F5.F5CAB5.v2026-06-19.q20

試験コード:	F5CAB5
試験名称:	BIG-IP Administration Support and Troubleshooting
認定資格:	F5
無料問題数:	20
バージョン:	v2026-06-19
アクセス数:	109
ページビュー数:	200
https://www.jpnpdf.com/F5.F5CAB5.v2026-06-19.q20-mondaishu.html	

最新問題: **1**
BIG-IP 管理者は、BIG-IP デバイスへの SSL 接続が失敗しているというレポートをユーザーから受け取ります。
ログファイルを確認したところ、管理者は「SSLトランザクション（TPS）レート制限に達しました。統計情報によると、クライアント側SSL TPSの最大値は1200、サーバー側SSL TPSの最大値は800です。このピークに対応するために必要なSSLライセンスの最小制限はいくらですか？」というエラーに気づきました。
A. 2000
B. 400
C. 800
D. 1200
Answer: D (メーッセージを残す)
SSLハンドシェイクの失敗をトラブルシューティングするには、システムのライセンスで定義されているリソース制限を解釈する必要があります8888。ログメッセージ「SSLトランザクション（TPS）レート制限に達しました」は、BIG-IPがライセンスされた「秒あたりのトランザクション数」の容量を超えたため、SSL接続を切断していることを示します。適切なライセンスレベルを決定するために統計情報を分析する際、管理者は「クライアント側」のSSL TPSに注目する必要があります。これは、ユーザーとBIG-IP仮想サーバー間の最初の暗号化ハンドシェイクを表します91。このシナリオでは、クライアント側のピーク需要は1200 TPSです。サーバー側の800トランザクションはバックエンドへの再暗号化を表しますが、F5の主要なSSL TPSライセンス制限は通常、トラフィックフローのクライアント側に適用されます。
したがって、断続的な接続の問題を解決し、ピーク時に仮想サーバーが確実に動作することを保証するには、ライセンスを少なくとも 1200 TPS949596969696.9798 にアップグレードする必要があります。統計を使用してこのピークを確認し、現在のライセンスと比較することは、SSL パフォーマンスの問題に対する標準的なトラブルシューティング手順です。

最新問題: **2**
再開が有効になっていて、ヘルスチェックが最初に失敗し、その後成功しますか?
A. オフライン（無効）
B. オフライン（有効）
C. 利用可能（無効）
D. 利用可能（有効）

Answer: A (メーッセージを残す)
BIG-IP管理サポートおよびトラブルシューティングドキュメントからの包括的かつ詳細な説明：手動再開」機能は、サービスのフラッピングやバックエンドアプリケーションの不安定さなどによりプールが期待どおりに動作しない場合に使用される安全機構です。通常、ヘルスモニターに障害が発生すると、プールメンバーは 「オフライン」（赤）とマークされ、モニターに合格すると自動的に 「使用可能」（緑）に戻ります47。しかし、 「手動再開」が有効になっている場合、BIG-IPは障害発生後もメンバーを自動的にローテーションに戻しません48。ヘルスチェックが再び合格し始めても、メンバーは 「オフライン（無効）」状態のままです49。そのため、管理者が手動で介入し、メンバーを再度有効化する必要があります。これはトラブルシューティング時によくある混乱点です。メンバーはヘルスチェックに合格しているように見えても、手動による管理者の 「再開」コマンドを待機しているため、トラフィックを受信できない場合があります。この機能は、エンジニアが最初の障害の根本原因が解決されたことを確認するまで、 「不健全な」サーバーがトラフィックを受信できないようにすることを目的としています。

最新問題**: 3**
BIG-IPデバイスがフェイルオーバーするたびにトラフィックに悪影響が出るという報告がユーザーから寄せられています。トラフィックは数分後に安定します。今後のフェイルオーバーの影響を軽減するために、BIG-IP管理者はどのような対策を講じるべきでしょうか？
A. フェイルオーバーマルチキャスト構成を有効にする
B. HAオーダーへのフェイルオーバー方式の設定
C. MACマスカレードを設定する
D. グローバルSNATリスナーを設定する
Answer: (解答を表示する**)**
フェイルオーバー後、トラフィックが 「数分後に安定する」場合、上流のルーターやスイッチのARPキャッシュに関連するネットワークレベルのパフォーマンス問題を示しています。各BIG-IPインターフェースには固有のハードウェアMACアドレスがあります。フェイルオーバー中、スタンバイデバイスはフローティングIPアドレスを引き継ぎますが、上流スイッチは引き続きそのIPアドレスをオフラインになったデバイスのMACアドレスに関連付けます。スイッチが新しいMACアドレスを学習するか、ARPエントリの有効期限が切れるまで、トラフィックは失われます。
「MACマスカレード」は、フローティングトラフィックグループに共有の仮想MACアドレスを作成することでこの問題を解決します。この仮想MACアドレスは、現在アクティブなデバイスによって使用されます。仮想サーバーIPのMACアドレスはネットワークの観点からは決して変化しないため、上流デバイスはARPテーブルを更新する必要はありません。このトラブルシューティングソリューションは、フェイルオーバーに伴う遅延を排除し、シームレスな移行を実現し、BIG-IPのHA状態が変化してもアプリケーショントラフィックフローが中断されないようにします。

最新問題**: 4**
添付資料を参照してください。BIG-IP管理者は、SSHトラフィックの負荷分散のために新しい仮想サーバーを作成しました。ユーザーはサーバーにログオンできません。BIG-IP管理者はこの問題を解決するために何をすべきでしょうか？（添付資料は、HTTPプロファイルが適用された標準仮想サーバーを示しています。）
A. プロトコルをUDP8に設定する
B. HTTPプロファイルをNone9に設定する
C. 送信元アドレスを10.1.1.210に設定する
D. 宛先アドレス/マスクを0.0.0.0/011に設定する
Answer: B (メーッセージを残す**)**
BIG-IP管理サポートおよびトラブルシューティングドキュメントからの包括的かつ詳細な説明：仮想サーバーが期待どおりに動作しない場合のトラブルシューティングでは、適用されているプロファイルが処理対象のトラフィックの種類と一致していることを確認することが重要です。SSH（セキュアシェル）は、TCP上で動作する非HTTPプロトコルです。図では、仮想サーバーにHTTPプロファイルが適用されていることを示

しています14。HTTPプロファイルは、BIG-IPシステムにトラフィックをHTTPとして解析するよう指示しますが、SSHトラフィックはHTTP仕様に準拠していないため、BIG-IPのパーサーはデータストリームを理解できず、通常、パケットのドロップや接続のリセットが発生します15。これを修正するには、管理者はHTTPプロファイルを「なし」16に設定する必要があります。これにより、仮想サーバーは「標準」または「FastL4」リスナーとして機能し、アプリケーション層の検査を試みることなく、暗号化されたSSHデータをバックエンドプールメンバーに透過的に渡すことができます。これは、一般的なトラブルシューティング手順を強調表示します。つまり、L7 プロファイルが L4 トラフィックに誤って適用され、クライアントとサーバー間の予期されるトラフィック フローが中断されないことを確認します。

最新問題: **5**
BIG-IP管理者は、既存の高使用率のプールに新しいプールメンバーを追加しました。その後すぐに、一部のユーザーでアプリケーションの読み込みに失敗するという報告がありました。BIG-IP管理者は、プールレベルのどの設定を確認すべきでしょうか？
A. 可用性要件
B. SNATを許可する
C. サービスダウン時のアクション
D. スローランプタイム
Answer: D (メーッセージを残す**)**
新規メンバーを追加した後にプールが正常に動作しなくなった場合のトラブルシューティングでは、「Slow Ramp Time（低速ランプ時間）」設定が主な原因と考えられます。プールの負荷が既に高く、「Least Connections（最小接続）」ロードバランシング方式を使用している場合、新しく追加されたサーバーには接続が全くありません。Slow Ramp Timeが設定されていない場合、BIG-IPは他のサーバーとの「バランス」をとるために、大量の新規接続をすぐに新しいサーバーに送り込んでしまいます。これは
「雷鳴のような群れ」現象は、新しく初期化されたアプリケーションサーバーがキャッシュをウォームアップしたり、独自のデータベース接続を確立したりする時間がないうちにクラッシュさせる可能性があります。「スローランプタイム」（通常は秒単位）を設定することで、管理者はBIG-IPが新規メンバーへの接続比率を徐々に高めるようにすることができます。これにより、サーバーは時間の経過とともに安定し、パフォーマンスを向上することができます。ユーザーから、特にプールの拡張と一致する断続的な障害が報告された場合、この設定を確認することは、メンテナンス中にプールの健全性を維持するための重要なトラブルシューティング手順です。

最新問題: **6**
QKView サポート ファイルを生成するには、BIG-IP 構成ユーティリティのどのメニューを使用する必要がありますか? (1 つの回答を選択してください)
A. システム > 構成
B. システム > アーカイブ
C. システム > サポート
D. システム > ログ
Answer: C (メーッセージを残す**)**
BIG-IP の管理、サポート、およびトラブルシューティングに関するドキュメントからの包括的かつ詳細な 150 ～ 250 語の説明:
QKViewファイルは、F5サポートがBIG-IPシステムの問題をトラブルシューティングするために使用する主要な診断サポートバンドルです。実行構成、ライセンスの詳細、モジュールのプロビジョニング、ハードウェアステータス、ソフトウェアバージョン、ログファイル、統計情報、そして多数の診断コマンドの出力など、包括的なシステム情報が含まれています。パフォーマンスの問題や構成の問題を調査する場合、あるいはF5にサポートケースを提出する場合、QKViewの生成は標準的な推奨手順です。

BIG-IP設定ユーティリティ（GUI）では、QKViewを生成するための適切な場所は「システム」> 「サポート」です。このメニューは、サポートとトラブルシューティング業務のために特別に設計されています。このセクションから、管理者はQKViewファイルを生成し、作成の進捗状況を監視したり、ローカルにダウンロードしたり、F5 iHealthに直接アップロードして自動分析を行ったりすることができます。このワークフローは、BIG-IP管理およびサポートガイドに明確に記載されており、F5のベストプラクティスに準拠しています。
その他のメニュー オプションは適切ではありません。
システム > 構成は、DNS、NTP、デバイス ID などのシステム全体の設定に使用されます。
システム > アーカイブは、診断バンドルではなく構成バックアップである UCS バックアップ ファイルを作成するために使用されます。
システム > ログは、システム ログの表示にのみ使用され、サポート ファイルの生成には使用されません。
したがって、「システム > サポート」が正しい唯一の有効な回答です。

最新問題: **7**
新しいメンバーを追加した後にプールが期待どおりに機能しないビジーな環境では、新しいメンバーへのトラフィックを管理するためにどの設定が重要ですか?
A. 可用性要件
B. SNATを許可する
C. サービスダウン時のアクション
D. スローランプタイム
Answer: (解答を表示する**)**
忙しい環境に新しいメンバーを追加した直後にプールが期待通りに動作しない場合は、
「低速ランプ時間」の設定は重要な要素です
「最少接続数」負荷分散方式を採用したプールでは、新規メンバーはアクティブな接続がゼロの状態で開始します5858。スローランプタイムが設定されていない場合、BIG-IPは大量の新規トラフィックをこのサーバーに即座に送信し、他のメンバーと「均等化」させます。この急激なトラフィック増加は、サーバーのアプリケーションスタックが完全に初期化またはキャッシュのウォームアップを完了する前に過負荷となり、障害につながる可能性があります。「スローランプタイム」を設定することで、管理者は指定された期間にわたって、システムが新規メンバーに送信されるトラフィック量を徐々に増加させることが可能になります。送信されるトラフィック量は、ランプタイム設定62に対するメンバーの可用性時間に比例します。アプリケーションが新しいサーバーにルーティングされたユーザーに対してのみ障害が発生する場合は、この設定を確認することで、サービスパフォーマンスを低下させることなく、新しい容量をプールに統合することができます。

最新問題: **8**
FTPアプリケーションとHTTPウェブサイトの両方に、別々のBIG-IPプールを介して複数のサーバーが使用されています。サーバーサポートチームから、一部のサーバーが他のサーバーよりもトラフィック量が非常に多いという報告がありました。接続数を均等にするために、BIG-IP管理者はどの負荷分散方法を適用すべきでしょうか？
A. 比率（メンバー）
B. 最小接続数（メンバー）
C. 最小接続数（ノード）
D. 比率（ノード）
Answer: (解答を表示する**)**
複数のサービスをホストするハードウェア間で負荷分散が期待どおりに機能していない場合、管理者は「メンバー」レベルと「ノード」レベルのアルゴリズムを区別する必要があります102102102102。「メンバー」とは特定のIPアドレスとポート番号（例1:0.1.1.1:80）であり、「ノード」とは

ポート番号に関わらず物理サーバーのIPアドレス（10.1.1.1）です103。サーバーがFTPサービスとHTTPサービスを別々のプールでホストしている場合、「最小接続数（メンバー）」を使用すると、各プール内のみで接続が分散されます。そのため、たとえ数百件ものFTP接続で過負荷状態であっても、HTTP接続数が最も少ないサーバーが新しいHTTP接続に選択されるという偏った分散が発生する可能性があります。「最小接続数（ノード）」を適用することで、BIG-IPはすべてのポートとプールにおける物理ハードウェアへの接続数の合計を追跡します106106106106。これにより、管理者はサーバー群全体のワークロードを均等に分散させることができ、サーバーサポートチームから報告されるトラフィックの不均等な分散の報告を解決できます。

最新問題: **9**
BIG-IPデバイスがフェイルオーバーするたびにトラフィックに悪影響が出るという報告がユーザーから寄せられています。トラフィックは数分後に安定します。今後のフェイルオーバーの影響を軽減するために、BIG-IP管理者はどのような対策を講じるべきでしょうか？
A. MACマスカレードを設定する
B. グローバルSNATリスナーを構成する
C. フェイルオーバーマルチキャスト構成を有効にする
D. HAオーダーへのフェイルオーバー方式の設定
Answer: A (メーッセージを残す**)**
フェイルオーバー後、トラフィックが「数分後に安定する」場合、上流のルーターやスイッチのARPキャッシュに関連するネットワークレベルのパフォーマンス問題を示しています。各BIG-IPインターフェースには固有のハードウェアMACアドレスがあります。フェイルオーバー中、スタンバイデバイスはフローティングIPアドレスを引き継ぎますが、上流スイッチは引き続きそのIPアドレスをオフラインになったデバイスのMACアドレスに関連付けます。スイッチが新しいMACアドレスを学習するか、ARPエントリの有効期限が切れるまで、トラフィックは失われます。「MACマスカレード」は、フローティングトラフィックグループに共有の仮想MACアドレスを作成することでこの問題を解決します。この仮想MACアドレスは、現在アクティブなデバイスによって使用されます。仮想サーバーIPのMACアドレスはネットワークの観点からは決して変化しないため、上流デバイスはARPテーブルを更新する必要はありません。このトラブルシューティングソリューションは、フェイルオーバーに伴う遅延を排除し、シームレスな移行を実現し、BIG-IPのHA状態が変化してもアプリケーショントラフィックフローが中断されないようにします。

最新問題: **10**
BIG-IP構成ユーティリティにおいて、ユーザーはすべての仮想サーバーとそれに関連付けられたプールメンバー、および使用中のiRuleのステータスを確認するための単一画面ビューを要求します。BIG-IP管理者は、ユーザーにこのビューをどこで見つけられるか指示する必要がありますか？32
A. ローカルトラフィック > モニター
B. ローカルトラフィック > 仮想サーバー
C. ローカルトラフィック > ネットワークマップ
D. 統計
Answer: C (メーッセージを残す**)**
BIG-IP A41管理サポートおよびトラブルシューティングドキュメントからの包括的かつ詳細な説明：複雑な環境全体の機能を確認するには、「ネットワークマップ」が構成ユーティリティ43の中で最も効率的なトラブルシューティングツールです。ネットワークマップは、トラフィック管理オブジェクトを階層的に視覚的に表示します44。管理者は、仮想サーバーのステータス（緑/赤/黄）、関連付けられたプールのステータス、個々のプールメンバーの健全性、現在アタッチされているiRuleを一目で確認できます45。このビューは、オブジェクト間の依存関係をマッピングするため、トラブルシューティングにおいて標準の「仮想サーバーリスト」よりも優れています46。例えば、仮想サーバーが「赤」の場合、ネットワークマップには、そのステータスが障害が発生したプールから継承されたものなのか、プールメンバー上の特定のモニターの障害から継承されたも

のなのかが表示されます。ネットワークマップでこれらの基本統計を確認することで、管理者は障害がサービスレベル（仮想サーバー）、ロジックレベル（iRule）、ハードウェアレベル（プールメンバー）のいずれにあるかを迅速に特定できます。

最新問題: **11**
BIG-IP管理者は、バックエンドサーバーを使用して、サーバーごとに複数のサービスをホストしています。複数の仮想サーバーとプールが定義されており、それらは同じバックエンドサーバーを参照しています。各バックエンドサーバーへの接続数を均等にするには、どの負荷分散アルゴリズムが最も適切でしょうか？17
A. 最小接続数（メンバー）
B. 最小接続数（ノード）
C. 予測（メンバー）
D. 予測（ノード）
Answer: B (メーッセージを残す**)**
BIG-IP管理サポートおよびトラブルシューティングドキュメントからの包括的かつ詳細な説明：負荷分散が期待通りに機能せず、接続が物理ハードウェア間で偏っているように見える場合、管理者は「メンバー」レベルと「ノード」レベルの負荷分散を区別する必要があります。
「メンバー」は特定のIPアドレスとポート番号の組み合わせ（例：10.1.1.1:80）を指しますが、「ノード」はポート番号に関係なく、基盤となるIPアドレス（10.1.1.1）を指します25。1台のサーバーが異なるプールにまたがって複数のサービス（Web、FTP、API）をホストしている場合、「最小接続数（メンバー）」を使用すると、各プール内の接続のみが分散されます26。これにより、1台のサーバーが接続を独占し、過負荷状態になるシナリオが発生する可能性があります。
「最少接続数」は3つの異なるプールで同時にカウントされます。「最少接続数（ノード）」を選択すると、BIG-IPは物理IPアドレスへの同時接続数を、それが属するすべてのプール27全体で追跡します。これにより、管理者はハードウェア全体に均等に作業を分散させることができ、複数のアプリケーションサービスをホストするバックエンドサーバーのパフォーマンス低下を防ぐことができます。

最新問題: **12**
ある組織から、パブリッククラウドでホストされているイントラネットウェブサイトへのアクセス速度が遅いという報告がありました。全従業員がインターネット接続に、パブリックIPアドレス104.219.110.168を持つ単一のプロキシサーバーを使用しています。イントラネットウェブサイトのBIG-IP管理者は、この問題を解決するために何をすべきでしょうか？
A. 送信元アドレスを104.219.110.168/32に変更します
B. 負荷分散方法を最小接続に変更
C. フォールバックパーシスタンスプロファイルをsource_addrに変更します
D. デフォルトの永続プロファイルをCookieに変更します
Answer: (解答を表示する**)**
このシナリオは、「メガプロキシ」問題として知られる典型的なネットワークパフォーマンスの問題を説明しています。組織が従業員のトラフィックをすべて単一のプロキシサーバー経由でルーティングする場合、BIG-IPは数千人のユニークユーザーが全く同じ送信元IPアドレスを持つと認識します。管理者が「送信元アドレスアフィニティ」パーシステンスを設定している場合、BIG-IPはルールに正しく従いますが、すべてのユーザーを同じ単一のバックエンドプールメンバーに誤ってルーティングします。これにより、1つのサーバーが過負荷になり、他のサーバーがアイドル状態になるという深刻な負荷不均衡が生じ、アプリケーションの応答時間が低下します。この問題を解決するには、管理者はパーシステンスプロファイルを「HTTP Cookie」に変更する必要があります。Cookieベースのパーシステンスにより、BIG-IPは各ユーザーのブラウザに一意の識別子を配置できるため、同じ送信元IPを共有する場合でも、システムは個々のセッションを区別できます。この修正により、トラフィックがプールメ

ンバー間で均等に分散され、期待される負荷分散機能が回復し、企業プロキシの背後にいるユーザーから報告されたパフォーマンスの低下が解消されます。

最新問題: **13**
デバイスグループは現在、 変更保留中」の同期ステータスにあります。BIG-IP管理者は、デバイスグループ内のどのメンバーが最新の設定を持っているかをどのように判断できますか？ 1つ選択してください）
A. デバイス管理 > 概要
B. デバイス管理 > デバイス
C. システム > 高可用性
D. デバイス管理 > デバイスグループ
Answer: D (メーッセージを残す**)**
BIG-IPデバイスグループが 変更保留中」ステータスを示している場合、グループ内の1つ以上のデバイスに、他のメンバーにまだ同期されていない設定変更があることを示します。どのデバイスが最新の（権限のある）設定を持っているかを特定するには、管理者はデバイスグループレベルで詳細な同期ステータスを確認する必要があります。
正しい場所は デバイス管理」> デバイスグループ」オプションD）です。このメニューでは、BIG-IP構成ユーティリティが各デバイスグループとその同期ステータスを表示し、変更が保留中のデバイスに関する詳細情報を提供します。このビューから、管理者は変更が保留中としてマークされているデバイスを明確に把握し、そのデバイスをグループへの同期操作を開始するためのソースデバイスとして指定できます。
その他のオプションでは、必要なレベルの詳細が提供されません。
デバイス管理 > 概要 (オプション A) には、一般的な HA ステータスが表示されますが、構成の所有権は表示されません。
デバイス管理 > デバイス (オプション B) ではデバイスが一覧表示されますが、どのデバイスに同期されていない変更が含まれているかは明確に識別されません。
システム > 高可用性 (オプション C) は、構成の同期状態ではなく、フェールオーバーとトラフィック グループに重点を置いています。
このワークフローは、構成同期に関する BIG-IP のベスト プラクティスに準拠しており、新しい構成を上書きせずに変更が正しく伝播されることを保証します。

最新問題: **14**
BIG-IP 管理者は、BIG-IP デバイスを最新の TMOS バージョンにアップグレードする予定です。
管理者が対象バージョンの既知の問題を確認するために活用できる 2 つのツールはどれですか? (2 つの回答を選択してください)
A. F5 エンドユーザー診断 (EUD)
B. F5 バグトラッカー
C. F5大学
D. F5 iHealth
E. F5 ダウンロード
Answer: B,D (メーッセージを残す**)**
BIG-IPシステムを新しいTMOSバージョンにアップグレードする前に、不安定性やリグレッションの発生を防ぐため、既知の問題を確認することが重要です。F5 Bug Tracker オプションB）は、このための主要なリソースです。管理者は、TMOSバージョン、モジュール、症状、またはバグIDで、文書化されたソフトウェアの不具合を検索できます。Bug Trackerを使用することで、管理者は未解決の問題、修正されたバグ、そしてトラフィック処理、高可用性、モジュール固有の機能など、特定の導入に影響を与える可能性のある動作の変更を特定できます。これは、プロアクティブなトラブルシューティングと情報に基づいたアップグレード計画を直接的にサポートします。

F5 iHealth オプションD）は、アップグレード準備時に使用するもう一つの重要なツールです。iHealthは、アップロードされたUCSまたはQKViewファイルを分析し、デバイス構成とソフトウェアバージョンをF5の既知の問題データベースと関連付けます。重大な不具合、アップグレードのリスク、相互運用性に関する懸念事項、推奨されるターゲットバージョンなど、実用的なレポートを提供します。iHealthは、デバイス上で実際に実行されている構成に基づいて既知の問題を文脈化できるため、特に有用です。
その他のオプションは、既知のソフトウェアの問題の検証には適していません。F5 End User Diagnostics オプションA）はクライアント側のトラブルシューティングツールであり、F5 University オプションC）はトレーニングプラットフォームです。F5 Downloads オプションE）は、既知の欠陥を詳細に分析するためではなく、主にソフトウェアイメージとリリースノートを取得するために使用されます。

最新問題: **15**
BIG-IP管理者は、ユーザーからBIG-IPデバイスへのSSL接続が失敗しているという報告を断続的に受けています。ログファイルを確認したところ、管理者は 「SSLトランザクション（TPS）のレート制限に達しました」というエラーに気づきました。統計情報を確認すると、クライアント側SSL TPSの最大値は1200、サーバー側SSL TPSの最大値は800です。このピークに対応するために必要なSSLライセンスの最小制限容量はいくらですか？
A. 2000
B. 400
C. 800
D. 1200
Answer: (解答を表示する**)**
SSL接続のリセットに関するトラブルシューティングでは、ライセンス制限と実際のリソース使用率を検証することがしばしば必要になります。F5デバイスは、「1秒あたりのトランザクション数」（TPS）ライセンスを使用して、デバイスが処理できるSSL処理量を制御します。ログエントリのSSLトランザクション（TPS）レート制限への到達は、トラフィック量がライセンス容量を超えたことを明確に示しています。必要なライセンスレベルを決定する際には、F5が主に 「クライアント側」SSL TPS、つまりユーザーと仮想サーバー間の暗号化された接続に対してライセンスと制限を適用していることを理解することが重要です。この特定のシナリオでは、ピーク需要が1秒あたり1200件のクライアント側トランザクションに達しました。800件のサーバー側トランザクション（BIG-IPからプールへの再暗号化）もありましたが、これらは通常、プライマリTPSライセンス制限に同様にカウントされません。したがって、ピーク負荷時に仮想サーバーが期待どおりに動作することを保証するには、管理者はライセンスを少なくとも1200 TPSにアップグレードする必要があります。このトラブルシューティングプロセスは、システムログエラーとライセンスによって課されるリソース制約を結び付けます。

最新問題: **16**
BIG-IP の 「手動再開」機能を使用する場合、ヘルス モニターの障害後、ヘルス チェックが再び成功し始めても、プール メンバーはどのような状態のままになりますか?
A. オフライン（無効）
B. オフライン（有効）
C. 利用可能（無効）
D. 利用可能（有効）
Answer: A (メーッセージを残す**)**
BIG-IP管理サポートおよびトラブルシューティングドキュメントからの包括的かつ詳細な説明：「手動再開」機能は、サービスのフラッピングやバックエンドアプリケーションの不安定化によりプールが期待通りに動作しなくなった場合に使用される安全機構です。通常、ヘルスモニターが失敗すると、プールメンバーは 「オフライン」（赤）とマークされ、モニターが成功すると自動的に 「使用可能」（緑）に戻ります47。しかし、 「手動再

開」が有効になっている場合、BIG-IPは失敗後もメンバーを自動的にローテーションに戻しません48。ヘルスチェックが再び成功し始めても、メンバーはオフライン状態のままです。
オフライン（無効）状態49。この場合、管理者が手動で介入し、メンバーを再度有効にする必要があります。
これはトラブルシューティングの際によくある混乱の原因です。メンバーがヘルスチェックに合格しているように見えても、管理者による手動の「再開」コマンドを待機しているためにトラフィックを受信できない場合があります。この機能は、エンジニアが最初の障害の根本原因が解決されたことを確認するまで、「正常でない」サーバーがトラフィックを受信できないようにすることを目的としています。

最新問題**: 17**
BIG-IP管理者は、既存の高使用率のプールに新しいプールメンバーを追加しました。その後すぐに、一部のユーザーでアプリケーションの読み込みに失敗するという報告がありました。BIG-IP管理者は、プールレベルのどの設定を確認すべきでしょうか？
A. スローランプタイム
B. 可用性要件
C. サービスダウン時のアクション
D. SNATを許可する
Answer: A (メーッセージを残す**)**
新しいメンバーを追加した後にプールが正常に動作しなくなった場合のトラブルシューティングでは、「スローランプタイム」設定が主な原因と考えられます。プールの負荷が既に高く、「最小接続」ロードバランシング方式を使用している場合、新しく追加されたサーバーには接続が全くありません。スローランプタイムが設定されていないと、BIG-IPは他のサーバーと「バランスを取る」ために、大量の新規接続を新しいサーバーに即座に送信します。この「雷鳴のような群れ」効果により、新しく初期化されたアプリケーションサーバーは、キャッシュのウォームアップや独自のデータベース接続の確立が完了する前にクラッシュする可能性があります。「スローランプタイム」（通常は秒単位）を設定することで、管理者はBIG-IPが新しいメンバーへの接続比率を徐々に高めるようにすることができます。これにより、サーバーは時間の経過とともにパフォーマンスを安定させ、スケールアップすることができます。ユーザーから、特にプールの拡張と同時期に断続的な障害が発生するという報告があった場合、この設定を確認することは、メンテナンス中にプールの健全性を維持するために不可欠なトラブルシューティング手順です。

最新問題**: 18**
BIG-IP管理者は、インターフェース1.1のトラフィックがリンクの最大帯域幅容量を超えると予想されるという通知を受けました。このインターフェースにはVLANが1つあります。利用可能な帯域幅を増やすために、BIG-IP管理者はどのような対策を講じるべきでしょうか？
A. VLANに2つのインターフェースを割り当てる
B. インターフェース1.1のメディア速度を手動で設定します
C. 2つのインターフェースを持つトランクオブジェクトを作成する
D. インターフェース1.1を使用してVLANのMTUを増やす
Answer: (解答を表示する**)**

物理ネットワークリンク（インターフェース1.1など）が最大容量に達すると、ボトルネックが発生し、ネットワークレベルのパフォーマンスに悪影響を及ぼします。単一インターフェースの物理的な限界を克服するために、BIG-IP管理者は「トランキング」を使用します。これは、F5用語でリンクアグリゲーション（多くの場合、LACPを介して実装されます）を意味します。トランクオブジェクトは、複数の物理インターフェースを単一の論理リンクにまとめます。2つ以上のインターフェースを持つトランクを作成することで、BIG-IPはトラフィック負荷をトランクのすべてのメンバーに分散させ、関連付けられたVLANで利用可能な帯域幅を実質的に2倍または3倍にすることができます。パフォーマンス以外にも、冗長性のトラブルシューティングではトランクが使用されることが多くあります。トランク内の1本のケーブルに障害が発生しても、他のケーブルがトラフィックを伝送し続けるため、完全な停止を回避できます。これは、MTUを単純に増やす（エンドツーエンドのサポートが必要）か、メディア速度を手動で設定するよりも優れたソリューションです。高可用性環境では、トラフィックの急増がリンク飽和によるパケットロスにつながらないようにするために、トランクの設定はトラブルシューティングと最適化の基本的なステップとなります。

最新問題: **19**
復号化せずに、パケット キャプチャで HTTPS セッションのどの部分を表示できますか? (回答を 1 つ選択してください)
A. HTTPレスポンスヘッダー
B. 送信元IPアドレス
C. HTTPリクエストヘッダー
D. クッキー
Answer: (解答を表示する**)**
HTTPSセッションでは、アプリケーション層のペイロード（HTTPリクエストヘッダー、レスポンスヘッダー、Cookie、本文コンテンツなど）がSSL/TLSを使用して暗号化されます。トラフィックを復号化せずに（例えば、BIG-IPによるSSLオフロードや秘密鍵へのアクセスなしで）、パケットキャプチャではHTTPレベルの詳細を明らかにすることはできません。
ただし、暗号化が使用されている場合でも、ネットワーク層およびトランスポート層の情報は引き続き表示されます。これには、送信元および宛先IPアドレス、送信元および宛先ポート、TCPフラグ、シーケンス番号、TLSハンドシェイクメタデータが含まれます。したがって、送信元IPアドレス（オプションB）は、復号化されていないHTTPSトラフィックのパケットキャプチャで表示されます。
選択肢A、C、Dは誤りです。HTTPSが確立されると、HTTPヘッダーとCookieは暗号化されたペイロードの一部となるためです。BIG-IPのトラブルシューティングドキュメントでは、tcpdumpを使用して暗号化されたトラフィックフローを分析する際にこの区別が強調されています。SSLインスペクションまたは復号化が設定されていない限り、管理者はIP、ポート、およびタイミング情報に頼らなければならないためです。

最新問題: **20**
BIG-IP管理者は、アプリケーションを実行しているサーバーの1つがトラフィックを受信していないことに気付きました。BIG-IP管理者は、アプリケーションの設定状態を確認し、表示されている監視設定と影響を受けるプールメンバーの状態を確認します。

この問題の原因は何でしょうか? (回答を 1 つ選択してください)

A. ノード ヘルス モニターが応答していません。

B. アプリケーションは、予期される受信文字列で応答していません。

C. HTTP 1.1 は監視目的には適していません。

D. BIG-IP デバイスはプールに到達できません。

Answer: A (メーッセージを残す**)**

この図表の重要な手がかりは、プールメンバーの可用性が 才フライン（有効)- 親ノードがダウン」と表示されていることです。BIG-IPの用語で は、プールメンバーは親ノードのステータスを継承します。ノードがダウンとマークされた場合（例え ば、ノードレベルのモニターやデフォルトの ノードがダウン」状態によって)、そのノードIPを使用するすべてのプールメンバーもダウンとマークされ、メンバーポート上のアプリケーションサービスが正常であっても、トラフィックを受信できなくなります。

HTTPS モニター構成（送受信文字列は表示されますが、ステータスはサービスレベルの障害ではなく、ノード（親の障害を示しています。問題がアプリケーションが受信文字列と一致しないことにある場合、通常は 親のダウン」ではなく、メンバーのモニターの障害が原因でメンバーがダウンしている状態 (ステータスにはモニター障害の詳細が反映されます)が表示されます。オプション D は範囲が広すぎます。BIG-IP は通常サブネットに到達でき（他のサーバーは動作)、この症状は特定のノードの状態を示しています。オプション C は誤りです。HTTP/1.1 はモニタリングによく使用され、適切にフォーマットされている場合（特に Host ヘッダーがある場合)は有効です。したがって、最も可能性の高い原因は、ノードのヘルスモニターが応答していないためにノード、ひいてはメンバーがダウン状態とマークされていることです。