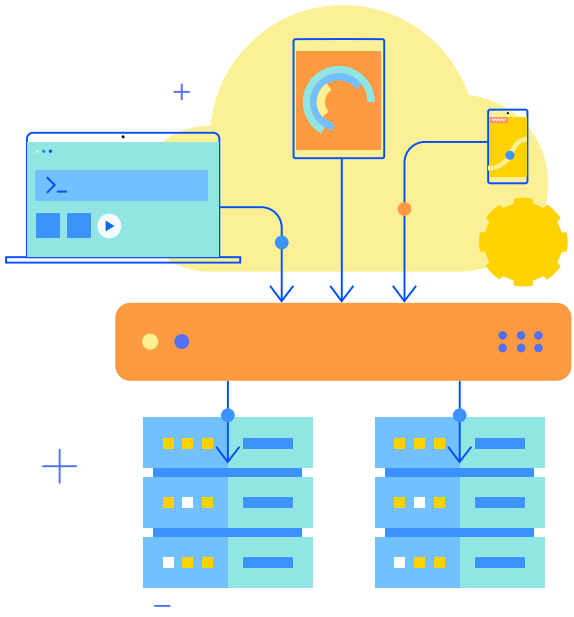
Progress Kemp LoadMaster

製品概略



Updated 2022/9/19

目次

1 Progress Kemp LoadMaster 製品の紹介 7
1.1 LoadMaster 製品 7
1.2 LoadMaster ロードバランサの機能 7
2 LoadMaster ネットワーク トポロジ 8
2.1 One-Armed バランサー 8
2.2 Two-Armed バランサー 9
2.3 高可用性 (HA) 構成 10
2.4 クラスタリング 12
2.5 Direct Server Return – DSR 構成例 14
3 スケジューリング方法 15
3.1 ラウンドロビン 15
3.2 加重ラウンドロビン 15
3.3 最小接続 15
3.3.1 最小接続遅延開始時間 16
3.4 加重最小結合 16
3.5 エージェントベースのアダプティブ バランシング 16
3.6 リソースベース (SDN アダプティブ) 17
3.7 固定加重 18
3.8 加重応答時間 18
3.9 ソース IP ハッシュ 18
4 パーシステンス 19
4.1 パーシステンスの紹介 19
4.2 パーシステンスが必要かどうかを知る方法は? 20
4.3 タイムアウト 20
4.4 レイヤ 7 のパーシステンス化方法 22
4.4.1 サーバー Cookie のパーシステンス 22
4.4.2 アクティブ Cookie のパーシステンス 22
4.4.3 サーバー Cookie またはソース IP パーシステンス 23

4.4.4 アクティブな Cookie またはソース IP のパーシステンス 23
4.4.5 すべての Cookie のパーシステンスをハッシュ 23
4.4.6 すべての Cookie またはソース IP パーシステンスをハッシュする 23
4.4.8 スーパーHTTP 24
4.4.9 URL ハッシュ 24
4.4.10 HTTP ホスト ヘッダー 25
4.4.11 HTTP クエリ アイテムのハッシュ 25
4.4.12 選択されたヘッダー 25
4.4.13 SSL セッション ID 25
4.4.14 UDP セッション開始プロトコル (SIP) 25
4.5 パーシステンスと HTTPS/SSL 26
4.6 ポートフォローイング 26
5 アプリケーション フロント エンド 26
5.1 侵入防止システム 27
5.1.1 侵入処理 27
5.1.2 検出レベル 28
5.1.3 警告 28
5.1.4 侵入アラート 29
5.1.5 IPS ルールの更新 29
5.2 キャッシング 29
5.2.1 キャッシュのフラッシュ 30
5.2.2 最大キャッシュ サイズ 30
5.3 データ圧縮 31
6 SSL アクセラレーション/オフロード 32
7 エッジ セキュリティ パック (ESP) 33
7.1 事前認証のエンドポイント認証 34
7.2 ユーザー ロギングのパーシステンスなロギングとレポート 34
7.3 仮想サービス全体でのシングル サインオン 34
7.4 LoadMaster から Active Directory への LDAP 認証 34
7.5 クライアントから LoadMaster への基本認証通信 34
7.6 RADIUS 認証 35

7.7 RSA SecurID 2 要素認証 35
7.8 Kerberos 制約付き委任 (KCD) 認証 35
7.9 クライアント証明書認証 36
7.10 二要素認証 36
7.11 OIDC OAUTH ESP 認証 36
8 Web アプリケーション ファイアウォール パック(WAF) 37
8.1 従来のファイアウォールの課題 37
8.2 Progress Kemp WAF のメリット 38
8.3 Progress Kemp WAF 対応 LoadMaster の概要 38
9 GEO 40
10 サブ仮想サービス (SubVS) 41
11 証明書 42
11.1 自己署名証明書と CA 署名証明書 42
11.2 証明書の基本 42
11.3 運用上の違い 42
11.4 ACME 証明書 43
11.4.1 証明書を暗号化 44
14.4.2 デジサート証明書 44
12 ルールベースのコンテンツ スイッチング 45
12.1 用語 46
12.2 コンテンツ スイッチングの使用 46
13 ヘルスチェック 46
13.1 概要 46
13.2 サービスおよび非サービスベースのヘルスチェック 47
14 SNMP サポート 50
15 LoadMaster ソフトウェアのアップグレード 51
15.1 オンラインアップグレード 51
16 ユーザー管理 52
16.1 役割・権限 53
16.1.1 Real Servers 53
16.1.2 仮想サービス 53

16.1.3 ルール 53
16.1.4 システムバックアップ 54
16.1.5 証明書の作成 54
16.1.6 中間証明書 54
16.1.7 証明書のバックアップ 54
16.1.8 ユーザー管理 54
16.1.9 すべての権限 54
16.1.10 GEO コントロール 54
17 WUI の認証と承認 54
18 ボンディングと VLAN 56
18.1 概要 56
18.2 前提条件 (スイッチの互換性) 56
18.2.1 スイッチ構成 56
18.3 ボンディング/チーミング (802.3ad/アクティブ バックアップ) 57
18.4 VLAN タギング 57
19 IPsec トンネリング 58
20 その他 58
20.1 IPv6 サポート 58
20.2 リモート Syslog サポート 59
20.3 ライセンスの取得方法 59
20.4 バックアップと復元 60
20.5 WUI へのアクセスの無効化/有効化 61
20.6 L4 と L7 仮想サービス間の相互運用性 61
20.7 ログ情報 61
20.8 デバッグ ユーティリティ 62
20.8.1 すべての Transparency を無効にする 62
20.8.2 L7 デバッグ トレースを有効にする 62
20.8.3 PS を実行する 62
20.8.4 l7adm を実行する 62
20.8.5 Ping ホスト 62
20.9 RESTful API インターフェイス 62

21 ネットワーク テレメトリ 63

1 Progress Kemp LoadMaster 製品の紹介

1.1 LoadMaster 製品

機能豊富なアプリケーション デリバリー コントローラーとサーバー ロード バランサー アプライアンスの Kemp LoadMaster ファミリーは、ユーザー トラフィックとアプリケーションを自動的かつインテリジェントに管理し、あらゆる規模の企業とマネージド サービス プロバイダーに Web サイトの整合性を提供します。 Kemp 製品は、IT コストを合理化しながら、高可用性、高性能、柔軟なスケーラビリティ、管理の容易さ、安全な運用によって定義される Web インフラストラクチャを最適化します。

LoadMaster は、ネットワーク化されたリソースの管理を簡素化し、さまざまなサーバー、コンテンツ、およびトランザクション ベースのシステムへのユーザー アクセスを最適化および高速化します。多くの組織にとって、会社の Web サイトまたはイントラネットにアクセスでき、安全で継続的に運用できるようにすることは非常に重要です。 Kemp の強力な Application Delivery Controller (ADC) またはロード バランサーを使用すると、Web サーバーのパフォーマンスを大幅に向上させ、コストを削減し、顧客の Web エクスペリエンスを向上させる、高価値で信頼性の高いインフラストラクチャ アプライアンスをビジネスに提供できます。

1.2 LoadMaster ロードバランサの機能

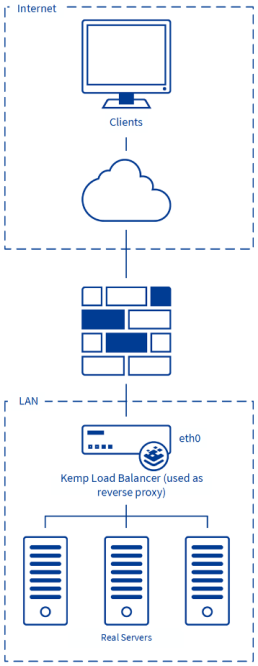
LoadMaster Application Delivery Controller (ADC) は、LoadMaster オペレーティング ソフトウェアと Web ユーザー インターフェイス (WUI) で次の機能を提供します。

- バランス方法
- 持続性
- アプリケーション フロント エンド
- SSL アクセラレーション/オフロード
- ルールベースのコンテンツ スイッチング
- ヘルスチェック
- SNMP サポート
- ユーザー管理
- IPv6 サポート
- ボンディングと VLAN

- エッジ セキュリティ

2 LoadMaster ネットワーク トポロジ

2.1 One-Armed バランサー



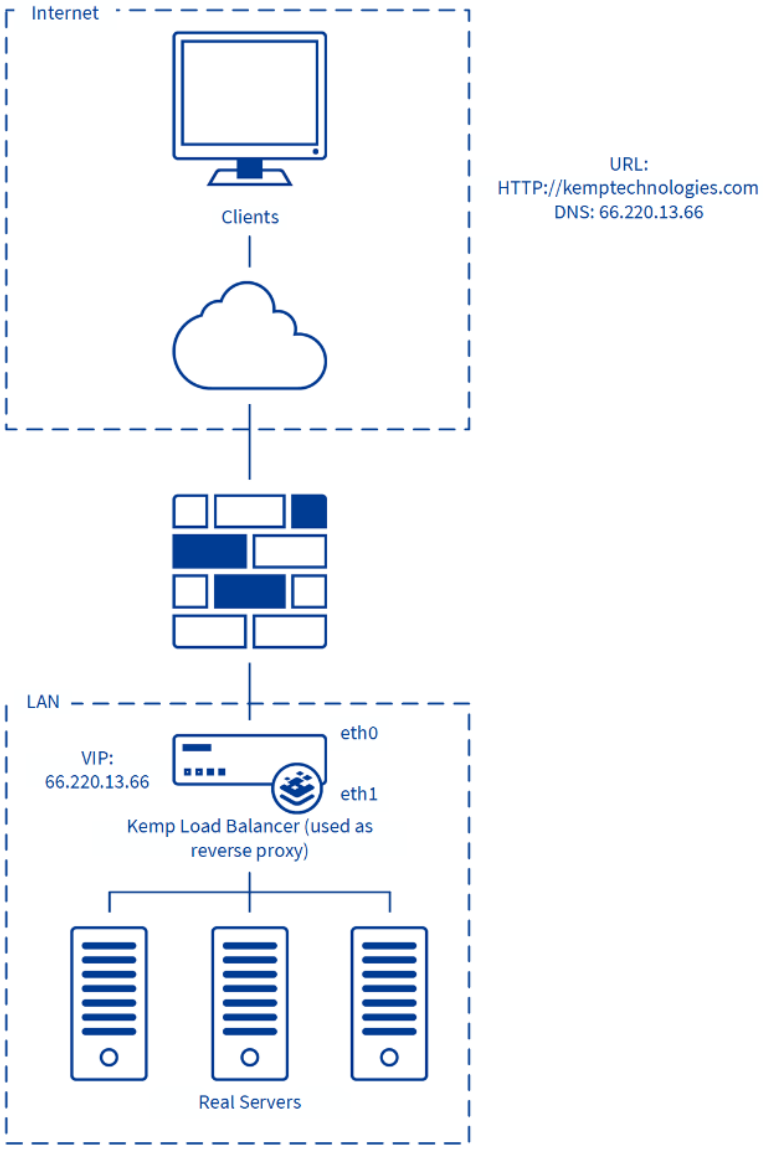
ワンアーム構成が選択されている場合、次のことが当てはまります。

- eth0 イーサネット インターフェイスのみが使用されます (インバウンド トラフィックとアウトバウンド トラフィックの両方に)
- Real Server と仮想サービスは同じ論理ネットワーク (フラットベースと呼ばれることもあります) の一部になります。これは、インターネット内のサービスに使用される場合、両方がパブリック IP アドレスを持つことを意味します。
- Server NAT は、ワンアーム構成には意味がありません。
- Real Server での Direct Server Return (DSR) メソッドの使用を自動的に意味するものではありません
- クライアントが DSR 構成の LoadMaster と同じ論理ネットワーク上にある場合、IP アドレス透過性は適切に機能します。 クライアントが NAT 構成の LoadMaster と同じ論理ネットワーク上にある場合、IP アドレスの透過性はサポートされません。

One-Armed ソリューションは、シングル構成と HA 構成の両方でセットアップできます。

2.2 Two-Armed バランサー

2 つのアームを持つ LoadMaster サイトの例は、次のようになります。



システムは次のように構成されています。

- LoadMaster 上に、HTTP サービス用の 66.220.13.66 の IP アドレスを持つ仮想サービスが作成されました。
- 仮想サービスは、実サーバー (サーバー 1、2、および 3) 間で受信トラフィックのバランスを取るように構成されています。

- ユーザーが URL http://www.kemptechnologies.com をリクエストします。URL は DNS によって IP アドレス 66.220.13.66 に解決されます。
- リクエストは LoadMaster にルーティングされ、LoadMaster はこの IP アドレスをネットワーク インターフェイス eth0 の IP エイリアスとして提供します。
- LoadMaster は、ネットワーク インターフェイス eth1 を使用してサーバー ファーム サブネット 10.0.0.0 に接続されています。
- LoadMaster は、要求されたアドレス 66.220.13.66 に割り当てられ、必要なコンテンツを配信できる 3 つの実サーバーがこのサブネットにあることを認識しています。
- LoadMaster は、構成された負荷分散方法 (重み付きラウンド ロビンなど) を使用して、3 つの実サーバーのいずれかに要求を送信します。
- Two-Armed 構成に関するその他の注意事項は次のとおりです。
  - eth0 (ネット側) と eth1 (ファーム側) の両方のインターフェイスが使用されます。追加のポートは、マルチアーム構成のためにファーム側に接続されます
  - LoadMaster (eth0) とサーバー ファームが別々の論理ネットワーク上にあることを意味します。NAT ベースのトポロジーと呼ばれることもあります。
  - サーバー ファームは、ルーティング不可能な (RFC1918) IP アドレスを使用する場合があります。
  - サーバー NAT は、このような構成で役立つ場合があります
  - クライアントが NAT (共通) および DSR (非共通) 構成の両方で LoadMaster と同じ論理ネットワーク上にある場合、IP アドレス透過性は適切に機能します。
  - 仮想サービスは、任意のイーサネット インターフェイスで作成できます。

1 つのポートを活用し、「Additional Subnet」機能を構成すると、Two-Armed と見なされます。

2.3 高可用性 (HA) 構成

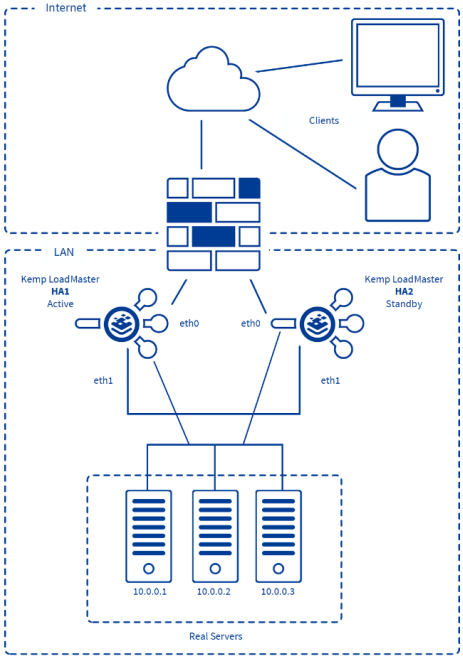
LoadMaster の高可用性機能により、サーバー ファームの可用性が保証されます。 HA は、ホットスタンバイのフェールオーバー メカニズムによって実現されます。 2 つの同一の LoadMaster ユニットが、クラスターとしてネットワークに統合されています。 1 台のマシンがアクティブな LoadMaster として機能し、2 台目のマシンはスタンバイのアイドル状態のままで、常にアクティブなサーバーからアクティビティを引き継ぐ準備ができています。これ
クラスターは、インターネット側およびサーバー ファーム側の接続からは単一の論理ユニットとして表示されます。 HA クラスターでは、各ネットワーク インターフェイスに個別の IP アドレスと 1

つの共有 IP アドレスがあります。

パートナーユニットと共有されます。共有 IP アドレスは両方の LoadMaster アプライアンスで同一ですが、常にアクティブな LoadMaster にのみ関連付けられます。 LoadMaster がサーバーのデフォルト ゲートウェイとして設定されている場合は、HA ペアの共有アドレスを使用することを忘れないでください。このアドレスは常に使用できるからです。

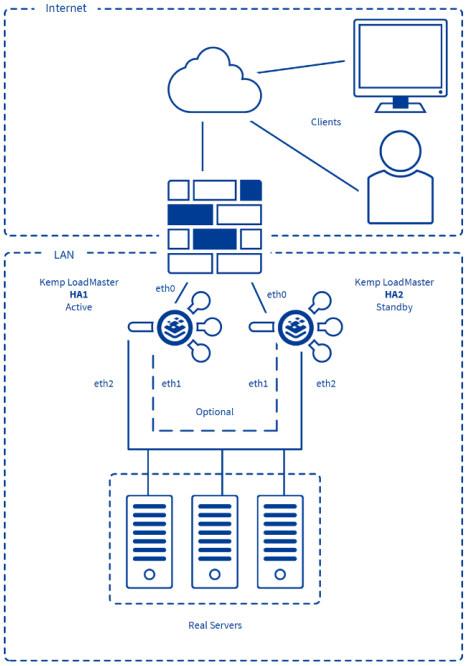
通常の動作中、各ノードは eth0 および eth1 接続を介してヘルス チェック メッセージを定期的に送信し、ピア アプライアンスの可用性を確認します。明示的に無効にされていない限り、ヘルスチェックは有効になっています。アクティブな LoadMaster に障害が発生した場合、スタンバイ アプライアンスがアクティブになり、バランシングのタスクを引き継ぎます。

HA シングル アームのトポロジーは次のようになります。



LoadMaster HA1 と HA2 は eth0 を使用してネットワーク (ファイアウォール) とサーバーに接続し、2 つのポート間で 1 つの共有 IP アドレスを持ちます。 さらに、各ユニットの eth1 はパッチケーブルを使用して直接接続されます。ポートは自動検出されるため、ケーブルがストレートかリバースかに関係なく、追加の HA ヘルス チェック専用に使用されます。 eth0 での HA チェックが何らかの理由で中断された場合に、マスター間の状況を防ぐために、eth1 に直接接続リンクをセットアップすることが重要です。

HA デュアル アームのトポロジーは次のようになります。



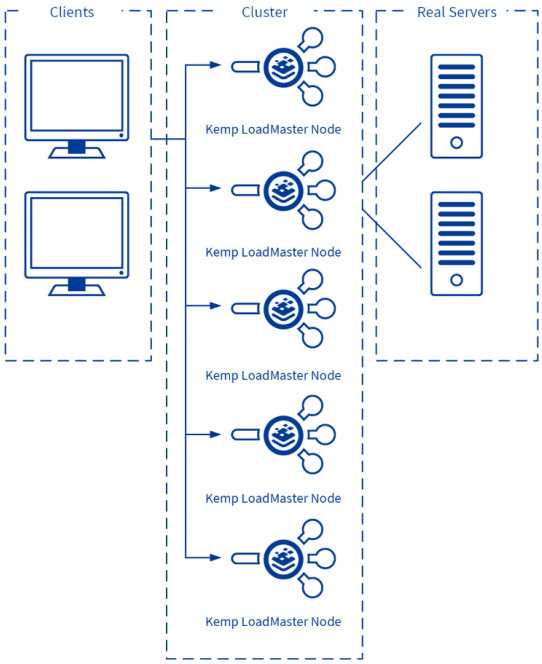
HA1 と HA2 は両方とも eth0 を使用してネットワーク (ファイアウォール) に接続し、eth2 をサーバーへの接続に使用します。 2 つの eth0 ポートには 1 つの共有 IP アドレスがあり、2 つの eth2 ポートには別の共有 IP アドレスがあります。 2 つの LoadMaster 間のヘルス チェックは、両方の eth ポート間で行われます。 必要に応じて、各ユニットの eth1 をパッチ ケーブルを使用して直接接続して、HA ヘルス チェックを追加することもできますが、HA ペア間には既に 2 つのヘルス チェック ルートがあるため、まったく不要です。

HA1 と HA2 は、同じデフォルト ゲートウェイを持つ同じサブネット上にあり、同じ物理サイト内に配置されている必要があります。 サイト内リンクでそれらを分離してはならず、同じゲートウェイを使用してトラフィックを返す必要があります。
複数のサブネットにまたがる HA を実行すると、それらの間のリンクに障害が発生した場合にハードウェアの冗長性が提供されません。 複数のサイト間のトラフィック バランシングが必要な場合は、GEO LoadMaster が正しいソリューションです。 この Progress Kemp の DNS ベースのアプライアンスは、サイトの停止を回避するためにヘルス チェックを採用しています。

2.4 クラスタリング

クラスタリングには、各ノードがアクティブにトラフィックを渡す単一の管理および制御ドメインとして、複数の LoadMaster インスタンス (ノード) を展開することが含まれます。これらのノードのい

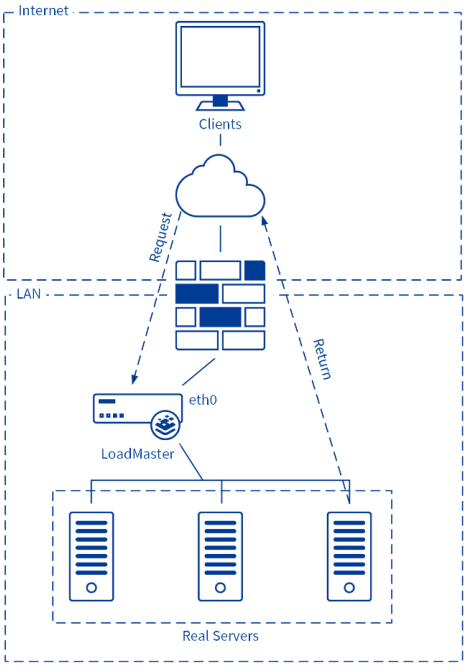
ずれかに障害が発生した場合、残りのノードは引き続きリモート クライアントにサービスを提供し、回復力を提供します。クラスタリングはスケーリングをサポートします - LoadMaster ノードをクラスタに追加またはクラスタから削除できるため、ビジネス要件に合わせて容量を動的に調整できます。クラスタにロードマスター ノードを追加するたびに、スループットとパフォーマンスが直線的に向上します。クラスターに追加できるノードの最大数は、ご使用条件によって定義されます。ユースケクラスターとしては、休暇期間中に Web サイトのトラフィックが通常よりも多くなり、トラフィック量を事前に予測できない場合、多くの場合、急増するこれらのリクエストを処理するためにキャパシティーが過剰にプロビジョニングされます。最も簡単な解決策の 1 つは、LoadMaster をクラスターに展開し、容量要件 (同時接続とパフォーマンス要件) の増加に応じて新しいノードを追加することです。



LoadMaster クラスタリングを使用すると、同じ仮想サービスに LoadMaster を追加することで、必要に応じて負荷分散機能を拡張できます。 障害が発生したノードに向けられたトラフィックは、既存のノードに渡されるか、残りのノード間で負荷分散されます。 LoadMaster はすべて並行して動作します。 LoadMaster ノードに障害が発生した場合、トラフィックは残りのノード間で再分配されます。 各 LoadMaster でヘルスチェックが実行されます。 ほとんどの管理上の変更は、共有 IP アドレス インターフェイスで行う必要があります。 これらの変更は、1 秒もかからずに LoadMaster に反映されます。 ユニットの WUI に直接アクセスして、個々の LoadMaster のローカル管理を実行することもできます。 ローカル LoadMaster の WUI には、限られた構成オプションが含まれています。 クラスタリングの詳細については、LoadMaster クラスタリング、機能の説明を参照してくだ

さい。

2.5 Direct Server Return – DSR 構成例



1. LoadMaster によってインターセプトされた受信リクエスト
2. サーバー 1 にルーティング
3. サーバー 1 からの応答
4. LoadMaster なしでクライアントに直接応答

この機能は、実サーバーが LoadMaster を介さずにクライアントに直接応答する必要がある場合にのみ実装する必要があります。この構成では、ロードマスターと並行してルーターを追加するなど、ロードマスターを経由しないクライアントへのパスが Real Server に必要です。 DSR 構成でサポートされる永続化オプションは、ソース IP のみです。 DSR では、レイヤー 7/アプリケーション機能は使用できません。また、DSR は One-Armed 構成でのみ使用できます。Two-Armed ソリューションのループバック インターフェイスを使用するリアル サーバーでルーティングの問題が発生するためです。

DSR は、MAT (MAC アドレス変換) と変更されたリアル サーバー構成の組み合わせを使用します。RS は通常どおり IP アドレスで構成されますが、VIP の IP アドレスも与えられます。通常、同じ IP アドレスを持つネットワーク上に 2 台のマシンを配置することはできません。これを回避するには、サーバーが VIP アドレスでの ARP 要求に応答しないように、Real Server の VIP アドレスを

構成する必要があります。Real Server (Linux と Windows の両方) を構成する方法の詳細については、DSR 用の実サーバーの構成、テクニカル ノート ドキュメントを参照してください。

3 スケジューリング方法

LoadMaster には、「スケジューリング方法」または「アルゴリズム」と呼ばれる負荷分散方法がいくつか用意されています。 これらについては、以下のセクションで説明します。

3.1 ラウンドロビン

この方法では、着信要求はサーバー ファーム (クラスター)、つまり使用可能なサーバー全体に順次分散されます。 この方法を選択した場合、仮想サービスに割り当てられたすべてのサーバーは、同様のリソース容量を持ち、同一のアプリケーションをホストする必要があります。 すべてのサーバーのパフォーマンスが同じか類似しており、同じ負荷を実行している場合は、ラウンド ロビンを選択します。 この前提条件の下では、ラウンド ロビン システムはシンプルで効果的な配布方法です。 ただし、サーバーの容量が異なる場合、ラウンド ロビン システムを使用すると、現在の問い合わせをまだ処理できていなくても、能力の低いサーバーが次の問い合わせを受信する可能性があります。 これにより、弱いサーバーが過負荷になる可能性があります。

3.2 加重ラウンドロビン

この方法は、単純なラウンド ロビンの弱点を補います。サーバーごとに事前に割り当てることができる静的な「重み付け」を考慮しながら、着信要求はクラスター全体に順次分散されます。 管理者は、サーバーに重みを付けて、使用可能なサーバーの容量を定義するだけです。 たとえば、最も効率的なサーバー A には重み 100 が与えられ、それよりはるかに強力でないサーバー (B) には重み 50 が与えられます。これは、サーバー B が最初の要求を受け取る前に、サーバー A が常に 2 つの連続した要求を受け取ることを意味します。

3.3 最小接続

どちらのラウンド ロビン方式も、システムが特定の時間内に維持されている接続の数を認識していないことを考慮していません。したがって、このサーバーのユーザーは接続をより長く維持するため、サーバー B がサーバー A よりも少ない接続を受け取るにもかかわらず、サーバー B が過負荷になる可

能性があります。これは、接続、つまりサーバーの負荷が累積することを意味します。この潜在的な問題は、「最小接続」方式で回避できます。リクエストは、すべてのサーバーが現在維持している接続に基づいて分散されます。アクティブな接続の数が最も少ないクラスター内のサーバーが、次の要求を自動的に受け取ります。基本的に、単純なラウンド ロビンと同じ原則がここで適用されます。仮想サービスに関連するサーバーは、理想的には同様のリソース容量を持つ必要があります。トラフィック レートが低い構成では、トラフィックのバランスが取れず、最初のサーバーが優先されることに注意してください。これは、すべてのサーバーが等しい場合、最初のサーバーが優先されるためです。最初のサーバーが継続的にアクティブなトラフィックを持つレベルにトラフィックが達するまで、最初のサーバーが常に選択されます。

3.3.1 最小接続遅延開始時間

最小接続と加重最小接続のどちらのスケジューリング方法でも、Real Server が最初にオンラインになるときに、接続数が最初に制限され、徐々に増加する期間を設定できます。 これにより、Real Server が起動時に接続のフラッドによって過負荷にならないようにするための「ランプアップ時間」が提供されます。 この値は、L7 構成画面で構成されます。

3.4 加重最小結合

サーバーのリソース容量が異なる場合は、「加重最小接続」方式の方が適しています。 管理者によって定義されたさまざまな重みとアクティブな接続の数を組み合わせることで、両方の利点を利用できるため、サーバーを非常にバランスよく使用できます。 これは、一般に、接続数とサーバーの重みの比率を使用するため、非常に公平な分散方法です。 比率が最も低いクラスター内のサーバーが、次の要求を自動的に受け取ります。 低トラフィック レートに関する最小接続数の警告がここにも適用されることに注意してください。

3.5 エージェントベースのアダプティブ バランシング

「リソースベース (アダプティブ)」スケジューリング方式では、仮想サービス内のすべての実サーバーを定期的にチェックして、実サーバーの可用性ステータスを単独のヘルスチェックよりも詳細に説明する整数値を確認します。 これにより、LoadMaster は負荷分散の決定を行う際に、より複雑なロジックを適用できます。 この方法を機能させるには、仮想サービス内の各 Real Server が、Real Server の可用性レベルを示す整数値を単純な ASCII テキスト ファイルに入力する必要があります。

たとえば、0 はサーバーがアイドル状態であることを示し、100 はサーバーが完全にロードされていることを示します。 LoadMaster は、整数を含むテキスト ファイルの HTTP GET 要求を使用して、Real Server から定期的にこのファイルを取得します。 このメソッドを強力にする利点の 1 つは、LoadMaster が特定のリターン コードに応答して特定のアクションを実行することです。 例えば：

- Real Server から報告された負荷が 0 を超える場合、スケジューリング アルゴリズムは、収集された負荷値から重み付け比率を計算し、それに従って接続を分散します。 そのため、サーバーの過剰な過負荷が発生した場合、重み付けはシステムによって透過的に再調整されます。 これは、使用可能なサーバーに異なる重みを割り当てることによって、より均等な分散が実現される加重ラウンド ロビン方式に似ています。
- サーバーから報告された負荷値が 0 の場合 (または LoadMaster が何らかの理由でサーバーから整数値の取得に失敗した場合)、LoadMaster は代表的なサンプル負荷分散を構築してサーバーの重みを変更することができません。 この場合、LoadMaster は一時的にラウンド ロビン選択方式に切り替わります。 Real Server がより大きな負荷値を返し始めて代表的なトラフィック サンプルを構築すると、ロードマスターは適応方式に戻ります。

負荷値を決定し、LoadMaster が取得できるようにそれをテキスト ファイルに配置する何らかの方法でリアル サーバーを構成するのは、管理者の責任です。 多くのお客様は、この目的のためにサーバー上で実行される「適応型エージェント スクリプト」を使用しています。 Real Server の可用性ステータスを LoadMaster に伝達するために使用される整数プロトコルの詳細については、Linux システムと Windows システムの両方の適応型エージェント スクリプトのサンプルに加えて、Progress Kemp のドキュメント ページにあるリソース ベースの Adaptive Server エージェントのテクニカル ノートの記述を参照してください。 .

3.6 リソースベース (SDN アダプティブ)

Kemp LoadMaster には、Software Defined Networking (SDN) コントローラで使用できる適応負荷分散テクノロジが含まれています。 従来のネットワークでは、ネットワーク パスのエンド ツー エンドの可視性がなく、アプリケーションが常に最適にルーティングされるとは限りません。 SDN コントローラー ソリューションと統合された LoadMaster は、重要なフロー パターン データを利用できるようにすることで、この問題を解決します。 LoadMaster は、Controller を使用してネットワーク内のスイッチからレイヤー 2/レイヤー 3 情報を取得します。 LoadMaster は、レイヤー 2/3 の情報をレイヤー 4/7 の情報と組み合わせて、より最適化されたトラフィック分散の決定を行いま

す。 LoadMaster を使用して、ネットワーク パスのエンド ツー エンドの可視性を提供し、サーバーおよびスイッチング インフラストラクチャ全体でアプリケーションのルーティングを最適化できます。 Kemp SDN ソリューションは、以下を可能にすることで効率を高めます。

- ネットワークに対するアプリケーションの可視性
- Application Delivery Controller (ADC) によって取得されるネットワーク データ
- アダプティブ ロード バランシング

適応スケジューリング方式を使用している仮想サービスは、制御システムと見なすことができます。その目的は、実サーバー上で均等に分散された負荷を実現することであり、コントローラーはこれからエラー値を計算します (これは、望ましい均等な分散からの偏差を表します)。 また、エラー値を減らす方法でシステムにフィードバックされる一連の制御値 (実サーバーの重み) も計算します。 SDN アダプティブ ロード バランシングの詳細については、SDN アダプティブ ロード バランシングの機能説明を参照してください。

3.7 固定加重

重みが最も高い Real server は、他の実サーバーに低い重み値が与えられている場合にのみ使用されます。 ただし、最も重み付けされたサーバーに障害が発生した場合は、次に優先度の高い番号を持つ実サーバーがクライアントにサービスを提供するために利用可能になります。 各 Real Server の重みは、Real Server 間の優先度に基づいて割り当てる必要があります。

3.8 加重応答時間

トラフィックは、加重ラウンド ロビン方式を使用してスケジュールされます。 加重ラウンド ロビン方式で使用される加重は、ヘルス チェック リクエストからの応答時間を使用して計算されます。 各ヘルスチェック リクエストは、応答にかかる時間を確認するために時間を計られます。 ヘルス チェックの速度はマシンの速度に依存するため、常にそうとは限らないことに注意してください。
仮想サービス上のすべての Real Server の合計応答時間が合計され、そこから個々の Real Server の重みが計算されます。 重みは、約 15 秒ごとに再計算されます。

3.9 ソース IP ハッシュ

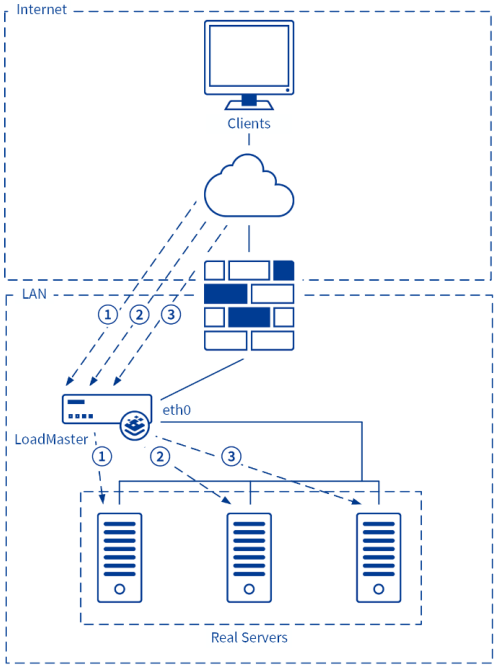
ソース IP のハッシュが生成され、正しい実サーバーを見つけるために使用されます。 これは、Real Server が同じホストから常に同じであることを意味します。 このスケジューリング方法では、送信

元 IP の永続性は必要ありません。 これにより、実際のサーバーの不均衡が発生する可能性があります。

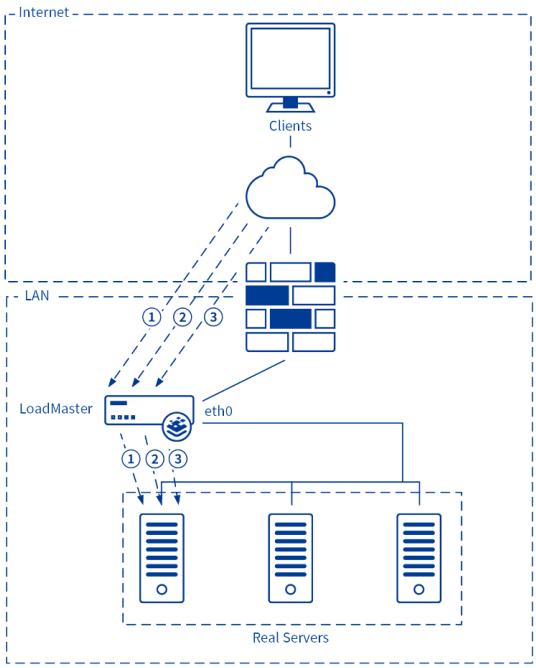
4 パーシステンス

4.1 パーシステンスの紹介

永続性（「アフィニティ」、「サーバー アフィニティ」、または「サーバー スティッキー」とも呼ばれる）は、個々のクライアントからのすべての要求をサーバー ファーム内の同じサーバーに送信できるようにするプロパティです。 パーシステンスはデフォルトではオンになっていませんが、仮想サービスごとに構成可能なオプションです。 パーシステンスがない場合、LoadMaster は、ラウンドロビン、加重ラウンドロビンなどの負荷分散アルゴリズムに従ってトラフィックを転送します（下の図）。



パーシステンスを使用すると、LoadMaster は負荷分散アルゴリズムに従って新しい接続を送信しますが、返される接続は同じサーバーに送信されます（下の図）。



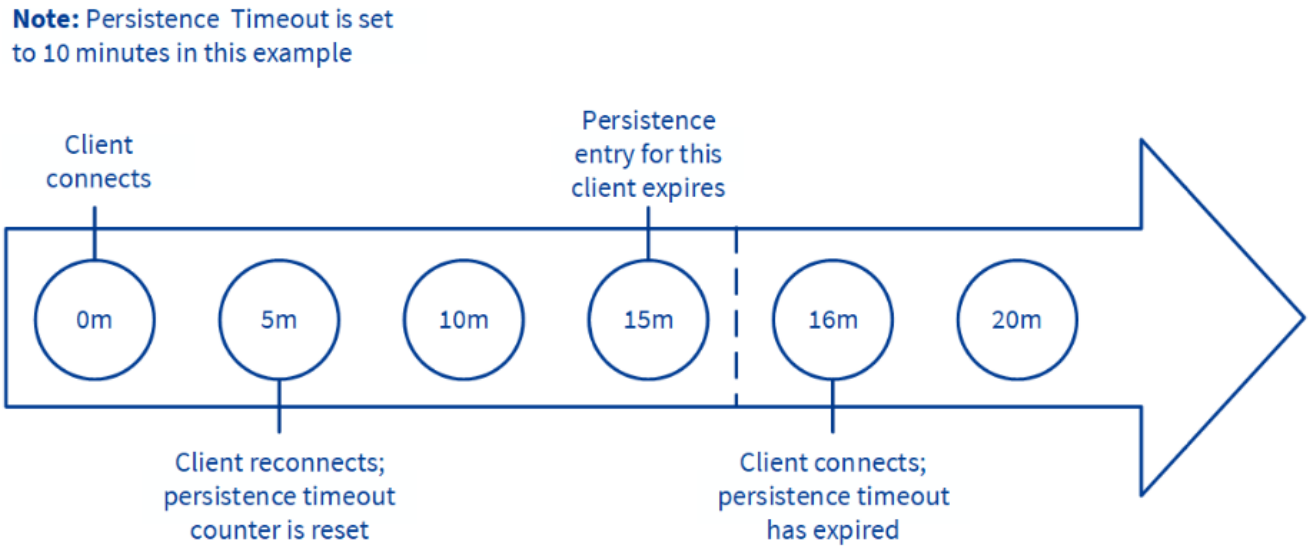
4.2 パーシステンスが必要かどうかを知る方法は?

使用しているサイトがインタラクティブなサイトである場合、おそらくパーシステンスが必要になります。 これは、ある種のログインを必要とするサイトに特に当てはまります。 実行しているサイトが静的で、静的なテキストと画像のみを提供している場合、持続性は必要ないかもしれません。 ほとんどの場合、必要がない場合でも、持続性が害になることはありません。 多くの Web サイト プログラミング言語 (ASP、PHP など) のセッション処理メカニズムは、「ステートフル」として知られています。 ユーザーに対して確立された一意のセッションがあり、その「状態」は同じサーバーに保持されます。 このステートフルな情報には、ログイン資格情報からショッピング カートの内容まですべてが含まれる可能性があり、通常、サーバー間で共有されることはありません。 そのため、複数のサーバーを使用する場合、相互作用の間、個々のユーザーを特定の Web サーバーに関連付けておくことが重要であり、それがパーシステンスの出番です。

4.3 タイムアウト

パーシステンス方法ごとに、各ユーザーの永続化が受け入れられる期間を決定する構成可能なタイムアウト値があり、1 分から 28 日まで選択できます。 このタイムアウト クロックは、最初の接続が確立されたときに開始されます。 持続タイムアウト
クライアントがタイムアウト期間内に再接続すると、値が更新されます。 たとえば、持続タイムアウ

トが 1 時間に設定されていて、クライアントが午後 2 時に接続を開始した場合、クライアントが切断して午後 3 時前に再接続した場合でも、クライアントは同じ実サーバーに持続します。 また、これを反映するためにパーシステンスレコードが更新され、このクライアントのパーシステンスカウントダウン タイマーが 1 時間にリセットされます。



クライアントがタイムアウト期間内に繰り返し仮想サービスに接続した場合、永続性は無期限に尊重されます。 たとえば、次のシナリオがあるとします。

- 持続タイムアウトは 10 分に設定されています
- ユーザーは 20 分間に複数の要求を行いますが、接続間の時間は常に 1 分未満です

要求は、利用可能な (つまり、ヘルスチェックに合格している) 限り、正しい実サーバーに送信する必要があります。 ユーザーが 20 分間アイドル状態になると、次の接続は新しいセッションとしてカウントされ、スケジュールに応じて別のサーバーに送信される場合があります。 接続が 10 分以上開かれ、クライアントが切断して再接続した場合、パーシステンスレコードは期限切れになり、LoadMaster はそのクライアントの新しい永続エントリを作成し、場合によってはクライアントを新しい Real Server に送信します。 これは、接続の終了時ではなく、接続が確立されると持続カウントダウンが開始されるためです。 持続性の問題が発生している場合は、持続性タイムアウトが十分に長くないことが原因である可能性があります。 これが十分な長さでない場合は、タイムアウト値をより大きな値に設定する必要があります。 一般に、この値をサーバーのタイムアウト値と一致させることをお勧めします。

4.4 レイヤ 7 のパーシステンス化方法

これらは、IP アドレスとポートの先を見て、レイヤー 7 のパーシステンスを実現するためのさまざまなオプションを提供する方法です。

4.4.1 サーバー Cookie のパーシステンス

サーバー Cookie オプションは、サーバーから生成された既存の Cookie を使用してユーザーを送信するサーバーを決定するレイヤー 7 機能です。 LoadMaster は Cookie を生成または管理せず、HTTP ストリーム内の Cookie のみを監視するため、このメソッドは「パッシブ Cookie」と呼ばれることがあります。 サーバー Cookie パーシステンスでは、LoadMaster が参照する Cookie を認識できるように、Cookie 名オプションを設定する必要があります。 サーバー Cookie の永続性が最適に機能するためには、サーバーによって生成される Cookie が個々のユーザーごとに一意の値を持つ必要があります。

4.4.2 アクティブ Cookie のパーシステンス

アクティブ Cookie メソッドは、前のメソッドと同様に Cookie を使用するレイヤー 7 の機能ですが、アクティブ Cookie を使用すると、Cookie はサーバーではなく LoadMaster によって生成されます。アクティブ Cookie が設定された LoadMaster 仮想サービスに接続が入ると、LoadMaster は特定の Cookie を探します。その Cookie が存在しない場合、LoadMaster は Set-Cookie ディレクティブを使用して HTTP ストリームに挿入します。既存の Cookie は影響を受けません。サーバー Cookie パーシステンス方式と同様に、LoadMaster が生成した Cookie の値は各ユーザーに固有であるため、LoadMaster はユーザーを区別できます。この方法の利点は、サーバーによって Cookie を管理または生成する必要がないため、サーバー構成の負担が軽減されることです。クライアント接続ごとの分散を改善するには、L7 構成で「Add Port to Active Cookie」機能を有効にします。アクティブ Cookie 永続性を使用すると、Cookie はセッションの間、または永続時間が期限切れになるまで有効です。たとえば、持続タイムアウトを 10 分に設定してアクティブ Cookie 持続を使用し、クライアントが午後 2 時に接続し、その後切断して午後 2 時 5 分に再接続した場合、持続タイムアウト値がリセットされます。パーシステンスタイムアウトの期限が切れた後にクライアントが仮想サービスに接続しようとすると、古い Cookie が提示されます。 LoadMaster はパーシステンステーブルをチェックし、有効なエントリがないことを確認します。その後、LoadMaster はクライアント用の新し

い Cookie を生成し、持続性テーブルを更新します。

4.4.3 サーバー Cookie またはソース IP パーシステンス

サーバー Cookie または送信元 IP の設定は、サーバー Cookie の設定と同じですが、送信元 IP アドレスのフォールバック方法が追加されています。 何らかの理由で、期待される Cookie が存在しない場合 (これは、クライアント ブラウザーが Cookie を拒否するように構成されている場合に発生する可能性があります)、パーシステンスを判断するためにソース IP アドレスが使用されます。

4.4.4 アクティブな Cookie またはソース IP のパーシステンス

アクティブ Cookie またはソース IP の設定は、アクティブ Cookie の持続性と同じです。 何らかの理由で、期待される Cookie が存在しない場合は、ソース IP アドレスを使用して持続性を判断します。 すべての条件が同じであれば、レイヤ 7 のパーシステンスを使用する場合は、これが推奨される方法です。 サーバーでの設定は不要で、LoadMaster はパーシステンス関連のすべての Cookie を管理し、Cookie がクライアントによって拒否された場合はソース IP アドレスにフォールバックします。

4.4.5 すべての Cookie のパーシステンスをハッシュ

Hash All Cookies メソッドは、HTTP ストリーム内のすべての Cookie の値のハッシュを作成します。 リクエストごとに同じ値の Cookie が同じサーバーに送信されます。 値が変更された場合、接続は新しい接続として扱われます。 クライアントは、負荷分散アルゴリズムに従ってサーバーに割り当てられます。

4.4.6 すべての Cookie またはソース IP パーシステンスをハッシュする

Hash All Cookies または Source IP は、Hash All Cookies と同じですが、HTTP 文字列に Cookie がない場合に Source IP パーシステンスにフォールバックするという追加機能があります。

4.4.7 ソース IP アドレスのパーシステンス

ソース IP アドレスのパーシステンスでは、着信要求のソース IP アドレスを使用してユーザーを区別します。 これはパーシステンスの最も簡単な方法であり、HTTP に関連しないプロトコルを含むすべての TCP プロトコルで機能します。 ソース IP アドレスの永続性は、コンテンツ スイッチングまた

は Direct Server Return 展開と組み合わせて使用できる唯一のパーシステンスオプションです。

4.4.7.1 送信元 IP アドレスの弱点

ソース IP のパーシステンスが望ましくない場合や、パーシステンスを適切に維持する上で効果がない場合もあります。 これらの状況は次のとおりです。

- 多くの (またはすべての) ユーザーが単一の IP アドレスから来ているように見える場合
- ユーザーが IP アドレスを切り替えるとき

最初のケースは、かなりの数のユーザー要求が単一のプロキシを通過し、単一の IP から送信されたように見える場合によく発生します。ソース IP パーシステンスを使用すると、これらのすべてのユーザーが 1 人のユーザーとして表示されることになります。これが発生するもう 1 つの原因は、すべてのクライアント要求が 1 つのオフィスからインターネット経由で送信された場合です。通常、オフィス ルーターはすべてのオフィス システムを 1 つの IP アドレスに NAT 変換するため、すべてのユーザーとすべての要求が 1 人のユーザーのように見えます。これにより、ロード バランシングが不均一になる可能性があります。これは、到着した新しいユーザー セッションがすべて同じ実サーバーに転送され、バランスがとれないためです。 2 番目のケースは、AOL や Earthlink などの一部のメガインターネット サービス プロバイダー (ISP) のプロキシ サーバーに関係する、主に歴史的な問題です。場合によっては、プロキシ構成またはネットワークの問題により、IP アドレスが時々切り替わることがあります。 IP アドレスが変更されると、ユーザーは SRC パーシステンスに対して別のユーザーとして表示されます。これらのケースのそれぞれで、レイヤー 7 の永続性は、送信元の IP に関係なく、問題を解決します。ただし、これは HTTP プロトコル (およびセッションが LoadMaster で終了する場合は HTTPS/SSL) でのみ機能します。

4.4.8 スーパーHTTP

Super HTTP パーシステンスは、クライアント ブラウザの一意のフィンガープリントを作成することで機能し、そのフィンガープリントを使用して正しい Real Server への接続を維持します。 フィンガープリントは、User-Agent フィールドと、存在する場合は Authorization ヘッダーの値を組み合わせたものに基づいています。 同じヘッダーの組み合わせを持つ接続は、同じ実サーバーに送り返されます。

4.4.9 URL ハッシュ

URL ハッシュの永続性により、LoadMaster は同じ URL を持つリクエストを同じサーバーに送信し

ます。

4.4.10 HTTP ホスト ヘッダー

HTTP Host ヘッダーの永続性により、LoadMaster は HTTP Host: ヘッダーに同じ値を含むすべてのリクエストを同じサーバーに送信します。

4.4.11 HTTP クエリ アイテムのハッシュ

このメソッドは、検査される名前付きアイテムが URL のクエリ文字列内のクエリ アイテムであることを操作します。 同じクエリ アイテム値を持つすべてのクエリは、同じサーバーに送信されます。

4.4.12 選択されたヘッダー

選択されたヘッダーのパーシステンスにより、LoadMaster は、指定されたヘッダーに同じ値を含むすべてのリクエストを同じサーバーに送信します。

4.4.13 SSL セッション ID

SSL セッション ID は、SSL サービスがオフロードされていない場合でも使用できるパーシステンス方法です。 これは、クライアントが完全なユーザー セッションに対して同じ SSL セッション ID を維持することに依存しています。 これに対するブラウザのサポートはむらがあります。 そのため、これを HTTPS サービスで使用することはお勧めしません。 このパーシステンス方式を利用するには、サービス タイプを Generic に設定する必要があります。 SSL セッション ID は、仮想サービスのサービス タイプが汎用であり、SSL アクセラレーションが無効になっている場合にのみ、パーシステンスモードとして使用できます。

4.4.14 UDP セッション開始プロトコル (SIP)

このパーシステンスモードは、Force L4 が無効になっている場合に UDP 仮想サービスでのみ使用できます。 SIP は、HTTP と同様に、要求と応答のトランザクションを使用します。 多数のヘッダー フィールドを含む最初の INVITE 要求が送信されます。 これらのヘッダー フィールドはパーシステンスに使用できます。 LoadMaster でこのモードを選択すると、[Header filed name] というテキスト ボックスが表示されます。 パーシステンス情報のベースとして使用されるヘッダー フィールドをここに入力する必要があります。

4.5 パーシステンスと HTTPS/SSL

HTTPS/SSL では、考慮すべき点がいくつかあります。 LoadMaster で SSL セッションを終了しない場合、唯一のオプションはソース IP アドレスのパーシステンスまたは SSL セッション ID のパーシステンスです。 ストリームは非終了セッションで暗号化されるため、LoadMaster は HTTP ヘッダーやその他のレイヤー 7 情報を見ることができません。 LoadMaster で HTTPS/SSL セッションを終了する場合は、LoadMaster のパーシステンスオプションのいずれかを使用できます。
HTTPS/SSL セッションが終了しているため、LoadMaster は暗号化されていないすべてのトラフィックを認識し、HTTP ストリームを確認できます。 これは、ロードマスターで HTTPS/SSL セッションを終了し、リアル サーバーとの SSL セッションを再確立する場合にも当てはまります。

4.6 ポートフォローイング

ユーザーがアイテムを選択してリストに追加する「shopping card」のようなサービスを使用する場合、以前のタイプのパーシステンスを使用できます。 ユーザーがアイテムの支払いを決定すると、これは通常、安全な SSL (https) サービスを使用して実行されます。 ポート フォローイングがオンになっている場合、「shopping cart」接続がアクティブな実サーバーが SSL セッション用に選択されます。 この選択は、(送信元 IP アドレスによって決定される) 同じクライアントからの接続がまだ開かれている場合、および SSL サービスが「shopping cart」サービスと同じ IP アドレスを持っている場合にのみ発生します。 たとえば、www.somewebsite.com の HTTP サービスに接続し、同じアドレスに新しい SSL 接続を確立すると、SSL セッションは元の HTTP サービスと同じ Real Servr に転送されます。 必要に応じて、UDP 接続と TCP 接続の間でポートの追跡を行うことができます。

5 アプリケーション フロント エンド

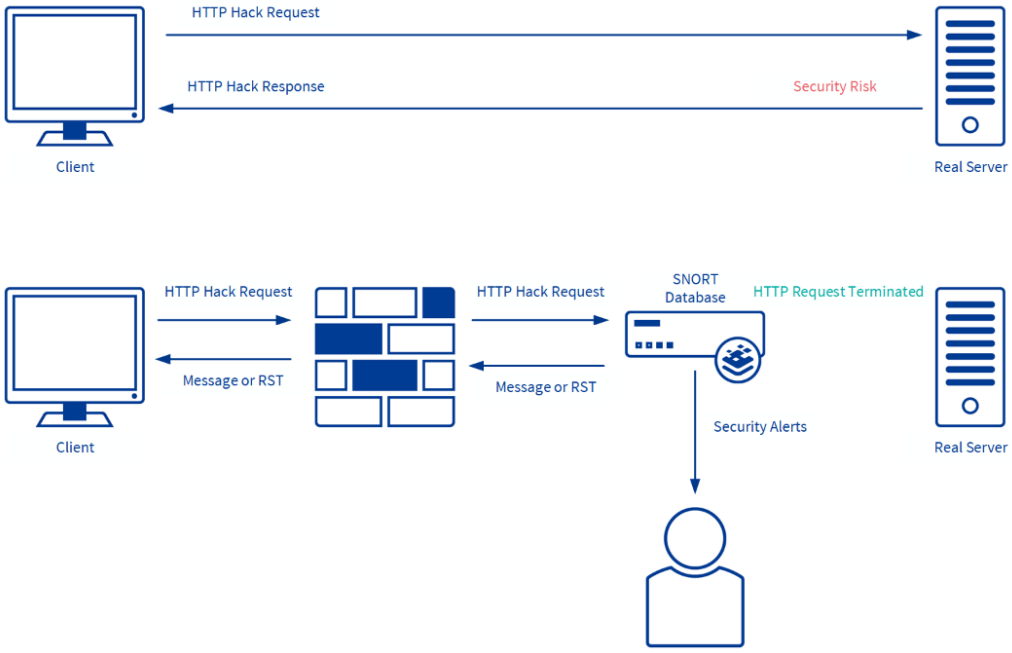
アプリケーション フロント エンドは、Web アプリケーションの配信とネットワークの最適化を中心に展開する一連の機能です。 LoadMaster Application Front-End Services (AFE) の導入により、帯域幅とサーバーの使用率が向上すると同時に、LoadMaster が展開と管理が容易な透過的な負荷分散アプライアンスであり続けることで、非常に重要な要件が解決されます。 LoadMaster AFE サービスには以下が含まれます。

- 侵入防止システム (IPS)
- キャッシング

- データ圧縮

各機能は、Web 仮想サービスごとに展開できます。 AFE 機能はライセンス ベースです。 これらの機能がなく、必要な場合は、Progress Kemp の販売担当者にお問い合わせください。

5.1 侵入防止システム



LoadMaster は、HTTP 侵入防止機能を備えた確立された堅牢なインターネット アプライアンスです。 LoadMaster が提供する Secure Socket Layer (SSL)、DoS サポートに加えて、侵入防止システム (IPS) サービスは、攻撃をリアルタイムで軽減し、サーバーを分離することにより、Real Server のインライン保護を提供します。 実サーバー。 侵入防止は、業界標準の SNORT データベースに基づいており、リアルタイムの侵入アラートを提供します。 LoadMaster は、バージョン 2.9 以下の SNORT ルールをサポートしています。 IPS は、HTTP およびオフロードされた HTTPS 仮想サービスで使用できます。

5.1.1 侵入処理

SNORT ルールに一致する要求の処理には、ドロップ接続または送信拒否の 2 つのオプションがあります。 どちらのオプションも、要求が Real Server に到達するのを防ぎます。 このオプションは、悪意のあるリクエストを送信したクライアントに返されるレスポンスを構成します。

5.1.1.1 ドロップ接続侵入処理

ルールが一致しても、HTTP 応答は生成されません。 TCP 接続は終了します。HTML コンテンツはクライアントに配信されません。

5.1.1.2 送信 拒否 侵入処理

ルールが一致すると、クライアントへの応答が HTTP 400「Invalid Request」に設定され、対応するエクスプロイト ノートが HTML ドキュメントでクライアントに配信されます。
サンプル リクエスト: http://<VIP>/modules/articles/index.php?cat_id=SQL
サンプル応答: <html><head><title>400 Invalid Request</title></head><body>Invalid Request: COMMUNITY WEB-PHP Xoops module Articles SQL Injection Exploit</body>

5.1.2 検出レベル

ルール マッチングの積極性は、SNORT 優先度レベルに従ってアプライアンスに対してグローバルに設定できます。詳細は http://www.snort.org/docs/ で入手できます。

- 低 = 拒否せずにロギングのみ
- デフォルト = 優先度 1 (高) ルールはブロックされ、それ以外はすべてログに記録されます
- 高 = 優先度 1 (高) および 2 (中) のルールはブロックされ、それ以外はすべてログに記録されます
- Paranoid = すべての優先レベルがブロックされ、ログに記録されます

5.1.3 警告

IPS システムは悪意のある接続をすべて破棄しますが、必ずしも危険ではなく、何かが間違っている可能性があることを示す要求がいくつかあります。 これらはブロックされず、デフォルトではログに記録されません。WARNING オプションをオンにすると、これらの要求のログが許可されます。
危険でない操作の例は、snort ルール ファイルでその他のアクティビティとして指定されている要求です。
URI: "/OvCgi/OpenView5.exe?Context=Snmp&Action=Snmp&Host=&Oid="
これは「WEB-MISC HP OpenView Manager DOS」と記載されており、疑わしいだけです。

5.1.4 侵入アラート

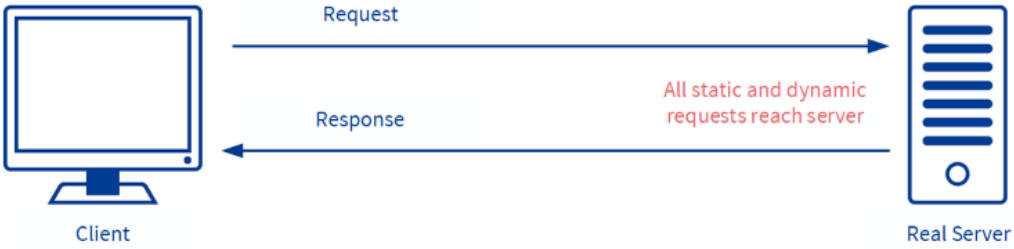
すべての侵入アラートは、システム ログと警告ログに記録されます。 アラート通知は syslog 機能でも取得できます。最小レベルは Notice Host であり、電子メール アラート機能は最小レベルが Notice Recipient です。 記録保持のために、侵入アラートなどの重要なシステム メッセージを syslog 機能で記録することをお勧めします。

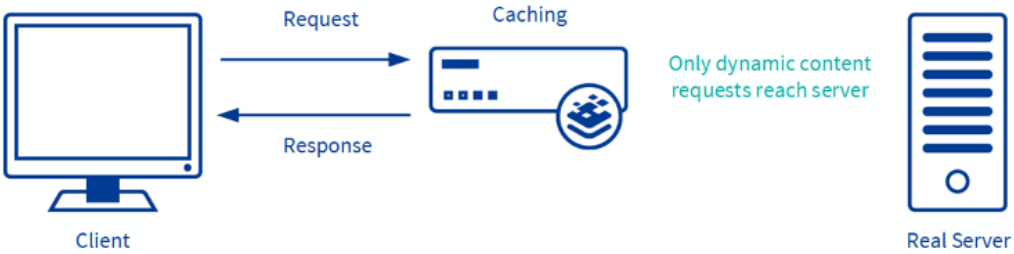
5.1.5 IPS ルールの更新

ルールは www.snort.org からダウンロードできます。 新しいルール セットを取得または作成したら、WUI を使用し、[System Configuration] > [Miscellaneous Options] > [AFE Configuration] に移動して、ルール セットをロードできます。 [Choose File] ボタンを使用して、ダウンロードしたコミュニティ ルール ファイルを選択し、[Install new Rules] をクリックします。 コミュニティ ルール ファイルは、拡張子 tar.gz で終わり、「communityrules」という名前のディレクトリを含む Tar および Gzip ファイルにエンコードする必要があります。LoadMaster はこのファイルを解凍し、新しいルール ファイルを再ロードします (tar.gz は標準です www.snort.org からルールをダウンロードするための形式)。 新しい規則ファイルをインストールすると、現在の規則が置き換えられます。 LoadMaster は、デフォルトで General Public License (GPL) に基づくコミュニティ ルールと共に出荷されます。

5.2 キャッシング

LoadMaster の高度なキャッシング エンジンは、重要なコア ビジネス アプリケーション ロジックの実行に専念できる貴重な Real Server の処理能力と帯域幅を節約します。 キャッシュを実装すると、サーバーのパフォーマンスが大幅に向上します。 HTTP などの会話プロトコルでは、静的リソースをフェッチするために接続を頻繁に作成および閉じる必要があり、Real Server とネットワークで不要なリソース使用率が発生します。 LoadMaster キャッシングを有効にすることで、接続関連のリソースをより関連性の高いビジネス ロジックに転用できます。 LoadMaster キャッシングを導入することで、Real Server への Web トラフィックを大幅に削減し、Real Server の前の帯域幅を節約することもできます。





キャッシングは、HTTP およびオフロードされた HTTPS 仮想サービスで利用できます。 RFC 2616 に従って、no-cache ヘッダーを含む HTTP/HTTPS リクエストはキャッシュをバイパスします。キャッシュは遅延方式で満たされます。静的コンテンツがキャッシュされるまで数秒お待ちください。 RFC 2616 に従って、クエリ文字列 (rel_path 部分に疑問符記号 (?) を含むもの) を含む URL はキャッシュされません。

5.2.1 キャッシュのフラッシュ

LoadMaster は、Real Server 上のファイルの変更を監視せず、仮想サービス内に保持されているキャッシュを自動リロードしません。 [Enable Caching] チェックボックスを選択解除して選択すると、キャッシュを強制的に再読み込みできます。 非キャッシュ要求を送信して、キャッシュされたオブジェクトをリロードすることもできます。 ほとんどのブラウザーは、左 Shift キーを押しながらリロードをクリック (または F5 キーを押す) することでこれをサポートします。

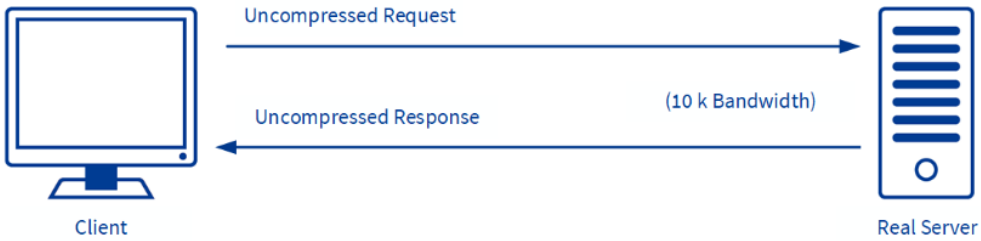
5.2.2 最大キャッシュ サイズ

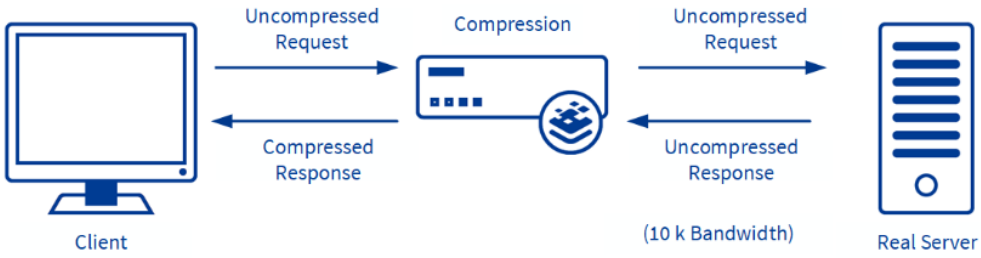
キャッシュに使用できるグローバル メモリの量を構成できます。 値は、実際のメモリと線形関係にあります。 これを設定するには、LoadMaster WUI で [Virtual Services] > [View/Modify Services] > [Modify] > [Advanced Properties] に移動します。

5.3 データ圧縮

LoadMaster のデータ圧縮機能は、最新のすべての Web ブラウザーで利用可能な gzip 圧縮を利用することで、HTTP オブジェクト用に転送されるデータの量を削減します。 Lempel-Ziv (LZ) 圧縮と HTTP/1.1 GNU zip (gzip) コンテンツ エンコーディングを活用することで、テキスト ファイル (HTML、CSS、および JavaScript) などの高圧縮ファイルの帯域幅使用率が削減されます。 データ圧縮により、LoadMaster は要求ごとにアプリケーション ペイロードを圧縮できるため、コンテンツの品質と応答時間を低下させることなくネットワーク帯域幅の消費を削減し、エンド ユーザーの全体的なエクスペリエンスを向上させることができます。 データ圧縮はすべてのファイルでサポートされています。

圧縮率はファイルの種類によって異なります。 サイズが 100Mb 以上のファイルの圧縮はお勧めしません。





圧縮機能は、リアルタイムのインライン圧縮要件を軽減するために、キャッシング機能と同時に展開する必要があります。 圧縮のみを使用すると、ハードウェア プラットフォームによっては仮想サービスのスループットがボトルネックになる可能性があります。

圧縮は、HTTP ごと、およびオフロードされた HTTPS 仮想サービスごとに有効にすることができます。 圧縮は、gzip をサポートするクライアントに依存します。 クライアントの HTTP トラフィックをトレースすることで、仮想サービスへの圧縮された接続が存在することを確認できます。

LoadMaster から Contentencoding: gzip ヘッダーを見つけることができれば、LoadMaster へのクライアント通信は圧縮されています。

6 SSL アクセラレーション/オフロード

LoadMaster シリーズは、仮想サービスの SSL ターミネーション/アクセラレーションを提供します。 SSL アクセラレーションを使用すると、SSL セッションは LoadMaster で終了します。 LoadMaster は、SSL 3.0、TLS 1.0、TLS 1.2、および TLS 1.3 をサポートしています。 SSL アクセラレーションには、主に次の 2 つの利点があります。

- LoadMaster は実サーバーから SSL ワークロードをオフロードします。
- LoadMaster はレイヤ 7 処理を実行します: 持続性またはコンテンツ スイッチング

LoadMaster で SSL セッションを終了しないと、ヘッダーとコンテンツを読み取ることができないため、パーシステンスを行うことができません。 SSL セッションが LoadMaster で終了されない場合に使用できる唯一の一貫して信頼できるパーシステンス方法は、ソース IP です。 SSL アクセラレーションにより、LoadMaster は専用のプロセッサを使用して SSL 機能を実行します。 この SSL アクセラレーション ハードウェアにより、LoadMaster は非 SSL 接続を処理するのと同じくらい簡単に SSL 接続を処理します。 すべての LoadMaster は SSL ターミネーションを実行できます。
SSL ターミネーション機能には、次の 2 つのタイプがあります。

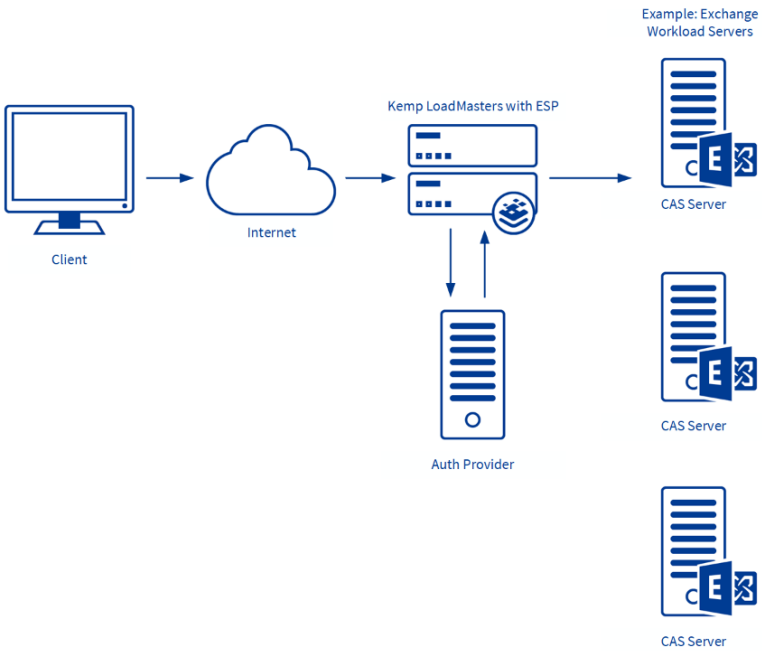
- ハードウェア SSL
- ソフトウェア SSL

Virtual LoadMaster では、ソフトウェア SSL のみを使用できます。
機能的には、ハードウェア SSL とソフトウェア SSL は同じです。 違いは、SSL 操作に関連する実際の暗号化機能を処理する LoadMaster の部分です。 ソフトウェア SSL では、LoadMaster の汎用プロセッサが暗号化/復号化タスクを処理します。 これらのタスクは、ロード バランシング、ヘルス チェック、その他の管理タスクなど、LoadMaster が実行する他のタスクと共有されます。 SSL 操作は CPU を集中的に使用するため、ソフトウェア SSL は低レベルの SSL トラフィックには十分ですが、高レベルの SSL トラフィックには不十分です。 ソフトウェア SSL ロードマスターでの SSL の接続率が高いと、ロードマスターの全体的なパフォーマンスが低下する可能性があります。
ハードウェア SSL では、LoadMaster にはすべての SSL 機能を処理する別の専用プロセッサがあります。 SSL 接続のレベルに関係なく、LoadMaster の一般的なプロセッサには負荷がかかりません。 この特殊なハードウェアは SSL 専用に構築されており、SSL トラフィックの非常に高い接続率

(TPS) を処理できます。 SSL の詳細については、SSL Accelerated Services の機能説明を参照してください。

7 エッジ セキュリティ パック (ESP)

Kemp Edge Security Pack (ESP) パックは、以前に Microsoft の Threat Management Gateway (TMG) を展開して Microsoft アプリケーションを公開していたお客様に、ロード バランサーの Progress Kemp LoadMaster ラインを使用したソリューションを提供します。



Progress Kemp ESP は、次の主要な機能を提供します。

- 事前認証のエンドポイント認証
- ユーザー ロギングの永続的なロギングとレポート
- 仮想サービス全体でのシングル サインオン (SSO)
- LoadMaster から Active Directory への LDAP 認証
- クライアントから LoadMaster への基本およびフォームベースの認証通信
- リモート アクセス ダイヤルイン ユーザー サービス (RADIUS) 認証
- RSA SecurID 2 要素認証
- Kerberos 制約付き委任 (KCD) 認証
- クライアント証明書認証
- 二要素認証

7.1 事前認証のエンドポイント認証

LoadMaster 上の仮想サービスにアクセスしようとしているクライアントは、クライアントがサービスにアクセスする権利を検証するために ESP によって使用される認証情報を提供する必要があります。 成功した場合、クライアントはサービスにアクセスできるようになります。 障害が発生した場合、クライアントは有効な資格情報が提供されるまでブロックされます。

7.2 ユーザー ロギングのパーシステンスなロギングとレポート

クライアントがサービスにアクセスしようとすると、ESP の一部として LoadMaster に記録されます。 これにより、管理者による監視が可能になります。

7.3 仮想サービス全体でのシングル サインオン

LoadMaster は、独自のワークロードをサポートする複数の仮想サービスを処理するように設計されています。 これらの仮想サービスは、同じシングル サインオン (SSO) ドメインに関連付けることで結合できます。 これが機能するには、仮想サービスが同じドメイン (ecp.example.com と www.example.com など) にある必要があります。

ESP の SSO により、クライアントは最初の仮想サービスにアクセスするときにのみ認証情報を入力できるようになり、その後、シングル サインオン ドメインに関連付けられた他のサービスにアクセスするために同じ情報が使用されます。 したがって、Exchange にアクセスするクライアントは、同じシングル サインオン ドメインに関連付けられている場合、SharePoint やその他のワークロードにもアクセスできます。

7.4 LoadMaster から Active Directory への LDAP 認証

Active Directory は、Microsoft ワークロードの標準的な認証プロバイダーです。 LoadMaster は、LoadMaster と Active Directory の間の主要な接続タイプをサポートしています。

7.5 クライアントから LoadMaster への基本認証通信

LoadMaster with ESP は現在、クライアントと LoadMaster 間の基本認証とフォームベース認証をサポートしており、クライアントに最適な認証エクスペリエンスを提供します。 将来のリリースで

は、NTLM もサポートする予定です。 大小の企業は、サポートするために多数のインターネット向けアプリケーションを展開しています
ますます拡大するビジネス要件。 この急速に増加するサーバー数は、スケーラブルで信頼性の高いものである必要があります。 とりわけ、これらのサーバーとサービスへのアクセスは安全である必要があります。 ESP の追加により、LoadMaster は、機能豊富で費用対効果の高いスケーラビリティと高い信頼性の要件に引き続き対応しながら、TMG のない世界でインターネットに接続するアプリケーションに対する顧客のセキュリティ要件を引き続き提供します。

7.6 RADIUS 認証

リモート アクセス ダイヤル イン ユーザー サービス (RADIUS) サーバーを使用して、Kemp LoadMaster にログインするユーザーを認証できます。 LoadMaster はユーザーの詳細を RADIUS サーバーに渡し、RADIUS サーバーはユーザーが認証されているかどうかを LoadMaster に通知します。 Windows Server 2008 R2 の RADIUS は、ネットワーク ポリシーとアクセス サービスによって行われます。 詳細については、『RADIUS Authentication and Authorization, Technical Note』を参照してください。

7.7 RSA SecurID 2 要素認証

Kemp Edge Security Pack (ESP) の一部として、LoadMaster は RSA SecurID 認証方式をサポートしています。 このスキームは、RSA SecurID サーバーでユーザーを認証します。 認証方法として RSA が有効になっている場合、ログイン プロセス中に、ユーザーは、個人識別番号 (PIN) と RSA SecurID オーセンティケーターに表示される番号であるトークン コードの 2 つの数字を組み合わせたパスワードを入力するよう求められます。 (ドングル)。 次の 2 つのチャレンジ/レスポンス モードが追加されています。次のトークンと新しい PIN です。 詳細については、RSA 2 要素認証、機能の説明を参照してください。

7.8 Kerberos 制約付き委任 (KCD) 認証

KCD を認証プロトコルとして使用する場合、ロードマスターは、提供された資格情報がそのような環境で直接有効でない場合でも、Kerberos レルム内の保護されたリソースへのシームレスなアクセスを提供します。 KCD 認証プロトコルは、ネットワーク上のリソースにアクセスしようとしているユーザーの ID を確認するために使用されます。 KCD 認証は、秘密鍵によって暗号化および復号化さ

れ、ユーザー パスワードを含まないチケットを使用します。 これらのチケットは、Kerberos メッセージで要求され、配信されます。 ユーザーのパスワードが提供されていない場合、信頼できる管理者ユーザー アカウントを使用して、サービスとユーザーに代わってチケットを取得します。 詳細については、Kerberos Constrained Delegation (KCD) の機能の説明を参照してください。

7.9 クライアント証明書認証

認証に証明書を使用することは、ユーザーがユーザー名とパスワードを知っているだけでは何かにアクセスできないため、より安全であると見なすことができます。 証明書を使用すると、クライアント マシン上のキー ロガーやその他のマルウェアがキーストロークをキャプチャしてユーザー アカウントとパスワードを特定することを防止できます。 LoadMaster は、KCD 認証による証明書の使用をサポートしています。 詳細については、Kerberos Constrained Delegation (KCD) の機能の説明を参照してください。

7.10 二要素認証

一部の認証メカニズムは、Active Directory とセカンダリ メカニズムの両方が順番に使用される二重要素アプローチを前提としています。 これらの場合、フォームにはユーザー名、パスワード、およびユーザー名とパスワードの後にチェックされるパスコードも含まれます。

7.11 OIDC OAUTH ESP 認証

Open ID Connect (OIDC) は、OAuth2.0 プロトコルに追加された ID レイヤーであり、ID プロバイダー (IdP) (Oauth では承認サーバーの役割と呼ばれます) によって提供されるトークンを介してユーザーの認証を可能にします。 OIDC は一般に、ユーザーのシングル サインオンを有効にするために使用されます

単一の ID プロバイダーを介して複数のアプリケーション間で。 OIDC は、OAuth2 からの標準化されたメッセージ フローを使用して ID サービスを提供します。 OIDC を使用する場合、ロードマスターはリソース サーバーの役割を実行し、認証トークンを介してアプリケーションへのアクセスを許可または拒否します。 これには、Microsoft Azure AD Identity Management などのユーザーの認証に ID プロバイダーを使用する必要があります。

詳細については、OIDC OAUTH ESP 認証、機能の説明を参照してください。

8 Web アプリケーション ファイアウォール パック(WAF)

Web アプリケーション ファイアウォール (WAF) サービスは、Kemp LoadMaster にネイティブに統合されています。 これにより、Web アプリケーションの安全な展開が可能になり、レイヤー 7 攻撃を防ぎながら、優れたアプリケーション配信パフォーマンス、高可用性、およびスケーラビリティを保証するコア ロード バランシング サービスを維持できます。 WAF は、LoadMaster の既存のセキュリティ機能を直接強化して、Web アプリの多層防御を作成するため、Web アプリケーション リソースの安全でコンプライアンスに準拠した生産的な使用が可能になります。 従来のファイアウォールを使用する際に直面する課題のいくつかを以下のセクションに示します。 Kemp WAF の利点の一部は、従来のファイアウォールの課題セクションに記載されています。

8.1 従来のファイアウォールの課題

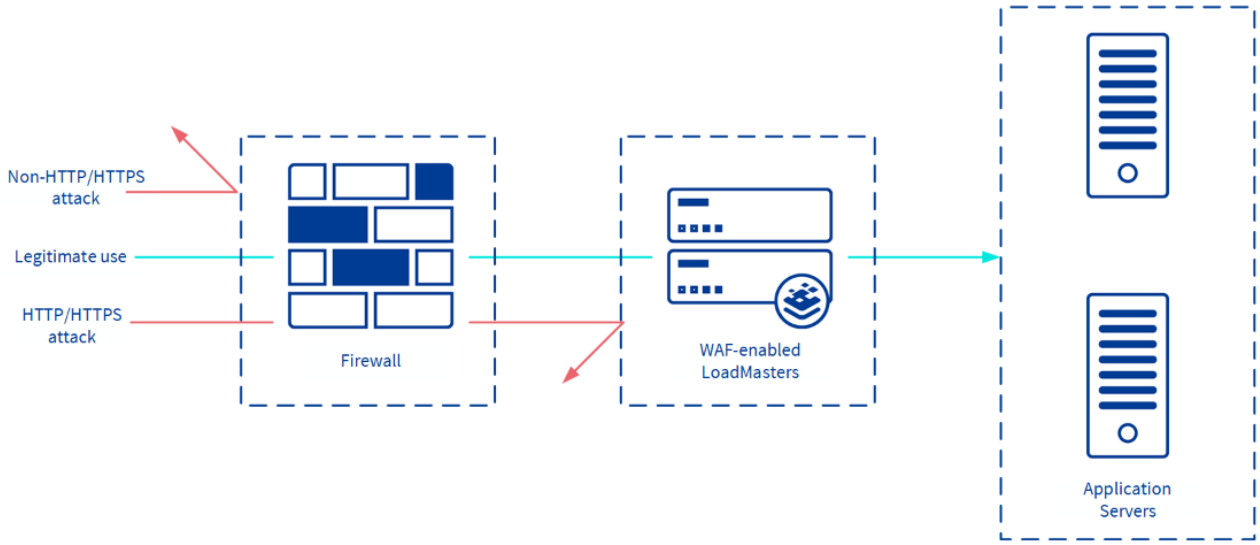
従来のファイアウォールには、次のような多くの制限があります。

- 通常、レイヤ 4 の下で動作します
- プロトコル インスペクションのサポートが制限されている (つまり、パケット フィルタリング)
- 「ポートとソケット」しか認識していない

現代のハッカー攻撃は、次のような事実により、多くのセキュリティ上の課題を提示します。

- ますます複雑化
- 攻撃ベクトルを頻繁に変更する
- アプリケーションの脆弱性に焦点を当てる
- ファイアウォールでの検出とブロックが困難

8.2 Progress Kemp WAF のメリット



上の図に示されているように、Kemp WAF には次のような多くの利点があります。

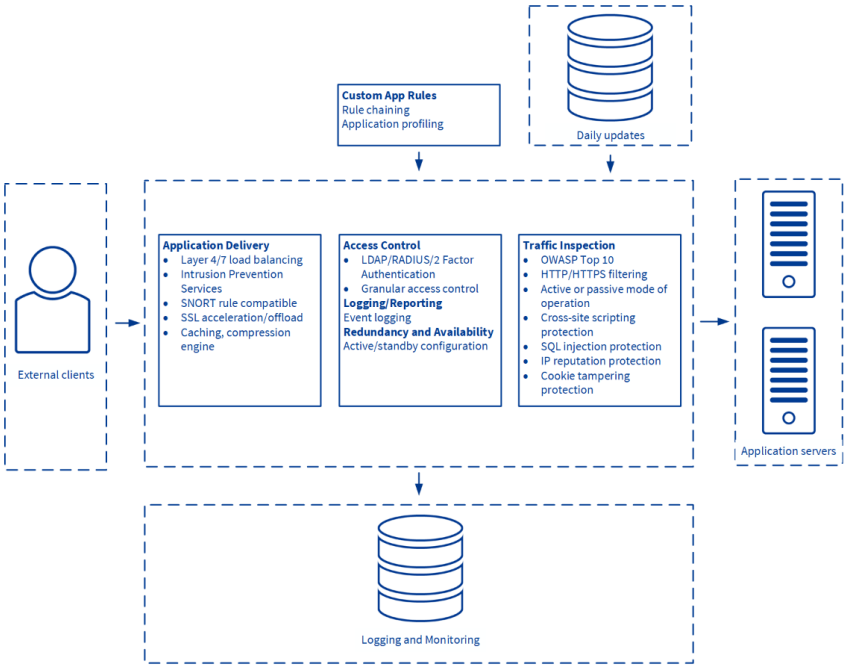
- Web ベースのトラフィック、つまり HTTP/HTTPS を処理します
- 最新のアプリケーション攻撃ベクトルを検出できます
- 境界防御とアプリケーション サーバーの間に展開される
- 完全なアプリケーション攻撃を提供するために、既存のセキュリティ技術と連携して動作し防止ます

8.3 Progress Kemp WAF 対応 LoadMaster の概要

Kemp の統合された L7 WAF プラットフォームは、業界をリードするルール エンジンに基づいており、Open Web Application Security Project (OWASP) のトップ 10 や重要なベースライン保護など、公開されているすべてのアプリケーションの脅威をリアルタイムでカバーします。また、集中型の Kemp Application Delivery Controller (ADC) アプライアンスで既存のルールを使用することもできます。 WAF-ADC 統合により、Progress Kemp は LoadMaster プラットフォームで利用可能な既存のセキュリティ機能を強化します。これは現在、リバース プロキシ、シングル サインオン (SSO)、事前認証、SMTP ドメイン フィルタリング、デュアル要素認証、侵入防止システム (IPS)、および安全なトラフィック フローのための SSL ブリッジング。 Kemp の商用ルールには、IP レピュテーション、ボットネット攻撃検出、Web ベースのマルウェア検出、Webshell/バックドア検出、HTTP サービス拒否 (DoS) 攻撃検出などの攻撃カテゴリも含まれています。

LoadMaster には、WAF 機能とセキュリティ サービスが含まれています。これにより、ネットワーク管理者は次のことができるようになります。

- ネットワークへの影響を最小限に抑え、最大限の保護でアプリケーションを保護
- この統合ソリューションでインフラストラクチャを簡素化
- 必要な Application Delivery Controller (ADC) と WAF SSL オーバーレイ サービスを 1 つの製品に集中化



上の図に示すように、Kemp WAF は次のような多くの便利な機能を提供します。

- フル機能のロード バランシングとコンテンツ スイッチング
- 侵入防止システム (IPS) とコンテンツ フィルタリング
- Open Web Application Security Project (OWASP) の上位 10 の脆弱性に対する保護
- 標準およびカスタム アプリケーションのサポート
- アクティブ (ブロックおよびログ) モード操作のサポート
- パッシブ (ログのみ) モード操作のサポート
- SQL インジェクション保護
- クロスサイト スクリプティングの緩和
- クロスサイト リクエスト フォージェリ (CSRF) の防止
- クッキーやフォームの改ざん防止
- 分散型サービス妨害 (DDOS) の緩和
- トロイの木馬対策

- IP レピュテーションチェック
- データ漏洩保護
- 組み込みのレポート
- ログ フィールドのマスキング (つまり、クレジット カード番号) を含む組み込みのログ記録

WAF を構成する手順を含む詳細については、Web アプリケーション ファイアウォール (WAF) の機能の説明を参照してください。

9 GEO

GEO は、Microsoft Exchange などの Web ベースのアプリケーションを最適に使用するために、最高のパフォーマンスを発揮し、地理的に最も近いデータセンターへのシームレスなフェイルオーバーとフェイルバックを保証します。 サービスの中断が発生した場合、トラフィックは設定されたポリシーに基づいて自動的に制御され、影響と手動介入の必要性を最小限に抑えます。

GEO 製品は、次の 2 つの形式で利用できます。

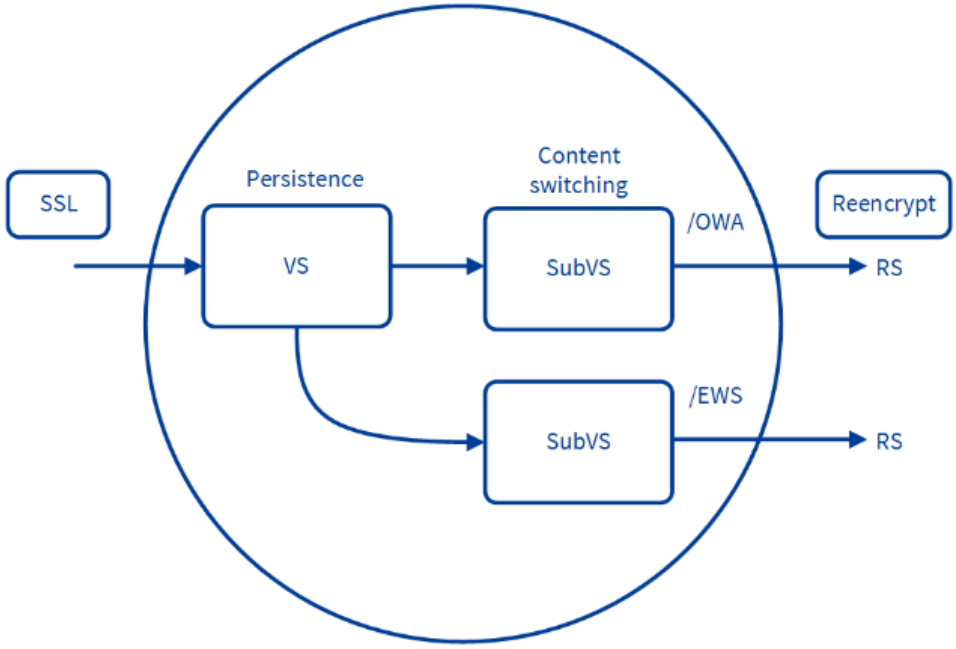
- スタンドアロンの GEO 製品
- Progress Kemp LoadMaster 製品の一部である Global Sever Load Balancing (GSLB) Feature Pack

GEO は、ラウンド ロビン、加重ラウンド ロビン、固定加重、リアル サーバー ロード、ロケーション ベース、プロキシミティなど、多くのロード バランシング アルゴリズムを提供します。 「ラウンド ロビン」ロード バランシングは、すべてのアクティブなデータ センターで使用できます。これには、重み付けのサポートと、災害復旧のためのチェーン フェールオーバー オプションが含まれます。ロケーション ベースの負荷分散により、GEO は、作成されたポリシーで定義されたクライアントの国または大陸に基づいて、クライアントをデータ センターに誘導できます。 Proximity は Location Based をさらに一歩進めて、経度と緯度の粒度で近接度を定義できるようにします。 GEO は LoadMaster と安全かつシームレスに統合して、「リアル サーバー ロード」ロード バランシングを提供します。GEO は、LoadMaster が提供するローカル データ センター メトリックを使用して、クライアントが最も負荷の低いデータ センターに接続できるようにします。 GEO は分散 (アクティブ/アクティブ) 高可用性構成で展開でき、複数のアプライアンスが情報を安全に同期します。既存の権威ドメイン ネーム サービス (DNS) に GEO を導入すると、最小限の統合作業とリスクが必要になるため、既存の DNS への投資を最大限に活用できます。 GEO の詳細については、Progress

Kemp ドキュメント ページの GEO 機能の説明を参照してください。

10 サブ仮想サービス (SubVS)

仮想サービス内から、1 つ以上の「サブ仮想サービス」(SubVS) を作成できます。 SubVS は「親」仮想サービスにリンクされ、その IP アドレスを使用します。 サブ VS は、親仮想サービスに対して、および相互に異なる設定 (ヘルス チェック メソッド、コンテンツ ルールなど) を持つ場合があります。 これにより、すべて同じ IP アドレスを使用して、関連する仮想サービスをグループ化できます。 これは、Exchange や Lync など、通常多数の仮想サービスで構成される複雑な構成がある場合に役立ちます。



SubVS を使用すると、次のような多くの利点があります。

- SubVS は「親」仮想サービスにリンクされ、その IP アドレスを使用します
- SubVS を使用すると、Lync や Exchange などのアプリケーションに必要な IP アドレスの数が減ります
- SubVS は非透過性を必要としない
- SubVS は、親仮想サービスに対して、および相互に異なる設定 (コンテンツ ルールなど) を持つことができます。
- SubVS を使用すると、同じ仮想サービスでコンテンツの切り替えと永続性を実現できます。

- SubVS を使用すると、同じ仮想サービスで複数のヘルス チェックを実行できます。
- SubVS は ESP とうまく連携しますが、ESP は必須ではありません

11 証明書

11.1 自己署名証明書と CA 署名証明書

SSL 証明書は、すべての SSL トランザクションに必要であり、SSL 対応のすべての仮想サービスにも必要です。 LoadMaster には、次の 2 種類の SSL 証明書があります。

- LoadMaster 自体によって生成された自己署名証明書
- Verisign や Thawte などの CA (認証局) によって署名された証明書

LoadMaster で SSL 対応の仮想サービスを設定すると、自己署名証明書が自動的にインストールされます。 一般に、自己署名証明書は、公開されている実稼働 Web サイトには使用しないでください。次のような他のシナリオでの使用が許容される場合があります。

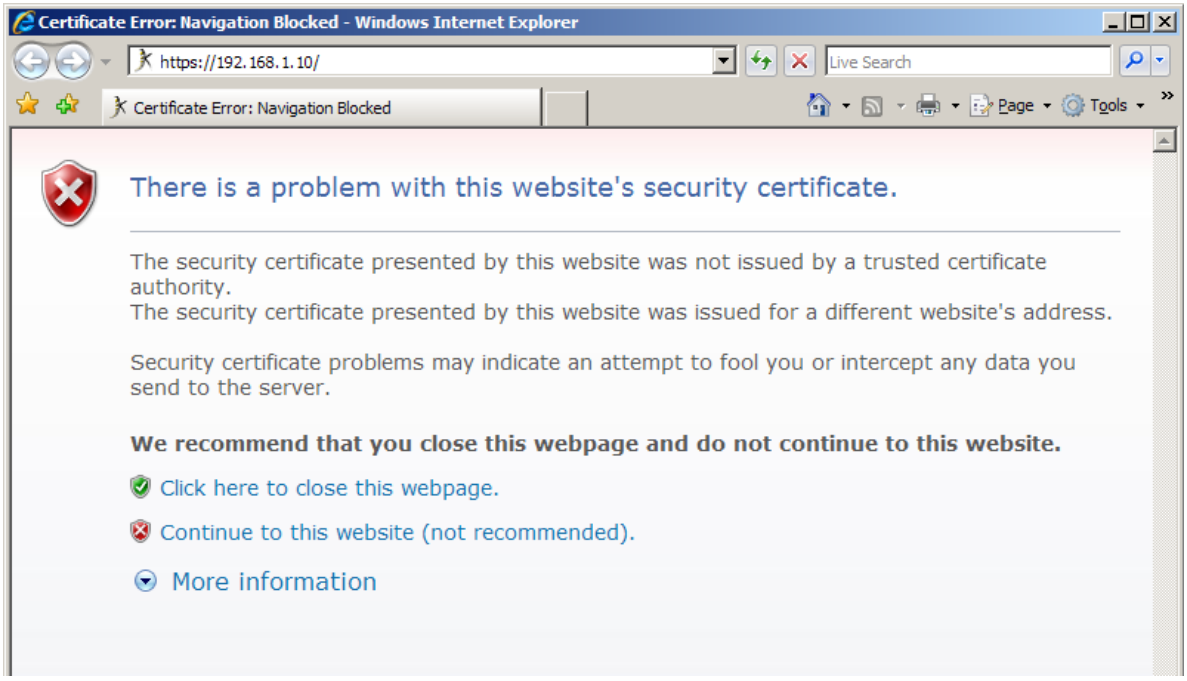
- イントラネット サイト
- Web サイトがテストされているが一般に公開されていない QA サイト

11.2 証明書の基本

自己署名証明書と CA 署名証明書の両方が、移動中のデータの暗号化を提供します。 CA が署名した証明書は、認証も提供します。これは、サイトが偽の Web サイトではなく、報告されたものであることを保証するレベルです。

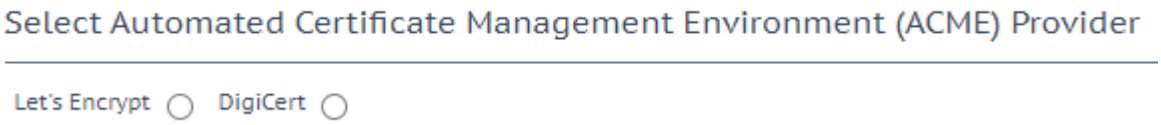
11.3 運用上の違い

自己署名証明書と CA 証明書の主な操作上の違いは、自己署名証明書の場合、ブラウザーは通常、証明書が CA によって発行されたものではないことを警告する何らかのエラーを表示することです。 自己署名証明書エラーの例を図 1 に示します。



これは、WUI が自己署名証明書を使用するため、LoadMaster WUI に接続するときに受け取る警告メッセージと同じです。 通常、この警告は、ブラウジング セッションごとに 1 回だけ発生します。

11.4 ACME 証明書



LoadMaster は、2 つの Automated Certificate Management Environment (ACME) プロバイダーのオプションを提供します。

- 暗号化しよう
- デジサート

現在、Let's Encrypt または DigiCert のいずれかを選択できます。 将来のリリースでは、両方を同時に使用できるようになります。 詳細については、以下の関連セクションを参照してください。

DigiCert に関連する詳細情報については、Progress Kemp ドキュメント ページの DigiCert 機能の説明を参照してください。

11.4.1 証明書を暗号化

Let's Encrypt は、無料で自動化されたオープンな認証局 (CA) です。 Internet Security Research Group (ISRG) が提供するサービスです。 ウェブサイトの HTTPS (SSL/TLS) をユーザーフレンドリーな方法で有効にするためのデジタル証明書が無料で発行されます。 Let's Encrypt の主な原則は次のとおりです。

- 無料: ドメイン名を所有している人なら誰でも、Let's Encrypt を使用して信頼できる証明書を無料で取得できます
- 自動: Web サーバー上で実行されているソフトウェアは、Let's Encrypt とやり取りして、簡単に証明書を取得し、安全に使用できるように構成し、更新を自動的に処理できます。安全: Let's Encrypt は、CA 側と、サイト オペレーターがサーバーを適切に保護するのを支援することの両方で、TLS セキュリティのベスト プラクティスを推進するためのプラットフォームとして機能します。
- 透明性: すべての証明書の問題または失効は公に記録され、誰でも閲覧できます
- オープン: 自動発行および自動更新プロトコルは、他のユーザーが採用できるオープン スタンダードとして公開されています。
- 協力: 基礎となるインターネット プロトコル自体と同じように、Let's Encrypt は、1 つの組織の制御を超えてコミュニティに利益をもたらすための共同の取り組みです。

Progress Kemp を使用すると、アプリケーション全体で証明書の更新と更新を自動化することで、Let’s Encrypt 証明書の価値を活用できます。

- HTTP-01 ドメイン検証メソッドのサポート
- 鍵の生成
- 証明書の発行 (証明書署名要求 (CSR) の作成と証明書の要求)
- LoadMaster での証明書の自動/手動更新と、更新された証明書の自動更新

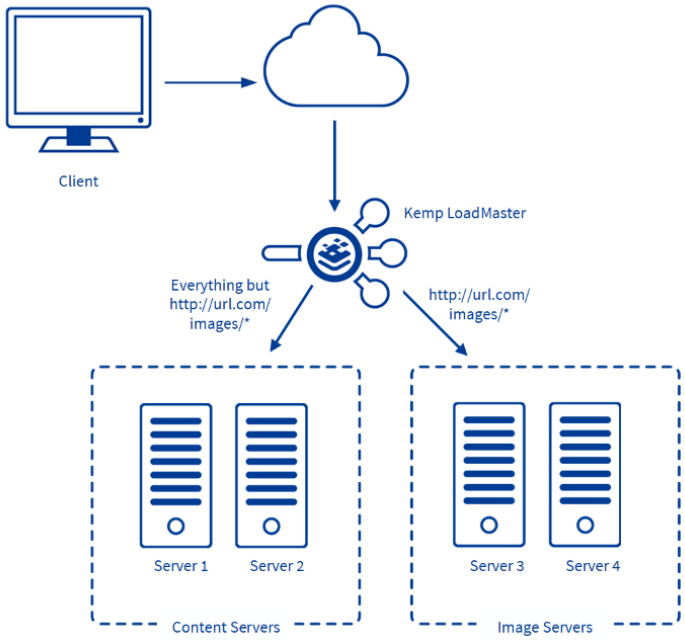
14.4.2 デジサート証明書

DigiCert は、すべての公開鍵インフラストラクチャ (PKI)、モノのインターネット (IoT)、および署名ワークフロー全体で信頼を管理および提供するための高保証 TLS/SSL 証明書と自動化ソリューションを提供する世界的リーダーです。 LoadMaster ファームウェア バージョン 7.2.58 の時点で、Kemp を使用すると、アプリケーション全体で証明書の更新と更新を自動化することで、DigiCert 証明書の価値を活用できます。

- HTTP-01 ドメイン検証メソッドのサポート
- 鍵の生成
- 証明書の発行 (証明書署名要求 (CSR) および要求証明書の作成)
- LoadMaster での証明書の自動/手動更新と、更新された証明書の自動更新

12 ルールベースのコンテンツ スイッチング

LoadMaster シリーズのロード バランサーは、コンテンツ スイッチング (URL スイッチングと呼ばれることもあります) をサポートしています。 これにより、LoadMaster は、要求された URL の内容に基づいて、特定の要求を特定のリアル サーバーに送信できます。



たとえば、2 つのサーバー グループがあるとします。 1 つのグループは画像を提供し、もう 1 つのグループは他のすべてのコンテンツを提供します。コンテンツ ルールを作成して、これら 2 つのクラスの要求を分離できます (図 1)。

「http://url.com/images/party.jpg」など、/images を含むすべての URL または「http://url.com/images/dogs.jpg」はサーバー 3 と 4 に送信され、それ以外はサーバー 1 と 2 に送信されます。

これは、さまざまな機能を実行するサーバー (アプリケーション サーバー、静的コンテンツ サーバー、マッピング サーバー、特殊なコンテンツ生成サーバーなど) がある場合に非常に便利です。

同じ一般的なホスト名 (たとえば、www.websitename.com) から提供されます。

12.1 用語

コンテンツ スイッチングという用語は、レイヤ 2 スイッチングに関連するプロセスを指すものではありません。 代わりに、コンテンツ スイッチングとは、要求されたコンテンツに応じて、異なるサーバー間でトラフィックを切り替えることを指します。

12.2 コンテンツ スイッチングの使用

コンテンツ スイッチングの設定には、コンテンツ ルールと仮想サービス設定の 2 つの部分があります。 コンテンツ ルールはロードマスター上でグローバルに設定され、さまざまなルールが仮想サービスの下で動作する特定の実サーバーに適用されます。

13 ヘルスチェック

13.1 概要

LoadMaster はヘルス チェックを利用して、実サーバーと仮想サービスの可用性を監視します。 いずれかのサーバーが定義された時間間隔内に定義された回数ヘルス チェックに応答しない場合、このサーバーの重みはゼロに減らされます。 このゼロ重み付けには、実サーバーがオンラインに戻ったと判断できるまで、仮想サービス構成から実サーバーを削除する効果があります。 LoadMaster は、WUI で指定できるヘルス チェックを使用します。 デフォルトでは、最高のヘルス チェックが仮想サービスに関連付けられています。 LoadMaster は、次のポートに対してレイヤー 7 ヘルス チェックを実行します。

Service Port	Protocol
FTP 21	TCP
TELNET 23	TCP
SMTP 25	TCP
HTTP 80	TCP
HTTPS 443	TCP
POP3 110	TCP
NNTP 119 T	TCP

IMAP 143	TCP
DNS 53	UDP
LDAP 389/636	UDP/TCP

仮想サービスを作成し、汎用以外のサービス タイプを使用する場合、追加のヘルス チェック プロトコルを使用できます。 たとえば、Remote Terminal というサービス タイプは、Remote Terminal Protocol によるチェックを許可します。リモート ターミナル プロトコルは、ネットワーク レベル認証をサポートします。

その他のポートについては、LoadMaster は TCP サービスに対してレイヤー 4 ヘルス チェックを使用し、UDP サービスに対してレイヤー 3 ヘルス チェックを使用します。 ヘルス チェックの設定は、仮想サービス ウィザードを使用してデフォルト設定から変更し、非標準設定に対応することができます。 たとえば、ポート 80 ではなく 8080 で http サービスを実行し、ヘルス チェックをデフォルトのレイヤ 4 チェックではなく HTTP に変更できます。 これらのグローバル設定は、ファーム内のすべてのサーバーに適用されます。つまり、サーバーごとに異なるタイムアウトを割り当てることはできません。 LoadMaster で仮想サービスを定義するときは、サービス チェック オプションの 1 つを使用する必要があります。

13.2 サービスおよび非サービスベースのヘルスチェック

レイヤ 3 のヘルス チェックでは、ICMP ベースのエコー リクエスト (ping) を使用して、実サーバーにネットワーク経由で到達できるかどうかをテストします。 レイヤー 3 チェックは、仮想サービス固有のものではありません。たとえば、失敗した場合、対応する実サーバーは、それを使用するすべての仮想サービスから削除されます。 レイヤー 3 ヘルス チェックとは対照的に、レイヤー 4 とレイヤー 7 ヘルス チェックのサービス ベースのヘルス チェックは仮想サービス ベースです。 実サーバーがそのようなチェックに失敗すると、
対応する仮想サービスからのみ削除されます。この実サーバーを使用する他のすべての仮想サービスは影響を受けません。

タイプ	説明
ICMP	LoadMaster は ICMP エコー要求 (ping) を実サーバーに送信します。 実サーバーは、構成された再試行回数に対して構成された応答時間内に ICMP エコー応答で応答しない場合、このチェックに失敗します。

TCP	LoadMaster は、構成されたサービス ポートで実サーバーへの TCP 接続を開こうとします。サービス ポートでサーバーに TCP SYN パケットを送信します。 サーバーは、応答時間間隔内に TCP SYN ACK で応答する場合、チェックに合格します。 この場合、LoadMaster は TCP RESET を送信して接続を閉じます。 サーバーが設定された回数の設定された応答時間内に応答しない場合、停止していると見なされます。
FTP	LoadMaster は、サービス ポート (ポート 21) で実サーバーへの TCP 接続を開きます。 サーバーがステータス コード 220 のグリーティング メッセージで応答した場合、LoadMaster は QUIT コマンドをサーバーに送信し、接続を閉じてアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。
TELNET	LoadMaster は、サービス ポート (ポート 23) で実サーバーへの TCP 接続を開きます。 サーバーが文字「0xff」で始まるコマンド文字列で応答すると、ロードマスターは接続を閉じ、サーバーをアクティブとしてマークします。 サーバーが設定された回数の設定された応答時間内に応答しない場合、または別のコマンド文字列で応答する場合、サーバーは停止していると見なされます。
SMTP	LoadMaster は、サービス ポート (ポート 25) で実サーバーへの TCP 接続を開きます。 サーバーがステータス コード 220 のグリーティング メッセージで応答した場合、LoadMaster は QUIT コマンドをサーバーに送信し、接続を閉じてアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。
HTTP	LoadMaster は、サービス ポート (ポート 80) で実サーバーへの TCP 接続を開きます。 LoadMaster は HTTP/1.0 HEAD リクエストをサーバーに送信し、ページ「/」をリクエストします。 サーバーがステータス コード 2 (200-299、301、302、401) の HTTP 応答を送信すると、LoadMaster は接続を閉じ、サーバーをアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。 HTTP 1.0

	および 1.1 のサポートが利用可能です。 HTTP 1.1 を使用すると、ホスト ヘッダーが有効な Web サーバーを確認できます。
HTTPS	LoadMaster は、サービス ポート (ポート 443) でリアル サーバーへの SSL 接続を開きます。 LoadMaster は HTTP/1.0 HEAD リクエストをサーバーに送信し、ページ「/」をリクエストします。 サーバーがステータス コード 2 (200-299、301、302、401) の HTTP 応答を送信すると、LoadMaster は接続を閉じ、サーバーをアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。 HTTP 1.0 および 1.1 のサポートが利用可能です。 HTTP 1.1 を使用すると、ホスト ヘッダーが有効な Web サーバーを確認できます。
POP3	LoadMaster は、サービス ポート (ポート 110) で実サーバーへの TCP 接続を開きます。 サーバーが +OK で始まる挨拶メッセージで応答すると、LoadMaster は QUIT コマンドをサーバーに送信し、接続を閉じてアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。
NNTP	LoadMaster は、サービス ポート (ポート 119) で実サーバーへの TCP 接続を開きます。 サーバーがステータス コード 200 または 201 のグリーティング メッセージで応答した場合、LoadMaster は QUIT コマンドをサーバーに送信し、接続を閉じてアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。
IMAP	143)。 サーバーが「+ OK」または「* OK」で始まる挨拶メッセージで応答した場合、LoadMaster はサーバーに LOGOUT コマンドを送信し、接続を閉じてアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。
DNS	ネーム サーバー (DNS) プロトコルの値は、仮想サービス プロトコルが udp に設定されている場合、[実サーバー チェック方法] ドロップダウン リストでのみ使用できます。 LoadMaster は、UDP ポート 53 を介してサー

	バー上の A レコードに対して nslookups を実行します。サーバーが DNS クエリに正常に応答すると、LoadMaster はそれをアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しない場合、または A レコードへの応答に失敗した場合、サーバーはダウンしていると見なされます。
RDP	LoadMaster は、RDP ルーティング トークンを実サーバーに送信します。RDP ヘルス チェックは、ネットワーク レベル認証をサポートしています。
Binary	実サーバーに送信する 16 進文字列を指定します。 実サーバーから返される応答で検索される 16 進数の文字列を指定します。 LoadMaster が応答でパターンを見つけた場合、実サーバーは稼働していると見なされます。 応答パターンを検索するバイト数を指定します。
LDAP	ヘルスチェックに使用する LDAP エンドポイントを選択します。 LDAP ヘルス チェックでは、LDAP エンドポイントで指定された LDAP クレデンシャルとプロトコルが使用されます。 ヘルス チェックは、実サーバーの IP アドレスとポートに対して実行されます。 LDAP ヘルス チェックは、ロードマスターがリアル サーバーに接続し、指定されたユーザー資格情報を検証することで構成されます。 ヘルスチェックは次の 2 つのステップで実行されます。 ステップ 1: 実サーバーの指定されたポートが稼働しており、使用可能かどうかを確認します。 ステップ 2: LDAP で指定された資格情報を使用してリアル サーバーへのログインを試みます。 ステップ 1 とステップ 2 が true の場合、ヘルスチェックは合格です。 ステップ 1 またはステップ 2 が失敗した場合、ヘルスチェックは失敗します。
None	ヘルスチェックは実行されません。

14 SNMP サポート

簡易ネットワーク管理プロトコル (SNMP) は、リモート管理ステーション (SNMP マネージャー) からネットワーク経由で多数のネットワーク デバイスを管理できるようにするプロトコルです。マネージャ ステーションは、管理対象ステーション (SNMP エージェント) からデータを要求したり、エー

ジェント上のデータの値を変更したりできます。管理対象ステーション (SNMP エージェント) は、ユニットのフェイルオーバーなどの事前定義されたイベントが発生したときにマネージャに警告するように設定することもできます。アラート メカニズムは、イベント トラップを使用します。現在のバージョンは SNMPv3 です。使用されている以前の 2 つのリビジョンは、SNMPv1 と SNMPv2c (コミュニティベースの SNMPv2) です。 LoadMaster の SNMP サポートは SNMPv3 に基づいており、下位互換性があるため、上記の 3 つのバージョンすべてを使用できます。ただし、SNMPv1 は 64 ビット値 (LoadMaster Management Information Base (MIB) で使用される) をサポートしていないため、SNMPv2c または SNMPv3 を使用することをお勧めします。 MsgSecurity は、SNMP v1 および v2c でのみサポートされています。 HA モードで LoadMaster を監視する場合は、適切なイーサネット アドレスで個々のアプライアンスを監視してください。すべての LoadMaster 固有のデータ オブジェクトに関する情報は、以下に示すエンタープライズ固有の MIB に保存されます。

ONE4NET-MIB.txt	enterprise id
IPVS-MIB.txt	Virtual Server stats
B-100-MIB.txt	LoadMaster configuration data
CERTS-MIB.txt	SSL certificate information

www.kemptechnologies.com/documentation からダウンロードできるこれらの MIB は、SNMP を使用してロードマスターのパフォーマンス/構成データを要求できるようにするために、SNMP マネージャー マシンにインストールする必要があります。

SNMP は、レイヤ 4 とレイヤ 7 の両方で、IPv4 と IPv6 の両方の仮想サービスでサポートされています。SNMP のサポートは、デフォルトで無効になっています。 SNMP を使用して、ファイル名、証明書のサブジェクト名、証明書のシリアル番号、証明書の開始日、証明書の終了日、証明書の発行者情報などの SSL 証明書情報を取得できます。 SNMP は、最大 256 個の SSL 証明書についてこの情報を表示できます。 SNMP を使用して、ディスク容量の使用状況の詳細を取得することもできます。 /var/log および /var/log/userlog パーティション情報が利用可能です。

15 LoadMaster ソフトウェアのアップグレード

15.1 オンラインアップグレード

LoadMaster は、オンラインでソフトウェアの更新とアップグレードを実行する機能を提供します。パッチは Kemp から提供されます。 これらのパッチは、FTP、HTTP、または SSH デーモンをサポ

ートするマシンにインストールする必要があります。 パッチはチェックサム (MD5 を使用) され、データの破損や改ざんから保護するために暗号化されます。 パッチは、次の 2 つの方法のいずれかを使用してインストールできます。

- コンソール ライン インターフェイス (CLI) の使用
- WUI の使用

CLI の使用

[Configuration] メニューを使用して、[Utilities] > [Software Upgrade] メニュー オプションを選択します。 パッチがダウンロードされると、パッチが解凍されてチェックされます。 パッチが有効な場合、パッチのバージョンが表示され、ユーザーはパッチをインストールするかどうかを尋ねられます。 パッチが正常にインストールされたら、LoadMaster を再起動して新しいバージョンを有効にする必要があります。

WUI の使用

WUI を使用してソフトウェアをアップグレードするには、次の手順に従います。

1. LoadMaster WUI のメイン メニューで、[System Configuration] > [System Administration] > [Software Upgrade] を選択します。
2. [Browse] ボタンをクリックし、パッチを参照して選択します。
3. [Upgrade Machine] ボタンをクリックします。

パッチのインストールが成功したら、LoadMaster を再起動して新しいバージョンを有効にする必要があります。 パッチが正しくインストールされない場合は、構成メニューまたは WUI を使用して、ソフトウェアの以前のバージョンを再アクティブ化することができます。 ライセンス情報は、ライセンス、機能の説明で説明されているように、WUI に入力できます。

資料。 ライセンス キーを更新した後、新しい機能を有効にするために再起動を実行する必要があります。 パッチのサポートは期限切れになる可能性があります。 これが発生した場合は、アップグレード手順中に通知されます。 「Update not permitted」というメッセージが表示された場合は、Progress Kemp に連絡して再ライセンスを取得してください。

16 ユーザー管理

LoadMaster は、[System Configuration] > [System Administration] > [User Manageent] に移動して管理できる、さまざまなレベルのアクセスを持つ複数のユーザー ログインをサポートしていま

す。 各ユーザー名は、最小 3 文字、最大 14 文字にする必要があります。 パスワードは 6 文字以上にする必要があります。 ここで作成されたユーザーは WUI にのみアクセスでき、SSH を使用したリモート アクセスはサポートされていません。 LoadMaster は、認証プロセスで RADIUS サーバーまたはクライアント証明書を使用するように構成できます。 一般的なユーザー管理、およびクライアント証明書 WUI 認証の詳細については、ユーザー管理、機能の説明を参照してください。
RADIUS WUI 認証の詳細については、『RADIUS Authentication and Authorization, Technical Note』を参照してください。

16.1 役割・権限

工場出荷時のデフォルトのユーザー名は bal で、デフォルトのパスワードは 1fourall です。 工場出荷時のデフォルト ユーザーは、最高レベルのアクセスを保持します。 作成されたすべてのユーザーは、デフォルト アカウントによって許可されたアクセスのサブセットを持ちます。 ユーザーの役割の変更は、リアルタイムで有効になります。 役割は組み合わせることができ、相互に排他的です。
ユーザーのデフォルト アクセスは、証明書署名要求 (CSR) を生成する LoadMaster WUI への読み取り専用アクセス、ログ ファイルへの読み取りアクセス、および基本的なデバッグを実行する機能です。

16.1.1 Real Servers

このロールは、Real Server の有効化と無効化を許可します。
Real Server 権限を持つユーザーは、SubVS を追加できません。

16.1.2 仮想サービス

このロールは、仮想サービスの管理を許可します。 これには、SubVS が含まれます。 許可される仮想サービスの変更には、任意のサブネットの追加、削除、および変更が含まれます。

16.1.3 ルール

このロールは、ルールの管理を許可します。 許可されるルールの変更には、追加、削除、および変更が含まれます。

16.1.4 システムバックアップ

このロールは、システム バックアップの実行を許可します。

16.1.5 証明書の作成

この役割は、SSL 証明書の管理を許可します。 証明書の管理には、SSL 証明書の追加、削除、および変更が含まれます。

16.1.6 中間証明書

この役割は、中間証明書の管理を許可します。 証明書管理には、中間証明書を追加および削除する機能が含まれています。

16.1.7 証明書のバックアップ

この役割は、証明書をエクスポートおよびインポートする機能を許可します。

16.1.8 ユーザー管理

このロールは、[System Configuration] > [System Administration] > [User Management] 画面内のすべての機能にアクセスできます。

16.1.9 すべての権限

このロールは、bal パスワードを変更する権限と、他のユーザーを作成または削除する権限を除くすべての権限をユーザーに付与します。

16.1.10 GEO コントロール

この役割は、LoadMaster GEO 製品でのみ使用されます。 GEO および Global Server Load Balancing (GSLB) Feature Pack の詳細については、Progress Kemp ドキュメント ページの GEO 機能の説明を参照してください。

17 WUI の認証と承認

WUI の [認証と承認] 画面では、利用可能な認証 (ログイン) および承認 (許可されたアクセス許可)

オプションを管理できます。 認証

LoadMaster にログオンする前に、ユーザーを認証する必要があります。 LoadMaster では、RADIUS と LDAP の認証方法、およびローカル ユーザー認証を使用して、ユーザーの認証を実行できます。 すべての認証方法が選択されている場合、LoadMaster は以下を使用してユーザーを認証しようとします。

次の順序で認証方法を説明します。

1. RADIUS
2. LDAP
3. ローカル ユーザー

たとえば、RADIUS サーバーが使用できない場合は、LDAP サーバーが使用されます。 LDAP サーバーも使用できない場合は、ローカル ユーザー認証方法が使用されます。

RADIUS と LDAP のどちらの認証方法も選択されていない場合は、ローカル ユーザー認証方法がデフォルトで選択されます。

LoadMaster にログオンする前に、ユーザーを認証する必要があります。 LoadMaster では、LDAP 認証方法とローカル ユーザー認証を使用してユーザーの認証を実行できます。

Authorization

LoadMaster では、RADIUS またはローカル ユーザー認証を使用してユーザーを認証できます。 ユーザーの権限によって、ユーザーが持つ権限のレベルと、LoadMaster で実行できる機能が決まります。 RADIUS 認証方式を使用している場合は、RADIUS 認証方式のみを使用できます。

両方の承認方法が選択されている場合、LoadMaster は最初に RADIUS を使用してユーザーを承認しようとします。 この認証方法が利用できない場合、LoadMaster は次のことを試みます。

ローカル ユーザー認証を使用してユーザーを認証します。 LDAP を使用した承認はサポートされていません。 RADIUS 認証方法が選択されていない場合は、デフォルトでローカル ユーザー認証方法が選択されます。 以下は、許可が機能するために RADIUS サーバー上にある必要がある構成の例です。 以下の例は、Linux 専用です。

Reply-Message は、それが許可する許可について自明である必要があります。 これらは、「All Permission」を除いて、WUI のユーザー権限ページと一致する必要があります。

```
LMUSER Cleartext-Password := "1fourall"
```

Reply-Message = "real,vs,rules,backup,certs,cert3,certbackup,users"

bal ユーザーは常に、ローカル ユーザー認証および承認方法を使用して認証および承認されます。

18 ボンディングと VLAN

18.1 概要

LoadMaster ボンディング/VLAN タギングは、WUI を使用して簡単にセットアップおよび構成できます。 展開を成功させるには、前提条件が満たされている必要があります。 このガイドは、LoadMaster でのインターフェイス ボンディングと VLAN 構成。 ボンディングのサポートは、すべてのネットワーク モジュールで利用できます。

18.2 前提条件 (スイッチの互換性)

前提条件のリストは次のとおりです。

- VLAN タギング
- IEEE 802.1Q
- ボンディング/チーミング (802.3ad/アクティブ バックアップ)
- IEEE 802.1AX/IEEE 802.3ad/LACP

18.2.1 スイッチ構成

通常、Active-Backup モードを有効にする場合、スイッチの介入は必要なく、LoadMaster で直接設定できます。 802.3ad ボンディング モードを使用するには、スイッチ上で LoadMaster と連携してリンク アグリゲーション グループを構成する必要があります。 スイッチのドキュメントを読んで、対応するチーム/ボンド、リンク アグリゲーションの一般的な用語を確立してください。 「イーサネット トランク」、「NIC チーミング」、「ポート チャネル」、「ポート チーミング」、「ポート トランキング」、「リンク バンドリング」、「イーサチャネル」、「マルチリンク トランキング (MLT)」、「NIC ボンディング」、「 ネットワーク フォールト トレランス (NFT)」および「LAG」。
スイッチ ポートで VLAN トランキングを有効にする場合は、適切なモードをサポートするようにポートを構成してください。 一般、アクセス、またはトランキング。 一般的な説明は次のとおりです (詳細については、スイッチのドキュメントを確認してください)。

- 一般: ポートは VLAN に属し、各 VLAN はタグ付きまたはタグなしとしてユーザー定義

されます (フル 802.1Q モード)

- アクセス: ポートは単一のタグなし VLAN に属します
- トランク: ポートは、すべてのポートがタグ付けされている VLAN に属しています。

18.3 ボンディング/チーミング (802.3ad/アクティブ バックアップ)

- ボンディング/チームを作成する際に留意すべき重要な点がいくつかあります。
  親より上位のインターフェイスのみを結合できるため、ポート 10 から開始することを選択した場合は、ポート 11 以降のみを追加できます。
- VLAN のタグ付けが必要な場合は、最初にリンクを結合し、結合が構成された後に VLAN を追加します。
- 結合されたインターフェースにリンクを追加するには、最初に追加するリンクから IP アドレッシングを削除する必要があります
- Active-Backup モードを有効にする場合、通常、スイッチの介入は必要ありません
- eth0 と eth1 の結合は重大な問題を引き起こす可能性があり、発生することは許可されていません

スイッチと LoadMaster の両方で、結合されたすべてのインターフェイスが同じリンク速度に設定されていることを確認します。 ポート 0 をボンディングする場合、Kemp は、ボンディングが完全に構成されて機能するまで、Web 管理インターフェースおよび/またはリモート SSH アクセスを一時的に別のポートに移動することをお勧めします。

18.4 VLAN タギング

注意事項:

- 必要に応じて、最初にスイッチで VLAN タギングを構成します。
- ボンディングが必要かどうかを決定することから始めます。 そうである場合は、まず結合構成を確立し、
  次に、VLAN タグ情報を追加して続行します。
- VLAN は、物理インターフェイスまたは結合されたインターフェイスに追加できます

19 IPsec トンネリング

インターネット プロトコル セキュリティ (IPsec) は、インターネット全体のノードとネットワーク間の安全な接続を提供するために設計され、使用されています。 IPsec は、ほとんどの IP バーチャル プライベート ネットワーク (VPN) テクノロジの標準になっています。 IPsec は、ポイント ツー ポイント (別名ホスト ツー ホスト) 構成またはサイト ツー サイト (別名ネットワーク ツー ネットワーク) 構成で動作できます。 IPsec の実装は、セキュリティ ゲートウェイ (SG) として、または独立したデバイスとしてホスト内で動作し、IPv4 と IPv6 の両方の IP トラフィックを保護します。(セキュリティ ゲートウェイは、IPsec を実装する中間システムです。たとえば、IPsec 対応のファイアウォール、ルーター、またはゲートウェイです。) IPsec を使用することには多くの利点があります。 これらには以下が含まれますが、これらに限定されません。

- 分散した企業全体に提供される安全な接続
- 従来の高価なワイド エリア ネットワーク (WAN) インフラストラクチャよりも優れた帯域幅の利点
- 従来の高価な WAN インフラストラクチャよりも優れたコストメリット
- セキュリティ - IPsec VPN は本質的に高度なデータ セキュリティを提供します。
- 柔軟性 - インターネットを使用して IPsec VPN を確立し、利用可能にすることができます
- インターネット経由で利用可能な重要で機密性の高いアプリケーションの回復力と高可用性 (HA)

ロードマスターが IPsec トンネリングと連携するように構成する方法の詳細な手順を含む詳細については、IPsec トンネリング、機能の説明を参照してください。

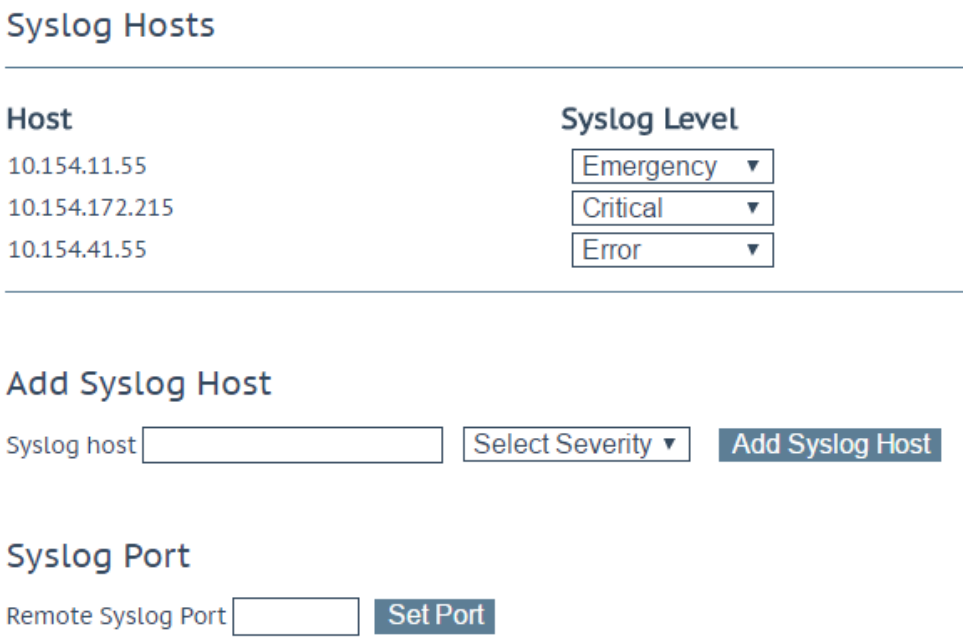
20 その他

20.1 IPv6 サポート

このバージョンの LoadMaster ソフトウェアには、レイヤー 4 とレイヤー 7 の両方での IPv6 サポートが含まれています。ネットワーク アドレスをレイアウトする前に、IPv4 のままにするものと IPv6 に変換するものを検討してください。 LoadMaster は、ネットワークとは異なり、IPv4 と IPv6 をサポートし、変換することができます。 したがって、IPv6 の内部ネットワークがあり、外部 IPv4 ネットワークに相互接続する場合があります。 レイヤー 4 での IPv6 の FTP はサポートされていません。

20.2 リモート Syslog サポート

LoadMaster は、syslog プロトコルを使用して、さまざまな警告およびエラー メッセージを生成できます。 これらのメッセージは通常、ローカルに保存されます。



また、[Syslog ホスト] テキスト ボックスに関連する IP アドレスを入力し、重大度を選択して [Syslog ホストの追加] をクリックすることにより、これらのエラー メッセージをリモート Syslog サーバーに送信するように LoadMaster を構成することもできます。 6 つの異なるエラー メッセージ レベルが定義されています。 各レベルのメッセージは、異なるホスト サーバーに送信される場合があります。 通知メッセージは情報提供のみを目的として送信されます。 緊急メッセージは、通常、即時のユーザー アクションを必要とします。 リモート Linux サーバーの syslog プロセスが LoadMaster から syslog メッセージを受信できるようにするには、syslog を「-r」フラグで開始する必要があります。

20.3 ライセンスの取得方法

LoadMaster ソフトウェアのロックを解除するには、ライセンスが必要です。 ライセンスは、アクセス コードと組み合わせて、LoadMaster インスタンスごとに個別に生成されます。 LoadMaster に対して取得できる 3 つの異なるライセンスがあります。

- トライアル ライセンス - これは、最大 30 日間有効なフル機能のライセンスです。
- 完全な無期限の LoadMaster ライセンス
- 2 台のマシンで構成される LoadMaster High Availability (HA) クラスターの完全な無期限ライセンス

トライアル ライセンスは、フル シングルまたはフル HA ライセンスにアップグレードできます。 ライセンス情報は、[System Configuration] > [System Administration] > [License Management] の Web ユーザー インターフェイスで更新できます。 HA システムを使用している場合は、2 番目の LoadMaster に対してこのプロセスを繰り返します。 Progress Kemp は、ライセンスの更新後に再起動することを推奨しています。 初めて Virtual LoadMaster のライセンスを取得するには、Kemp ID が必要です。 Kemp ID を持っていない場合は、ライセンス、機能の説明を参照して、設定方法を確認してください。 Kemp ID をお持ちの場合は、提供されている WUI オプションを使用して Virtual LoadMaster のライセンスを取得できます。 ライセンスをアップグレードする必要がある場合は、Progress Kemp にお問い合わせください。

20.4 バックアップと復元

必要に応じて、LoadMaster 構成設定をバックアップおよび復元できます。 手動でバックアップを作成できますが、リモート サーバーにバックアップを保存することもできます。 LoadMaster の完全な構成 (仮想サービス、GEO、ESP、および基本構成) は、統計データとともにサーバー上の単一のファイルに保存されます。 バックアップには SSL 証明書情報は含まれません。 サーバーは FTP デーモンまたは SSH デーモンを実行している必要があります。 デフォルトのリモート プロトコルは FTP ですが、SCP に変更できます。 構成を復元するときは、構成のどの部分を復元するかを指定します。

- 仮想サービス構成のみ
- LoadMaster の基本構成のみ
- GEO 構成のみ
- ESP SSO 構成のみ
- 仮想サービス、GEO、ESP、またはロードマスターの基本構成の組み合わせ

基本構成には、LoadMaster の基本構成に関する情報、つまり、さまざまなインターフェースの IP アドレスと、キーボードとタイムゾーンの設定に関する情報が含まれています。仮想サービス構成には、仮想サービスと実サーバーに関連する設定のみが含まれます。 GEO 構成には、GEO 構成に関連する設定のみが含まれます。 ESP SSO 構成には、SSO ドメイン、LDAP エンドポイント、および

SSO カスタム イメージ セットが格納されます。これは、仮想サービスの設定を復元しません。それらを復元するには、VS 構成オプションを使用します。構成を復元する前に、構成を受け取る LoadMaster が、バックアップが作成されたときと同じ高可用性 (HA) モードであることを確認してください。 LoadMaster の基本構成では、現在、個々のユニットから個々のユニットへ、または HA から HA への移行のみが許可されています。これは現在、HA 構成タイプを超えることはできません。 HA の設定方法の詳細については、高可用性 (HA) 機能の説明の「HA の設定」セクションを参照してください。
ケンプのドキュメンテーションページ。日単位または週単位で自動バックアップを構成できます。

20.5 WUI へのアクセスの無効化/有効化

特定の状況では、ユーザーは LoadMaster WUI へのアクセスを無効にしたい場合があります。 これを行うには、LoadMaster WUI で [Certificate & Security] > [Remote Access] に移動し、[Allow Web Administrative Access] チェック ボックスをオフにします。 アクセスが無効になっている場合、ユーザーは LoadMaster WUI を使用できなくなります。 これは、セキュリティまたはその他の理由により、特定の状況で必要になる場合があります。

20.6 L4 と L7 仮想サービス間の相互運用性

サービスが 1 つのパーシステンス方法から別の永続化方法に切り替えられると、すべての仮想サービスおよび実サーバー カウンターの絶対値がゼロにリセットされます。 これにより、相対値 (1 秒あたりのバイト数など) を表示するときに、サービス グラフにピークが発生することがあります。たとえば、バイト カウンターがテラバイト値からゼロにジャンプした場合です。

20.7 ログ情報

ログ ファイルは、[System Configuration] > [Log Options] > [System Log Files] の WUI で表示できます。

- Boot.msg ファイルには、Linux 標準の起動情報が含まれています
- 警告メッセージ ファイルには、コア ロード バランシング エンジンによって生成されたイベントのリストが含まれています
- システム メッセージ ファイルには、コア ロード バランシングおよび基盤となる Linux オペレーティング システムによって生成されたイベントのリストが含まれています。

ログ ファイルは揮発性です。 LoadMaster でのリサイクル時に重要なログ情報を利用できるようにするには、syslog 機能を使用してください。

20.8 デバッグ ユーティリティ

デバッグ ユーティリティは、[System Configuration] > [Log Options] > [System Log Files] > [Debug Options] の WUI で実行できます。 これらは、Progress Kemp サポート チームと連携する際に最もよく利用されます。

20.8.1 すべての Transparency を無効にする

すべての仮想サービスの Transparency を無効にする - このオプションは、Progress Kemp サポート チームの承認を得てのみ変更する必要があります。

20.8.2 L7 デバッグ トレースを有効にする

システム メッセージ ログに記録される追加のデバッグ情報を有効にします。

20.8.3 PS を実行する

プロセス ステータス (PS) を報告します。

20.8.4 l7adm を実行する

レイヤー 7 仮想サービスに関する詳細情報を表示します。

20.8.5 Ping ホスト

任意の IPv4 デバイスに ICMP エコー要求を発行します。 ターゲット IP が ICMP をサポートしていることを確認してください。

20.9 RESTful API インターフェイス

LoadMaster は、リモート アプリケーションがシンプルかつ一貫した方法でアクセスできるように設計されたインターフェイスを提供します。 インターフェイスは REST に似たインターフェイスです。 REST (REpresentational State Transfer) は、
分散システムのソフトウェア アーキテクチャ スタイルであり、主要な Web サービス設計モデルの

1 つです。 LoadMaster RESTful API は、ユーザーまたはアプリケーションが HTTP リクエストを LoadMaster に渡すことを許可することで機能します。 LoadMaster は、XML 形式の応答で要求に応答します。 インターフェイスはデフォルトで無効になっています。 インターフェイスの有効化の詳細については、Web ユーザー インターフェイス (WUI)、構成ガイドを参照してください。 RESTful API の詳細については、Kemp のドキュメント ページにある RESTful API、インターフェイスの説明ドキュメントを参照してください。

21 ネットワーク テレメトリ

LoadMaster は、そのインターフェースを通過するネットワーク トラフィックを監視し、IP フロー情報エクスポート (IPFIX) 形式で豊富なネットワーク テレメトリを生成できます。 IPFIX は、ネットワーク インフラストラクチャでアプリケーションおよびトランザクション データを識別および収集するために使用されるフロー エクスポート標準です。フロー データは、アプリケーション トラフィックの使用率と構造をいつでも可視化して、アプリケーションのワークロードに関連する主要なネットワーク パフォーマンス メトリックをレポートできるようにします。これは、ネットワーク インフラストラクチャを継続的に監視するための完全なパケット キャプチャと分析の代替手段としてよく利用されます。通常、スイッチ、ファイアウォール、ロード バランサー、ルーターなどのさまざまなネットワーク デバイスがフローベースのフィードをコレクターに提供し、コレクターはパフォーマンスの監視および分析ツールセットによって分析されます。 LoadMaster は、ネットワーク テレメトリ機能を使用して、互換性のある IPFIX データ分析システムと連携して、フロー データの可視化に参加できるようになりました。 Kemp は、このデータ分析に Flowmon Collector を使用することを推奨しています。 Progress Kemp Flowmon Collector は、正規化、視覚化、分析などのフロー データをキャプチャ、保存、処理する理想的なネットワーク監視アプライアンスです。ネットワーク テレメトリの詳細については、ネットワーク テレメトリ機能の説明を参照してください。