。このアクションは、誰かがエピソードの解決に取り組んでいることを示し、他のユーザーによる重複した作業を防ぎます。参考 :ITSIにおけるエピソードレビューの概要、[エピソードレビューにおけるエピソードアクション]

最新問題**: 14**
分散検索では、検索ヘッド以外のインスタンスにインストールする必要があるコンポーネントはどれですか?
A. インデクサー上の SA-IndexCreation および SA-ITSI-Licensechecker。
B. インデクサー上の SA-IndexCreation および SA-ITOA。ライセンス マスター上の SA-ITSI-Licensechecker および SA-UserAccess。
C. イデクサーの SA-IndexCreation;ライセンス マスター上の SA-ITSI-Licensechecker および SA-UserAccess。
D. インデクサーの SA-ITSI-Licensechecker。
Answer: A (メーッセージを残す**)**
SA-IndexCreation はすべてのインデクサーで必須です。非クラスタの分散環境では、SA-IndexCreation を個々のインデクサーの $SPLUNK_HOME/etc/apps/ にコピーしてください。
参考資料: https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallDD 分散検索では、検索ヘッド以外のインスタンスにインストールする必要があるコンポーネントは、インデクサー上のSA-IndexCreationとSA-ITSI-Licensecheckerです。SA-IndexCreationは、itsi_summaryやitsi_tracked_alertsなど、ITSIに必要なインデックスを作成するアドオンです。SA-ITSI-Licensecheckerは、ITSIのライセンス使用状況を監視し、ライセンス制限を超えた場合や期限切れが近づいた場合にアラートを生成するアドオンです。これらのコンポーネントは、ITSIのデータの取り込みと保存機能を処理するため、インデクサーにインストールする必要があります。ITSIアプリやSA-ITOAなどのその他のコンポーネントは、ITSI

の検索管理と表示機能を処理するため、検索ヘッドにインストールする必要があります。
参考資料: 分散環境へのITサービスインテリジェンスのインストール

最新問題: **15**
単一の検索ヘッドに ITSI をインストールするにはどの手順が必要ですか?
A. <splunk home>/etc/apps にある ITSI パッケージを解凍します。
B. splunk_apply shcluster-bundle を実行します。
C. Splunk -> Manage Apps ダッシュボードを使用してダウンロードおよびインストールします。
D. 上記のすべて。
Answer: (解答を表示する**)**
Splunk IT Service Intelligence (ITSI) を単一のサーチヘッドにインストールする最も簡単な方法の一つは、Splunk Web インターフェース、特に「Manage Apps」ダッシュボードを使用して ITSI をダウンロードおよびインストールすることです。この方法はユーザーフレンドリーで、手動でのファイル操作やコマンドライン操作は必要ありません。Splunk Web インターフェースの「Manage Apps」に移動すると、ユーザーはアプリリポジトリで ITSI を見つけるか、以前にダウンロード済みの ITSI インストールパッケージをアップロードできます。そこから Splunk Web インターフェースを介してインストールプロセスが開始され、セットアッププロセスが簡素化されます。このアプローチにより、インストールは Splunk の標準的なアプリインストール手順に従って行われるため、一般的なインストールエラーを回避し、ITSI が Splunk 環境に正しく統合されます。

最新問題: **16**
異常が検出されるとどうなりますか?
A. これを表示するには、別の相関検索を作成する必要があります。
B. SNMP トラップが送信されます。
C. コア Splunk の index=main に異常アラートが表示されます。
D. 異常アラートは、エピソードレビューで注目すべきイベントとして表示されます。
Answer: (解答を表示する**)**
Splunk IT Service Intelligence (ITSI) で異常が検出されると、通常は注目すべきイベントが生成され、エピソードレビューダッシュボードで確認および管理できます。エピソードレビューは、ITSI のイベント分析フレームワークの一部であり、異常検出によって生成されたイベントを含む注目すべきイベントの確認、注釈付け、管理を一元的に行うための場所です。このプロセスにより、IT オペレーターとアナリストは、異常アラートによって強調表示された潜在的な問題を効率的に特定し、優先順位を付けて対応することができます。異常アラートをエピソードレビューダッシュボードに統合することで、IT サービス管理とオペレーショナルインテリジェンスのより広範なコンテキスト内で、これらのアラートを管理および調査するためのワークフローが効率化されます。

最新問題**: 17**
反復的な ITSI 展開を開始するために最も効果的なサービスを特定するためのベスト プラクティスは次のどれですか。
A. 複数のサービスで使用される場合にのみ KPI を含めます。
B. ビジネスを分析して最も重要なサービスを決定します。
C. 低レベルのサービスに焦点を当てます。
D. 多数の重要なサービスを早期に定義します。
Answer: B (メーッセージを残す**)**
参考: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/MKA
反復的なITSI導入を開始する上で最も効果的なサービスを特定するためのベストプラクティスは、ビジネスを分析し、収益、顧客満足度、その他の主要業績評価指標 KPI）に最も影響を与える最も重要なサービスを特定することです。サービスアナライザーを使用すると、これらのサービスの優先順位付けと監視が可能です。参考資料 :サービスアナライザー

最新問題**: 18**
ITSI がこのデータを使用する必要があると仮定して、Splunk インデックスにデータをオンボードする際に考慮すべきことは何ですか?
A. カスタム フィールドで | 統計関数を使用して、KPI 計算用のデータを準備します。
B. データがモジュールから事前構築された KPI を活用できるかどうかを確認し、適切な TA を使用してデータをオンボードします。
C. すべてのフィールドが CIM に準拠していることを確認し、対応するモジュールを使用して関連サービスをインポートします。
D. ITSIが活用できるデータモデルをできるだけ多く構築する計画を立てる
Answer: B (メーッセージを残す**)**
参考: https://newoutlook.it/download/book/splunk/advanced-splunk.pdf Splunk インデックスにデータをオンボードする場合、ITSI がこのデータを使用する必要があると想定して、次の点を考慮する必要があります。
B). データがモジュールから事前に構築された KPI を活用できるかどうかを確認し、適切な TA を使用してデータをオンボードします。
これは、モジュールが、オペレーティングシステム、データベース、Webサーバーなど、特定の種類のデータ ソース向けに設計された、サービス、KPI、ダッシュボードをパッケージ

化したセットであるためです。モジュールは、ベストプラクティスと業界標準に基づいてITサービスを迅速にセットアップおよび監視するのに役立ちます。モジュールを使用するには、モジュールに必要なデータフィールドを抽出および正規化する適切なテクニカルアドオン（TA）をインストールして構成する必要があります。
その他のオプションは、次の理由により検討すべきものではありません。
A) カスタムフィールドで統計関数を使用してKPI計算用のデータを準備する。これは正しくありません。
| カスタム フィールドの統計関数は、KPI の計算時にパフォーマンスの問題や不正確な結果を引き起こす可能性があります。
| stats 関数は、カスタム フィールドではなく、基本検索またはアドホック検索でのみ使用する必要があります。
C). すべてのフィールドが CIM に準拠していることを確認し、対応するモジュールを使用して関連サービスをインポートします。
これは正しくありません。すべてのモジュールがCIM準拠のデータソースを必要とするわけではないからです。一部のモジュールには、そのデータソースに固有のデータモデルとフィールド抽出機能があります。各モジュールのドキュメントを確認し、どのようなデータ要件と依存関係があるかを確認してください。
D) ITSIが活用できるデータモデルをできるだけ多く構築する計画を立てましょう。しかし、これは正しくありません。データモデルを過剰に構築すると、Splunk環境のパフォーマンスが低下し、リソース消費も増加するからです。ITSIのユースケースに必要かつ関連性のあるデータモデルのみを構築すべきです。
参考資料: ITSI のモジュールの概要、[ITSI モジュールのテクニカル アドオンのインストール]

最新問題**: 19**
アクティブな注目のイベントはどのインデックスに保存されますか?
A. 注目すべきアーカイブ
B. 注目すべき監査
C. itsi_tracked_alerts
D. itsi_tracked_groups
Answer: C (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) では、重要なイベントは Event Analytics フレームワークのコンテキスト内で作成および管理されます。これらの重要なイベントは、itsi_tracked_alerts インデックスに保存されます。このインデックスは、さまざまなサービスとその KPI に定義された条件に基づく ITSI の相関検索によって生成されるアクティブな重要なイベントを保持するために特別に設計されています。重要なイベントとは、基本的に調査して解決する必要があるアラートまたは問題です。itsi_tracked_alerts インデックスは、これらのイベントを効率的に保存、クエリ、および管理することを可能にし、ITSI のイベント管理およびレビュー プロセスを容易にします。その他のオプション

(itsi_notable_archive、itsi_notable_audit など) は、それぞれ解決済みの重要なイベントのアーカイブや重要なイベント設定の変更の監査など、異なる目的で使用されます。したがって、アクティブな重要なイベントの保存場所として正しい答えは、itsi_tracked_alerts インデックスです。

最新問題: **20**
KPI しきい値の時間ポリシーを構成する場合、次のどれが適用されますか?
A. ユーザーは 1 日の各時間につき 1 つずつ、合計 24 個のポリシーのみを設定できます。
B. 1:00の通常の動作が5:00の通常の動作と異なると予想される場合に最適です。
C. KPI が毎日のサイクルを通じて大幅に変化することが予想される場合は、KPI を使用しないでください。
D. 複数の時間ポリシーが重複する可能性があります。
Answer: (解答を表示する**)**
時間ポリシーは、KPIワークロードの変化に対応するために、1日または1週間の異なる時間帯で使用されるユーザー定義のしきい値です。時間ポリシーは、サービス全体の使用状況における通常の変動に対応し、KPIとサービスヘルススコアの精度を向上させます。例えば、組織のピークアクティビティが標準的な就業時間中である場合、就業時間中は使用率が高く、オフタイムや週末は使用率が低いことを考慮するKPIしきい値時間ポリシーを作成できます。KPIしきい値の時間ポリシーを構成する際に適用されるステートメントは次のとおりです。
* B. 1:00 の通常の動作が 5:00 の通常の動作と異なることが予想される場合に最適です。これは、時間ポリシーによって、午前/午後、勤務時間/休業時間、平日/週末など、異なる時間帯ごとに異なるしきい値を定義できるためです。これにより、時間帯や週によってKPIデータに生じる可能性のある変動を考慮できます。
その他の記述は、以下の理由により適用されません。
* A. 1人が設定できるポリシーは、1日の各時間につき1つずつ、合計24個までです。これは誤りです。3時間ブロック、2時間ブロック、1時間ブロックなど、異なる時間ブロックの組み合わせを使用することで、24個を超えるポリシーを設定できます。
* C. KPIが日周期で大きく変動すると予想される場合は、そのKPIを使用しないでください。時間ポリシーは、Webトラフィック量やCPU負荷率など、日周期で大きく変動するKPIに対応するように設計されているため、これは正しくありません。
* D. 複数の時間ポリシーが重複することは可能です。ただし、アクティブな時間ポリシーは常に1つだけであるため、これは正しくありません。新しい時間ポリシーを作成すると、以前の時間ポリシーは上書きされ、復元することはできません。
参考資料: ITSI で時間ベースの静的 KPI しきい値を作成する

最新問題: **21**
ITSI 保存済み検索スケジュールは、realtime_schedule = 0 を使用するように構成されています。この構成について正しい記述はどれですか。

A. この値が 0 に設定されている場合、スケジューラは現在の時刻に基づいて次にスケジュールされた検索実行時刻を決定します。
B. この値が 0 に設定されている場合、スケジューラは最後の検索実行時間に基づいて次にスケジュールされる検索を決定します。
C. この値が 0 に設定されている場合、スケジューラはスケジュールされた実行期間をスキップする場合があります。
D. この値が 0 に設定されている場合、スケジューラは最新の時間範囲で実行されている検索を確実に実行するために、いくつかの実行期間をスキップすることがあります。
Answer: B (メーッセージを残す**)**
ITSIの保存済み検索スケジューリングは、KPIのデータを入力するために定期的に実行される検索をスケジュールできる機能です。スケジュールされた検索には、検索頻度、時間範囲、cron式など、さまざまな設定が可能です。設定の一つであるrealtime_scheduleは、スケジューラがスケジュールされた検索の次回実行時刻を計算する方法を制御します。この設定に関する正確な記述は次のとおりです。
B) この値を0に設定すると、スケジューラは前回の検索実行時間に基づいて次回のスケジュール検索を決定します。これは継続スケジューリングと呼ばれます。0に設定すると、スケジューラはスケジュールされた実行期間をスキップすることはありません。ただし、スケジューラの負荷によっては、保存済み検索の実行が遅れる可能性があります。サマリーインデックスオプションを有効にする場合は、必ず継続スケジューリングを使用してください。
その他の記述は、以下の理由により正確ではありません。
A) この値が0に設定されている場合、スケジューラは次回のスケジュールされた検索実行時刻を現在の時刻に基づいて決定します。これは正しくありません。なぜなら、この値が0ではなく1に設定されている場合に、この動作が発生するからです。
C) この値が0に設定されている場合、スケジューラはスケジュールされた実行期間をスキップする可能性があります。これは正しくありません。これは、値が0ではなく1に設定されている場合に発生する現象です。
D) この値が0に設定されている場合、スケジューラは最新の時間範囲で実行されている検索を確実に実行するために、いくつかの実行期間をスキップすることがあります。これは正しくありません。なぜなら、この値が0ではなく1に設定されている場合に、このような現象が発生するからです。

最新問題**: 22**
カスタムの詳細分析を作成する場合、トポロジ ビュー内でメンテナンス モードのサービス/KPI は何色になりますか?
A. 灰色
B. 紫
C. ギアアイコン
D. 青

Answer: A (メーッセージを残す)
説明
メンテナンス ウィンドウによって完全にまたは部分的に影響を受けるサービス、エンティティ、および KPI は、サービス アナライザー、サービスとエンティティの詳細ページ、グラス テーブル、複数の KPI アラート、詳細分析などのヘルススコアを表示するページで濃い灰色で表示されます。

最新問題: **23**
社内のアプリケーション チームのサービス ツリーを計画および設計する際に最も役に立たない資料はどれですか。
A. アプリケーションとその相互接続の技術図。
B. 会社の組織図。
C. チームからの過去のインシデントと根本原因分析のレポート。
D. IT サービス管理ツールからのサービス トポロジ。
Answer: (解答を表示する)
Splunk ITSIでサービスツリーを計画・設計する際には、サービス、コンポーネント、依存関係の相互関係を理解することに重点が置かれます。これにより、ITSIはサービスの健全性、影響、ビジネス関連性を正確にモデル化できます。アプリケーションとその相互接続を示す技術図は、サービスツリーに含めるべきコンポーネントと依存関係を直接的に把握できます。過去のインシデントと関連する根本原因に関するレポートは、どのコンポーネントが重要か、どこで障害が発生したか、そして問題がどのように伝播したかを定義するための貴重なコンテキストを提供し、サービスモデリングに非常に役立ちます。ITサービスマネジメント（ITSM）ツールのサービストポロジーは、インフラストラクチャとサービス間の設定された関係を示すことで、モデリングプロセスに直接的な情報を提供します。これらの関係はインポートまたは参照することで、正確なサービスツリーを構築できます。一方、企業の組織図は、組織内の報告関係とチーム構造を示します。これは人事計画やエスカレーションパスには役立ちますが、ITSIにおけるサービスツリー設計には直接役立ちません。組織図は、アプリケーションコンポーネント、それらの実行時接続、または障害がサービス提供に与える影響に関する情報を提供しないため、技術面およびサービスの健全性を目的としてサービスツリーを設計する際には、最も役に立たない資料となります。したがって、企業組織図は一般的にITSIサービスモデリングには無関係です。

最新問題: **24**
マルチ KPI アラートを構成するのに最適なユースケースは次のどれですか?
A. 2 つの注目すべきイベントの内容を比較します。
B. 機械学習を使用して、データが予想されるパターンから外れた場合を評価します。
C. 2 つの KPI 間の異常検出を比較します。
D. 1 つ以上の KPI が停止が発生していることを示している場合にアラートを発します。
Answer: D (メーッセージを残す)

参考: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/MKA
マルチKPIアラートは、2つ以上のKPIに対して定義されたトリガー条件に基づく相関検索の一種です。各KPIのトリガー条件が同時に満たされると、検索によって注目すべきイベントが生成されます。例えば、CPU負荷率とWebリクエストという2つの一般的なKPIに基づいて、マルチKPIアラートを作成できます。
CPU負荷率とWebリクエストKPIの両方が同時に急上昇した場合、DDOS（分散型サービス拒否）攻撃の兆候である可能性があります。マルチKPIアラートは、このような傾向のある行動を早期に把握し、パフォーマンスへの影響を最小限に抑えるための対策を講じることができます。マルチKPIアラートは、複数のサービスにわたる複数のKPIのステータスを相関させるのに役立ちます。因果関係の特定、根本原因の調査、インフラ全体の行動に関する洞察の提供に役立ちます。マルチKPIアラートを設定する最適なユースケースは、サービスの健全性スコアが特定のしきい値を下回った場合や、複数のKPIの重大度が重大な場合など、1つ以上のKPIが障害の発生を示している場合にアラートを発報することです。参考資料 :ITSIでマルチKPIアラートを作成する

最新問題**: 25**
デフォルトのディープ ダイブを説明するのは次のどれですか。
A. 手動で生成され、サービス アナライザーを介してアクセスできます。
B. すべてのサービスのすべての KPI を含めます。
C. 自動生成され、サービス アナライザーを介してアクセスできます。
D. すべてのサービスのヘルススコアを含めます。
Answer: C (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) では、デフォルトのディープダイブが自動生成され、Service Analyzer からアクセスできます。ディープダイブは ITSI の重要な機能であり、サービスの健全性とパフォーマンス、および関連する KPI を詳細かつきめ細やかに把握できます。これらのデフォルトのディープダイブは各サービスに対して自動的に作成されるため、ユーザーはサービスの詳細な運用メトリクスとパフォーマンスデータを迅速にドリルダウンできます。Service Analyzer からこれらのディープダイブにアクセスすることで、ITSI ユーザーは問題を効率的に調査し、サービスの依存関係を理解し、最適なサービスの健全性を維持するための情報に基づいた意思決定を行うことができます。これらのデフォルトのディープダイブは自動生成されるため、監視と分析のプロセスが簡素化され、手動でのセットアップや設定を必要とせずに、サービスのパフォーマンスに関する洞察を即座に得ることができます。

最新問題**: 26**
分散検索では、検索ヘッド以外のインスタンスにインストールする必要があるコンポーネントはどれですか?
A. インデクサー上の SA-IndexCreation および SA-ITSI-Licensechecker。

B. インデクサー上の SA-IndexCreation および SA-ITOA。ライセンス マスター上の SA-ITSI-Licensechecker および SA-UserAccess。
C. イデクサーの SA-IndexCreation;ライセンス マスター上の SA-ITSI-Licensechecker および SA-UserAccess。
D. インデクサーの SA-ITSI-Licensechecker。
Answer: A (メーッセージを残す)
説明
SA-IndexCreation はすべてのインデクサーで必須です。非クラスタの分散環境の場合は、SA-IndexCreation を個々のインデクサーの $SPLUNK_HOME/etc/apps/ にコピーしてください。

最新問題**: 27**
サービス アナライザーの主な目的は何ですか?
A. すべてのサービスとエンティティのリストを表示します。
B. しきい値違反に基づいて外部アラートをトリガーします。
C. アナリストがアラートにコメントを追加できるようにします。
D. サービス全体と KPI のステータスを監視します。
Answer: D (メーッセージを残す)
参考:
https://docs.splunk.com/Documentation/MSExchange/4.0.3/Reference/ServiceAnalyzer
サービスアナライザーは、ITSI におけるサービス全体と KPI のステータスを監視できるダッシュボードです。サービスアナライザーには、すべてのサービスとそのヘルススコアのリストが表示されます。ヘルススコアは、各サービスがそれぞれの KPI に基づいてどの程度パフォーマンスを発揮しているかを示します。また、サービス内の各 KPI のステータスと値を確認したり、詳細な分析のために詳細な情報やグラステーブルにドリルダウンしたりすることもできます。サービスアナライザーは、サービスに影響を与える問題を特定し、その影響度と緊急度に基づいて優先順位を付けるのに役立ちます。サービスアナライザーの主な目的は次のとおりです。
D). サービス全体とKPIのステータスを監視します。これは、サービスアナライザーがサービスの健全性とパフォーマンス、そしてKPIの包括的なビューをリアルタイムで提供するためです。
その他のオプションは、次の理由により、サービス アナライザーの主な目的ではありません。
A) すべてのサービスとエンティティのリストを表示する。これは正しくありません。サービスアナライザーは、ITサービスを提供するために管理者の介入が必要となるITコンポーネントであるエンティティを表示しないためです。エンティティは、エンティティ管理やエンティティの健全性概要などの他のダッシュボードに表示されます。
B) しきい値違反に基づいて外部アラートをトリガーする。これは正しくありません。サービスアナライザーは、特定の条件が満たされたときに外部システムまたはユーザーに送信

される通知であるアラートをトリガーしないためです。アラートは、ITSIで設定された相関検索またはアラートアクションによってトリガーされます。
C) アナリストがアラートにコメントを追加できるようにする。これは正しくありません。サービスアナライザーでは、外部システムやユーザーに送信される通知であるアラートにアナリストがコメントを追加できないためです。

最新問題: **28**
ITSI の展開に関する推奨事項は次のどれですか? (該当するものをすべて選択してください。)
A. 多くの場合、展開では基本的な Splunk 要件を超えるハードウェア リソースの増加が必要になります。
B. 展開には専用の ITSI 検索ヘッドが必要です。
C. デプロイメントでは、KPI 検索の数に基づいて必要なインデクサーの数が増加する場合があります。
D. デプロイメントでは、インデクサーに可能な限り高速なディスク アレイを使用する必要があります。
Answer: A,B,C (メーッセージを残す**)**
環境によっては、独自の Enterprise Security 展開のハードウェア仕様を最小ハードウェア要件以上に引き上げる必要がある場合があります。
Splunk Enterprise Security を専用の検索ヘッドまたは検索ヘッド クラスターにインストールします。
Splunk プラットフォームは、インデクサーを使用して水平方向に拡張します。エンタープライズ セキュリティの導入に必要なインデクサーの数は、データ量、データの種類、保持要件、検索の種類、および検索の同時実行性によって異なります。
参考 :https://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning A、B、Cが正解です。ITSI導入では、大量のデータの取り込みと処理が必要となるため、Splunkの基本要件よりも多くのハードウェアリソースが必要になることが多いためです。また、ITSI導入では、ITSIアプリを実行し、ITSI関連の検索とダッシュボードをすべて処理する専用の検索ヘッドも必要です。KPI検索の回数と頻度に応じて、必要なインデクサーの数も増加する可能性があり、大量のサマリーデータが生成される可能性があります。参考 :ITSI導入の概要、ITSI導入計画

最新問題: **29**
KPI をそのサービス内のエンティティのみに自動的に制限し、各エンティティの KPI 値を生成するにはどうすればよいでしょうか。
A. 『エンティティごとに分割」と 『サービス内のエンティティにフィルター」の両方で 『はい」を選択します。
B. 『エンティティごとに分割」で 『いいえ」を選択し、 『サービス内のエンティティにフィルター」で 『はい」を選択します。

C. 「エンティティごとに分割」に「はい」を選択し、「サービス内のエンティティにフィルター」に「いいえ」を選択します。
D. 「エンティティごとに分割」と「サービス内のエンティティにフィルター」の両方で「いいえ」を選択します。
Answer: A (メーッセージを残す**)**
参考: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch A が正解です。「エンティティで分割」と「サービス内のエンティティにフィルター」の両方に「はい」を選択すると、KPI をそのサービス内のエンティティのみに自動的に制限し、各エンティティの KPI 値を生成できます。「エンティティで分割」では、KPI 検索結果をエンティティのエイリアスフィールドごとに分割し、各エンティティに対して個別の KPI 値を計算します。「サービス内のエンティティにフィルター」では、サービスに含まれないエンティティを KPI 検索結果から除外します。これにより、KPI がサービスに関連するエンティティのみを反映し、各エンティティの詳細な情報を提供できるようになります。参考: [ITSI での KPI 設定]

最新問題**: 30**
注目イベントが終了した後、そのイベントのメタデータはデフォルトで KV ストアにどのくらいの期間残りますか?
A. 6 か月。
B. 9か月。
C. 1 年。
D. 3か月。
Answer: (解答を表示する**)**
説明
デフォルトでは、KV ストアが大きくなりすぎないように、重要なイベント メタデータは 6 か月後にアーカイブされます。

最新問題**: 31**
次の項目のうち、ITSI のバックアップと復元の機能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. 事前に構成されたデフォルトの ITSI バックアップ ジョブが提供されており、変更はできますが、削除はできません。
B. ITSI バックアップには、KV ストア、ITSI 構成、およびインデックスの依存関係が含まれます。
C. kvstore_to_json.py は、スクリプトまたはコマンド ラインで使用して、ITSI を完全または部分的にバックアップできます。
D. ITSI バックアップは、JSON 形式のファイルのコレクションとして保存されます。
Answer: C,D (メーッセージを残す**)**

ITSI は、ITSI 構成データのバックアップ/復元、一括サービス KPI 操作の実行、ITSI オブジェクトのタイム ゾーン オフセットの適用、KPI 検索スケジュールの再生成を可能にする kvstore_to_json.py スクリプトを提供します。
バックアップ ジョブを実行すると、ITSI はデータを 1 つの ZIP ファイルに圧縮された一連の JSON ファイルに保存します。
参照：
https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/kvstorejson
https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/BackupandRestoreITSIconfig
C と D は正解です。ITSI のバックアップと復元機能では、kvstore_to_json.py をコマンドライン スクリプトとして、またはカスタム スクリプトの一部として使用して、完全または部分的なバックアップの ITSI データをバックアップします。ITSI バックアップは、サービス、KPI、ガラス テーブルなどの KV ストア オブジェクトを含む JSON 形式のファイルのコレクションとしても保存されます。A は、事前構成されたデフォルトの ITSI バックアップ ジョブが提供されていないため、正解ではありません。独自のバックアップ ジョブを作成するか、コマンドライン スクリプトまたはカスタム スクリプトを使用して ITSI データをバックアップできます。B は、ITSI バックアップにインデックスの依存関係が含まれていないため、正解ではありません。ITSI バックアップには、KV ストア オブジェクトと、オプションでいくつかの .conf ファイルのみが含まれます。インデックス データをバックアップするには、他の方法を使用する必要があります。参考資料: [ITSI KV ストア データのバックアップと復元の概要]、[ITSI の完全バックアップの作成]、[ITSI の部分バックアップの作成]

最新問題: **32**
マルチ KPI アラートの適切な使用例はどれですか?
A. 2 つ以上の KPI の値がメンテナンス モードになったときに警告します。
B. 2 つ以上の KPI の傾向がサービス障害が差し迫っていることを示している場合に警告します。
C. 2 つ以上の KPI が通常のパターンから逸脱している場合に警告します。
D. 2 つ以上の KPI の値を比較するときにアラートを出すと、異常な状態が発生していることを示します。
Answer: D (メーッセージを残す)

Splunk IT Service Intelligence (ITSI) のマルチKPIアラートは、複数の主要業績評価指標 (KPI) の状態に基づいてトリガーされるように設計されています。このタイプのアラートは、単一のKPIの状態だけでは問題を特定できない場合に特に有効です。しかし、複数のKPI間の相関関係から、新たな問題をより明確に把握できます。したがって、マルチKPIアラートの最適な使用例は、2つ以上のKPIの値を比較することで異常な状態が発生していることが示唆される場合です。これにより、個々のKPIの監視では検出できない複雑な問題を特定できる、より繊細でコンテキストに富んだアラートメカニズムが可能になります。このアプローチは、問題を正確に検出および診断するために、異なるパフォーマンス指標間の相互作用を考慮する必要がある複雑な環境で効果的です。

最新問題: **33**
ITSI を実装することで最もメリットが得られるシナリオはどれですか?
A. ビジネス サービス機能の監視。
B. システム ハードウェアの監視。
C. システムプロセスステータスの監視
D. 小売販売指標の監視。
Answer: (解答を表示する**)**
参照：
Splunk IT Service Intelligence (ITSI) は、人工知能と機械学習を活用して IT サービスの健全性とパフォーマンスに関する洞察を提供する監視および分析ソリューションです。ITSI を使用すると、アプリケーション、データベース、サーバー、ネットワークなど、IT インフラストラクチャの重要なコンポーネントを表すサービスを作成できます。その後、可用性、遅延、エラー率など、サービスの健全性の側面を測定する指標である主要業績評価指標 (KPI) を使用して、これらのサービスのステータスとパフォーマンスを監視できます。ITSI は、サービス アナライザー、グラス テーブル、ディープ ダイブ、エピソード レビューなど、サービスの問題を視覚化、調査、および警告するためのツールも提供します。ITSI を実装することで最もメリットが得られるシナリオは、ビジネス サービス機能の監視です。ITSI を使用すると、IT サービスの品質と信頼性を測定および改善し、ビジネス目標と一致させることができるためです。参考: Splunk IT Service Intelligence とは?

最新問題: **34**
ITSI の展開に関する推奨事項は次のどれですか? (該当するものをすべて選択してください。)
A. 多くの場合、展開では基本的な Splunk 要件を超えるハードウェア リソースの増加が必要になります。
B. 展開には専用の ITSI 検索ヘッドが必要です。
C. デプロイメントでは、KPI 検索の数に基づいて必要なインデクサーの数が増加する場合があります。

D. デプロイメントでは、インデクサーに可能な限り高速なディスク アレイを使用する必要があります。
Answer: A,B,C (メーッセージを残す**)**
環境によっては、独自の Enterprise Security 展開のハードウェア仕様を最小ハードウェア要件以上に引き上げる必要がある場合があります。
Splunk Enterprise Security を専用の検索ヘッドまたは検索ヘッド クラスターにインストールします。
Splunk プラットフォームは、インデクサーを使用して水平方向に拡張します。エンタープライズ セキュリティの導入に必要なインデクサーの数は、データ量、データの種類、保持要件、検索の種類、および検索の同時実行性によって異なります。
参照：
A、B、Cは正解です。ITSI導入では、大量のデータの取り込みと処理が必要となるため、Splunkの基本要件よりも多くのハードウェアリソースが必要になることが多いためです。また、ITSI導入では、ITSIアプリを実行し、ITSI関連の検索とダッシュボードをすべて処理する専用の検索ヘッドも必要です。また、KPI検索の回数と頻度に応じて必要なインデクサーの数が増える場合があり、大量のサマリーデータが生成される可能性があります。参考 :ITSI導入の概要、ITSI導入の計画

最新問題**: 35**
サービス アナライザーの主な目的は何ですか?
A. すべてのサービスとエンティティのリストを表示します。
B. しきい値違反に基づいて外部アラートをトリガーします。
C. アナリストがアラートにコメントを追加できるようにします。
D. サービス全体と KPI のステータスを監視します。
Answer: D (メーッセージを残す**)**
参照：
サービスアナライザーは、ITSIにおけるサービス全体とKPIのステータスを監視できるダッシュボードです。サービスアナライザーには、すべてのサービスとそのヘルススコアのリストが表示されます。ヘルススコアは、各サービスがKPIに基づいてどの程度パフォーマンスを発揮しているかを示します。また、サービス内の各KPIのステータスと値を確認できるほか、詳細な分析のために詳細な情報やグラステーブルにドリルダウンすることもできます。サービスアナライザーは、サービスに影響を与える問題を特定し、影響度と緊急度に基づいて優先順位を付けるのに役立ちます。サービスアナライザーの主な目的は次のとおりです。
D) サービス全体とKPIのステータスを監視します。これは、サービスアナライザーがサービスの健全性とパフォーマンス、そしてKPIをリアルタイムで包括的に表示するためです。
その他のオプションは、次の理由により、サービス アナライザーの主な目的ではありません。

A) すべてのサービスとエンティティのリストを表示する。これは正しくありません。サービスアナライザーは、ITサービスを提供するために管理者の関与を必要とするITコンポーネントであるエンティティを表示しないためです。エンティティは、エンティティ管理やエンティティの健全性概要などの他のダッシュボードに表示されます。
B) しきい値違反に基づいて外部アラートをトリガーする。これは正しくありません。サービスアナライザーは、特定の条件が満たされた際に外部システムまたはユーザーに送信される通知であるアラートをトリガーしないためです。アラートは、相関検索またはITSIで設定されたアラートアクションによってトリガーされます。
C) アナリストがアラートにコメントを追加できるようにする。これは正しくありません。サービスアナライザーでは、外部システムやユーザーに送信される通知であるアラートにアナリストがコメントを追加できないためです。

最新問題: **36**
SPL の記述を必要としないディープ ダイブ スイムレーン タイプはどれですか。
A. イベントレーン。
B. 自動レーン。
C. メトリックレーン。
D. KPI レーン。
Answer: D (メーッセージを残す)
KPIレーンは、SPLの作成を必要としないディープダイブスイムレーンの一種です。ドロップダウンリストからサービスとKPIを選択するだけで、ITSIが対応するデータを自動的にレーンに入力します。また、KPIレーンのしきい値設定と期間を調整することもできます。
参考 :[KPIレーン]

最新問題: **37**
集約ポリシーのスマート モードを有効にする方法について説明しているのは次のうちどれですか。
A. 設定 -> ポリシー -> スマートモード -> 有効化、「フィールド」を選択し、「保存」をクリックします。
B. 注目イベントレビューでグループ化を有効にし、「スマートモード」を選択し、「フィールド」を選択して「保存」をクリックします。
C. 集計ポリシーを編集し、スマートモードを有効にし、分析するフィールドを選択して、「保存」をクリックします。
D. 注目すべきイベントビューを編集し、スマートモードを有効にして「フィールド」を選択し、「保存」をクリックします。
Answer: C (メーッセージを残す)
1. ITSI メイン メニューから、[構成] > [重要なイベント集約ポリシー] をクリックします。
2. カスタム ポリシーまたはデフォルト ポリシーを選択します。
3. スマート モードのグループ化で、スマート モードを有効にします。

4. 「フィールドを選択」をクリックします。ダイアログに、過去24時間の注目イベントで見つかったフィールドが表示されます。
参照：
正解はCです。スマートモードは、イベント発生に最も影響を与えるフィールドに基づいて、ITSIが重要なイベントを自動的にグループ化できる集約ポリシーの機能です。集約ポリシーでスマートモードを有効にするには、ポリシーを編集し、スマートモードオプションを選択し、分析するフィールドを選択します。また、スマートモードをトリガーするイベントの最小数と、作成するグループの最大数を指定することもできます。参考 :ITSIで集約ポリシーのスマートモードを設定する

最新問題: **38**
ITSI エピソードはどのインデックスに含まれていますか?
A. itsi_tracked_alerts
B. グループ化されたアラート
C. 注目すべきアーカイブ
D. itsi_summary
Answer: B (メーッセージを残す**)**
参照：
Bが正解です。ITSIエピソードはitsi_grouped_alertsインデックスに保存されているためです。このインデックスには、事前定義された集約ポリシーに基づいてグループ化された重要なイベントが含まれています。エピソードは、アラートのノイズを減らし、インシデントの迅速な解決に集中するのに役立ちます。参考 :[ITSIのエピソードの概要]

最新問題: **39**
メンテナンス モードでは、KPI のどの機能が引き続き機能しますか?
A. KPI 検索は実行されますが、メンテナンス ウィンドウが終了するまでバッファリングされます。
B. メンテナンス モードでも KPI 検索は実行されますが、結果は itsi_maintenance_summary インデックスに送られます。
C. 新しい KPI を作成できますが、既存の KPI はロックされます。
D. KPI の計算としきい値設定を変更できます。
Answer: (解答を表示する**)**
メンテナンス作業の開始と終了の前後に15～30分のバッファを設けてメンテナンスウィンドウをスケジュールするのがベストプラクティスです。これにより、システムがメンテナンス状態に追いつく時間を確保し、メンテナンス作業中にITSIが誤検知を生成する可能性を低減できます。
参照：
Aが正解です。メンテナンスモード中もKPI検索は実行されますが、結果はメンテナンス期間が終了するまでバッファリングされます。つまり、メンテナンスモード中はアラートはトリガーされませんが、メンテナンス期間が終了するとバッファリングされた結果が処理

され、必要に応じてアラートが生成されます。メンテナンスモード中は、新しいKPIを作成したり、既存のKPIを変更したりすることはできません。参考 :[ITSIにおけるメンテナンス期間の概要]

最新問題: **40**
適応しきい値を使用するには、KPI データ セットの最小要件は何ですか?
A. 14日経過。
B. 7 日経過しました。
C. 30 日経過しました。
D. 10日目。
Answer: B (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) の適応型閾値設定を利用するには、主要業績評価指標 (KPI) データの最低要件として、7日以上経過している必要があります。適応型閾値設定は、過去のデータを使用し、観測されたパターンと傾向に基づいて閾値を動的に調整します。7日分のデータがあれば、システムは十分な量の情報を分析し、KPIの挙動における正常範囲と変動を特定できるため、より正確で状況に応じた適切な閾値を設定できます。この要件により、適応型閾値は、監視対象サービスの典型的な運用状況を反映する意味のあるデータセットに基づいていることが保証されます。

最新問題: **41**
モジュールを作成する前に必要な ITSI コンポーネントはどれですか?
A. 1 つ以上のエンティティ インポートの保存された検索。
B. KPI とそれに関連付けられた基本検索を持つ 1 つ以上のサービス。
C. 1 つ以上のデータモデル。
D. 1 つ以上の相関検索とそれに関連付けられたエンティティ。
Answer: C (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) でモジュールを作成するには、まず1つ以上のデータモデルを確立しておく必要があります。Splunk のデータモデルは、データを整理および解釈するための構造化されたフォーマットを提供し、これは ITSI 内のモジュールにとって非常に重要です。モジュールは、特に様々なソースにまたがる複雑なデータセットを扱う場合、データを意味のある方法で抽出、変換、提示するためにデータモデルを利用することがよくあります。データモデルは、モジュールがデータを効率的に分類および分析するための基盤として機能し、モジュールの特定のニーズに合わせた KPI、サービス、および可視化の作成を可能にします。これらのデータモデルを確立することで、モジュールが正しく機能し、監視対象の IT 環境に関する貴重な洞察を提供できるようになります。

最新問題: **42**
次のどれがエンティティを説明していますか? (該当するものをすべて選択してください。)

A. エンティティは、ルータやスイッチなどの IT デバイスである必要があり、IP 値、ホスト名、または MAC アドレスのいずれかで識別される必要があります。
B. 抽象 (疑似/論理) エンティティを使用して KPI を分割できますが、エンティティ ルールやフィルターを使用してデータを特定のサービスに制限することはできません。
C. 複数のエンティティは同じエイリアス値を共有できますが、ロール値は異なる必要があります。
D. KPI を特定のサービス内のエンティティのみに自動的に制限するには、 "サービス内のエンティティにフィルター」を選択します。
Answer: B,D (メーッセージを残す**)**
参照: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIfilter エンティティとは、ITサービスを提供するために経営陣が関与するITコンポーネントです。各エンティティは、固有の属性と他のITプロセスとの関係を持ち、それによってエンティティを一意に識別します。エンティティには、ITSIがインデックス付きイベントに関連付けるエイリアスフィールドと情報フィールドが含まれます。エンティティを説明する記述には、次のようなものがあります。
B) 抽象（擬似論理）エンティティはKPIの分割に使用できますが、エンティティルールやフィルタリングを使用してデータを特定のサービスに限定することはできません。抽象エンティティとは、物理的なホストやデバイスを表すのではなく、データソースの論理的なグループを表すエンティティです。例えば、組織内の各事業部門ごとに抽象エンティティを作成し、それを使用して収益や顧客満足度を測定するKPIの分割に使用できます。ただし、抽象エンティティにはインデックス付きイベントに一致するエイリアスフィールドがないため、エンティティルールやフィルタリングを使用して抽象エンティティに基づいてデータを特定のサービスに限定することはできません。
D) KPIを特定のサービス内のエンティティのみに自動的に制限するには、 "サービス内のエンティティにフィルター」を選択します。このオプションを使用すると、サービスに割り当てられているエンティティでKPIのデータソースをフィルターできます。例えば、Webサーバーのサービスがあり、各Webサーバーエンティティの CPU負荷率を監視したい場合、このオプションを選択すると、これらのエンティティからのイベントのみがKPI計算に使用されるようになります。
参考資料: ITSI におけるエンティティ統合の概要、[ITSI で KPI ベース検索を作成する]

最新問題**: 43**
有効な ITSI Glass Table エディターの機能は何ですか? (該当するものをすべて選択してください。)
A. ガラステーブルを作成します。
B. 相関検索の作成。
C. サービススワッピング構成。
D. ガラス テーブルに KPI メトリック レーンを追加します。
Answer: A,C,D (メーッセージを残す**)**

ガラス テーブルを作成して、IT サービスとビジネス サービス全体の相互関係と依存関係を視覚化し、監視します。
サービス交換設定は保存され、次回ガラステーブルを開いたときに適用されます。
KPI、アドホック検索、サービスヘルススコアなどの指標を、デザインした背景にリアルタイムで更新して表示できます。ガラステーブルには、KPIとサービスによって生成されたリアルタイムデータが表示されます。
参照：
ガラステーブルエディタは、ITSIでガラステーブルを作成および編集できるツールです。ガラステーブルエディタの機能の一部を以下に示します。
ガラステーブルを最初から、または既存のテンプレートから作成します。
ウィジェット上でサービススワッピングを構成して、異なるサービスからのメトリックの表示を切り替えます。
KPI 値の履歴傾向を表示するために、ガラス テーブルに KPI メトリック レーンを追加します。
グラステーブルエディタは相関検索の作成をサポートしていません。相関検索はITSIの別の機能で、データポイント間の関係性を探して重要なイベントを生成する検索を作成できます。参考 :ITSIのグラステーブルエディタの概要、[グラステーブルでのサービススワップの設定]、[グラステーブルへのKPIメトリックレーンの追加]、[ITSIにおける相関検索の概要]

最新問題: **44**
カスタム ディープ ダイブの特徴は次のどれですか?
A. itoa_analyst ロールがコメントを追加できるようにします。
B. 異常を示すには少なくとも 7 日間のデータが必要です。
C. メトリック、イベント、KPI、およびサービス ヘルス スコア レーンを組み合わせます。
D. ドリルダウンを使用して、異常検出によって注目すべきイベントを生成します。
Answer: C (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) のカスタムディープダイブは、多用途で高度にカスタマイズ可能なダッシュボードであり、ユーザーはさまざまな種類のデータを統合ビューで分析できます。カスタムディープダイブの重要な特徴の一つは、メトリクス、イベント、主要業績評価指標 (KPI)、サービスヘルススコアなど、異なるデータタイプのレーンを組み合わせることができることです。この多面的なアプローチにより、IT環境の包括的かつ階層化されたビューが提供され、アナリストやオペレーターはさまざまなデータタイプを相関させ、サービスの健全性とパフォーマンスに関するより深い洞察を得ることができます。これらの多様なデータレーンを組み込むことで、カスタムディープダイブは運用環境をより包括的に理解し、より効果的なトラブルシューティングと意思決定を支援します。

最新問題: **45**
ITSI ガラステーブルを最もよく表すのは次のどれですか?
A. KPI メトリックが重ねて表示されたシステム トポロジを表示するビュー。

B. トポロジを記述するビュー。
C. システム トポロジを表示するダッシュボード。
D. さまざまな視覚スタイルで KPI 値を表示するビュー。
Answer: A (メーッセージを残す**)**
ITSI Glass Tableは、システムのトポロジーにリアルタイムの主要業績評価指標 ⅏PI）メトリクスとサービスヘルススコアを重ねて表示できる、カスタマイズ可能なハイレベルビューを提供します。この可視化ツールにより、ユーザーはITインフラストラクチャ、アプリケーション、サービスの視覚的な表現を作成し、ライブデータを統合して各コンポーネントのヘルスとパフォーマンスを状況に応じて監視できます。KPIメトリクスをシステムトポロジーに重ねて表示できるため、IT部門とビジネス部門の関係者は、環境内のさまざまな要素の運用状況とヘルスを迅速に把握し、より情報に基づいた意思決定と迅速な問題対応が可能になります。

最新問題**: 46**
次の項目のうち、ITSI のバックアップと復元の機能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. 事前に構成されたデフォルトの ITSI バックアップ ジョブが提供されており、変更はできますが、削除はできません。
B. ITSI バックアップには、KV ストア、ITSI 構成、およびインデックスの依存関係が含まれます。
C. kvstore_to_json.py は、スクリプトまたはコマンド ラインで使用して、ITSI を完全または部分的にバックアップできます。
D. ITSI バックアップは、JSON 形式のファイルのコレクションとして保存されます。
Answer: C,D (メーッセージを残す**)**
説明
ITSI は、ITSI 構成データのバックアップ/復元、一括サービス KPI 操作の実行、ITSI オブジェクトのタイム ゾーン オフセットの適用、KPI 検索スケジュールの再生成を可能にする kvstore_to_json.py スクリプトを提供します。
バックアップ ジョブを実行すると、ITSI はデータを 1 つの ZIP ファイルに圧縮された一連の JSON ファイルに保存します。

最新問題: **47**
エンティティ凝集度異常検出を使用するために、KPI を分割する必要があるエンティティの最小数はいくつですか?
A. 3
B. 4
C. 5
D. 2
Answer: D (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) のエンティティ凝集度異常検出では、KPI を分割する必要があるエンティティの最小数は 2 です。異常検出手法としてのエンティティ凝集度は、同じグループまたはコホート内の他のエンティティと比較したエンティティの動作の偏差に基づいて異常を特定することに重点を置いています。ITSI では、最小で 2 つのエンティティのみを必要とするため、エンティティを比較して、潜在的な問題を示唆する可能性のある、あるエンティティのパフォーマンスまたは動作の大きな偏差を検出できます。この手法は、同様の機能を実行しているエンティティまたは同じサービス内のエンティティは同様の動作パターンを示すはずであり、大きな偏差は異常を示している可能性があるという考えに基づいています。最小要件が 2 つのエンティティという低い値であるため、この強力な異常検出機能は小規模な環境でも利用できます。

最新問題: **48**
異常検出を有効にできるのは次のどれですか?
A. KPI
B. 複数のKPIアラート
C. エンティティ
D. サービス
Answer: (解答を表示する**)**
A が正解です。ITSI では、KPI レベルで異常検出を有効にできます。異常検出を使用すると、KPI 検索結果からシステムの問題を示唆する可能性のある傾向や外れ値を特定できます。KPI 設定パネルで 2 つの異常検出アルゴリズムのいずれかを選択することで、KPI の異常検出を有効にすることができます。参考 :ITSI で KPI に異常検出を適用する

最新問題: **49**
ITSI の問題をトラブルシューティングするときに役立つエラー メッセージが含まれるインデックスはどれですか?
A. _introspection
B. _内部
C. itsi_summary
D. 注目すべき監査
Answer: (解答を表示する**)**
参照：

ITSI の問題のトラブルシューティング時に役立つエラー メッセージが含まれるインデックスは次のとおりです。
B) _internal。_internalインデックスには、splunkdやmetrics.logなどのSplunkプロセスによって生成されたログとメトリクスが含まれているため、このようになります。これらのログは、ITSIコンポーネントや機能を含むSplunk環境の問題の診断に役立ちます。
他のインデックスには、次の理由により、役立つエラー メッセージが含まれません。
A) _introspection です。_introspection インデックスには、CPU、メモリ、ディスク容量など、Splunk のリソース使用状況に関するデータが含まれているため、これは正しくありません。これらのデータは、Splunk 環境のパフォーマンスと健全性を監視するのに役立ちますが、エラーメッセージには役立ちません。
C) itsi_summary。これは正しくありません。itsi_summary インデックスには、KPI やサービスに関する要約データ（ヘルススコア、重大度レベル、しきい値など）が含まれているためです。これらのデータは IT サービスの傾向や異常の分析には役立ちますが、エラーメッセージには役立ちません。
D) itsi_notable_audit。これは正しくありません。itsi_notable_auditインデックスには、作成時間、所有者、イベント、エピソードなどの重要なイベントとエピソードの監査データが含まれているためです。

最新問題: **50**
メンテナンス ウィンドウを構成する際のベスト プラクティスは次のどれですか。
A. オープンメンテナンスウィンドウの一部である KPI を参照するガラステーブルを無効にします。
B. サービスのメンテナンス ウィンドウが開いているときに、サービスの重要なイベント生成を構成するための戦略を開発します。
C. メンテナンス ウィンドウにバッファ (実際のメンテナンス作業の前後 15 分など) を設定します。
D. サービス アナライザーで開いているメンテナンス ウィンドウの一部であるサービスとエンティティの色を変更します。
Answer: (解答を表示する**)**
メンテナンス作業の開始と停止の前後に 15 ～ 30 分の時間バッファを設けてメンテナンス ウィンドウをスケジュールすることがベスト プラクティスです。
参考 :https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW メンテナンスウィンドウとは、サービスまたはエンティティがメンテナンス作業中、またはアクティブな監視を必要としない期間です。メンテナンス作業の開始と停止の前後に15～30分のバッファを設けてメンテナンスウィンドウをスケジュールすることがベストプラクティスです。これにより、システムがメンテナンス状態に追いつく時間を確保し、ITSIがメンテナンス作業中に誤検知を生成する可能性を低減できます。例えば、サーバーがメンテナンスのために午後1時にシャットダウンされ、午後5時に再起動される場合、理想的なメンテナンスウィンドウは午後12時30分から午後5時30分です。15～30分のバッファ時間は、ほと

んどのKPIがデータ検索とアラートトリガーの特定のために設定されている15分間に基づいた概算です。参考 :ITSIにおけるメンテナンスウィンドウの概要

最新問題: **51**
新しい集約ポリシーの設定に含まれるのは次のどれですか?
A. フィルタリング基準
B. ポリシーバージョン
C. 注文を確認する
D. モジュールルール
Answer: A (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) で新しい集約ポリシーを設定する際、重要な要素の一つはフィルタリング基準の定義です。集約ポリシーのこの側面は、特定の条件または属性に基づいて、どのイベントを集約に含めるかを決定します。フィルタリング基準は、重大度、ソース、イベントタイプ、組織の監視戦略に関連するその他のカスタムフィールドなど、さまざまなイベントフィールドに基づくことができます。フィルタリング基準を指定することにより、ITSI 管理者は集約ポリシーが関連イベントにのみ適用されるようにすることができます。これにより、よりターゲットを絞った効果的なイベント管理が促進され、運用環境におけるノイズが削減されます。これにより、イベントの整理と優先順位付けがより効率的になり、ITSI におけるインシデント管理プロセス全体が強化されます。

最新問題: **52**
異常が検出されるとどうなりますか?
A. これを表示するには、別の相関検索を作成する必要があります。
B. SNMP トラップが送信されます。
C. コア Splunk の index=main に異常アラートが表示されます。
D. 異常アラートは、エピソードレビューで注目すべきイベントとして表示されます。
Answer: D (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) で異常が検出されると、通常は注目すべきイベントが生成され、エピソードレビューダッシュボードで確認および管理できます。エピソードレビューはITSIのイベント分析フレームワークの一部であり、異常検出によって生成されたイベントを含む注目すべきイベントを一元的に確認、注釈付け、管理するための場所として機能します。このプロセスにより、ITオペレーターとアナリストは、異常アラートによって強調表示された潜在的な問題を効率的に特定、優先順位付けし、対応することができます。
異常アラートをエピソード レビュー ダッシュボードに統合すると、IT サービス管理と運用インテリジェンスのより広範なコンテキスト内でこれらのアラートを管理および調査するためのワークフローが合理化されます。

最新問題: **53**

ITSI がこのデータを使用する必要があると仮定して、Splunk インデックスにデータをオンボードする際に考慮すべきことは何ですか?
A. すべてのフィールドが CIM に準拠していることを確認し、対応するモジュールを使用して関連サービスをインポートします。
B. データがモジュールから事前構築された KPI を活用できるかどうかを確認し、適切な TA を使用してデータをオンボードします。
C. ITSIが活用できるデータモデルをできるだけ多く構築する計画を立てる
D. カスタム フィールドで | 統計関数を使用して、KPI 計算用のデータを準備します。
Answer: B (メーッセージを残す)

最新問題**: 54**
ITSI を使用するために Splunk で設定する必要があるデフォルト ポートは次のどれですか。
A. SplunkWeb (8405)、SplunkD (8519)、HTTP Collector (8628)
B. SplunkWeb (8089)、SplunkD (8088)、HTTP Collector (8000)
C. SplunkWeb (8000)、SplunkD (8089)、HTTP Collector (8088)
D. SplunkWeb (8088)、SplunkD (8089)、HTTP Collector (8000)
Answer: (解答を表示する)
参考: https://splunk.github.io/docker-splunk/ARCHITECTURE.html
Cが正解です。ITSIは通信とデータ収集にSplunk Enterpriseのデフォルトポートを使用しているためです。SplunkWebはポート8000、SplunkDはポート8089、HTTPイベントコレクターはポート
8088。これらのポートは必要に応じて変更できますが、Splunk Enterprise の設定と一致する必要があります。
参考資料: ITSI が使用するポート

最新問題**: 55**
次の記述のうち、ITSI のデフォルトのガラステーブルについて説明しているものはどれですか?
A. サービス ヘルス スコアのデフォルトのガラス テーブル。
B. サービスごとにデフォルトのガラステーブルが 1 つあります。
C. サービス テンプレートのデフォルトのガラス テーブルが 1 つあります。
D. デフォルトのガラステーブルはありません。
Answer: D (メーッセージを残す)
Splunk IT Service Intelligence (ITSI) のグラステーブルは、組織の IT 環境、サービスの健全性とステータス、KPI を視覚的に表示する、完全にカスタマイズ可能なダッシュボードです。様々なプラットフォームでデフォルトで設定されている一部の設定済みビューやダッシュボードとは異なり、ITSI ではデフォルトのグラステーブルは提供されません。ユーザーは、それぞれの監視ニーズや運用ビューに合わせて、独自のグラステーブルを作成することができます。このアプローチにより、各組織は独自のインフラストラクチャ、アプリ

ケーション、サービス環境を最も適切に表現するグラステーブルを設計し、よりパーソナライズされた適切な運用概要を提供できます。

最新問題: **56**
ITSI 保存済み検索スケジュールは、realtime_schedule = 0 を使用するように構成されています。この構成について正しい記述はどれですか。
A. この値が 0 に設定されている場合、スケジューラは現在の時刻に基づいて次にスケジュールされた検索実行時刻を決定します。
B. この値が 0 に設定されている場合、スケジューラは最後の検索実行時間に基づいて次にスケジュールされる検索を決定します。
C. この値が 0 に設定されている場合、スケジューラはスケジュールされた実行期間をスキップする場合があります。
D. この値が 0 に設定されている場合、スケジューラは最新の時間範囲で実行されている検索を確実に実行するために、いくつかの実行期間をスキップすることがあります。
Answer: B (メーッセージを残す**)**
説明
0 に設定すると、スケジューラは検索の前回の実行時刻に基づいて、次回のスケジュールされた検索実行時刻を決定します。これは継続スケジューリングと呼ばれます。

最新問題: **57**
デフォルトのディープダイブを最もよく表しているのは次のうちどれですか?
A. 最初にすべてのサービスのヘルススコアが表示されます。
B. 最初に最も重要度の高い KPI が表示されます。
C. 最初に、選択したサービスのすべての KPI が表示されます。
D. 最初はすべてのエンティティ スイムレーンが表示されます。
Answer: C (メーッセージを残す**)**
参考 :https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/DeepDives デフォルトのディープダイブでは、選択したサービスのすべてのKPIが最初に表示されるため、Cが正解です。デフォルトのディープダイブは、別のダッシュボードからドリルダウンするか、ディープダイブ一覧ページからサービスを選択することで作成できます。デフォルトのディープダイブでは、ヘルススコア、重要度スコア、エンティティスイムレーンはデフォルトで表示されません。参考 :[ITSIでサービスのデフォルトのディープダイブを作成する]

最新問題: **58**
相関検索では、どのような構文を使用して動的フィールド値を指定できますか?
A. フィールド名
B. <フィールド名 /フィールド名>
C. %フィールド名%
D. eval(フィールド名)
Answer: B (メーッセージを残す**)**

参照：
正解はBです。相関検索では、<フィールド名/フィールド名>構文を使用して動的フィールド値を指定できます。この構文を使用すると、相関検索によって返されたフィールドの値を、メールの件名や本文などのアラートアクションに挿入できます。例えば、<ホスト/ホスト>は、ホストフィールドの値をメールに挿入します。参考 :[ITSIにおける相関検索での動的フィールド値の使用]

最新問題: **59**
管理者はどのようにして重要なイベントのグループ分けを手動で制御できますか?
A. 相関検索。
B. 複数の KPI アラート。
C. 注目すべきイベントのグループ化.conf
D. 集約ポリシー。
Answer: D (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) では、管理者は集約ポリシーを使用して重要なイベントのグループ化を手動で制御できます。集約ポリシーでは、重要なイベントをグループ化する基準を定義できます。これには、イベントフィールド、重大度、ソース、その他のイベント属性に基づくルールの設定が含まれます。これらのポリシーを通じて、管理者は環境固有のニーズに合わせてイベントのグループ化ロジックをカスタマイズし、関連するイベントを効率的な分析と対応を促進する方法でグループ化できます。この機能は、関連するイベントを管理しやすいグループに効果的に整理することで、イベントの量を管理し、最も重要な問題に集中するために不可欠です。

最新問題: **60**
次のどれがマルチ KPI アラートの有効なタイプですか?
A. 時間の経過に伴う価値。
B. 時間の経過に伴うステータス。
C. 複合スコアを超えます。
D. 上昇が走行を超える。
Answer: (解答を表示する**)**

最新問題: **61**
有効な ITSI Glass Table エディターの機能は何ですか? (該当するものをすべて選択してください。)
A. ガラステーブルを作成します。
B. 相関検索の作成。
C. サービススワッピング構成。
D. ガラス テーブルに KPI メトリック レーンを追加します。
Answer: (解答を表示する**)**

ガラス テーブルを作成して、IT サービスとビジネス サービス全体の相互関係と依存関係を視覚化し、監視します。
サービス交換設定は保存され、次回ガラステーブルを開いたときに適用されます。
KPI、アドホック検索、サービスヘルススコアなどの指標を、デザインした背景にリアルタイムで更新して表示できます。ガラステーブルには、KPIとサービスによって生成されたリアルタイムデータが表示されます。
参考: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/GTOverview ガラステーブルエディタは、ITSIでガラステーブルを作成および編集できるツールです。ガラステーブルエディタの機能の一部を以下に示します。
ガラステーブルを最初から、または既存のテンプレートから作成します。
ウィジェット上でサービススワッピングを構成して、異なるサービスからのメトリックの表示を切り替えます。
KPI 値の履歴傾向を表示するために、ガラス テーブルに KPI メトリック レーンを追加します。
ガラス テーブル エディターは相関検索の作成をサポートしていません。相関検索は ITSI の別の機能であり、データ ポイント間の関係を探し、注目すべきイベントを生成する検索を作成できます。
参考資料: ITSI のガラス テーブル エディターの概要、[ガラス テーブルでのサービス スワッピングの構成]、[ガラス テーブルへの KPI メトリック レーンの追加]、[ITSI の相関検索の概要]

最新問題: **62**
次の項目のうち、異常検出に当てはま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. データポイントのベースラインが確立されていないKPIにはADを使用します。これにより、MLパターンが効果的に機能します。
B. ITSI では、アドホック、トレンド、コヒーシブの 3 種類の異常検出がサポートされています。
C. 異常検出では、KPI データがパターンから逸脱すると、注目すべきイベントが自動的に生成されます。

D. 異常検出には最低 24 時間のデータが必要であり、凝集分析には最低 4 つのエンティティが必要です。
Answer: C,D (メーッセージを残す)

最新問題**: 63**
複数のサービスからの KPI 値を 1 つのウィジェットに表示するかどうかを切り替えるために使用できるガラス テーブル機能はどれですか。
A. サービス テンプレート。
B. サービスの依存関係。
C. アドホック検索。
D. サービスのスワッピング。
Answer: D (メーッセージを残す)
参考:
https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/Visualizations#collapseDesktop8 グラステーブルは、ITサービスとビジネスサービス間の相互関係と依存関係を監視できる可視化ツールです。KPI、アドホック検索、サービスヘルススコアなどの指標を、ユーザーがデザインした背景に対してリアルタイムで更新されるように追加できます。グラステーブルの機能の一つにサービススワッピングがあり、複数のサービスのKPI値を1つのウィジェット上で切り替えて表示できます。
サービススワッピングを使用すると、複数のグラステーブルやウィジェットを作成することなく、異なるサービス間でメトリクスを比較できます。参考資料 :ITSIのグラステーブルエディタの概要、[グラステーブルでのサービススワッピングの設定]

最新問題**: 64**
依存サービスのヘルススコアのデフォルトの重要度値は何ですか?
A. 11
B. 1
C. 未割り当て
D. 10
Answer: D (メーッセージを残す)
デフォルトでは、影響を与えるサービスの正常性スコアの重要度の値は 11 です。
参考: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/Dependencies サービステンプレートは、KPIとエンティティルールの事前定義されたセットであり、サービスまたはサービスグループに適用できます。サービステンプレートは、IT環境全体にわたる類似サービスの設定と監視を標準化するのに役立ちます。サービステンプレートには、別のサービスが適切に機能するために必要な依存サービスを含めることもできます。例えば、Web サーバーサービスは、データベースサービスとネットワークサービスに依存する場合があります。依存サービスのヘルススコアのデフォルトの重要度は次のとおりです。
D) 10. これは、依存サービスの重要度が親サービスの正常性スコアにどの程度貢献しているかを示しているためです。デフォルト値は10で、依存サービスが親サービスの正常性ス

コアに最も大きな影響を与えることを意味します。依存サービスの重要度は、サービステンプレートの設定で変更できます。
その他のオプションは、次の理由により正しくありません。
A) 11. 11は重要度を表す値として正しくありません。有効な範囲は1（最低から10（最高）です。
B). 1. これは正しくありません。1 は重要度の最低値であり、デフォルト値ではありません。値が 1 の場合、依存サービスは親サービスのヘルススコアに最も影響が少ないことを意味します。
C) 未割り当て。依存するすべてのサービスには重要度が割り当てられており、そのデフォルト値は10であるため、これは当てはまりません。
参考資料: ITSI でのサービス テンプレートの作成と管理、ITSI での KPI 重要度の値の設定

最新問題: **65**
KPI 検索パフォーマンスのトラブルシューティングを行う際、ジョブ アクティビティのどの検索名が基本検索を識別しますか?
A. インジケーター - XXXX - ベース検索
B. インジケーター - 共有 - xxxx - ITSI 検索
C. インジケーター - ベース - xxxx - 知識検索
D. インジケーター - ベース - XXXX - 共有検索
Answer: B (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) における KPI 検索パフォーマンスのトラブルシューティングにおいて、ジョブアクティビティ内のベース検索を識別する検索名は、通常「Indicator - Shared - xxxx - ITSI Search」というパターンに従います。これらのベース検索は、KPI 計算プロセスの基本的な構成要素であり、KPI によるさらなる分析のためにデータを集約および準備します。これらの検索はリソースを大量に消費し、システム全体のパフォーマンスに影響を与える可能性があるため、ジョブアクティビティ内でこれらのベース検索を識別することは、パフォーマンスの問題を診断する上で非常に重要です。この命名規則を理解することで、管理者やアナリストは特定の KPI に関連するベース検索を迅速に特定し、ITSI 環境における検索パフォーマンスのトラブルシューティングと最適化をより効果的に行うことができます。

最新問題: **66**
サービス テンプレートを変更すると、リンクされたサービスにデフォルトで追加されるのは次のどれですか。
A. しきい値。
B. エンティティ ルール。
C. 新しい KPI。
D. 健康スコア。
Answer: B (メーッセージを残す**)**

説明
複数のサービスをサービステンプレートにリンクすることで、IT Service Intelligence (ITSI) で一括管理できます。1 つのサービスは、一度に 1 つのサービステンプレートにのみリンクできます。サービスをサービステンプレートにリンクすると、サービス内の既存の KPI は保持され、テンプレート内の KPI がサービスに追加されます。エンティティルールは、追加、置換、または保持のいずれかを選択できます。

最新問題: **67**
次のどれがエンティティを説明していますか? (該当するものをすべて選択してください。)
A. エンティティは、ルータやスイッチなどの IT デバイスである必要があり、IP 値、ホスト名、または MAC アドレスのいずれかで識別される必要があります。
B. 抽象 (疑似/論理) エンティティを使用して KPI を分割できますが、エンティティ ルールやフィルターを使用してデータを特定のサービスに制限することはできません。
C. 複数のエンティティは同じエイリアス値を共有できますが、ロール値は異なる必要があります。
D. KPI を特定のサービス内のエンティティのみに自動的に制限するには、 "サービス内のエンティティにフィルター"を選択します。
Answer: B,D (メーッセージを残す**)**
参照：
エンティティとは、ITサービスを提供するために経営陣が管理する必要があるITコンポーネントです。各エンティティは、特定の属性と他のITプロセスとの関係を持ち、それによってエンティティを一意に識別します。エンティティには、ITSIがインデックス付きイベントに関連付けるエイリアスフィールドと情報フィールドが含まれます。エンティティを説明する記述には、次のようなものがあります。
B) 抽象（擬似論理）エンティティはKPIの分割に使用できますが、エンティティルールやフィルタリングを使用してデータを特定のサービスに限定することはできません。抽象エンティティとは、物理的なホストやデバイスを表すのではなく、データソースの論理的なグループを表すエンティティです。例えば、組織内の各事業部門ごとに抽象エンティティを作成し、それを使用して収益や顧客満足度を測定するKPIの分割に使用できます。ただし、抽象エンティティにはインデックス付きイベントに一致するエイリアスフィールドがないため、エンティティルールやフィルタリングを使用して抽象エンティティに基づく特定のサービスにデータを限定することはできません。
D) KPIを特定のサービス内のエンティティのみに自動的に制限するには、 "サービス内のエンティティにフィルター"を選択します。このオプションを使用すると、サービスに割り当てられているエンティティでKPIのデータソースをフィルターできます。例えば、Webサーバーのサービスがあり、各Webサーバーエンティティの CPU負荷率を監視したい場合、このオプションを選択すると、これらのエンティティからのイベントのみがKPI計算に使用されるようになります。

最新問題: **68**
マルチ KPI アラートがトリガーされたときに、Service Now インシデントを自動的に作成するにはどうすればよいですか? (該当するものをすべて選択してください)
A. カスタムetc/apps/SA-ITOA/workflow_rules.confを作成することにより
B. エンティティを Service-Now 構成項目にリンクします。
C. SNOW インシデントアクションを使用して注目すべきイベント集約ポリシーを作成します。
D. 関連する相関検索を編集し、アラート アクションを指定します。
Answer: C,D (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) でマルチ KPI アラートがトリガーされたときに ServiceNow インシデントを自動的に作成するには、次の方法を使用できます。
C) ServiceNow (SNOW) のインシデントアクションを含む重要なイベント集約ポリシーを作成する :ITSI では、特定の条件が満たされた場合に実行するアクションを指定できる重要なイベント集約ポリシーを作成できます。これらのアクションの1つとして、ServiceNow でのインシデント作成が挙げられ、ITSI のアラートメカニズムと ServiceNow のインシデント管理が直接連携されます。
D) 関連する相関検索を編集し、アラートアクションを指定する :ITSIにおける相関検索は、重要なイベントを示すパターンや条件を特定するために使用されます。これらの検索では、検索条件が満たされるたびにServiceNowインシデントを作成するなどのアラートアクションを実行するように設定できます。この直接統合により、相関検索で定義された特定の条件に基づいて、ServiceNowでインシデントが自動的に生成されます。
オプションAとBは、ITSIとServiceNowを統合してインシデントを自動生成するための標準的な方法ではありません。通常、構成には、ServiceNowなどの外部システムとの統合に特化した、ITSI内に実用的なアラートメカニズムを設定することが含まれます。

最新問題: **69**
ベース検索の特徴は次のどれですか?
A. 検索式、エンティティ分割ルール、およびしきい値は、基本検索レベルで構成されます。
B. サービスの KPI のメトリックを計算するために、サービスに割り当てられたエンティティをフィルタリングできます。
C. 共通のベース検索を共有する KPI が少ないほど、ベース検索の効率が向上し、異常検出も効率的になります。
D. ベース検索は、KPI が必要かどうかに関係なく実行されます。
Answer: B (メーッセージを残す**)**
参照：
ベース検索とは、同じデータソースを使用する複数のKPI間で共有できる検索定義です。ベース検索は、複数の類似KPIを統合することで、検索パフォーマンスを向上させ、検索負荷を軽減できます。ベース検索の特徴の一つは、サービスのKPIの指標を計算するためにサービスに割り当てられたエンティティをフィルタリングできることです。つまり、エン

ティティフィルタリングルールを使用して、ベース検索の結果に基づいて各KPIに関連するエンティティを指定できます。参考 :ITSIでKPIベース検索を作成する、[ベース検索に基づいてKPIのエンティティをフィルタリングする]

最新問題: **70**
KPI の集計値が計算されるときに、どの関数が呼び出されますか?
A. 統計
B. tstats
C. フィールドサマリー
D. 評価
Answer: B (メーッセージを残す**)**
Splunk IT Service Intelligence (ITSI) では、主要業績評価指標 (KPI) の集計値が計算されるときに、tstats 関数が頻繁に呼び出されます。Splunk の tstats 関数は、大量のデータに対する高速な統計クエリに使用され、ITSI では、膨大な可能性のあるデータセット全体の KPI の集計値を効率的に計算するために特に役立ちます。この機能により、インデックス付きデータの素早い集計と要約が可能になり、ITSI で KPI が表すパフォーマンス メトリックの監視と分析に不可欠です。すでに取得済みのイベントを操作する stats コマンドとは異なり、tstats はインデックス付きデータに対して直接動作するため、特に IT 環境で一般的な大量のデータを処理する場合に、より高速なパフォーマンスが得られます。したがって、tstats コマンドは、KPI の集計値を計算するための ITSI のバックエンド処理の基本となり、サービスの健全性とパフォーマンスのリアルタイムおよび履歴分析を可能にします。

最新問題: **71**
複数のサービスからの KPI 値を 1 つのウィジェットに表示するかどうかを切り替えるために使用できるガラス テーブル機能はどれですか。
A. サービス テンプレート。
B. サービスの依存関係。
C. アドホック検索。
D. サービスのスワッピング。
Answer: (解答を表示する**)**
参照：
グラステーブルは、ITサービスとビジネスサービス間の相互関係や依存関係を監視できる可視化ツールです。KPI、アドホック検索、サービスヘルススコアなどの指標を追加でき、これらはユーザーがデザインした背景に対してリアルタイムで更新されます。グラステーブルの機能の一つにサービススワッピングがあります。これは、複数のサービスのKPI値を1つのウィジェットに表示できる機能です。サービススワッピングを使用すると、複数のグラステーブルやウィジェットを作成することなく、異なるサービス間で指標を比較できます。参考 :ITSIのグラステーブルエディターの概要、[グラステーブルでのサービススワッピングの設定]

最新問題: **72**
KPI 値を保存するために使用されるインデックスはどれですか?
A. 要約指標を知る
B. say_metrics
C. itsi_service_health
D. itsi_summary
Answer: A (メーッセージを残す**)**
説明
IT サービス インテリジェンス (ITSI) メトリック サマリー インデックス
itsi_summary_metrics は、KPI データを格納するメトリック ベースのサマリー インデックスです。

最新問題: **73**
KPI しきい値の時間ポリシーを構成する場合、次のどれが適用されますか?
A. ユーザーは 1 日の各時間につき 1 つずつ、合計 24 個のポリシーのみを設定できます。
B. 1:00の通常の動作が5:00の通常の動作と異なると予想される場合に最適です。
C. KPI が毎日のサイクルを通じて大幅に変化することが予想される場合は、KPI を使用しないでください。
D. 複数の時間ポリシーが重複する可能性があります。
Answer: (解答を表示する**)**
時間ポリシーは、KPIワークロードの変化に対応するために、1日または1週間の異なる時間帯で使用されるユーザー定義のしきい値です。時間ポリシーは、サービス全体の使用状況における通常の変動に対応し、KPIとサービスヘルススコアの精度を向上させます。例えば、組織のピークアクティビティが標準的な就業時間中である場合、就業時間中は使用率が高く、オフタイムや週末は使用率が低いことを考慮するKPIしきい値時間ポリシーを作成できます。KPIしきい値の時間ポリシーを構成する際に適用されるステートメントは次のとおりです。
B) 午前1時の通常の行動が午前5時の通常の行動と異なることが予想される場合、これらは非常に有効です。これは、時間ポリシーを使用すると、午前/午後、勤務時間/休業時間、平日/週末など、異なる時間帯ごとに異なるしきい値を定義できるためです。これにより、時間帯や週に基づいてKPIデータの予想される変動を考慮できます。
その他の記述は、以下の理由により適用されません。
A) 1人が設定できるポリシーは、1日の各時間につき1つずつ、合計24個までです。これは誤りです。3時間ブロック、2時間ブロック、1時間ブロックなど、異なる時間ブロックの組み合わせを使用することで、24個を超えるポリシーを設定できます。
C) KPIが日次サイクルで大きく変動すると予想される場合は、そのKPIを使用しないでください。これは正しくありません。時間ポリシーは、Webトラフィック量やCPU負荷率など、日次サイクルで大きく変動するKPIに対応するように設計されているためです。

D) 複数の時間ポリシーが重複することは可能です。ただし、同時に有効な時間ポリシーは1つだけであるため、これは正しくありません。新しい時間ポリシーを作成すると、以前の時間ポリシーは上書きされ、復元することはできません。