Splunk.SPLK-2002.v2024-04-30.q113

試験コード:	SPLK-2002
試験名称:	Splunk Enterprise Certified Architect
認定資格:	Splunk
無料問題数:	113
バージョン:	v2024-04-30
アクセス数:	776
ページビュー数:	1130
https://www.jpnpdf.com/Splunk.SPLK-2002.v2024-04-30.q113-mondaishu.html	

最新問題: **1**
Splunk ユーザーは、src_ip というフィールドに IP アドレスを抽出することに成功しました。彼らの同僚はそれを見ることができません
src_ip を持つことが知られているイベントを含む検索結果のフィールド。説明できるのは次のうちどれですか?
問題？（該当するものをすべて選択。）
A. フィールドはプライベートナレッジオブジェクトとして抽出されました。
B. イベントは通信としてタグ付けされていますが、ネットワーク タグがありません。
C. 正規表現の置換を行う入力キューがブロックされています。
D. 同僚は検索でフィールドを明示的に使用せず、検索は高速モードに設定されていました。
Answer: D (メーッセージを残す**)**
説明/参照: https://answers.splunk.com/answers/657187/map-command-field-not-being-evaluated.html

最新問題: **2**
分散環境では、ナレッジ オブジェクト バンドルは検索ヘッドからどの場所に複製されますか
検索ピア上で?
A. SPLUNK_HOME/var/lib/searchpeers
B. SPLUNK_HOME/var/log/searchpeers
C. SPLUNK_HOME/var/run/searchpeers
D. SPLUNK_HOME/var/spool/searchpeers
Answer: (解答を表示する**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/Whatsearchheadssend

最新問題: **3**
サーチ ヘッド クラスターを計画する場合、次のどれが当てはまりますか?
A. すべてのサーチヘッドは同じオペレーティング システムを使用する必要があります。

B. すべてのサーチ ヘッドはクラスターのメンバーである必要があります (スタンドアロンのサーチ ヘッドは不可)。
C. サーチ ヘッド キャプテンは、クラスター内の最大のサーチ ヘッドに割り当てられる必要があります。
D. すべてのインデクサーは、基礎となるインデクサー クラスターに属している必要があります (スタンドアロン インデクサーは不可)。
Answer: D (メーッセージを残す**)**
説明
サーチ ヘッド クラスターを計画する場合、次のことが当てはまります。すべてのインデクサーは、基礎となるインデクサー クラスターに属している必要があります (スタンドアロン インデクサーは不可)。サーチヘッド クラスターは、構成、アプリ、および検索ジョブを共有するサーチヘッドのグループです。サーチヘッド クラスターにはデータ ソースとしてインデクサー クラスターが必要です。つまり、サーチヘッド クラスターにデータを提供するすべてのインデクサーは同じインデクサー クラスターのメンバーである必要があります。スタンドアロン インデクサー、またはインデクサー クラスターの一部ではないインデクサーは、サーチ ヘッド クラスターのデータ ソースとして使用できません。Splunk バージョンおよびインデクサー クラスターと互換性がある限り、すべてのサーチ ヘッドが同じオペレーティング システムを使用する必要はありません。スタンドアロンのサーチ ヘッドもインデクサー クラスターを検索できるため、すべてのサーチ ヘッドがクラスターのメンバーである必要はありませんが、構成のレプリケーションと負荷分散の利点は得られません。キャプテンは、CPU 負荷、ネットワーク遅延、検索負荷などのさまざまな基準に基づいてクラスター メンバーの中から動的に選出されるため、サーチ ヘッド キャプテンをクラスター内の最大のサーチ ヘッドに割り当てる必要はありません。

最新問題**: 4**
マルチサイト インデクサー クラスターですべてのサーチ ヘッド クラスター メンバーに site=site0 を設定するとどうなりますか?
A. 検索サイト アフィニティを無効にします。
B. すべてのメンバーを動的キャプテンに設定します。
C. マルチサイト検索アーティファクトのレプリケーションを有効にします。
D. 自動検索サイト アフィニティ検出を有効にします。
Answer: A (メーッセージを残す**)**
すべての検索ヘッド クラスター メンバーに site=site0 を設定すると、検索サイト アフィニティが無効になります。検索サイト アフィニティは、ネットワーク遅延と帯域幅の消費を削減するために、サーチ ヘッドがサーチ ヘッドと同じサイト内にあるピア ノードを優先的に検索できるようにする機能です。site=site0 (サイトがないことを示す特別な値) を設定すると、検索ヘッドはサイトに関係なくすべてのピアノードを検索します。site=site0 を設定しても、すべてのメンバーが動的キャプテンシーに設定されたり、マルチサイト検索アーティファクトのレプリケーションが有効になったり、自動検索サイト アフィニティ検出が有効になったりするわけではありません。動的キャプテンシーは、任意のメンバーがキャプテンになれる機能で、デフォルトで有効になっています。マルチサイト検索アーティファクト レプリケーションは、検索アーティファクトをサイト間でレプリケートできるようにする機能で、site_replication_factor を 1 より大きい値に設定することで有効になります。自動検索サイト アフィニティ検出は、検索ヘッドが次の情報に基づいてサイトを自動的に決定できるようにする機能です。ピアノードへのネットワーク遅延。これは site=auto を設定することで有効になります。

最新問題: **5**
単一サイトのインデックス レプリケーションからマルチサイト インデックス レプリケーションへの移行について説明しているのは次のうちどれですか?
A. 各サイトにマスター ノードが必要です。
B. マルチサイト ポリシーは新しいデータにのみ適用されます。
C. 単一サイト バケットはマルチサイト ポリシーを即座に受け取ります。
D. マルチサイトの合計値は、単一サイトの係数を超えてはなりません。
Answer: B (メーッセージを残す**)**
単一サイトからマルチサイトのインデックス レプリケーションへの移行は、既存のデータではなく、新しいデータにのみ影響します。マルチサイト ポリシーは新しいデータにのみ適用されます。つまり、移行後に取り込まれたデータはマルチサイトのレプリケーションと検索要素に従います。既存のデータ、または移行前に取り込まれたデータは、手動でマルチサイト バケットに変換しない限り、単一サイト ポリシーを保持します。単一サイト バケットは、マルチサイト ポリシーを即座には受信しません。また、自動的にマルチサイト バケットに変換されません。マルチサイトの合計値は、クラスター内のピアノードの数を超えない限り、単一サイトの係数を超えることができます。各サイトにマスター ノードは必要ありません。クラスター全体で必要なマスター ノードは 1 つだけです。

最新問題: **6**
Splunk インデックス作成は読み取り/書き込み集中型であるため、適切なディスク ストレージ ソリューションを選択することが重要です
展開ごとに。ディスク ストレージに関して正確なのは次のどれですか?
A. 高性能 SAN は決して使用しないでください。
B. ホット バケットおよびウォーム バケットを保存するために NFS を有効にします。
C. 推奨される RAID セットアップは RAID 10 (1 + 0) です。
D. Splunk インデクサーには通常、ベアメタルよりも仮想化環境が優先されます。
Answer: (解答を表示する**)**
説明/参照: https://www.splunk.com/pdfs/technical-briefs/splunk-deploying-vmware-tech-brief.pdf

最新問題: **7**
マルチサイト インデクサー クラスターですべてのサーチ ヘッド クラスター メンバーに site=site0 を設定するとどうなりますか?
A. 検索サイト アフィニティを無効にします。
B. すべてのメンバーを動的キャプテンに設定します。
C. マルチサイト検索アーティファクトのレプリケーションを有効にします。
D. 自動検索サイト アフィニティ検出を有効にします。
Answer: (解答を表示する**)**
説明
すべての検索ヘッド クラスター メンバーに site=site0 を設定すると、検索サイト アフィニティが無効になります。検索サイト アフィニティは、ネットワーク遅延と帯域幅の消費を削減するために、サーチ ヘッドがサーチ

ヘッドと同じサイト内にあるピア ノードを優先的に検索できるようにする機能です。site=site0 (サイトがないことを示す特別な値) を設定すると、検索ヘッドはサイトに関係なくすべてのピアノードを検索します。site=site0 を設定しても、すべてのメンバーが動的キャプテンシーに設定されたり、マルチサイト検索アーティファクトのレプリケーションが有効になったり、自動検索サイト アフィニティ検出が有効になったりするわけではありません。動的キャプテンシーは、任意のメンバーがキャプテンになれる機能で、デフォルトで有効になっています。マルチサイト検索アーティファクト レプリケーションは、検索アーティファクトをサイト間でレプリケートできるようにする機能で、site_replication_factor を 1 より大きい値に設定することで有効になります。自動検索サイト アフィニティ検出は、検索ヘッドが次の情報に基づいてサイトを自動的に決定できるようにする機能です。ピアノードへのネットワーク遅延。これは site=auto を設定することで有効になります。

最新問題: **8**
既存の Splunk 環境では、毎日作成される新しいインデックス バケットのサイズは、受信データの約半分です。各バケット内では、スペースの約 30% が生データに使用され、約 70% がインデックス ファイルに使用されます。インデクサー クラスタリングが実装されている場合、インデクサーごとの毎日のディスク消費量を計算するにはどのような追加情報が必要ですか?
A. 日次のインデックス作成量の合計、ピア ノードの数、および高速化された検索の数。
B. 日次のインデックス作成量の合計、ピア ノードの数、レプリケーション ファクター、および検索ファクター。
C. 1 日あたりの合計インデックス作成量、レプリケーション ファクター、検索ファクター、および検索ヘッドの数。
D. レプリケーション係数、検索係数、高速化された検索の数、およびクラスター全体の合計ディスク サイズ。
Answer: (解答を表示する**)**
説明
インデクサー クラスタリングが実装されている場合、インデクサーごとの毎日のディスク消費量を計算するために必要な追加情報は、毎日のインデックス作成ボリュームの合計、ピア ノードの数、レプリケーション係数、および検索係数です。これらの情報は、取り込まれるデータの量、維持される生データと検索可能なデータのコピーの数、クラスターに関与するインデクサーの数を見積もるのに必要です。高速化された検索の数、検索ヘッドの数、およびクラスター全体の合計ディスク サイズは、インデクサーごとの 1 日のディスク消費量の計算には関係ありません。詳細については、Splunk ドキュメントの 「ストレージ要件の見積もり」を参照してください。

最新問題: **9**
どの検索を実行すると、クライアント (UF) からのすべての展開クライアント メッセージが表示されますか?
A. インデックス=_内部コンポーネント= DC* ホスト=<uf> | メッセージごとの統計数
B. インデックス=_内部コンポーネント=DS* ホスト=<ds> | メッセージごとの統計数
C. インデックス=_audit コンポーネント=DC* ホスト=<uf> | メッセージごとの統計数
D. インデックス=_audit コンポーネント=DC* ホスト=<ds> | メッセージごとの統計数
Answer: B (メーッセージを残す**)**

最新問題: **10**

Splunk インデックス作成は読み取り/書き込み集中型であるため、各展開に適切なディスク ストレージ ソリューションを選択することが重要です。ディスク ストレージに関して正確なのは次のどれですか?
A. 高性能 SAN は決して使用しないでください。
B. ホット バケットおよびウォーム バケットを保存するために NFS を有効にします。
C. 推奨される RAID セットアップは RAID 10 (1 + 0) です。
D. Splunk インデクサーには通常、ベアメタルよりも仮想化環境が優先されます。
Answer: (解答を表示する**)**
説明/参照: https://www.splunk.com/pdfs/technical-briefs/splunk-deploying-vmware-tech-brief.pdf

最新問題**: 11**
Splunk Enterprise のパフォーマンスに関して正しいのは次のうちどれですか? （該当するものをすべて選択。）
A. 検索ピアを追加すると、検索結果の最大サイズが増加します。
B. 既存の検索ヘッドに RAM を追加すると、検索容量が追加されます。
C. 検索ピアを追加すると、検索負荷が増加するため、検索スループットが増加します。
D. サーチ ヘッドを追加すると、より多くの同時検索を実行するための追加の CPU コアが提供されます。
Answer: (解答を表示する**)**
説明
Splunk Enterprise のパフォーマンスに関しては、次の記述が当てはまります。
* 検索ピアを追加すると、検索負荷が増加するため、検索スループットが増加します。これは、検索ピアを追加すると、検索ワークロードがより多くのインデクサーに分散され、各インデクサーの負荷が軽減され、検索速度と同時実行性が向上するためです。
* サーチヘッドを追加すると、より多くの同時検索を実行するための追加の CPU コアが提供されます。これは、検索ヘッドを追加すると、並行して実行できる検索プロセスの数が増え、検索のパフォーマンスとスケーラビリティが向上するためです。Splunk Enterprise のパフォーマンスに関して、次の記述は誤りです。
* 検索ピアを追加しても、検索結果の最大サイズは増加しません。検索結果の最大サイズは、limits.conf ファイルの maxresultrows 設定によって決まり、検索ピアの数には関係ありません。
* 既存のサーチヘッドに RAM を追加しても、追加の検索能力は提供されません。サーチヘッドの検索能力は、RAM の量ではなく、CPU コアの数によって決まります。サーチヘッドに RAM を追加すると、検索パフォーマンスは向上しますが、検索能力は向上しません。詳細については、Splunk ドキュメントの「Splunk Enterprise のパフォーマンス」を参照してください。

最新問題**: 12**
監視コンソールの検索ダッシュボードは、分散展開がその容量に近づいていることを示しています。次のオプションのうち、検索パフォーマンスを最も向上させるのはどれですか?
A. 遅い検索を探し、オフピーク時に実行されるようにスケジュールを変更します。
B. インデクサー ストレージをソリッド ステート ドライブ (SSD) に置き換えます。
C. 検索ピアをさらに追加し、フォワーダーがすべてのインデクサーにデータを均等に分散するようにします。
D. 検索ヘッドをさらに追加し、検索タイプに基づいてユーザーを再分配します。
Answer: C (メーッセージを残す**)**

最新問題: **13**
インデクサー クラスターでは、クラスター マネージャーはどのようなタスクを実行しますか? （該当するものをすべて選択）
A. プライマリ検索可能なバケットのリストを生成および維持します。
B. インデクサー検出が有効な場合、利用可能なピアノードのリストをフォワーダーに提供します。
C. すべてのピアノードが常に同じバージョンの Splunk を使用していることを保証します。
D. アプリ バンドルをピアノードに配布します。
Answer: A,B,D (メーッセージを残す**)**
クラスター マネージャーがインデクサー クラスターで実行する正しいタスクは、A. プライマリ検索可能なバケットのリストを生成および維持する、B. インデクサー検出が有効な場合、利用可能なピア ノードのリストをフォワーダーに提供する、D. アプリ バンドルをフォワーダーに配布する、です。ピアノード。Splunk のドキュメント 1 によると、クラスター マネージャーはこれらのタスクに加えて、レプリケーションと検索要素の管理、レプリケーションと検索アクティビティの調整、クラスターの監視と管理のための Web インターフェイスの提供を担当します。オプション C は、すべてのピア ノードが常に同じバージョンの Splunk を使用するようにすることですが、これはクラスター マネージャーのタスクではなく、クラスターが適切に機能するための要件です2。したがって、選択肢 C は誤りであり、選択肢 A、B、および D は正しいです。
1: クラスター マネージャーについて 2: インデクサー クラスターの要件と互換性

最新問題: **14**
複数の検索パイプラインをいつ有効にすべきですか?
A. ディスク IOPS が 800 以上の場合のみ。
B. 同時ユーザーが 12 人未満の場合のみ。
C. Splunk Enterprise バージョン 6.6 以降を実行している場合のみ。
D. CPU とメモリのリソースが大幅に活用されていない場合のみ。
Answer: D (メーッセージを残す**)**
複数の検索パイプラインは、CPU とメモリのリソースが著しく十分に活用されていない場合にのみ有効にする必要があります。検索パイプラインは、検索コマンドを実行して結果を返すプロセスです。複数の検索パイプラインは、同時検索を並行して実行することにより、検索パフォーマンスを向上させることができます。ただし、複数の検索パイプラインはより多くの CPU リソースとメモリ リソースを消費するため、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ります。したがって、複数の検索パイプラインは、十分な CPU リソースとメモリ リソースが利用可能であり、システムがディスク I/O やネットワーク帯域幅によってボトルネックになっていない場合にのみ有効にする必要があります。同時ユーザー数、ディスク IOPS、Splunk Enterprise のバージョンは、複数の検索パイプラインを有効にするための要素ではありません。

最新問題: **15**
Splunk Enterprise のパフォーマンスに関して正しいのは次のうちどれですか? （該当するものをすべて選択。）
A. 検索ピアを追加すると、検索結果の最大サイズが増加します。
B. 既存の検索ヘッドに RAM を追加すると、検索容量が追加されます。

C. 検索ピアを追加すると、検索負荷が増加するため、検索スループットが増加します。
D. サーチ ヘッドを追加すると、より多くの同時検索を実行するための追加の CPU コアが提供されます。
Answer: (解答を表示する**)**
Splunk Enterprise のパフォーマンスに関しては、次の記述が当てはまります。
* 検索ピアを追加すると、検索負荷が増加するため、検索スループットが増加します。これは、検索ピアを追加すると、検索ワークロードがより多くのインデクサーに分散され、各インデクサーの負荷が軽減され、検索速度と同時実行性が向上するためです。
* サーチヘッドを追加すると、より多くの同時検索を実行するための追加の CPU コアが提供されます。これは、サーチヘッドを追加すると、並行して実行できる検索プロセスの数が増えるためです。
* 検索パフォーマンスとスケーラビリティが向上します。Splunk Enterprise のパフォーマンスに関して、次の記述は誤りです。
* 検索ピアを追加しても、検索結果の最大サイズは増加しません。検索結果の最大サイズは、limits.conf ファイルの maxresultrows 設定によって決まり、検索ピアの数には関係ありません。
* 既存のサーチヘッドに RAM を追加しても、追加の検索能力は提供されません。サーチヘッドの検索能力は、RAM の量ではなく、CPU コアの数によって決まります。サーチヘッドに RAM を追加すると、検索パフォーマンスは向上しますが、検索能力は向上しません。詳細については、Splunk ドキュメントの 「Splunk Enterprise のパフォーマンス」を参照してください。

最新問題**: 16**
IT サービス インテリジェンス (ITSI) は、Splunk 導入の計画にどのような影響を与えますか?
A. ITSI には専用の展開サーバーが必要です。
B. ITSI を使用するユーザーの数はパフォーマンスに影響しません。
C. Splunk 導入環境の ITSI には追加のハードウェア リソースは必要ありません。
D. 追跡されている主要業績評価指標によっては、追加のインフラストラクチャが必要になる場合があります。
Answer: D (メーッセージを残す**)**
説明
ITSI は、追跡されている主要業績評価指標 (KPI) に応じて、Splunk 導入の計画に影響を与える可能性があります。KPI は、IT サービスとビジネス プロセスの健全性とパフォーマンスを測定する指標です。ITSI は、Splunk のさまざまなデータ ソースから KPI データを収集、分析、表示します。KPI の数、頻度、複雑さに応じて、データの取り込み、処理、視覚化をサポートするために追加のインフラストラクチャが必要になる場合があります。ITSI には専用の展開サーバーは必要なく、ITSI を使用するユーザーの数にも影響しません。Splunk 導入における ITSI には、ITSI コンポーネントとアプリを実行するために CPU、メモリ、ディスク容量などの追加のハードウェア リソースが必要です。

最新問題: **17**
監視コンソールの検索ダッシュボードは、分散展開がその容量に近づいていることを示しています。次のオプションのうち、検索パフォーマンスを最も向上させるのはどれですか?
A. 検索ヘッドをさらに追加し、検索タイプに基づいてユーザーを再分配します。
B. インデクサー ストレージをソリッド ステート ドライブ (SSD) に置き換えます。
C. 検索ピアをさらに追加し、フォワーダーがすべてのインデクサーにデータを均等に分散するようにします。
D. 遅い検索を探し、オフピーク時に実行されるようにスケジュールを変更します。
Answer: D (メーッセージを残す**)**

最新問題: **18**
インデックス作成のパフォーマンスに影響を与えるインデックス作成時の props.conf 属性はどれですか? （該当するものをすべて選択。）
A. SHOULD_LINEMERGE する必要があります
B. ANNOTATE_PUNCT
C. LINE_BREAKER
D. レポート
Answer: A,C (メーッセージを残す**)**

最新問題: **19**
4 サイトのインデクサー クラスターで、元のサイトに 2 つの検索可能なコピー、site2 に 1 つの検索可能なコピー、合計 4 つの検索可能なコピーを保存する構成はどれですか?
A. site_search_factor = 起点:2、サイト 1:2、合計:4
B. site_search_factor = 起点:2、サイト 2:1、合計:4
C. site_replication_factor = 起点:2、サイト 1:2、合計:4
D. site_replication_factor = 起点:2、サイト 2:1、合計:4
Answer: B (メーッセージを残す**)**
4 サイトのインデクサー クラスターでは、元のサイトに 2 つの検索可能なコピー、site2 に 1 つの検索可能なコピー、合計 4 つの検索可能なコピーを保存する構成は、site_search_factor = Origin:2、site2:1、total:4 になります。この構成は、データの発信元サイトで検索可能なデータのコピーを 2 つ、サイト 2 で検索可能なデータのコピーを 1 つ、すべてのサイトで検索可能なデータのコピーを合計 4 つ保持するようにクラスターに指示します。site_search_factor は、各サイトのクラスターによって維持される検索可能なデータのコピーの数を決定します。site_replication_factor は、各サイトのクラスターによって維持される生データのコピーの数を決定します。詳細については、Splunk ドキュメントの 「server.conf を使用したマルチサイト インデクサー クラスターの構成」を参照してください。

最新問題: **20**
すべての検索の平均実行時間は、インデクサーで使用可能な CPU コアとどのように関係していますか?

A. インデクサー上の CPU コアの数が増えると、平均実行時間も長くなります。
B. インデクサー上の CPU コアの数が減少すると、平均実行時間は増加します。
C. 平均実行時間は、インデクサー上の CPU コアの数には依存しません。
D. インデクサー上の CPU コアの数が減少すると、平均実行時間は減少します。
Answer: B (メーッセージを残す**)**

最新問題**: 21**
サードパーティ システムとの統合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。）
A. Splunk は、Hadoop ファイル システム (HDFS) 内のデータを検索できます。
B. Splunk アラートを使用して、サードパーティ システム上でアクションをプロビジョニングできます。
C. 最初にインデックスを作成しなくても、Splunk フォワーダーからサードパーティ システムにデータを転送できます。
D. Hadoop アプリケーションは Splunk 内のデータを検索できます。
Answer: B,C (メーッセージを残す**)**

最新問題**: 22**
アプリが展開クライアントに表示されない場合、次の明確化手順のうちどれを実行する必要がありますか? （該当するものをすべて選択。）
A. デプロイメントサーバーのserverclass.confを確認します。
B. デプロイメント クライアントのdeploymentclient.confを確認します。
C. デプロイメントサーバーの SPLUNK_HOME/etc/apps の内容を確認します。
D. デプロイメントサーバーの splunkd.log で関連イベントを検索します。
Answer: A,B,D (メーッセージを残す**)**
説明
アプリが展開クライアントに表示されない場合は、次の明確化手順を実行する必要があります。
※ デプロイメントサーバーのserverclass.confを確認してください。このファイルは、サーバー クラスと、展開サーバーから受け取る必要があるアプリと構成を定義します。展開クライアントが正しいサーバー クラスに属していること、およびサーバー クラスに必要なアプリと構成があることを確認してください。
※ デプロイメントクライアントのdeploymentclient.confを確認してください。このファイルは、デプロイメント・クライアントが接続するデプロイメント・サーバーと、デプロイメント・クライアントが使用するクライアント名を指定します。デプロイメント・クライアントが正しいデプロイメント・サーバーを指していること、およびクライアント名がサーバー・クラス基準と一致していることを確認してください。
* デプロイメントサーバーの splunkd.log で関連イベントを検索します。このファイルには、展開クライアントへのアプリと構成の送信、クライアントのチェックインの検出、エラーや警告のログ記録など、展開サーバーのアクティビティに関する情報が含まれています。デプロイメント・サーバーまたはデプロイメント・クライアントの問題を示すイベントを探します。
* デプロイメントサーバーの SPLUNK_HOME/etc/apps の内容を確認することは、必要な明確化手順ではありません。このディレクトリには、デプロイメントクライアントに配布されるアプリや設定が含まれていないからです。

デプロイメントサーバーのアプリと設定は、SPLUNK_HOME/etc/deployment-apps に保存されます。詳細については、Splunk ドキュメントの デプロイメントサーバーとクライアントの構成」を参照してください。

最新問題: **23**
プライマリ バケットの分散を最適化するため。プライマリ リバランスはいつ自動的に行われますか? （該当するものをすべて選択。）
A. ローリング再起動が完了しました。
B. マスター ノードがクラスターに再参加します。
C. キャプテンがクラスターに参加または再参加します。
D. ピアノードがクラスターに参加または再参加します。
Answer: (解答を表示する**)**
プライマリ リバランスは、ローリング再起動が完了したとき、マスター ノードがクラスタに再参加したとき、またはピア ノードがクラスタに参加または再参加したときに自動的に行われます。これらのイベントにより、プライマリ バケットの分散が不均衡になる可能性があるため、マスター ノードは再バランス プロセスを開始して、各ピア ノードがほぼ同じ数のプライマリ バケットを持つようにします。キャプテンはインデクサー クラスター コンポーネントではなく、サーチ ヘッド クラスター コンポーネントであるため、キャプテンがクラスターに参加または再参加する場合には、プライマリ リバランスは発生しません。キャプテンは、インデクサー クラスタリングではなく、サーチヘッド クラスタリングを担当します。

最新問題: **24**
モニター入力のトラブルシューティングを行う場合、末尾のファイルのステータスをチェックするコマンドはどれですか?
splunk cmd btool 入力リスト | しっぽ
A. splunk cmd btool チェック入力レイヤー
B. curl https://serverhost:8089/services/admin/inputstatus/
C. TailingProcessor:FileStatus
カール https://serverhost:8089/services/admin/inputstatus/
D. TailingProcessor:Tailstatus
Answer: C (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/ 入力プロセスのトラブルシューティング #Troubleshoot_your_tailed_files

最新問題: **25**
導入計画に含めるべきものは次のうちどれですか?
A. 直接的または間接的な利害関係者の包括的なリスト。
B. 事業継続計画と災害復旧計画。
C. 現在のログの詳細とデータ ソース インベントリ。
D. IT 環境の現在および将来のトポロジー図。
Answer: (解答を表示する**)**

最新問題: **26**
インデクサー クラスター内で動作しているピア ノードを永続的に廃止するコマンドはどれですか?
A. スプランク停止 -f
B. splunk オフライン -f
C. splunk オフライン --enforce-counts
D. splunk のデコミッション -- カウントを強制する
Answer: C (メーッセージを残す**)**
splunk offline --enforce-counts コマンドは、インデクサー クラスター内で動作しているピア ノードを永続的に廃止します。このコマンドは、ピアノードをクラスターから削除し、そのデータを削除します。このコマンドは、ピアノードが不要になった場合、または別のノードに置き換えられる場合に使用する必要があります。スプランクストップ
-f コマンドはピアノード上の Splunk サービスを停止しますが、クラスターからサービスを停止しません。
splunk offline -f コマンドはピアノードをオフラインにしますが、データを削除したり、レプリケーションや検索要素を強制したりすることはありません。splunk decommission --enforce-counts コマンドは有効な Splunk コマンドではありません。詳細については、Splunk ドキュメントの 「インデクサー クラスターからピア ノードを削除する」を参照してください。

最新問題: **27**
次のオプションのうち、Splunk への syslog 配信の信頼性を向上できるのはどれですか? （該当するものをすべて選択。）
A. TCP syslog を使用します。
B. データを直接受信するように各 Splunk インデクサーの UDP 入力を構成します。
C. ネットワーク ロード バランサを使用して、syslog トラフィックをアクティブなバックエンド syslog リスナーに送信します。
D. 1 つ以上の syslog サーバーを使用して、Universal Forwarder でデータを保持し、Splunk インデクサーにデータを送信します。
Answer: (解答を表示する**)**
説明
Syslog は、さまざまなデバイスやアプリケーションから中央サーバーにログ メッセージを送信するための標準プロトコルです。Syslog は、トランスポート層プロトコルとして UDP または TCP を使用できます。UDP は高速ですが、メッセージの配信や順序が保証されないため、信頼性が低くなります。TCP は低速ですが、メッセージの配信と順序が保証されるため、信頼性が高くなります。したがって、Splunk への syslog 配信の信頼性を向上させるには、TCP syslog を使用することをお勧めします。
Splunk への syslog 配信の信頼性を向上させるもう 1 つのオプションは、1 つ以上の syslog サーバーを使用してユニバーサル フォワーダーでデータを保持し、データを Splunk インデクサーに送信することです。このようにして、syslog サーバーはバッファとして機能し、ネットワークまたは Splunk の停止の場合にデータを保存できます。Universal Forwarder は、利用可能なときに Splunk インデクサーにデータを転送できます。

ネットワーク ロード バランサーを使用して syslog トラフィックをアクティブなバックエンド syslog リスナーに送信することは、ネットワーク障害や Splunk の停止によるデータの損失や重複の可能性に対処できないため、信頼できるオプションではありません。
データを直接受信するように各 Splunk インデクサーで UDP 入力を構成することも、信頼できるオプションではありません。これは、インデクサーがネットワークに公開され、UDP の制限によりデータの損失や重複のリスクが増大するためです。

最新問題: **28**
Splunk Enterprise のパフォーマンスに関して正しいのは次のうちどれですか? （該当するものをすべて選択。）
A. 検索ピアを追加すると、検索結果の最大サイズが増加します。
B. 既存の検索ヘッドに RAM を追加すると、検索容量が追加されます。
C. 検索ピアを追加すると、検索負荷が増加するため、検索スループットが増加します。
D. サーチ ヘッドを追加すると、より多くの同時検索を実行するための追加の CPU コアが提供されます。
Answer: (解答を表示する**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/HowsavedsearchesaffectSplunkEnterpriseperform

最新問題: **29**
顧客は、1 日あたり 600 GB のデータを Splunk に取り込むことを計画しています。同時ユーザー数は 6 人であり、高いデータ可用性と高い検索パフォーマンスも求めています。お客様はコストを懸念しており、Splunk のハードウェアに最小限の費用をかけたいと考えています。この展開にはいくつのインデクサーが推奨されますか?
A. クラスター内にない 2 つのインデクサー。ユーザーが長時間の検索を多数実行すると想定されます。
B. クラスター内にない 3 つのインデクサー。データ保持期間が長いことを想定しています。
C. 高可用性が最優先であると想定して、2 つのインデクサーがクラスター化されています。
D. 大量の保存/スケジュールされた検索を想定して、2 つのインデクサーがクラスター化されています。
Answer: (解答を表示する**)**
クラスター化された 2 つのインデクサーは、1 日あたり 600 GB のデータを Splunk に取り込むことを計画しており、同時ユーザーが 6 人で、高いデータ可用性と高い検索パフォーマンスを必要とするお客様に推奨される導入です。
この導入により、顧客のニーズに十分なインデックス作成能力と同時検索が可能になると同時に、クラスター全体でのデータ レプリケーションと検索性も確保されます。また、インデクサーを 2 つだけ使用することで、ハードウェアのコストを節約することもできます。クラスター内にない 2 つのインデクサーでは、データのレプリケーションやフェイルオーバーがないため、高いデータ可用性が得られません。クラスター内にない 3 つのインデクサーは、より多くのインデックス作成能力と検索の同時実行性を提供しますが、ハードウェアのコストも増加し、データの可用性も失われます。顧客のデータ保持期間、長期検索の数、または保存/スケジュールされた検索の量は、インデクサーの数の決定には関係ありません。詳細については、Splunk ドキュメントの [リファレンス ハードウェア] および [インデクサー クラスターとインデックス レプリケーションについて] を参照してください。

最新問題: **30**

サーチ ヘッド クラスターでのキャプテンの作業負荷を軽減するには、キャプテンでのスケジュールされた検索の実行を妨げる設定は何ですか?
A. captain_is_adhoc_searchhead = true (すべてのメンバーに対して)
B. adhoc_searchhead = true (現在のキャプテンに対して)
C. adhoc_searchhead = true (すべてのメンバー上)
D. captain_is_adhoc_searchhead = true (現在のキャプテンに対して)
Answer: D (メーッセージを残す**)**

最新問題**: 31**
4 サイトのインデクサー クラスターで、元のサイトに 2 つの検索可能なコピー、site2 に 1 つの検索可能なコピー、合計 4 つの検索可能なコピーを保存する構成はどれですか?
A. site_search_factor = 起点:2、サイト 1:2、合計:4
B. site_search_factor = 起点:2、サイト 2:1、合計:4
C. site_replication_factor = 起点:2、サイト 1:2、合計:4
D. site_replication_factor = 起点:2、サイト 2:1、合計:4
Answer: B (メーッセージを残す**)**
説明
4 サイトのインデクサー クラスターでは、元のサイトに 2 つの検索可能なコピー、site2 に 1 つの検索可能なコピー、合計 4 つの検索可能なコピーを保存する構成は、site_search_factor = Origin:2、site2:1、total:4 になります。この構成は、データの発信元サイトで検索可能なデータのコピーを 2 つ、サイト 2 で検索可能なデータのコピーを 1 つ、すべてのサイトで検索可能なデータのコピーを合計 4 つ保持するようにクラスターに指示します。site_search_factor は、各サイトのクラスターによって維持される検索可能なデータのコピーの数を決定します。site_replication_factor は、各サイトのクラスターによって維持される生データのコピーの数を決定します。詳細については、Splunk ドキュメントの「server.conf を使用したマルチサイト インデクサー クラスターの構成」を参照してください。

最新問題**: 32**
どの検索を実行すると、クライアント (UF) からのすべての展開クライアント メッセージが表示されますか?
A. インデックス=_audit コンポーネント=DC* ホスト=<ds> | メッセージごとの統計数
B. インデックス=_audit コンポーネント=DC* ホスト=<uf> | メッセージごとの統計数
C. インデックス=_内部コンポーネント= DC* ホスト=<uf> | メッセージごとの統計数
D. インデックス=_内部コンポーネント=DS* ホスト=<ds> | メッセージごとの統計数

Answer: D (メーッセージを残す)
説明/参照: https://answers.splunk.com/answers/461939/after-all-clients-are-registered-to-a-deployment-s.html

最新問題**: 33**
新しい Splunk 顧客は、syslog を使用してポート 514 上のネットワーク デバイスからデータを収集しています。このデータを Splunk に取り込む練習をしますか?
A. 複数の Splunk インデクサーにデータを送信するように syslog を構成します。
B. Splunk インデクサーを使用して、ポート 514 上のネットワーク入力を直接収集します。
C. Splunk フォワーダーを使用して、ポート 514 で入力を収集し、データを転送します。
D. ログを書き込み、Splunk フォワーダーを使用してログを収集するように syslog を構成します。
Answer: D (メーッセージを残す)
説明/参照: https://docs.splunk.com/Documentation/SplunkCloud/8.0.0/Data/Monitornetworkports

最新問題**: 34**
プライマリ バケットの分散を最適化するため。プライマリ リバランスはいつ自動的に行われますか? （該当するものをすべて選択。）
A. ローリング再起動が完了しました。
B. マスター ノードがクラスターに再参加します。
C. キャプテンがクラスターに参加または再参加します。
D. ピアノードがクラスターに参加または再参加します。
Answer: A,B,D (メーッセージを残す)
説明
プライマリ リバランスは、ローリング再起動が完了したとき、マスター ノードがクラスタに再参加したとき、またはピア ノードがクラスタに参加または再参加したときに自動的に行われます。これらのイベントにより、プライマリ バケットの分散が不均衡になる可能性があるため、マスター ノードは再バランス プロセスを開始して、各ピア ノードがほぼ同じ数のプライマリ バケットを持つようにします。キャプテンはインデクサー クラスター コンポーネントではなく、サーチ ヘッド クラスター コンポーネントであるため、キャプテンがクラスターに参加または再参加する場合には、プライマリ リバランスは発生しません。キャプテンは、インデクサー クラスタリングではなく、サーチヘッド クラスタリングを担当します。

最新問題**: 35**
関係者は、検索可能なデータの高可用性を最優先事項として認識しています。この要件に最もよく対応するのは次のうちどれですか?
A. クラスター内のサーチヘッドの数を増やします。
B. クラスター内の検索係数を増やします。
C. クラスター内のレプリケーション係数を増やします。
D. クラスター内のインデクサーの CPU の数を増やします。
Answer: (解答を表示する)

最新問題**: 36**

顧客は 4 つのサイトのインデクサー クラスターを持っています。お客様には、検索可能なデータのコピーを 5 つ保存するという要件があり、そのうち 1 つは元のサイトに検索可能なデータのコピー、もう 1 つはディザスター リカバリー サイト (サイト 4) に検索可能なデータのコピーがあります。
これらの要件を満たす構成はどれですか?
A. site_replication_factor = 起点:2、サイト 4:1、合計:3
B. site_replication_factor = 起点:1、サイト 4:1、合計:5
C. site_search_factor = 起点:2、サイト 4:1、合計:3
D. サイト検索係数 = 起点:1、サイト 4:1、合計:5
Answer: B (メーッセージを残す**)**
顧客の要件を満たす正しい構成は、site_replication_factor = Origin:1、site4:1、total:5 です。これは、各バケットに元のサイトにコピーが 1 つ、災害復旧サイト (サイト 4) にコピーが 1 つ、その他のサイトにコピーが 3 つあることを意味します。合計部数はお客様のご希望に応じて5部となります。site_replication_factor は、マルチサイト インデクサー クラスター内のサイト全体に保存される各バケットのコピーの数を決定します1。site_search_factor は、マルチサイト インデクサー クラスター内のサイト全体で検索可能な各バケットのコピーの数を決定します2。したがって、選択肢 B が正解で、選択肢 A、C、D は不正解となります。
1: サイト レプリケーション係数を構成します。2: サイト検索係数を構成します。

最新問題**: 37**
serverclass.conf で使用できるクライアント フィルターは次のうちどれですか? （該当するものをすべて選択。）
A. DNS 名。
B. プラットフォーム (マシンタイプ)。
C. Splunk サーバーの役割。
D. IP アドレス。
Answer: A,D (メーッセージを残す**)**

最新問題**: 38**
Splunk 内部ログのデフォルトのログ サイズはどれくらいですか?
A. 10MB
B. 20 MB
C. 25MB
D. 30MB
Answer: C (メーッセージを残す**)**
説明
Splunk の内部ログは、デフォルトで SPLUNK_HOME/var/log/splunk ディレクトリに保存されます。Splunk 内部ログのデフォルトのログ サイズは 25 MB です。つまり、ログ ファイルが 25 MB に達すると、Splunk はそれをバックアップ ファイルにロールし、新しいログ ファイルを作成します。デフォルトのバックアップ ファイル数は 5 です。これは、Splunk がログ ファイルごとに最大 5 つのバックアップ ファイルを保持することを意味します。

最新問題**: 39**

2 つのインデクサーと 1 つの検索ヘッドを備えた Splunk 環境では、インデックス作成が遅く、リアルタイムの検索結果が遅れます。インデクサーでは十分な CPU とメモリが利用可能です。インデックス作成のパフォーマンスを向上させる可能性が最も高いのは次のうちどれですか?
A. limits.conf の検索パイプラインの最大サイズを減らします。
B. limits.conf でスケジュールされた同時検索の最大数を減らします。
C. indexes.conf のホット バケットの最大数を増やします。
D. server.conf 内の並列取り込みパイプラインの数を増やします。
Answer: B (メーッセージを残す**)**

最新問題**: 40**
デプロイヤーからの構成は、サーチ ヘッド クラスター メンバーのどの場所にマージされますか?
A. SPLUNK_HOME/etc/system/local
B. SPLUNK_HOME/etc/apps/APP_HOME/local
C. SPLUNK_HOME/etc/apps/search/default
D. SPLUNK_HOME/etc/apps/APP_HOME/default
Answer: B (メーッセージを残す**)**
説明
デプロイヤーからの設定は、サーチヘッドクラスターメンバーの SPLUNK_HOME/etc/apps/APP_HOME/local ディレクトリにマージされます。デプロイヤーは、アプリとその他の構成を構成バンドルの形式でサーチヘッドクラスターのメンバーに配布します。設定バンドルには、デプロイヤ上の SPLUNK_HOME/etc/shcluster/apps ディレクトリの内容が含まれています。サーチヘッドクラスターメンバーが設定バンドルを受信すると、バンドルの内容を独自の SPLUNK_HOME/etc/apps ディレクトリにマージします。ローカル ディレクトリの設定は、デフォルト ディレクトリの設定より優先されます。SPLUNK_HOME/etc/system/local ディレクトリは、アプリレベルの設定ではなく、システムレベルの設定に使用されます。SPLUNK_HOME/etc/apps/search/default ディレクトリは、デプロイヤからの設定ではなく、検索アプリのデフォルト設定に使用されます。

最新問題**: 41**
次の構成属性のうち、単一サイト インデクサー クラスターのクラスター マネージャーのサーバー conf で設定する必要があるのはどれですか?
A. master_uri
B. サイト
C. レプリケーション係数
D. site_replication_factor
Answer: A (メーッセージを残す**)**
単一サイトのインデクサー クラスターのクラスター マネージャーの server.conf に設定する正しい構成属性は、master_uri です。この属性は、クラスタ マネージャの URI を指定します。これは、ピア ノードとサーチ ヘッドがクラスタ マネージャと通信するために必要です1。他の属性は単一サイト インデクサー クラスターには必要ありませんが、マルチサイト インデクサー クラスターには使用されます。サイト属性は、マルチサイト インデクサー クラスター内の各ノードのサイト名を定義します2。replication_factor 属性は、マルチサイト インデクサー クラスター全体で維持する各バケットのコピーの数を定義します3。site_replication_factor 属性は、マルチサイト

インデクサー クラスター内の各サイトにわたって維持する各バケットのコピーの数を定義します4。したがって、選択肢 A が正解で、選択肢 B、C、D は不正解となります。
1: クラスターマネージャーの構成 2: サイト属性の構成 3: レプリケーション係数の構成 4: サイトレプリケーション係数の構成

最新問題: **42**
ヘビー フォワーダーの代わりにユニバーサル フォワーダーを使用する必要があるのはどのような場合ですか?
A. ほとんどのデータでマスキングが必要な場合。
B. 高速データ ソースがある場合。
C. データがデータベース サーバーから直接受信される場合。
D. モジュラー入力が必要な場合。
Answer: (解答を表示する**)**
Splunk ブログ 1 によると、ユニバーサル フォワーダーは、設置面積が小さくパフォーマンスが速いため、syslog サーバーなどの高速データ ソースからデータを収集するのに最適です。Universal Forwarder は最小限の処理を実行し、生のデータまたは解析されていないデータをインデクサーに送信することで、ネットワーク トラフィックとフォワーダーの負荷を軽減します。他のオプションは次の理由から false です。
* ほとんどのデータでマスキングが必要な場合は、データを転送する前に高度なフィルタリングとデータ変換を実行できるヘビー フォワーダーが必要です2。
* データがデータベース サーバーから直接受信される場合、DB Connect などのモジュラー入力を実行してさまざまなデータベースからデータを収集できるため、Heavy Forwarder が必要になります2。
* モジュラー入力が必要な場合、Universal Forwarder には、ほとんどのモジュラー入力に必要な Python のバンドル バージョンが含まれていないため、Heavy Forwarder が必要になります2。

最新問題: **43**
アプリが展開クライアントに表示されない場合、次の明確化手順のうちどれを実行する必要がありますか?
（該当するものをすべて選択。）
A. デプロイメントサーバーのserverclass.confを確認します。
B. デプロイメント クライアントのdeploymentclient.confを確認します。
C. デプロイメントサーバーの SPLUNK_HOME/etc/apps の内容を確認します。
D. デプロイメントサーバーの splunkd.log で関連イベントを検索します。
Answer: A,B,C (メーッセージを残す**)**
説明/参照: https://answers.splunk.com/answers/177021/why-is-deployment-client-not-picking-up-changes-.htmlへ

最新問題: **44**
インデックス作成のパフォーマンスへの影響が最も少ない props.conf 設定はどれですか?
A. SHOULD_LINEMERGE する必要があります
B. 切り捨て
C. 文字セット
D. TIME_PREFIX

Answer: C (メーッセージを残す)
Splunk のドキュメント1 によると、props.conf の CHARSET 設定は、ソース データの文字セット エンコーディングを指定します。この設定は、Splunk がデータのバイトを解釈する方法にのみ影響し、データの処理や変換方法には影響しないため、インデックス作成のパフォーマンスへの影響は最小限です。他のオプションは次の理由から false です。
* props.conf の SHOULD_LINEMERGE 設定は、Splunk がタイムスタンプまたは改行に基づいてイベントを中断するかどうかを決定します。この設定は、Splunk がデータを解析し、イベントの境界を識別する方法に影響するため、インデックス作成のパフォーマンスに大きな影響を与えます2。
* props.conf の TRUNCATE 設定は、Splunk がファイルの 1 行からインデックスを作成する最大文字数を指定します。この設定は、Splunk がインデックスに対して読み書きするデータの量に影響するため、インデックス作成のパフォーマンスに中程度の影響を与えます3。
* props.conf の TIME_PREFIX 設定では、イベント データのタイムスタンプの直前に付けるプレフィックスを指定します。この設定は、Splunk がタイムスタンプを抽出してイベントに割り当てる方法に影響するため、インデックス作成のパフォーマンスに中程度の影響を与えます。

最新問題**: 45**
インデクサー クラスター内のインデックスのレプリケーションをアクティブにするには、すべてのピアノードの Indexes.conf でどの属性を構成する必要がありますか?
A. repFactor = 0
B. 複製 = 0
C. repFactor = 自動
D. レプリケート = 自動
Answer: (解答を表示する)
インデクサー クラスター内のインデックスのレプリケーションをアクティブにするには、すべてのピアノードの Indexes.conf で repFactor 属性を構成する必要があります。この属性は、インデックスのレプリケーション係数を指定します。これにより、クラスターによって維持される生データのコピーの数が決まります。repFactor 属性を auto に設定すると、インデックスのレプリケーションが有効になります。Indexes.conf の replicate 属性は有効な Splunk 属性ではありません。Outputs.conf の repFactor 属性とdeploymentclient.conf のreplicate 属性は、インデクサー クラスター内のインデックスのレプリケーションに関連しません。詳細については、Splunk ドキュメントの「インデクサー クラスターのインデックスの構成」を参照してください。

最新問題**: 46**
マルチサイト インデクサー クラスターは、次のどれを使用して構成できますか? （該当するものをすべて選択。）
A. Splunk Web 経由。
B. SPLUNK_HOME/etc./system/local/server.conf を直接編集します。
C. CLI から Splunk edit cluster-config コマンドを実行します。
D. SPLUNK_HOME/etc/system/default/server.conf を直接編集します。
Answer: B,C (メーッセージを残す)
マルチサイト インデクサー クラスターは、直接編集して構成できます。

SPLUNK_HOME/etc/system/local/server.conf、または CLI から splunk edit cluster-config コマンドを実行します。これらのメソッドを使用すると、管理者は各インデクサー ノードのサイト属性と、クラスターの site_replication_factor および site_search_factor を指定できます。Splunk Web 経由でマルチサイト インデクサー クラスターを設定する方法や、SPLUNK_HOME/etc/system/default/server.conf を直接編集する方法はサポートされていません。
詳細については、Splunk ドキュメントの 『server.conf を使用したインデクサー クラスターの構成」を参照してください。

最新問題: **47**
Splunk 構成パラメータの設定は、異なるアプリ内に含まれる同じ名前の複数の .conf ファイル間で異なる場合があります。次のディレクトリのうち、最も優先順位が高いのはどれですか?
A. システムのローカル ディレクトリ。
B. システムのデフォルトのディレクトリ。
C. アプリのローカル ディレクトリ (ASCII 順)。
D. アプリのデフォルト ディレクトリ (ASCII 順)。
Answer: A (メーッセージを残す**)**
システム ローカル ディレクトリは、異なるアプリ内の同じ名前の Splunk 設定ファイルを含む次のディレクトリの中で最も高い優先順位を持ちます。Splunk 設定ファイルは、SPLUNK_HOME/etc ディレクトリの下のさまざまなディレクトリに保存されます。これらのディレクトリの優先順位によって、競合または重複がある場合にどの構成ファイル設定が有効になるかが決まります。SPLUNK_HOME/etc/system/local にあるシステム ローカル ディレクトリは、インスタンスに固有のシステムレベルの設定が含まれるため、すべてのディレクトリの中で最も優先されます。SPLUNK_HOME/etc/system/default にあるシステムのデフォルト ディレクトリは、Splunk によって提供されるシステムレベルの設定が含まれており、変更しないでください。そのため、すべてのディレクトリの中で優先順位が最も低くなります。SPLUNK_HOME/etc/apps/APP_NAME/local にあるアプリのローカル ディレクトリは、SPLUNK_HOME/etc/apps/APP_NAME/default にあるアプリのデフォルト ディレクトリよりも優先されます。これは、ローカル ディレクトリにはアプリが含まれているためです。- インスタンスに固有の -レベルの構成。一方、デフォルトのディレクトリには、アプリによって提供されるアプリレベルの構成が含まれているため、変更しないでください。アプリのローカル ディレクトリとデフォルト ディレクトリは、アプリ名の ASCII 順序に応じて異なる優先順位を持ち、ASCII 順序で後のアプリ名ほど優先順位が高くなります。

最新問題: **48**

診断を作成するときに検索アーティファクトを除外する方法は次のうちどれですか?
A. SPLUNK_HOME/bin/splunk diag --exclude
B. SPLUNK_HOME/bin/splunk diag --debug --refresh
C. SPLUNK_HOME/bin/splunk diag --disable=dispatch
D. SPLUNK_HOME/bin/splunk diag --filter-searchstrings
Answer: (解答を表示する**)**
説明
splunk diag --exclude コマンドは、診断の作成時に検索アーティファクトを除外する方法です。diag は、さまざまなログ、設定、その他の情報を含む Splunk インスタンスの診断スナップショットです。
検索アーティファクトは、検索ジョブによって生成され、ディスパッチ ディレクトリに保存される一時ファイルです。
--exclude オプションを使用し、ディスパッチ ディレクトリを指定することで、検索アーティファクトを診断から除外できます。splunk diag --debug --refresh コマンドは、デバッグ ログを有効にして診断を作成し、診断がすでに存在する場合は更新する方法です。--disable オプションが存在しないため、splunk diag --disable=dispatch コマンドは有効なコマンドではありません。splunk diag --filter-searchstrings コマンドは、diag 内の検索文字列から機密情報をフィルターで除外する方法です。

最新問題**: 49**
モニター ･スタンザの正規表現の解釈に問題があると思われる場合、どのログ ･ファイルを検索して検証しますか?
A. splunkd.log
B. metrics.log
C. tailing_processor.log
D. btool.log
Answer: (解答を表示する**)**

最新問題**: 50**
可能な限り中間フォワーダーを避けるべきなのはなぜですか?
A. ライセンスの使用量とコストを最小限に抑えるため。
B. 平均故障間隔を短縮します。
C. 中間フォワーダーはデプロイメントサーバーによって管理できないためです。
D. 潜在的なパフォーマンスのボトルネックを排除します。
Answer: D (メーッセージを残す**)**
中間フォワーダーは、他のフォワーダーからデータを受信し、そのデータをインデクサーに送信するフォワーダーです。これらは、ネットワーク帯域幅やセキュリティの制約によりインデクサーに直接転送できない場合や、転送中にデータをルーティング、クローン作成、または変更する必要がある場合など、一部のシナリオで役立つ場合があります。
ただし、中間フォワーダーはデータ パイプラインにさらなる複雑さとオーバーヘッドをもたらし、データ取り込みのパフォーマンスと信頼性に影響を与える可能性があります。したがって、中間フォワーダーは可能な限り避け、明確な利点や要件がある場合にのみ使用する必要があります。中間フォワーダーの欠点には次のようなものがあります。

* データ フロー内のホップと接続の数が増加し、遅延や遅延が発生する可能性があります。
* データの損失または破損のリスクが増加します。
* これらは、CPU、メモリ、ディスク、ネットワーク帯域幅など、実行されるホスト上のリソースをより多く消費し、それらのホスト上の他のアプリケーションやプロセスのパフォーマンスに影響を与える可能性があります。
* 入力、出力、負荷分散、セキュリティ、監視、トラブルシューティングの設定など、追加の構成とメンテナンスが必要です。
* クローン作成やルーティング ルールを使用する場合など、適切に構成されていない場合、データの重複や不整合が発生する可能性があります。
この答えをサポートする参考文献の一部は次のとおりです。
* 中間フォワーダーを構成します。 中間フォワーダーは、フォワーダーが 1 つ以上のフォワーダーからデータを受信し、そのデータを別のインデクサーに送信します。この種のセットアップは、たとえば、異なるホストに多数のホストがある場合に便利です。データをインデクサーに転送する前に、これらのフォワーダーからそのリージョンの中央ホストにデータを送信したい場合は、すべての種類のフォワーダーが中間フォワーダーとして機能します。ただし、これにより展開が複雑になり、パフォーマンスに影響を与える可能性があるため、必要な場合にのみ使用してください。」
* ユニバーサルおよびヘビー フォワーダーを使用した中間データ ルーティング: 「このドキュメントでは、技術要件とビジネス要件の両方に対処するデータをルーティングするためのさまざまな Splunk オプションの概要を説明します。全体的な利点 splunkd 中間データ ルーティングを使用すると、次のような全体的な利点が得られます。このドキュメントで説明されているルーティング戦略により、大規模なデータを確実に処理するための柔軟性が可能になります。中間ルーティングにより、イベントレベルのデータおよび転送中のセキュリティが向上します。以下は、splunkd 中間データ ルーティングのユースケースとイネーブラーのリストです: ...制限事項 splunkd 中間データ ルーティングには次の制限があります: ... 複雑さとリソース消費量の増大 splunkd 中間データ ルーティングはデータ パイプラインに複雑さを加え、それが実行されるホスト上のリソースを消費します。これは、データ インジェストとデータ取り込みのパフォーマンスと信頼性に影響を与える可能性があります。したがって、中間ルーティングは可能な限り避け、明確な利点や要件がある場合にのみ使用する必要があります。」
* フォワーダーを使用して Splunk Enterprise にデータを取得します。これには、「フォワーダーは Apache データを取得し、インデックス作成のために Splunk Enterprise デプロイメントに送信します。これにより、データが統合、保存され、検索に使用できるようになります。リソース フットプリントが削減されるため、, フォワーダーによる Apache サーバーへのパフォーマンスへの影響は最小限に抑えられます ... 注: 別のフォワーダーにデータを送信し、そのデータをインデクサーに送信するようにフォワーダーを構成することもできます。これは中間転送と呼ばれます。
ただし、これにより展開が複雑になり、パフォーマンスに影響を与える可能性があるため、必要な場合にのみ使用してください。」

最新問題**: 51**
Splunk アーキテクトは Buttercup Games での Splunk 導入を継承しましたが、エンド ユーザーは、Web ソースタイプに対してイベントの形式が一貫していないことに不満を抱いています。さらに調査を進めると、すべての Web ログが同じインフラストラクチャを通過するわけではないことが判明しました。データの一部は重度のフォワーダーを経由し、一部のフォワーダーは別の部門によって管理されています。

この問題の原因として考えられる項目は次のどれですか?
A. 他の部門によって管理されているフォワーダーは、他の部門よりも古いバージョンです。
B. データ入力がすべてのフォワーダーにわたって適切に構成されていません。
C. インデクサーは、ヘビー フォワーダーとは異なる構成を持つ場合があります。
D. 検索ヘッドの構成はインデクサーとは異なる場合があります。
Answer: A (メーッセージを残す**)**

最新問題**: 52**
ナレッジ バンドルのレプリケーション中に .delta レプリケーションが失敗した場合、Splunk のフォールバック方法は何ですか?
A. .splunkd を再起動します。
B. .delta レプリケーション。
C. .bundle レプリケーション。
D. mongod を再起動します。
Answer: C (メーッセージを残す**)**
これは、ナレッジ バンドルのレプリケーション中に .delta レプリケーションが失敗した場合の Splunk のフォールバック方法です。ナレッジ バンドルのレプリケーションは、ルックアップ、マクロ、フィールド抽出などのナレッジ オブジェクトをサーチ ヘッド クラスターからインデクサー クラスターに分散するプロセスです1。Splunk は、.delta レプリケーションと .bundle レプリケーション 1 という 2 つのナレッジ バンドル レプリケーション方法を使用します。デルタ レプリケーションは、ナレッジ オブジェクトに対する変更または更新のみをレプリケートするため、デフォルトで推奨される方法であり、ネットワーク トラフィックとディスク領域の使用量が削減されます1。ただし、破損したファイルやネットワーク エラーなどの何らかの理由で .delta レプリケーションが失敗した場合、Splunk は変更や更新に関係なく、ナレッジ バンドル全体を複製する .bundle レプリケーションに自動的に切り替わります1。これにより、ナレッジ オブジェクトがサーチ ヘッド クラスターとインデクサー クラスター間で常に同期されるようになりますが、より多くのネットワーク帯域幅とディスク領域を消費します1。他のオプションは、Splunk の有効なフォールバック方法ではありません。オプション A の splunkd の再起動は、ナレッジ バンドルのレプリケーションの方法ではなく、ノード 2 で Splunk デーモンを再起動する方法です。これにより、.delta レプリケーションの失敗が修正される場合と修正されない場合がありますが、ナレッジ オブジェクトの同期は保証されません。オプション B の .δ レプリケーションはフォールバック方法ではなく、質問 1 で失敗したと想定されるナレッジ バンドル レプリケーションの主要な方法です。オプション D の mongod の再起動は、ナレッジ バンドル レプリケーションの方法ではなく、ノード 3 上で MongoDB デーモンを再起動する方法です。これはナレッジ バンドルのレプリケーションではなく、別のプロセスである KV ストアのレプリケーションに関連しています3。したがって、選択肢 C が正解で、選択肢 A、B、D は不正解となります。
1: ナレッジバンドルのレプリケーションの仕組み 2: Splunk Enterprise の起動と停止 3: KV ストアの再起動

最新問題**: 53**
ファイアウォール データが関係するユースケースを考えてみましょう。Splunk がサポートするテクニカル アドオンはありませんが、ベンダーが構築しています。アドオンをインストールする前に評価する必要がある項目は何ですか? （該当するものをすべて選択。）

A. スケジュールされた検索またはリアルタイムの検索の数を特定します。
B. このテクニカル アドオンがデータ モデルのイベント データを有効にするかどうかを検証します。
C. Technical Add-On がサポートできるフォワーダーの最大数を特定します。
D. テクニカル アドオンをサーチ ヘッドまたはインデクサーの両方にインストールする必要があるかどうかを確認します。
Answer: A,B (メーッセージを残す**)**
テクニカル アドオン (TA) は、データ収集、解析、強化のための設定を含む Splunk アプリです。また、データ モデルのイベント データを有効にすることもできます。これは、ダッシュボードやレポートの作成に役立ちます。したがって、TA をインストールする前に、データ モデルを使用するスケジュールされた検索またはリアルタイム検索の数を特定し、TA がデータ モデルのイベント データを有効にするかどうかを検証することが重要です。TA はフォワーダーではなくインデクサーまたはサーチ ヘッドにインストールされるため、TA がサポートできるフォワーダーの数は関係ありません。TAの設置場所はデータの種類やユースケースによって異なるため、固定的な要件ではありません

最新問題**: 54**
Splunk インデクサーのクラスタリングに関する正しい記述は次のうちどれですか?
A. サーチヘッドはピアノードと同じかそれ以降の Splunk バージョンを実行する必要があります。
B. マスターノードは、サーチヘッドと同じかそれ以降の Splunk バージョンを実行する必要があります。
C. すべてのピアノードは、まったく同じ Splunk バージョンを実行する必要があります。
D. ピアノードはマスターノードと同じかそれ以降の Splunk バージョンを実行する必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 55**
クラスター化インデックス内のバケットにはどのような種類のファイルが存在しますか? （該当するものをすべて選択）
A. 複製されたバケット内には生データのみがあります。
B. 検索可能なバケット内には tsidx のみがあります。
C. 検索可能なバケット内には、tsidx と rawdata があります。
D. レプリケートされたバケット内には、tsidx と rawdata の両方が存在します。
Answer: (解答を表示する**)**
Splunk のドキュメント 1 によると、クラスター化インデックス内のバケットには、圧縮形式の生データ (rawdata) と生データを指すインデックス (tsidx ファイル) の 2 つの主要なタイプのファイルが含まれています。バケットは、両方のタイプのファイルが含まれるか、生データ ファイルのみが含まれるかに応じて、複製または検索可能になります。複製されたバケットは、データ複製の目的で、あるピアノードから別のピアノードにコピーされたバケットです。検索可能なバケットは、rawdata ファイルと tsidx ファイルの両方を含むバケットであり、検索ヘッドによって検索できます。クラスター化インデックス内のバケットに存在するファイルの種類は次のとおりです。
* 検索可能なバケット内には、tsidx と rawdata が存在します。検索可能なバケットにはデータとインデックス ファイルの両方が含まれており、検索ヘッド 1 によって検索できるため、これは当てはまります。

* 複製されたバケット内には、tsidx と rawdata の両方が存在します。データ ファイルとインデックス ファイルの両方が含まれている場合、レプリケートされたバケットは検索可能なバケットにもなり得るため、これは当てはまります。ただし、レプリケーション係数と検索係数の設定によっては、一部のバケットには生データ ファイルのみが存在する可能性があるため、レプリケートされたバケットのすべてが検索可能であるわけではありません1。
他のオプションは次の理由から false です。
* 複製されたバケット内には生データのみが存在します。複製されたバケットが検索可能なバケットである場合、そのバケットにも tsidx ファイルが存在する可能性があるため、これは false です。複製されたバケットが検索不可能なバケットの場合、レプリケートされたバケットには生データ ファイルのみが含まれます。つまり、別のピア ノード 1 から tsidx ファイルを取得するまで、サーチ ヘッドによる検索はできません。
※検索可能なバケット内にはtsidxのみが存在します。これは、データの検索に必要なため、検索可能なバケットには常に tsidx ファイルと rawdata ファイルの両方が含まれるため、これは false です。検索可能なバケットには、tsidx ファイルが指す実際のデータが含まれているため、生データ ファイルがなければ存在できません1。

最新問題**: 56**
Splunk Enterprise プラットフォームのインストルメンテーションは、Splunk Enterprise 導入環境がログに記録するデータを指します。
_イントロスペクションインデックス。このインデックスに含まれるログは次のうちどれですか? （該当するものをすべて選択。）
A. 監査ログ
B. metrics.log
C. ディスクオブジェクト.ログ
D. resource_usage.log
Answer: (解答を表示する**)**
説明
次のログは _introspection インデックスに含まれており、Splunk Enterprise デプロイメントがプラットフォーム インストルメンテーションについてログに記録するデータが含まれています。
* ディスクオブジェクト.ログ。このログには、バケット、インデックス、ファイルなど、Splunk が作成および管理するディスク オブジェクトに関する情報が含まれています。このログは、ディスク領域の使用状況とバケットのライフサイクルを監視するのに役立ちます。
* resource_usage.log。このログには、CPU、メモリ、ディスク、ネットワークなどの Splunk プロセスのリソース使用状況に関する情報が含まれています。このログは、Splunk のパフォーマンスを監視し、リソースのボトルネックを特定するのに役立ちます。次のログは _introspection インデックスには含まれていませんが、_internal インデックス。Splunk が内部ログ用に生成するデータが含まれます。
* 監査ログ。このログには、ユーザーアクション、設定変更、検索アクティビティなど、Splunk が記録する監査イベントに関する情報が含まれています。このログは、Splunk の操作とセキュリティを監査するのに役立ちます。
* metrics.log。このログには、データ スループット、データ レイテンシー、検索の同時実行性、検索時間など、Splunk が収集するパフォーマンス メトリックに関する情報が含まれています。このログは、Splunk のパフォーマンスと効率を測定するのに役立ちます。詳細については、「Splunk Enterprise のログ記録について」を参照してください。

Splunk ドキュメントの [_introspection インデックスについて]。

最新問題**: 57**
インデックスの数とサイズを設計するとき、次の考慮事項のうちどれを適用する必要がありますか?
A. 予想される毎日の取り込み量、アクセス制御、同時ユーザー数
B. インストールされているアプリの数、予想される毎日の取り込み量、データ保持期間ポリシー
C. データ保持期間ポリシー、インストールされているアプリの数、アクセス制御
D. 予想される毎日の取り込み量、データ保持期間ポリシー、アクセス制御
Answer: (解答を表示する**)**
インデックスの数とサイズを設計するときは、次の考慮事項を適用する必要があります。
* 予想される 1 日あたりの取り込み量: これは、Splunk プラットフォームによって 1 日に取り込まれ、インデックス付けされるデータの量です。これは、Splunk 導入のストレージ容量、インデックス作成パフォーマンス、ライセンスの使用状況に影響します。インデックスの数とサイズは、Splunk 導入でデータ負荷を処理し、ビジネス要件を満たすことができるように、予想される毎日の取り込み量とピーク時の取り込み量に応じて計画する必要があります12。
* データ保持期間ポリシー: これは、データが保存され、Splunk プラットフォームによって検索できる期間です。これは、Splunk 導入のストレージ容量、データの可用性、データ コンプライアンスに影響します。インデックスの数とサイズは、Splunk 導入で必要な期間データを保持し、法的または規制上の義務を確実に満たすことができるように、データ保持時間ポリシーおよびデータ ライフサイクルに従って計画する必要があります13。
* アクセス制御: これは、Splunk ユーザーまたはロールによるデータへのアクセスを許可または制限するためのメカニズムです。これは、Splunk 導入のデータ セキュリティ、データ プライバシー、データ ガバナンスに影響します。インデックスの数とサイズは、Splunk 導入で不正または不適切なアクセスからデータを保護し、倫理または組織の基準を満たすことができるように、アクセス制御およびデータの機密性に応じて計画する必要があります14。
オプション D は、インデックスの数とサイズを設計する際の最も関連性が高く重要な考慮事項を反映しているため、正解です。選択肢 A は不正解です。同時ユーザー数はインデックスの数とサイズを設計するための直接的な要素ではなく、サーチ ヘッドの容量とサーチ ヘッドのクラスタリング構成を設計するための要素であるからです5。選択肢 B は不正解です。インストールされているアプリの数は、インデックスの数とサイズを設計するための直接的な要因ではなく、アプリの互換性とアプリのパフォーマンスを設計するための要因です。オプション C は、インデックスの数とサイズを設計する上で重要な要素である、予想される毎日の取り込み量が省略されているため、不正解です。
参考文献:
1: Splunk 検証済みアーキテクチャ 2: [インデクサーのキャパシティ プランニング] 3: [インデックスのリタイアおよびアーカイブ ポリシーの設定] 4: [Splunk Enterprise のセキュリティについて] 5: [サーチヘッドのキャパシティ プランニング] : [アプリのインストールと管理の概要]

最新問題**: 58**
Splunk インスタンスの SPLUNK_HOME/etc/system/local/server.conf には次の設定があります。
[クラスタリング]
モード = マスター

レプリケーション係数 = 2
pass4SymmKey = パスワード123
この Splunk インスタンスについて説明しているのは次のどれですか? （該当するものをすべて選択。）
A. この Splunk インスタンスを再起動する必要があります。
B. これはマルチサイト クラスターです。
C. このインスタンスには master_uri 属性がありません。
D. このクラスターの検索係数は 2 です。
Answer: A,C (メーッセージを残す**)**

最新問題**: 59**
アーカイブバケットを解凍するにはどのコマンドが使用されますか?
A. Splunk dbinspect
B. Splunk 変換
C. Splunk の再構築
D. Splunk 収集
Answer: (解答を表示する**)**

最新問題**: 60**
次の文のうち、サーチ ヘッド クラスター (SHC) のキャプテン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。）
A. SHC 全体のジョブ スケジューラです。
B. アラート アクションの抑制 (スロットリング) を管理します。
C. メンバー リストを KV ストア プライマリと同期します。
D. SHC のナレッジ バンドルを検索ピアに複製します。
Answer: A,D (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture#role_of_the_captain

最新問題**: 61**
サーチ ヘッド クラスター デプロイヤにとって適切なプラクティスは次のうちどれですか?
A. デプロイヤは、サーチ ヘッド クラスタ メンバーが "ホームに電話する"ときにのみ構成を配布します。
B. デプロイヤーは、複製不可能な構成をサーチ ヘッド クラスター メンバーに配布するために使用する必要があります。
C. デプロイ担当者は、有効な構成となるように、サーチ ヘッド クラスター メンバーに構成を配布する必要があります。
D. デプロイヤーは、splunk apply shcluster-bundle を使用して、サーチヘッドクラスターメンバーに設定を配布するだけです。
Answer: B (メーッセージを残す**)**
説明
以下は、サーチ ヘッド クラスター デプロイヤの推奨事項です。デプロイヤは、複製不可能な構成をサーチ ヘッド クラスタ メンバーに配布するために使用する必要があります。レプリケート不可能な構成とは、アプリや

server.conf設定などの検索要素によってレプリケートされない構成です。デプロイヤーは、これらの設定をサーチヘッドクラスターメンバーに配布し、それらが同じ設定であることを保証する Splunk サーバーの役割です。デプロイヤは、サーチ ヘッド クラスタ メンバーが 「ホームに電話」するときに構成を配布するだけではありません。これにより、構成の不一致や遅延が発生する可能性があります。
デプロイヤーは、構成が有効な構成となるようにサーチ ヘッド クラスター メンバーに構成を配布しません。これは、構成がデプロイヤなしでは無効であることを意味します。デプロイヤは、splunk apply shcluster-bundle を使用して検索ヘッド クラスター メンバーに設定を配布するだけではありません。これは、管理者による手動介入が必要となるためです。詳細については、Splunk ドキュメントの 「デプロイヤを使用してアプリと設定の更新を配布する」を参照してください。

最新問題**: 62**
関係者は、検索可能なデータの高可用性を最優先事項として認識しています。次のうちどれ
この要件に最もよく対処できるでしょうか?
A. クラスター内の検索係数を増やします。
B. クラスター内のレプリケーション係数を増やします。
C. クラスター内のサーチヘッドの数を増やします。
D. クラスター内のインデクサーの CPU の数を増やします。
Answer: B (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture

最新問題**: 63**
顧客は、異なる DNS 名を使用して、500 台のユニバーサル フォワーダーを古い展開サーバーから新しい展開サーバーに移行しています。新しい展開サーバーが構成され、実行されています。
古いデプロイメントサーバーは、更新されたdeploymentclient.confファイルを含むアプリをすべてのフォワーダーにデプロイし、新しいデプロイメントサーバーを指すようにしました。アプリは 500 のフォワーダーすべてに正常にデプロイされました。
すべてのフォワーダーが依然として古い展開サーバーに電話をかけているのはなぜですか?
A. フォワーダーと新しい展開サーバーの間にバージョンの不一致があります。
B. 新しい展開サーバーはフォワーダーからの接続を受け入れていません。
C. フォワーダーは、$SPLUNK_HOME/etc/system/local にある古いデプロイメントサーバーを使用するように設定されています。

D. pass4SymmKey は、新しい展開サーバーとフォワーダーで同じです。
Answer: C (メーッセージを残す**)**
フォワーダーは $SPLUNK_HOME/etc/system/local にある古いデプロイメント サーバーを使用するように設定されているため、すべてのフォワーダーは依然として古いデプロイメント サーバーに電話をかけ続けます。これは、デフォルト設定をオーバーライドする設定が含まれるローカル構成ディレクトリです。
$SPLUNK_HOME/etc/system/default。ローカル ディレクトリ内のdeploymentclient.conf ファイルは、フォワーダーが構成の更新とアプリのために接続するデプロイメント サーバーの targetUri を指定します。フォワーダーがローカル ディレクトリに古いデプロイメント サーバーの targetUri を持っている場合、ローカル設定はデプロイされた設定よりも優先されるため、フォワーダーは古いデプロイメント サーバーによってデプロイされた更新されたdeploymentclient.conf ファイルを無視します。この問題を解決するには、フォワーダーはローカル ディレクトリからdeploymentclient.conf ファイルを削除するか、新しいデプロイメント サーバーの targetUri でファイルを更新する必要があります。
選択肢 C が正解です。オプション A は不正解です。フォワーダーと新しいデプロイメント サーバーのバージョンが一致しない場合でも、バージョンに互換性がある限り、フォワーダーが新しいデプロイメント サーバーに電話をかけることは妨げられません。オプション B は不正解です。新しい展開サーバーが構成されて実行されており、フォワーダーからの接続を受け入れていない兆候はないからです。
pass4SymmKey は展開サーバーとフォワーダーが相互に認証するために使用する共有秘密キーであるため、オプション D は不正解です。両側で同じである限り、新しい展開サーバーに電話をかけるフォワーダーの機能には影響しません12。
1: https://docs.splunk.com/Documentation/Splunk/9.1.2/Updating/Configuredeploymentclients 2: https://docs.splunk.com/Documentation/Splunk/9.1.2/Admin/設定ファイルの場所

最新問題**: 64**
インデックス バケット内の次のファイル タイプのうち、最もディスクを消費する可能性があるのはどのファイル タイプですか?
A. 生データ
B. ブルームフィルター
C. メタデータ (.data)
D. 逆インデックス (.tsidx)
Answer: B (メーッセージを残す**)**

最新問題**: 65**
制限、conf の次のオプションのうち、転送層でパフォーマンス上の利点を提供できるものはどれですか?
A. Indexed_realtime_use_by_default 属性を有効にします。
B. maxKBps 属性を増やします。
C. ParallelngestionPipelines 属性を増やします。
D. max_searches per_cpu 属性を増やします。
Answer: (解答を表示する**)**
正解は C です。ParallelngestionPipelines 属性を増やします。これは、フォワーダーが複数のデータ入力を並行して処理できるようにするため、フォワーディング層でパフォーマンス上の利点を提供する可能性があ

る、limits.conf のオプションです1。ParallelIngestionPipelines 属性は、フォワーダーがさまざまなソースからデータを取り込むために使用できるパイプラインの数を指定します1。この値を増やすことで、フォワーダーはスループットを向上させ、データ配信の遅延を短縮できます1。他のオプションは、転送層でパフォーマンス上の利点を提供する効果的なオプションではありません。オプション A (indexed_realtime_use_by_default 属性を有効にする) は、フォワーダーがデータを受信するとすぐにインデクサーにデータを送信できるようにするため、推奨されません。これにより、ネットワークと CPU の負荷が増加し、パフォーマンスが低下する可能性があります2。オプション B の maxKBps 属性を増やすことは、フォワーダーがインデクサー 3 にデータを送信するために使用できる最大帯域幅 (キロバイト/秒) を増やすため、適切なオプションではありません。これにより、データ転送速度が向上する可能性がありますが、ネットワークが飽和状態になり、輻輳やパケット損失が発生する可能性もあります3。オプション D の max_searches_per_cpu 属性を増やすことは、インデクサーまたは検索ヘッドの検索パフォーマンスにのみ影響し、フォワーダー 4 の転送パフォーマンスには影響しないため、関係ありません。したがって、選択肢 C が正解で、選択肢 A、B、D は不正解となります。
1: 並列取り込みパイプラインを構成する 2: リアルタイム転送を構成する 3: フォワーダー出力を構成する 4: 検索パフォーマンスを構成する

最新問題**: 66**
高速ソースでインデクサーへの転送遅延が発生しないようにするには何が必要ですか?
A. サーバー conf の sessionTimeout のデフォルト値を増やします。
B. limits.conf の maxKBps のデフォルト制限を増やします。
C. 出力の ForceTimebasedAutoLB の値を減らします。会議
D. deploymentclient .conf 内のphoneHomeIntervallInSecs のデフォルト値を減らします。
Answer: (解答を表示する**)**
高速ソースでインデクサーへの転送遅延が発生しないようにするには、limits.conf の maxKBps のデフォルト制限を増やす必要があります。このパラメータは、フォワーダーがインデクサーにデータを送信するために使用できる最大帯域幅を制御します。デフォルトでは 256 KBps に設定されていますが、大容量のデータ ソースには不十分な場合があります。この制限を増やすと、転送遅延が短縮され、フォワーダーのパフォーマンスが向上します。ただし、これはネットワーク帯域幅とインデクサーの負荷に影響を与える可能性があるため、注意して行う必要があります。選択肢 B が正解です。オプション A は不正解です。server.conf の sessionTimeout パラメータは、帯域幅制限ではなく、フォワーダーとインデクサー間の TCP 接続の継続時間を制御するためです。オプション C は不正解です。outputs.conf の ForceTimebasedAutoLB パラメーターは、帯域幅制限ではなく、インデクサー間の負荷分散の頻度を制御するためです。オプション D は不正解です。帯域幅制限ではなく、deploymentclient.conf の phoneHomeIntervallInSecs パラメータがフォワーダがデプロイメント サーバーに接続する間隔を制御するためです12。
1: https://docs.splunk.com/Documentation/Splunk/9.1.2/Admin/Limitsconf#limits.conf.spec 2: https://docs.splunk.com/Documentation/Splunk/9.1.2/Forwarding/Routeandfilterdatad#Set_the_maximum_bandw

最新問題**: 67**
インデクサー クラスターのナレッジ バンドルについて正しいのは次のうちどれですか?
A. app-name/local のみがプッシュされます。

B. app-name/default と app-name/local はプッシュする前にマージされます。
C. app-name/default のみがプッシュされます。
D. app-name/default および app-name/local は変更せずにプッシュされます。
Answer: B (メーッセージを残す**)**
Splunk のドキュメント 1 によると、インデクサー クラスター ナレッジ バンドルは、クラスター マスターがクラスター設定バンドルの一部としてピア ノードに配布する設定ファイルです。ナレッジ バンドルには、データのインデックス付けと検索に関連するイベント タイプ、タグ、ルックアップなどのナレッジ オブジェクトが含まれています。クラスター マスターは、マスター ノード上に存在するアプリの app-name/default ディレクトリと app-name/local ディレクトリをマージすることにより、ナレッジ バンドルを作成します。次に、クラスター マスターはナレッジ バンドルをピア ノードにプッシュします。ナレッジ バンドルはピア ノードの下に存在します。$SPLUNK_HOME/var/run ディレクトリ 2. 他のオプションは次の理由から false です。
※アプリ名/ローカルのみプッシュされます。これは false です。クラスター マスターは、app-name/default ディレクトリと app-name/local ディレクトリの両方をマージした後、ピア ノードにプッシュするからです。app-name/local ディレクトリにはアプリ構成のローカル カスタマイズが含まれ、app-name/default ディレクトリにはデフォルトのアプリ構成が含まれます3。
※アプリ名/デフォルトのみプッシュされます。これは false です。クラスター マスターは、app-name/default ディレクトリと app-name/local ディレクトリの両方をマージした後、ピアノードにプッシュするからです。app-name/default ディレクトリにはデフォルトのアプリ構成が含まれ、app-name/local ディレクトリにはアプリ構成のローカル カスタマイズが含まれます3。
※ app-name/default と app-name/local はそのままプッシュされます。これは false です。クラスターが
* マスターは、ピアノードにプッシュする前に、app-name/default ディレクトリと app-name/local ディレクトリをマージします。これにより、ピア ノードにアプリの最新かつ一貫した構成が確実に適用されます3。

最新問題**: 68**
監視コンソールの検索ダッシュボードは、分散展開がその容量に近づいていることを示しています。次のオプションのうち、検索パフォーマンスを最も向上させるのはどれですか?
A. インデクサー ストレージをソリッド ステート ドライブ (SSD) に置き換えます。
B. 検索ヘッドをさらに追加し、検索タイプに基づいてユーザーを再分配します。
C. 遅い検索を探し、オフピーク時に実行されるようにスケジュールを変更します。
D. 検索ピアをさらに追加し、フォワーダーがすべてのインデクサーにデータを均等に分散するようにします。
Answer: D (メーッセージを残す**)**
検索ピアをさらに追加し、フォワーダーがすべてのインデクサーにデータを均等に分散するようにすると、分散展開のキャパシティに近づいたときに検索パフォーマンスが最大限に向上します。
検索ピアをさらに追加すると、検索の同時実行性が向上し、各インデクサーの負荷が軽減されます。
すべてのインデクサーにデータを均等に分散すると、検索ワークロードのバランスが確保され、ボトルネックになるインデクサーがなくなります。インデクサー ストレージを SSD に交換すると検索パフォーマンスが向上しますが、コストと時間がかかるオプションです。インデクサーがボトルネックになっている場合、検索ヘッドを追加しても検索パフォーマンスは向上しません。低速検索をオフピーク時に実行するようにスケジュールを変更すると、検索の競合は軽減されますが、個々の検索の検索パフォーマンスは向上しません。詳細については、Splunk ド

キュメントの 「インデクサー クラスターのスケール」および 「インデクサー全体にデータを分散する」を参照してください。

最新問題: **69**
関係者は、検索可能なデータの高可用性を最優先事項として認識しています。この要件に最もよく対応するのは次のうちどれですか?
A. クラスター内の検索係数を増やします。
B. クラスター内のレプリケーション係数を増やします。
C. クラスター内のサーチヘッドの数を増やします。
D. クラスター内のインデクサーの CPU の数を増やします。
Answer: A (メーッセージを残す**)**
説明
https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture

最新問題: **70**
検索へのリンクを受け取ったユーザーがリンクを開いたときに、「不明な sid」エラー メッセージが表示されます。なぜこうなった?
A. ユーザーには十分な権限がありません。
B. アドオンを更新する必要があります。
C. 検索ジョブの有効期限が切れました。
D. 1 つ以上のインデクサーが停止しています。
Answer: (解答を表示する**)**
Splunk のドキュメント1 によると、「Unknown sid」エラー メッセージは、リンクに関連付けられた検索ジョブの有効期限が切れたか、削除されたことを意味します。sid (検索 ID) は、検索ジョブごとに一意の識別子であり、検索結果を取得するために使用されます。SID が見つからない場合、検索は表示できません。
他のオプションは次の理由から false です。
* ユーザーの権限が不十分な場合は、「このページを表示する権限がありません」または 「この検索を実行する権限がありません」など、別のエラー メッセージが表示されます1。
* 更新が必要なアドオンは、検索が無効またはアクセス不能になるような方法で検索構文またはデータ ソースを変更しない限り、SID の有効性には影響しません1。
* SID はインデクサーではなくサーチヘッドに保存されるため、1 つ以上のインデクサーが停止しても 「不明な SID」エラーは発生しません。ただし、「ピアに配布できません」や 「検索ピアに次のメッセージが表示されます: ディスク容量が不足しています」など、他のエラーが発生する可能性があります1。

最新問題: **71**
3 ノードのサーチ ヘッド クラスターが、時間の経過とともに多数の検索をスキップしています。サーチヘッドクラスター上のスケジュールされた検索容量を増やすにはどうすればよいですか?
A. クラスター上にジョブ サーバーを作成します。
B. max_searches_per_cpu のlimits.conf 値をより高い値に変更します。

C. server.confcaptain_is_adhoc_searchhead = true。
D. 別の検索ヘッドをクラスターに追加します。
Answer: (解答を表示する**)**

最新問題**: 72**
サーチ ヘッド クラスター (SHC) のメンバーを追加または削除する場合、適切な操作順序は何ですか?
A. 1. レプリケーションをトリガーします。
2. クラスターからマスターノードを削除します。
3. クラスターのリバランス操作を初期化します。
B. 1. Splunk Enterprise が存在する場合は削除します。
2. インスタンスをインストールして初期化します。
3. SHC に参加します。
C. 1. クラスターのリバランス操作を初期化します。
2. クラスターからマスターノードを削除します。
3. レプリケーションをトリガーします。
D. 1. インスタンスをインストールして初期化します。
2. Splunk Enterprise が存在する場合は削除します。
3. SHC に参加します。
Answer: D (メーッセージを残す**)**

最新問題**: 73**
ライセンス関連のイベントを含む Splunk 内部インデックスはどれですか?
A. _内部
B. _監査
C. _イントロスペクション
D. _ライセンス
Answer: A (メーッセージを残す**)**

最新問題**: 74**
3 ノードのサーチ ヘッド クラスターが、時間の経過とともに多数の検索をスキップしています。サーチヘッドクラスター上のスケジュールされた検索容量を増やすにはどうすればよいですか?
A. クラスター上にジョブ サーバーを作成します。
B. 別の検索ヘッドをクラスターに追加します。
C. server.confcaptain_is_adhoc_searchhead = true。
D. max_searches_per_cpu のlimits.conf 値をより高い値に変更します。
Answer: D (メーッセージを残す**)**
説明
max_searches_per_cpu のlimits.conf の値をより高い値に変更することは、長期間にわたって多数の検索がスキップされる場合に、サーチ ヘッド クラスターでスケジュールされた検索容量を増やすための最良のオプションです。

この値は、サーチ ヘッドの各 CPU コアで同時に実行できるスケジュールされた検索の数を決定します。
この値を増やすと、より多くのスケジュールされた検索を同時に実行できるようになり、スキップされる検索の数が減ります。クラスター上にジョブ サーバーを作成すること、server.confcaptain_is_adhoc_searchhead = true コマンドを実行すること、またはクラスターに別のサーチヘッドを追加することは、サーチヘッド クラスター上でスケジュールされた検索容量を増やすための最良のオプションではありません。詳細については、Splunk ドキュメントの「Configurelimits.conf」を参照してください。

最新問題**: 75**
監視対象のログ ファイルがフォワーダー上で変更されています。ただし、Splunk 検索では、追加された新しいデータが見つかりません。考えられる原因は何ですか? （該当するものをすべて選択）
A. 管理者はインデクサーで splunk cleaneventdata -index <indexname> を実行しました。
B. 管理者がフォワーダー上の Splunk フィッシュバケットを削除しました。
C. 監視対象ファイルの最後の 256 バイトは変更されていません。
D. 監視対象ファイルの最初の 256 バイトは変更されていません。
Answer: B,C (メーッセージを残す**)**
監視対象のログ ファイルがフォワーダー上で変更されていますが、Splunk 検索では追加された新しいデータが見つかりません。これは、次の 2 つの理由が考えられます。
B: 管理者がフォワーダー上の Splunk フィッシュバケットを削除しました。
C: 監視対象ファイルの最後の 256 バイトは変更されていません。選択肢 B は正解です。Splunk フィッシュバケットは、Splunk によって監視されているファイルに関する情報 (ファイル名、サイズ、変更時刻、CRC チェックサムなど) を保存するディレクトリであるからです。管理者がフィッシュバケットを削除すると、Splunk は以前にインデックス付けされたファイルを追跡できなくなり、それらのファイルからの新しいデータのインデックス付けが行われなくなります。選択肢 C は正解です。Splunk は監視対象ファイルの最後の 256 バイトの CRC チェックサムを使用して、ファイルが最後に読み取られてから変更されたかどうかを判断します。ファイルの最後の 256 バイトが変更されていない場合、Splunk はファイルが変更されていないと想定し、そのファイルから新しいデータのインデックスを作成しません。オプション A は不正解です。インデクサーで splunk cleaneventdata -index <indexname> コマンドを実行すると、指定されたインデックスからすべてのデータが削除されますが、新しいデータをインデクサーに送信するフォワーダーの機能には影響しません。Splunk は監視対象ファイルの最初の 256 バイトを使用してファイルが変更されたかどうかを判断しないため、オプション D は不正解です12
1: https://docs.splunk.com/Documentation/Splunk/9.1.2/Data/Monitorfilesanddirectories 2: https://docs.splunk.com/Documentation/Splunk/9.1.2/Troubleshooting/Didyouloseyourfishbucket

最新問題**: 76**
インデックス作成のパフォーマンスを最大化するためのベスト プラクティスは次のうちどれですか?
A. 自動ソース入力を使用します。
B. Splunk のデフォルト設定を使用します。
C. 事前トレーニングされたソースタイプを使用しません。
D. 構成の汎用性を最小限に抑えます。
Answer: (解答を表示する**)**

説明
インデックス作成のパフォーマンスを最大化するためのベスト プラクティスは、構成の汎用性を最小限に抑えることです。構成の汎用性とは、ソース タイプ、ホスト、インデックス、タイムスタンプなどのデータ入力に対する汎用設定またはデフォルト設定の使用を指します。構成の汎用性を最小限に抑えるということは、各データ入力に具体的で正確な設定を使用することを意味し、これにより処理のオーバーヘッドが削減され、インデックス作成のスループットが向上します。自動ソース タイピングの使用、Splunk のデフォルト設定の使用、および事前トレーニングされたソース タイプの使用なしは、構成の一般性の例であり、インデックス作成のパフォーマンスに悪影響を与える可能性があります。

最新問題**: 77**
サーチ ヘッド クラスター デプロイヤにとって適切なプラクティスは次のうちどれですか?
A. デプロイヤは、サーチ ヘッド クラスタ メンバーが ホームに電話する」ときにのみ構成を配布します。
B. デプロイヤーは、複製不可能な構成をサーチ ヘッド クラスター メンバーに配布するために使用する必要があります。
C. デプロイ担当者は、有効な構成となるように、サーチ ヘッド クラスター メンバーに構成を配布する必要があります。
D. デプロイヤーは、splunk apply shcluster-bundle を使用して、サーチヘッドクラスターメンバーに設定を配布するだけです。
Answer: B (メーッセージを残す**)**
以下は、サーチ ヘッド クラスター デプロイヤの推奨事項です。デプロイヤは、複製不可能な構成をサーチ ヘッド クラスタ メンバーに配布するために使用する必要があります。レプリケート不可能な構成とは、アプリや server.conf設定などの検索要素によってレプリケートされない構成です。デプロイヤーは、これらの設定をサーチヘッドクラスターメンバーに配布し、それらが同じ設定であることを保証する Splunk サーバーの役割です。デプロイヤは、サーチ ヘッド クラスタ メンバーが ホームに電話」するときに構成を配布するだけではありません。これにより、構成の不一致や遅延が発生する可能性があります。
デプロイヤーは、構成が有効な構成となるようにサーチ ヘッド クラスター メンバーに構成を配布しません。これは、構成がデプロイヤなしでは無効であることを意味します。デプロイヤは、splunk apply shcluster-bundle を使用して検索ヘッド クラスター メンバーに設定を配布するだけではありません。これは、管理者による手動介入が必要となるためです。詳細については、Splunk ドキュメントの デプロイヤを使用してアプリと設定の更新を配布する」を参照してください。

最新問題: **78**
次のサーバーのどれですか。conf スタンザは、マスター ノード上でインデクサー検出機能が完全に構成されていない (再起動が保留中) ことを示していますか?

A.
```
[indexer_discovery]
pass4SymmKey = $7$XcXl1lu4630Jbui14oVe295+mvx6gCKKv6kf2zEaVB6Ie4DcZ318nLVlfW
```

B.
```
[clustering]
mode = forwarder
pass4SymmKey = $7$PU9SBXww63Vz3UJdDYGIN0UrdscRh83ssC2pEpwE6P3gn50iNFO94g==
```

C.
```
[clustering]
mode = master
pass4SymmKey = $7$tYTXzke+1r+3DULTHHDUTmYOXdtZJPxm21XwMARrJE20jsmicp9C3ni0
```

D.
```
[indexer_discovery]
pass4SymmKey = idxdiscovery
```

Answer: A (メーッセージを残す**)**
インデクサー検出機能を使用すると、フォワーダーはインデクサー クラスター内の使用可能なピア ノードに動的に接続できます。この機能を使用するには、マネージャー ノードを [indexer_discovery] スタンザと pass4SymmKey 値で構成する必要があります。フォワーダーも、同じ pass4SymmKey 値とマネージャー ノードの master_uri を使用して構成する必要があります。pass4SymmKey 値は、splunk _encrypt コマンドを使用して暗号化する必要があります。したがって、オプション A は、pass4SymmKey 値が暗号化されていないため、インデクサー検出機能がマネージャー ノード上で完全には構成されていないことを示します。他のオプションは、インデクサー検出機能に関連しません。オプション B は、インデクサー クラスターの一部であるフォワーダーの構成を示します。
オプション C は、インデクサー クラスターの一部であるマネージャー ノードの構成を示しています。オプション D は、pass4SymmKey 値が暗号化されておらず、フォワーダーの pass4SymmKey 値と一致しないため、[indexer_discovery] スタンザの無効な構成を示しています12
1: https://docs.splunk.com/Documentation/Splunk/9.1.2/Indexer/indexerdiscovery 2: https://docs.splunk.com/Documentation/Splunk/9.1.2/Security/Secureyourconfigurationfiles#Encrypt_the_pass4S

最新問題: **79**
サーチヘッド クラスタにおけるキャプテンの作業負荷を軽減するには、スケジュールされたサーチが実行されないようにする設定は次のとおりです。
船長を追いかける？
A. adhoc_searchhead = true (すべてのメンバー上)
B. adhoc_searchhead = true(現在のキャプテン上)
C. captain_is_adhoc_searchhead = true(すべてのメンバーに対して)
D. captain_is_adhoc_searchhead = true(現在のキャプテンに対して)
Answer: (解答を表示する**)**

説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Adhocclustermember

最新問題**: 80**
Splunk Enterprise プラットフォームのインストルメンテーションは、Splunk Enterprise 導入環境がログに記録するデータを指します。
_イントロスペクションインデックス。このインデックスに含まれるログは次のうちどれですか? （該当するものをすべて選択。）
A. 監査ログ
B. metrics.log
C. ディスクオブジェクト.ログ
D. resource_usage.log
Answer: C,D (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.1/Troubleshooting/ プラットフォーム計測フレームワークについて

最新問題**: 81**
Splunk Enterprise データ パイプラインのどのフェーズでインデックス付き抽出設定が処理されますか?
A. 入力
B. 検索
C. 解析中
D. インデックス作成
Answer: C (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/ 構成パラメータとデータパイプライン

最新問題**: 82**
既存の Splunk 環境では、毎日作成される新しいインデックス バケットのサイズは、受信データの約半分です。各バケット内では、スペースの約 30% が生データに使用され、約 70% がインデックス ファイルに使用されます。インデクサー クラスタリングが実装されている場合、インデクサーごとの毎日のディスク消費量を計算するにはどのような追加情報が必要ですか?
A. 1 日あたりの合計インデックス作成量、複製係数、検索係数、および検索ヘッドの数。
B. レプリケーション係数、検索係数、高速化された検索の数、およびクラスター全体の合計ディスク サイズ。
C. 日次インデックス作成量の合計、ピア ノードの数、レプリケーション ファクター、および検索ファクター。
D. 日次のインデックス作成量の合計、ピア ノードの数、および高速化された検索の数。
Answer: B (メーッセージを残す**)**

最新問題**: 83**
serverclass.conf で使用できるクライアント フィルターは次のうちどれですか? （該当するものをすべて選択。）
A. DNS 名。
B. IP アドレス。
C. Splunk サーバーの役割。

D. プラットフォーム (マシンタイプ)。
Answer: A,B (メーッセージを残す**)**
説明/参照:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Filterclients#Define_filters_through_serverclass.conf

最新問題**: 84**
マルチサイト インデクサー クラスターですべてのサーチ ヘッド クラスター メンバーに site=site0 を設定するとどうなりますか?
A. 検索サイト アフィニティを無効にします。
B. すべてのメンバーを動的キャプテンに設定します。
C. マルチサイト検索アーティファクトのレプリケーションを有効にします。
D. 自動検索サイト アフィニティ検出を有効にします。
Answer: (解答を表示する**)**
説明
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/DeploymultisiteSHC

最新問題**: 85**
Search Job Inspector を使用して調査できる問題は次のうちどれですか?
A. Splunk Web の検索バーの下にエラー メッセージが表示されます。
B. ページの読み込み時にダッシュボード パネルに 㐀キューに入れられたジョブの開始を待機しています」と表示されます。
C. 異なるユーザーには、同じ検索から抽出された異なるフィールドが表示されます。
D. イベントは新しい順に並べ替えられていません。
Answer: A (メーッセージを残す**)**
Splunk のドキュメント 1 によると、Search Job Inspector は、検索パフォーマンスのトラブルシューティングと、検索内のイベント タイプ、タグ、ルックアップなどのナレッジ オブジェクトの動作を理解するために使用できるツールです。現在実行中の検索ジョブ、または最近終了した検索ジョブを検査できます。
検索ジョブ インスペクターは、検索文字列、検索モード、検索タイムライン、検索ログなどの検索ジョブの詳細を表示できるため、Splunk Web の検索バーの下に表示されるエラー メッセージを調査するのに役立ちます。検索プロファイルと検索プロパティ。この情報を使用してエラーの原因を特定し、修正できます2。他のオプションは次の理由から false です。
* ページ読み込み時に 㐀キューに入れられたジョブの開始を待機しています」と表示されるダッシュボード パネルは、検索ジョブがまだ開始されていないことを示すため、検索ジョブ インスペクターを使用して調査できる問題ではありません。これ
* 検索スケジューラがビジー状態であるか、検索の優先順位が低いことが原因である可能性があります。[ジョブ] ページまたは監視コンソールを使用して、検索ジョブのステータスを監視し、必要に応じて優先順位または同時実行設定を調整できます3。
* 同じ検索から異なる抽出フィールドが異なるユーザーに表示されることは、ユーザーの権限とナレッジ オブジェクトの共有設定に関連しているため、検索ジョブ インスペクターを使用して調査できる問題ではありませ

ん。[アクセス制御] ページまたはナレッジ マネージャーを使用して、ユーザーの役割とナレッジ オブジェクトの可視性を管理できます4。
* イベントが新しい順に並べ替えられていない場合は、検索構文と並べ替えコマンドに関連するため、検索ジョブ インスペクターを使用して調査できる問題ではありません。 検索マニュアル」または 検索リファレンス」を使用すると、sort コマンドとそのオプションを使用して、フィールドまたは基準によってイベントを並べ替える方法を学習できます。

最新問題**: 86**
Enterprise Security をサーチ ヘッド クラスターにインストールする場合、次のどれを実行する必要がありますか? （該当するものをすべて選択。）
A. Enterprise Security をデプロイヤーにインストールします。
B. Enterprise Security をステージング インスタンスにインストールします。
C. Enterprise Security 構成をデプロイヤーにコピーします。
D. デプロイヤを使用して、Enterprise Security をクラスタ メンバーにデプロイします。
Answer: A,D (メーッセージを残す**)**
説明
Enterprise Security をサーチ ヘッド クラスター (SHC) にインストールする場合は、次の手順を実行する必要があります。
Enterprise Security をデプロイヤーにインストールし、デプロイヤーを使用して Enterprise Security をクラスターメンバーにデプロイします。Enterprise Security は、Splunk のセキュリティ分析と監視機能を提供するプレミアム アプリです。Enterprise Security は、アプリやその他の構成を SHC メンバーに配布するスタンドアロン インスタンスであるデプロイヤーを使用して SHC にインストールできます。Enterprise Security は、まずデプロイヤーにインストールしてから、splunk apply shcluster-bundle コマンドを使用してクラスターメンバーにデプロイする必要があります。ステージング インスタンスは SHC 導入プロセスの一部ではないため、Enterprise Security をステージング インスタンスにインストールしないでください。Enterprise Security 構成は、Enterprise Security アプリ パッケージに既に含まれているため、デプロイヤにコピーしないでください。

最新問題**: 87**
モニター入力のトラブルシューティングを行う場合、末尾のファイルのステータスをチェックするコマンドはどれですか?
A. splunk cmd btool 入力リスト | しっぽ
B. splunk cmd btool チェック入力レイヤー
C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus
D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus
Answer: (解答を表示する**)**
curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus コマンドは、モニター入力のトラブルシューティング時に末尾ファイルのステータスを確認するために使用されます。モニター入力は、ファイルまたはディレクトリーで新しいデータを監視し、そのデータをインデックス作成のために Splunk に送信する入力です。TailingProcessor:FileStatus エンドポイントは、ファイル名、パス、サイズ、位置、ステータスなど、テーリン

グ プロセッサによって監視されているファイルに関する情報を返します。Splunk cmd btool 入力リスト | tail コマンドは、inputs.conf ファイルからの入力構成をリストし、出力を tail コマンドにパイプするために使用されます。splunk cmd btool check inputslayer コマンドは、入力構成の構文エラーと階層化をチェックするために使用されます。カール https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus コマンドは存在せず、有効なエンドポイントではありません。

最新問題: **88**
サーチ ヘッド クラスター (SHC) のメンバーを追加または削除する場合、適切な操作順序は何ですか?
A. 1. レプリケーションをトリガーします。2. クラスターからマスターノードを削除します。3. クラスターのリバランス操作を初期化します。
B. 1. クラスターのリバランス操作を初期化します。2. クラスターからマスターノードを削除します。3. レプリケーションをトリガーします。
C. 1. Splunk Enterprise が存在する場合は削除します。2. インスタンスをインストールして初期化します。3. SHC に参加してください。
D. 1. インスタンスをインストールして初期化します。2. Splunk Enterprise が存在する場合は削除します。3. SHC に参加してください。
Answer: (解答を表示する**)**

最新問題: **89**
次のインデックスのうち、どのインデックスのデータが取り込みベースのライセンスに対してカウントされますか?
A. 概要
B. メイン
C. _metrics
D. _イントロスペクション
Answer: B (メーッセージを残す**)**
Splunk Enterprise ライセンスは、Splunk プラットフォームによって 1 日に取り込まれインデックス付けされるデータの量に基づいています1。ライセンスの対象となるデータは、ユーザーに表示され、Splunk ソフトウェアで検索可能なインデックスに保存されているデータです2。デフォルトで表示および検索可能なインデックスは、メイン インデックスと、ユーザーまたはアプリによって作成されたカスタム インデックスです3。メインインデックスは、特に指定がない限り、Splunk Enterprise がすべてのデータを保存するデフォルトのインデックスです4。オプション B は正解です。メイン インデックスのデータは、デフォルトで表示および検索可能なインデックスであるため、取り込みベースのライセンスに対してカウントされます。オプション A は不正解です。サマリー インデックスは、スケジュールされたレポートや高速化されたデータ モデルの結果を保存する特別なタイプのインデックスであり、ライセンスにはカウントされません。オプション C は不正解です。_metrics インデックスは、Splunk プラットフォームのパフォーマンスに関するメトリクス データを保存する内部インデックスであり、ライセンスにはカウントされません。選択肢 D は不正解です。

_introspection インデックスは、CPU、メモリ、ディスク、ネットワークの使用状況など、ホスト システムに対する Splunk ソフトウェアの影響に関するデータを保存する別の内部インデックスであり、ライセンスにはカウントされません。
参考文献:
1: Splunk Enterprise ライセンスの仕組み - Splunk ドキュメント 2: ライセンスに対してカウントされるデータは何ですか? - Splunk ドキュメント 3: [インデックスとインデクサーについて - Splunk ドキュメント] 4: [メイン インデックス - Splunk ドキュメント] : [サマリー インデックス作成 - Splunk ドキュメント] : [メトリクス インデックスについて - Splunk ドキュメント] : [モニタリング コンソールについて - Splunk ドキュメント] 】

最新問題**: 90**
ユーザーは、Splunk 管理者に対し、最近凍結されたバケットを頻繁に解凍するよう要求しています。Splunk 管理者はバケットを解凍する必要性を減らすために何ができるでしょうか?
A. f rozenTimePeridlnSecs をより大きな値に変更します。
B. maxTotalDataSizeMB をより小さい値に変更します。
C. maxHotSpanSecs をより大きな値に変更します。
D. coldToFrozenDir を別の場所に変更します。
Answer: A (メーッセージを残す**)**
正解は A です。frozenTimePeriodInSecs をより大きな値に変更します。これは、バケットが凍結されてインデックスから削除されるまでの時間が長くなるため、バケットを解凍する必要性を減らすための可能な解決策です 1。FrozenTimePeriodInSecs 属性は、インデックスに含めることができるデータの最大存続期間を秒単位で指定します1。より大きな値に設定すると、Splunk 管理者はデータをインデックスに長期間保存し、バケットを頻繁に解凍する必要がなくなります。他のオプションは、バケットを解凍する必要性を減らす効果的なソリューションではありません。オプション B (maxTotalDataSizeMB をより小さい値に変更する) では、index2 の最大サイズ (メガバイト単位) が減少するため、実際にはバケットを解凍する必要性が増加します。これは、インデックスがより早くサイズ制限に達し、より多くのバケットが凍結および削除されることを意味します。オプション C の maxHotSpanSecs をより大きな値に変更すると、ホット バケットの最大存続期間 (秒単位) が変更されるだけであるため、バケットを解凍する必要性には影響しません3。これは、熱いバケツが長時間熱いままであることを意味しますが、最終的にバケツが凍るのを防ぐことはできません。オプション D の coldToFrozenDir を別の場所に変更しても、凍結されたバケットの宛先ディレクトリが変更されるだけであるため、バケットを解凍する必要性は減りません4。これは、バケットは引き続き凍結され、インデックスから削除されますが、別の場所に保存されることを意味します。したがって、選択肢 A が正解で、選択肢 B、C、D は不正解となります。
1: リタイアおよびアーカイブのポリシーを設定する 2: インデックス サイズを構成する 3: バケットのローテーションと保持 4: インデックス付きデータをアーカイブする

最新問題**: 91**
クラスター化された Splunk 導入におけるライセンスについて説明しているのは次のどれですか? （該当するものをすべて選択。）
A. クラスタ メンバーは同じライセンス プールとライセンス マスターを共有する必要があります。
B. 各クラスタ メンバーには独自のクラスタリング ライセンスが必要です。

C. レプリケートされたデータはライセンスの対象となりません。
D. 無料ライセンスはクラスタリングをサポートしません。
Answer: (解答を表示する**)**

最新問題: **92**
顧客は、1 日あたり 600 GB のデータを Splunk に取り込むことを計画しています。同時ユーザー数は 6 人であり、高いデータ可用性と高い検索パフォーマンスも求めています。お客様はコストを懸念しており、Splunk のハードウェアに最小限の費用をかけたいと考えています。この展開にはいくつのインデクサーが推奨されますか?
A. クラスター内にない 3 つのインデクサー。データ保持期間が長いことを想定しています。
B. 高可用性が最優先であると想定して、2 つのインデクサーがクラスター化されています。
C. クラスター内にない 2 つのインデクサー。ユーザーが長時間の検索を多数実行すると想定されます。
D. 大量の保存/スケジュールされた検索を想定して、2 つのインデクサーがクラスター化されています。
Answer: D (メーッセージを残す**)**

最新問題: **93**
Splunk インデックス作成は読み取り/書き込み集中型であるため、各展開に適切なディスク ストレージ ソリューションを選択することが重要です。ディスク ストレージに関して正確なのは次のどれですか?
A. 高性能 SAN は決して使用しないでください。
B. ホット バケットおよびウォーム バケットを保存するために NFS を有効にします。
C. 推奨される RAID セットアップは RAID 10 (1 + 0) です。
D. Splunk インデクサーには通常、ベアメタルよりも仮想化環境が優先されます。
Answer: (解答を表示する**)**
Splunk のインデックス作成には、さまざまなソースからのデータの読み取り、ディスクへのデータの書き込み、検索とレポートのためのディスクからのデータの読み取りが含まれるため、読み取り/書き込みが集中します。したがって、パフォーマンス、信頼性、コストの要件に基づいて、各展開に適切なディスク ストレージ ソリューションを選択することが重要です。Splunk インデクサーに推奨される RAID セットアップは、パフォーマンスと信頼性の最適なバランスを提供する RAID 10 (1 + 0) です。RAID 10 は、RAID 1 (ミラーリング) と RAID 0 (ストライピング) の利点を組み合わせたもので、データの冗長性とデータ分散の両方を提供します。RAID 10 は、同じミラーリングされたペアにない限り、複数のディスク障害に耐えることができ、複数のディスクに並行してアクセスできるため、読み取りおよび書き込み速度を向上させることができます2。高性能 SAN (ストレージ エリア ネットワーク) は、Splunk インデクサーですが、ローカル ディスクよりも高価で複雑なため、お勧めできません。また、SAN では追加のネットワーク遅延と依存関係が発生し、Splunk インデクサーのパフォーマンスと可用性に影響を与え

る可能性があります。SAN は、読み取り/書き込み負荷が低く、CPU 負荷が高いため、Splunk サーチヘッドに適しています。2 NFS (ネットワーク ファイル システム) は、データ破損、データ損失、およびパフォーマンスを引き起こす可能性があるため、ホット バケットおよびウォーム バケットの保存には使用しないでください。劣化。NFS は、複数のクライアントがリモート サーバー上の同じファイルにアクセスできるようにするネットワーク ベースのファイル システムです。NFS は、Splunk インスタンス間で競合や不整合が発生する可能性があるため、Splunk インデックス レプリケーションおよびサーチ ヘッド クラスタリングと互換性がありません。また、NFS はネットワーク帯域幅と可用性に依存するため、ローカル ディスクよりも遅く、信頼性も低くなります。NFS は、アクセス頻度が低く、Splunk 操作にとって重要性が低いため、コールド バケットおよびフリーズ バケットの保存に使用できます2。仮想化環境は、追加のオーバーヘッドと複雑性が生じる可能性があるため、Splunk インデクサーには通常、ベア メタルよりも好まれません。仮想化環境は、物理リソースやネットワークを他の仮想マシンと共有するため、Splunk インデクサーのパフォーマンスと信頼性に影響を与える可能性があります。仮想化環境では、抽象化と構成のレイヤーが追加されるため、Splunk インデクサーの監視とトラブルシューティングが複雑になる場合もあります。仮想化環境は Splunk インデクサーに使用できますが、最適なパフォーマンスと可用性を確保するには、慎重な計画と調整が必要です2

最新問題**: 94**
インデクサー クラスター内のインデックスのレプリケーションをアクティブにするには、すべてのピアノードの Indexes.conf でどの属性を構成する必要がありますか?
A. repFactor = 0
B. 複製 = 0
C. repFactor = 自動
D. レプリケート = 自動
Answer: C (メーッセージを残す**)**
説明
インデクサー クラスター内のインデックスのレプリケーションをアクティブにするには、すべてのピアノードの Indexes.conf で repFactor 属性を構成する必要があります。この属性は、インデックスのレプリケーション係数を指定します。これにより、クラスターによって維持される生データのコピーの数が決まります。repFactor 属性を auto に設定すると、インデックスのレプリケーションが有効になります。Indexes.conf の replicate 属性は有効な Splunk 属性ではありません。Outputs.conf の repFactor 属性とdeploymentclient.conf のreplicate 属性は、インデクサー クラスター内のインデックスのレプリケーションに関連しません。詳細については、Splunk ドキュメントの「インデクサー クラスターのインデックスの構成」を参照してください。

最新問題**: 95**
Splunk が syslog データのサイズを見積もるために提供するガイダンスは、元のデータ サイズの 50% です。これにより、インデックス内のファイルがどのように分割されるのでしょうか?
A. rawdata は: 10%、tsidx は: 40%
B. rawdata は: 15%、tsidx は: 35%
C. rawdata は: 35%、tsidx は: 15%
D. rawdata は: 40%、tsidx は: 10%

Answer: (解答を表示する**)**
説明/参照: https://answers.splunk.com/answers/147951/what-is-the-compression-ratio-of-raw-data-in-splunk.html

最新問題**: 96**
インデクサー クラスター内で動作しているピア ノードを永続的に廃止するコマンドはどれですか?
A. スプランク停止 -f
B. splunk オフライン -f
C. splunk オフライン --enforce-counts
D. splunk のデコミッション -- カウントを強制する
Answer: (解答を表示する**)**
説明
splunk offline --enforce-counts コマンドは、インデクサー クラスター内で動作しているピア ノードを永続的に廃止します。このコマンドは、ピアノードをクラスターから削除し、そのデータを削除します。このコマンドは、ピアノードが不要になった場合、または別のノードに置き換えられる場合に使用する必要があります。スプランクストップ
-f コマンドはピアノード上の Splunk サービスを停止しますが、クラスターからサービスを停止しません。
splunk offline -f コマンドはピアノードをオフラインにしますが、データを削除したり、レプリケーションや検索要素を強制したりすることはありません。splunk decommission --enforce-counts コマンドは有効な Splunk コマンドではありません。詳細については、Splunk ドキュメントの 「インデクサー クラスターからピア ノードを削除する」を参照してください。

最新問題**: 97**
顧客は、1 日あたり 600 GB のデータを Splunk に取り込むことを計画しています。同時ユーザー数は 6 人であり、高いデータ可用性と高い検索パフォーマンスも求めています。お客様はコストを懸念しており、Splunk のハードウェアに最小限の費用をかけたいと考えています。この展開にはいくつのインデクサーが推奨されますか?
A. クラスター内にない 2 つのインデクサー。ユーザーが長時間の検索を多数実行すると想定されます。
B. クラスター内にない 3 つのインデクサー。データ保持期間が長いことを想定しています。
C. 高可用性が最優先であると想定して、2 つのインデクサーがクラスター化されています。
D. 大量の保存/スケジュールされた検索を想定して、2 つのインデクサーがクラスター化されています。
Answer: C (メーッセージを残す**)**
説明
https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Distsearchsystemrequirements

最新問題**: 98**
Splunk ジョブとは何ですか? （該当するものをすべて選択。）
A. ユーザー定義の Splunk 機能。
B. 使用量クォータの対象となる検索。
C. レポートまたはアラートによって開始された検索プロセス。
D. splunkd プロセスから明示された子 OS プロセス。
Answer: B,C,D (メーッセージを残す**)**

説明
Splunk ジョブは、レポート、アラート、またはユーザー アクションによって開始される検索プロセスです。Splunk ジョブは、メインの Splunk デーモンである splunkd プロセスから明示される子 OS プロセスです。Splunk ジョブには、メモリ、CPU、ディスク容量などの使用量クォータが適用されます。これらのクォータは、limits.conf ファイルで設定できます。Splunk ジョブは、Splunk プラットフォームの中核機能であるため、ユーザー定義の Splunk 機能ではありません。

最新問題: **99**
Splunk インデクサー クラスターを構成する場合、レプリケーションと検索要素のデフォルト値は何ですか?
レプリケーション係数 = 2
A. 検索係数 = 2
レプリケーション係数 = 2
B. 検索係数 = 3
レプリケーション係数 = 3
C. 検索係数 = 2
レプリケーション係数 = 3
D. 検索係数 = 3
Answer: C (メーッセージを残す**)**

最新問題: **100**
次のセキュリティ オプションのうち、明示的に構成する必要があるのはどれですか (つまり、デフォルトで有効になっていないオプションはどれですか)?
A. Splunk Web と splunkd 間のデータ暗号化。
B. フォワーダーとインデクサー間の証明書認証。
C. Splunk Web とサーチヘッド間の証明書認証。
D. 検索ヘッドとインデクサー間の分散検索のためのデータ暗号化。
Answer: B (メーッセージを残す**)**
次のセキュリティ オプションはデフォルトでは有効になっていないため、明示的に構成する必要があります。
* フォワーダーとインデクサー間の証明書認証。このオプションを使用すると、フォワーダーとインデクサーが SSL 証明書を使用して互いの ID を検証できるため、不正なデータ送信やスプーフィング攻撃が防止されます。このオプションは、管理者がフォワーダーとインデクサーの証明書を生成して配布する必要があるため、デフォルトでは有効になっていません。詳細については、「を参照してください。
Splunk ドキュメントの [フォワーダーとインデクサー間の通信を保護する]。次のセキュリティ オプションがデフォルトで有効になっています。
* Splunk Web と splunkd 間のデータ暗号化。このオプションは、SSL を使用して Splunk Web インターフェイスと splunkd デーモン間の通信を暗号化し、データの傍受や改ざんを防ぎます。Splunk はこの目的のために自己署名証明書を提供するため、このオプションはデフォルトで有効になっています。詳細については、Splunk ドキュメントの SSL による Splunk Enterprise の保護について」を参照してください。

* Splunk Web とサーチヘッド間の証明書認証。このオプションを使用すると、Splunk Web インターフェイスとサーチヘッドが SSL 証明書を使用して互いの ID を検証できるようになり、不正なアクセスやスプーフィング攻撃を防止できます。Splunk はこの目的のために自己署名証明書を提供するため、このオプションはデフォルトで有効になっています。詳細については、Splunk ドキュメントの 「SSL による Splunk Enterprise の保護について」を参照してください。
* サーチヘッドとインデクサー間の分散検索のためのデータ暗号化。このオプションは、SSL を使用して検索ヘッドとインデクサー間の通信を暗号化し、データの傍受や改ざんを防ぎます。Splunk はこの目的のために自己署名証明書を提供するため、このオプションはデフォルトで有効になっています。詳細については、Splunk ドキュメントの 「分散検索環境の保護」を参照してください。

最新問題**: 101**
KV ストアの復元力を最も向上させるのは次のうちどれですか?
A. 検索ヘッド間の待ち時間を短縮します。
B. アーティファクトのレプリケーションを改善するために、検索ヘッドに高速ストレージを追加します。
C. インデクサーの CPU とメモリを追加して、検索遅延を短縮します。
D. 操作ログのサイズを増やします。
Answer: (解答を表示する**)**
* KV ストアは、アプリがアプリのコンテキスト内でデータを保存および取得できるようにする Splunk Enterprise の機能です1。
* KV ストアはサーチ ヘッド上に常駐し、サーチ ヘッド クラスタのメンバー間でデータを複製します1。
* KV ストアの復元力とは、障害や中断が発生した場合にデータの可用性と一貫性を維持する KV ストアの能力を指します2。
* KV ストアの復元力に影響を与える要因の 1 つは、検索ヘッド間のネットワーク遅延であり、データ レプリケーションの速度と信頼性に影響を与える可能性があります2。
* サーチヘッド間のレイテンシを短縮すると、データ損失、不整合、または破損の可能性が減り、KV ストアの回復力が向上します2。
* 他のオプションは、KV ストアの復元性に直接関係しません。より高速なストレージ、インデクサーの CPU とメモリ、操作ログのサイズは、Splunk のパフォーマンスの他の側面に影響を与える可能性がありますが、KV Store345 には影響しません。
参考資料: 1: アプリキーバリューストアについて 2: Splunk Enterprise を使用した KV ストアの設定とデプロイ 3: Splunk での KV ストアの作成と CRUD : パート 1 4: KV ストアのトラブルシューティング ツール 5: 解決済み: Re: KV ストアの無効化

最新問題**: 102**
ライセンス関連のイベントを含む Splunk 内部インデックスはどれですか?
A. _監査
B. _ライセンス
C. _内部
D. _イントロスペクション

Answer: C (メーッセージを残す)
説明
_internal インデックスには、ライセンスの使用状況、ライセンス クォータ、ライセンス プール、ライセンス スタック、ライセンス違反などのライセンス関連のイベントが含まれています。これらのイベントは、ライセンス マネージャーによって、_internal インデックスの一部であるlicense_usage.log ファイルに記録されます。_audit インデックスには、ユーザー アクション、構成変更、検索アクティビティなどの監査イベントが含まれます。これらのイベントは、_audit インデックスの一部である Audit.log ファイルの監査証跡によって記録されます。ライセンス関連のイベントは _internal インデックスに保存されるため、_license インデックスは Splunk には存在しません。_introspection インデックスには、リソースの使用状況、ディスク オブジェクト、検索アクティビティ、データの取り込みなどのプラットフォーム インストルメンテーション データが含まれています。これらのデータは、イントロスペクション ジェネレーターによって、_introspection インデックスの一部である resource_usage.log、disk_objects.log、search_activity.log、data_ingestion.log などのさまざまなログ ファイルに記録されます。詳細については、Splunk ドキュメントの 「Splunk Enterprise ログについて」および 「internal インデックスについて」を参照してください。

最新問題**: 103**
Splunk インデクサーの最小参照サーバー仕様は何ですか?
A. 28 CPU コア、32GB RAM、1200 IOPS
B. 24 CPU コア、16GB RAM、1200 IOPS
C. 12 CPU コア、12GB RAM、800 IOPS
D. 16 CPU コア、16GB RAM、800 IOPS
Answer: (解答を表示する)

最新問題**: 104**
Splunk インデクサーのクラスタリングに関する正しい記述は次のうちどれですか?
A. すべてのピアノードは、まったく同じ Splunk バージョンを実行する必要があります。
B. マスター ノードは、サーチ ヘッドと同じかそれ以降の Splunk バージョンを実行する必要があります。
C. ピアノードはマスターノードと同じかそれ以降の Splunk バージョンを実行する必要があります。
D. サーチヘッドはピアノードと同じかそれ以降の Splunk バージョンを実行する必要があります。
Answer: (解答を表示する)
Splunk インデクサーのクラスタリングについては、次のことが当てはまります。
* すべてのピアノードはまったく同じ Splunk バージョンを実行する必要があります。異なる Splunk バージョンには、相互に互換性のない異なるデータ形式や機能が含まれる可能性があるため、これはインデクサー クラスタリングの要件です。すべてのピア ノードは、マスター ノードおよびサーチ ヘッドと同じ Splunk バージョンを実行する必要があります。
* クラスターに接続します。
* サーチヘッドはピアノードと同じかそれ以降の Splunk バージョンを実行する必要があります。新しい Splunk バージョンには、検索機能やパフォーマンスを向上させる新機能やバグ修正が含まれている可能性があるため、これはインデクサー クラスタリングに対する推奨事項です。検索エラーや失敗が発生する可能性があるため、検索

ヘッドはピアノードよりも古い Splunk バージョンを実行しないでください。Splunk インデクサーのクラスタリングに関する次の記述は誤りです。
* マスターノードは、サーチヘッドと同じまたはそれ以降の Splunk バージョンを実行する必要があります。マスター ノードは検索プロセスに参加しないため、これはインデクサー クラスタリングの要件または推奨事項ではありません。マスターノードは、クラスターの互換性と機能を確保するため、ピアノードと同じ Splunk バージョンを実行する必要があります。
* ピア ノードは、マスター ノードと同じかそれ以降の Splunk バージョンを実行する必要があります。ピア ノードはクラスター アクティビティーを調整しないため、これはインデクサー クラスター化の要件または推奨事項ではありません。ピアノードはマスターノードと同じ Splunk バージョンを実行する必要があります。これにより、クラスターの互換性と機能が確保されます。詳細については、Splunk ドキュメントの 「インデクサー クラスターとインデックス レプリケーションについて」および 「インデクサー クラスターのアップグレード」を参照してください。

最新問題: **105**
Splunk 内部ログのデフォルトのログ サイズはどれくらいですか?
A. 10MB
B. 20 MB
C. 25MB
D. 30MB
Answer: C (メーッセージを残す**)**
Splunk の内部ログは、デフォルトで SPLUNK_HOME/var/log/splunk ディレクトリに保存されます。Splunk 内部ログのデフォルトのログ サイズは 25 MB です。つまり、ログ ファイルが 25 MB に達すると、Splunk はそれをバックアップ ファイルにロールし、新しいログ ファイルを作成します。デフォルトのバックアップ ファイル数は 5 です。これは、Splunk がログ ファイルごとに最大 5 つのバックアップ ファイルを保持することを意味します。

最新問題: **106**
分散環境では、ナレッジ オブジェクト バンドルは検索ヘッドから検索ピアのどの場所に複製されますか?
A. SPLUNK_HOME/var/lib/searchpeers
B. SPLUNK_HOME/var/log/searchpeers
C. SPLUNK_HOME/var/run/searchpeers
D. SPLUNK_HOME/var/spool/searchpeers
Answer: C (メーッセージを残す**)**

最新問題: **107**
metrics.log は、ライセンス使用率に関する定期レポートをデフォルトのどの間隔で生成しますか?
A. 10 秒
B. 30 秒
C. 60 秒
D. 300 秒
Answer: B (メーッセージを残す)

最新問題: **108**
デプロイメントクライアントがデプロイメントサーバーに接続する頻度は何によって制御されますか?
A. Outputs.conf のpolling_interval 属性
B. Outputs.conf のphoneHomeIntervalInSecs 属性
C. deploymentclient.conf のpolling_interval 属性
D. deploymentclient.conf のphoneHomeIntervalInSecs 属性
Answer: D (メーッセージを残す)
説明
デプロイメント ･クライアントがデプロイメント ･サーバーに接続する頻度は、deploymentclient.conf の phoneHomeIntervalInSecs 属性によって制御されます。この属性は、展開クライアントが受信する必要があるアプリおよび構成の更新を取得するために展開サーバーにチェックインする頻度を指定します。Outputs.conf の polling_interval 属性は、フォワーダーがインデクサーまたは別のフォワーダーにデータを送信する頻度を制御します。deploymentclient.conf のpolling_interval 属性およびoutputs.conf のphoneHomeIntervalInSecs 属性は、有効な Splunk 属性ではありません。詳細については、Splunk ドキュメントの デプロイメントクライアントの構成」および ｏutputs.conf を使用したフォワーダーの構成」を参照してください。

最新問題: **109**
3 ノードのサーチ ヘッド クラスターが、時間の経過とともに多数の検索をスキップしています。サーチヘッドクラスター上のスケジュールされた検索容量を増やすにはどうすればよいですか?
A. クラスター上にジョブ サーバーを作成します。
B. 別の検索ヘッドをクラスターに追加します。
C. server.confcaptain_is_adhoc_searchhead = true。
D. max_searches_per_cpu のlimits.conf 値をより高い値に変更します。
Answer: (解答を表示する)
max_searches_per_cpu のlimits.conf の値をより高い値に変更することは、長期間にわたって多数の検索がスキップされる場合に、サーチ ヘッド クラスターでスケジュールされた検索容量を増やすための最良のオプションです。
この値は、サーチ ヘッドの各 CPU コアで同時に実行できるスケジュールされた検索の数を決定します。

この値を増やすと、より多くのスケジュールされた検索を同時に実行できるようになり、スキップされる検索の数が減ります。クラスター上にジョブ サーバーを作成すること、server.confcaptain_is_adhoc_searchhead = true コマンドを実行すること、またはクラスターに別のサーチヘッドを追加することは、サーチヘッド クラスター上でスケジュールされた検索容量を増やすための最良のオプションではありません。詳細については、Splunk ドキュメントの 「configurelimits.conf」を参照してください。

最新問題: **110**
Enterprise Security をサーチ ヘッド クラスターにインストールする場合、次のどれを実行する必要がありますか? （該当するものをすべて選択。）
A. Enterprise Security をデプロイヤーにインストールします。
B. Enterprise Security をステージング インスタンスにインストールします。
C. Enterprise Security 構成をデプロイヤーにコピーします。
D. デプロイヤを使用して、Enterprise Security をクラスタ メンバーにデプロイします。
Answer: A,D (メーッセージを残す**)**
Enterprise Security をサーチ ヘッド クラスター (SHC) にインストールする場合は、次の手順を実行する必要があります。
Enterprise Security をデプロイヤーにインストールし、デプロイヤーを使用して Enterprise Security をクラスターメンバーにデプロイします。Enterprise Security は、Splunk のセキュリティ分析と監視機能を提供するプレミアム アプリです。Enterprise Security は、アプリやその他の構成を SHC メンバーに配布するスタンドアロン インスタンスであるデプロイヤーを使用して SHC にインストールできます。Enterprise Security は、まずデプロイヤーにインストールしてから、splunk apply shcluster-bundle コマンドを使用してクラスターメンバーにデプロイする必要があります。ステージング インスタンスは SHC 導入プロセスの一部ではないため、Enterprise Security をステージング インスタンスにインストールしないでください。Enterprise Security 構成は、Enterprise Security アプリ パッケージに既に含まれているため、デプロイヤにコピーしないでください。

最新問題: **111**
インデクサー クラスター内で動作しているピア ノードを永続的に廃止するコマンドはどれですか?
A. スプランク停止 -f
B. splunk オフライン -f
C. splunk オフライン --enforce-counts
D. splunk のデコミッション -- カウントを強制する
Answer: (解答を表示する**)**
説明/参照: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Takeapeeroffline

最新問題: **112**
モニター入力のトラブルシューティングを行う場合、末尾のファイルのステータスをチェックするコマンドはどれですか?
A. splunk cmd btool 入力リスト | しっぽ
B. splunk cmd btool チェック入力レイヤー
C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus

D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus
Answer: C (メーッセージを残す**)**
説明
curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus コマンドは、モニター入力のトラブルシューティング時に末尾ファイルのステータスを確認するために使用されます。モニター入力は、ファイルまたはディレクトリーで新しいデータを監視し、そのデータをインデックス作成のために Splunk に送信する入力です。TailingProcessor:FileStatus エンドポイントは、ファイル名、パス、サイズ、位置、ステータスなど、テーリング プロセッサによって監視されているファイルに関する情報を返します。Splunk cmd btool 入力リスト | tail コマンドは、inputs.conf ファイルからの入力構成をリストし、出力を tail コマンドにパイプするために使用されます。splunk cmd btool check inputslayer コマンドは、入力構成の構文エラーと階層化をチェックするために使用されます。カール
https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus コマンドは存在せず、有効なエンドポイントではありません。

最新問題**: 113**
エンタープライズ セキュリティのストレージ サイズ要件に大きな影響を与えるのは次のうちどれですか?
A. スケジュールされた (相関) 検索の数。
B. 設定された Splunk ユーザーの数。
C. 環境で使用されるソース タイプの数。
D. 加速されたデータ モデルの数。
Answer: D (メーッセージを残す**)**
データ モデル アクセラレーションは、生データをより効率的な形式に要約することで、大規模なデータ セットの高速検索を可能にする機能です。データ モデル アクセラレーションは、生データと要約データの両方を保存するため、追加のディスク領域を消費します。必要なディスク容量は、データ モデルのサイズと複雑さ、要約データの保存期間、およびデータの圧縮率によって異なります。Splunk Enterprise Security の計画およびインストール マニュアルによると、データ モデルの高速化は、エンタープライズ セキュリティのストレージ サイズ要件に大きな影響を与える要素の 1 つです。その他の要素は、データ ソースの量と種類、データの保持ポリシー、インデックス クラスターのレプリケーション ファクターと検索ファクターです。スケジュールされた (相関) 検索の数、構成された Splunk ユーザーの数、および環境で使用されるソース タイプの数は、エンタープライズ セキュリティのストレージ サイズ要件とは直接関係ありません1
1: https://docs.splunk.com/Documentation/ES/6.6.0/Install/Plan#Storage_sizing_requirements