KEMP ロードマスター

製品概要

バージョン: 1.3
更新: 2013 年 9 月

著作権

制限事項：著作権に関する文書およびその内容のすべては、所有者が提示しているままを記載しています。弊社は、ここに提示された情報が正しいことを確認するための努力を払っていますが、この情報の正確性については明示または黙示的に保証するものではありません。弊社は、このドキュメント上のすべての資料の誤りや不正確な情報に対して、可能であれば使用者が法律上または衡平法上の唯一かつ排他的な救済手段として受け入れられる適切な矯正の通知を提示します。この文書に記載されている情報の使用者は、受取人、または第三者によるコンパイル、またはこのドキュメントを提供したり、通信や公開の任意のアクションまたは不作為からの傷害または損害、およびこれらに限定されない現在または将来失われる利益および損失を含むあらゆる直接的、特殊的、付随的または派生的損害（を含むがこれらに限らず、あらゆる種類の損失、のれんの損傷）に対して、弊社が責任を負うことはできないことを認めるものとします。

このガイドで使われるインターネット・プロトコル（IP）アドレス、電話番号または他のデータが、実際に存在する連絡先に似ている場合も、実際のアドレス、電話番号または連絡先であることを目的としません。この文書に含まれる例、コマンド出力、ネットワークトポロジ図、およびその他の図は説明のみを目的として提示されています。例示の内容に、実際のアドレスや連絡先情報が使用されている場合は、意図的なものではなく偶然の一致によるものです。

懲戒的、間接的損害（代替製品やサービスの調達費用、または、これらに限定されない使用不能損失、データ、または利益の損失、または事業の中断による損失）、またはいかなる原因およびその理論による債務、いかなる契約、厳格責任、または不法行為（不注意、またはその他を含む）による損害に対して、何ら責任を負わないものとします。

ソフトウェアおよびドキュメントに含まれる見解および結論は著者のものであり、上記著作権者の表現、または暗黙な公式方針を表すものではありません。

ロードマスターのソフトウェアの一部分は、1989、1991 年に、51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA にある Free Software Foundation, Inc.と KEMP Technologies Inc.が著作権を保有し、GNU ライセンスのバージョン 2（1991 年 6 月）の要件に完全に準拠しています。このライセンス文書の写しをコピーして、正確に言葉通りに頒布することは誰もが許可されていますが、それを変更することは許されません。

このソフトウェアの一部は、カリフォルニア大学のリージェンツが 1988 年に著作権を所有し、すべての権利を保有しています。

この部分については、ソースおよびバイナリ形式での再配布および使用は、広告材料、およびそのような流通と使用に関連した資料、フォーム、ドキュメンテーションに、上記著作権表示と、ソフトウェアがカリフォルニア大学バークレー校によって開発されたことを認めるこの文節を複写して行うことで許可されています。大学の名前は、特定の書面による事前の許可なしに、本ソフトウェアから派生する製品を是認または促進するために使用することはできません。

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

（参考訳）
本ソフトウェアは“現状有姿”で提供され、特定の目的に対する商品性および適合性の黙示の保証に限定されずに明示的または黙示的ないかなる保証も致しません。

このソフトウェアの一部は、マサチューセッツ工科大学が 1998 年に著作権を保有しています。

この部分のソフトウェアおよび関連文書のファイル（“ソフトウェア”）は、変更、コピー、配布、他のソフトウェアとの併合、サブライセンスの発行、本ソフトウェアのコピーの販売、および/または本ソフトウェアの他製品への組み込みは、以下の条件に従うすべての人へ制限なしに許可されます。

ソフトウェアがすべてそのまま複製されているか、または重要な部分として使用されている場合、上記著作権表示および本許諾表示を記載しなければなりません。

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

（参考訳）
本ソフトウェアは、“現状有姿”で提供され、明示または黙示の保証を含み、それに限定されない特定の目的に適合するような黙示的な保証は放棄されています。いかなる場合においても、作者または著作権者は、ソフトウェアの使用またはその他の扱いに関連して、または関連しないで生じる、契約、不法行為またはその他の行為によるいかなる請求、損害、またはその他の責任の債務は負いません。

このソフトウェアの一部（1995 年に発行、2004 年に修正）は、Jean-loup Gailly および Mark Adler が著作権を所有しています。

この部分のソフトウェアは“現状有姿”で、明示または黙示の保証なく提供されています。いかなる場合においても、作者はこのソフトウェアの使用から生じるいかなる損害に対しても責任を負いません。

このソフトウェアは、次の制限事項を例外として、自由に変更、再配布し、商用アプリケーションへの使用を含めあらゆる目的に対して誰でも使用することを許可されます。

1. このソフトウェアの出所について虚偽の表示をしてはなりません。あなたが、オリジナルのソフトウェアを書いたと主張してはいけません。任意の製品でこのソフトウェアを使用した場合は、必須ではありませんが、製品ドキュメント内にその旨を述べていただければ感謝します。

2. ソースを変更したバージョンを使用する場合、オリジナルのソフトウェアとして誤解されないように、その旨を明示しなければなりません。

3. このソースを配布する場合は、これらの通知を削除したり変更したりすることはできません。

このソフトウェアの一部は、2003 年に Internet Systems Consortium が著作権を所有しています。

この部分に関して、手数料の有無にかかわらず、本ソフトウェアを使用、コピー、変更、および/または任意の目的での配布は、上記の著作権表示とこの許可告知文があらゆるコピーに表示されている限り許可されます。

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

（参考訳）

本ソフトウェアは、"現状有姿"で提供され、作書は、市場への適合性や適切性へのすべての黙示的保証を含め、本ソフトウェアに関して一切の保証をいたしません。作者は、いかなる場合においても、本ソフトウェアの性能、使用または不使用によって生じるいかなるデータまたは利益の損失、契約、過失、またはその他の不法行為から生じる特別、直接的、間接的は損害、または結果的損害に対して一切の責任を負いません。

使用許諾、米国特許 No. 6,473,802 および 6,374,300 に基づいて使用

目次

1 KEMP テクノロジー社とロードマスター製品のご紹介

1.1 KEMP テクノロジー

KEMP テクノロジーは、中小規模レベルのアプリケーション配信（ADC）／負荷分散装置を手ごろな価格で購入をご検討のお客様へ、最高の価格/性能比の提案を提供できる業界のリーダーです。当社製品の汎用性と強力なアーキテクチャは、従業員の皆様が、パートナーや顧客とビジネスを行うためのインターネットベースのインフラストラクチャに依存した事業への最適化を可能にしながら、最高レベルの価値を提供します。

1.2 ロードマスター製品

KEMP テクノロジー社のロードマスターファミリーは、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する機能豊富なアプリケーション・デリバリ・コントローラおよびサーバー・ロード・バランサ・アプライアンスです。あらゆる規模の企業とマネージドサービスプロバイダにウェブサイトの完全性を提供します。

KEMP 製品は、IT コストを効率化しながら、高可用性、高パフォーマンス、柔軟な拡張性、操作がしやすいセキュアな管理方法により、Web インフラストラクチャを最適化します。ロードマスターは、ネットワークリソースの管理を簡素化し、多様なサーバー、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し、加速させます。

あなたの組織にとって、ウェブサイトやイントラネットの使用が重要である場合は、安全で継続的な稼動とアクセス可能なサイトがあなたの成功への鍵です。KEMP テクノロジー社の強力で、高い信頼性のインフラストラクチャアプライアンスである ADC／ロード•バランサは、コストを削減させながら大幅な Web サーバーのパフォーマンスの向上による顧客の Web アクセス体感を高めてあなたのビジネスを支えるでしょう。

1.3 ロードマスター・ロードバランサの特長

ロードマスター・ロードバランサは、バランサ用 OS（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）を持ち合わせ、次の機能を提供します。

- 多種バランシング方式
- 多種パーシステンシー（持続性）
- アプリケーションのフロントエンド（ADC）
- SSL アクセラレーション/オフロード
- コンテンツスイッチングベースのルール
- 各種ヘルスチェック

- SNMP サポート
- ユーザー管理
- IPv6 のサポート
- ボンディングおよび VLAN
- エッジセキュリティ

これらの機能は、次の章で詳しく説明されています。

2 ロードマスター・ネットワークトポロジの例

2.1 1 アーム・バランサ

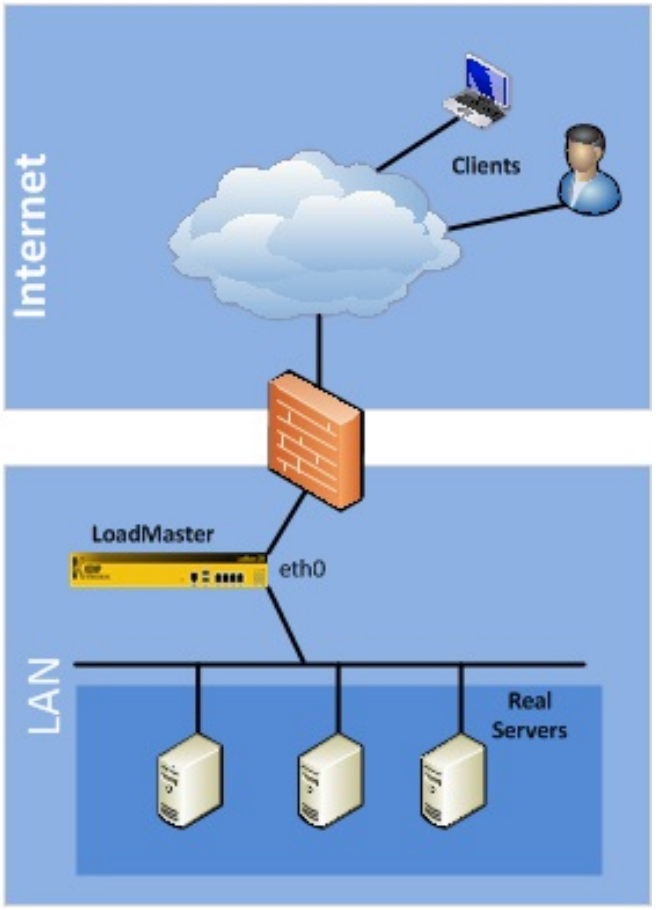


図 2-1: ロードマスターシングル、1 アームの構成

1 アームの設定が選択されている場合は、次のことが当てはまります。

- eth0 のみのイーサネットインターフェイス（イン／アウトバウンド両方のトラフィック用）が使用されます。
- 実サーバーおよび仮想サービスが同じ論理ネットワーク上の一部になります - 時にはフラットベースと呼ばれます - これは、インターネット上のサービスとして使用される場合は、両方がパブリック IP アドレスを持っていることを意味します
- 1 アーム構成では、サーバーNAT は意味を持ちません。
- 実サーバー上の自動的なダイレクト・サーバー・リターン（DSR）方式を使用することを意味するものではありません。
- クライアントがロードマスターと同じ論理ネットワーク上に存在するならば、クライアントのソース IP アドレスの実サーバーへの透明的な転送は、'DSR'方式を

使用することで正しく機能します。もう一つの転送モードである'NAT'方式では、透過的なソース IP アドレスの転送はサポートされません。

1 アーム型ソリューションは、シングルおよび HA 構成の両方で使用されます。

2.2 2 アーム・バランサ

下図は、2 アームにてロードマスターを構成した例です。

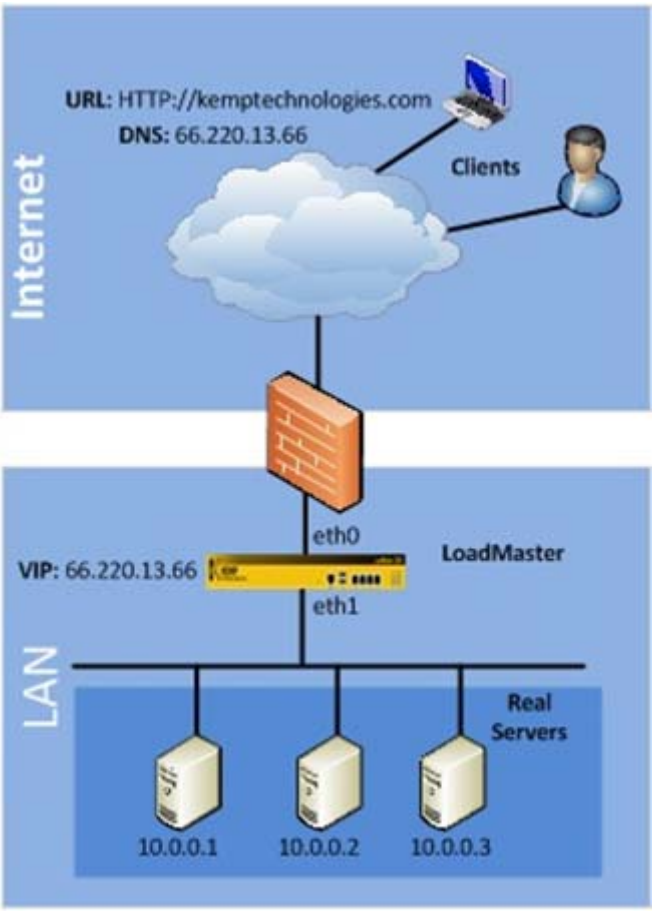


図 2-2：ロードマスターシングル、2 アームの構成

システムは、次のように構成されています。

- 66.220.13.66 の IP アドレスを持つ HTTP サービス用仮想サービス（VS）は、ロードマスター上に作成されています。
- VS は実サーバー（RS）であるサーバー1、2、3 間の着信トラフィックの負荷バランスをとるように設定されています。
- Web ユーザーの要求 URL は、http://www.kemptechnologies.com です。
- DNS によって、この URL が IP アドレス 66.220.13.66 に解決されます。
- リクエストは、eth0 のネットワーク・インターフェイスの IP エイリアスとして、この IP アドレスを持つロードマスターにルーティングされます。

- ロードマスターは、ネットワーク·インターフェイス eth1 経由でサーバーファームのサブネット 10.0.0.0 に接続されています。
- ロードマスターは、要求されたアドレス 66.220.13.66 の為に、必要なコンテンツを配信することができる 3 つの実サーバーがこのサブネット内に割り当てられていることを知っています。
- ロードマスターは、3 つの実サーバーのいずれかに要求を送信するために、あなたが設定した負荷分散方式、例えば、重み付けラウンドロビンを使用します。
- 2 アーム構成での設定に関する注意すべき他の項目は、次のとおりです：
- イーサポート 0（ネットワーク側）とイーサポート 1（ファーム側）の両方のインターフェイスが使用されます。マルチアームでは、他のイーサポートもファーム用として追加されます。
- ロードマスターのネットワーク側とサーバーファームは、NAT ベーストポロジと呼ばれる独立した論理ネットワーク上に位置します。
- サーバーファームは、ルーティング不能（RFC1918）の IP アドレスを使用することができます。
- S-NAT は、このような構成で有益です。
- ロードマスターとクライアントが同じ論理ネットワークに位置している場合、IP アドレスが透過モード（トランスペアレンシー）でも仮想サービスへのアクセスは正しく機能します。
- 仮想サービスは、どのイーサポートのサブネットを使用しても作成可能です。
- 実サーバーは、どのイーサポートにでも存在できます。しかしながら、イーサポート 0 への設定は、2 アーム構成時には推奨されません。

1 アーム、2 アームに関係なく、各ポートに一つ以上のサブネットを追加可能です。

2.3 ハイ・アベイラビリティ ハイ・アベイラビリティ (HA) の設定

ロードマスターのハイ・アベイラビリティ機能（HA）は、システム上のサービスの可用性を保障するものです。HA は、ホット-スタンバイ、およびフェイルオーバー・メカニズムにより実現されます。 2 つのまったく同じロードマスターのユニットが、ネットワーク上で融合されます。1 台のユニットがアクティブ・バランサとして実トラフィックを処理し、2 台目がスタンバイ・バランサとして、アクティブ・バランサに障害が発生した時にいつでも活動を引き継げるように、準備状態になっています。この 2 ユニット・クラスターは、ネットワークサイドとサーバーファームの両方からは、シングルの論理ユニットとして見えます。

2 つのロードマスターが、相互に監視しあって構成されている HA クラスターとして稼動中ならば、各ネットワーク・インターフェイスは独自の IP アドレスとシェアード IP アドレス（フローティングとも呼ばれる）を持ちます。シェアード IP アドレスは、両方のロードマスター・ノードで共用されます。しかし、アクティブなロードマスター装置だけにこのアドレスの実使用が許されます。

ロードマスター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、必ず HA ペアの共有アドレスを使用してください（このアドレスは常に利用可能となるため）。

通常稼動中は、各ノードが一定周期で相手のマシンの可用性を 2 つの接続（通常イーサポート 0 と 1）を介してハートビート・メッセージ（hb 方式）、もしくはブロードキャスト（carp 方式）を送ることで相互にチェックし合っています。何らかの異常が起こり、アクティブのロードマスターがダウンしたならば、スタンバイ・マシンがアクティブとなり、負荷分散の全タスクを引き継ぎます。

HA モードでの 1 アームトポロジは下図のようになります：

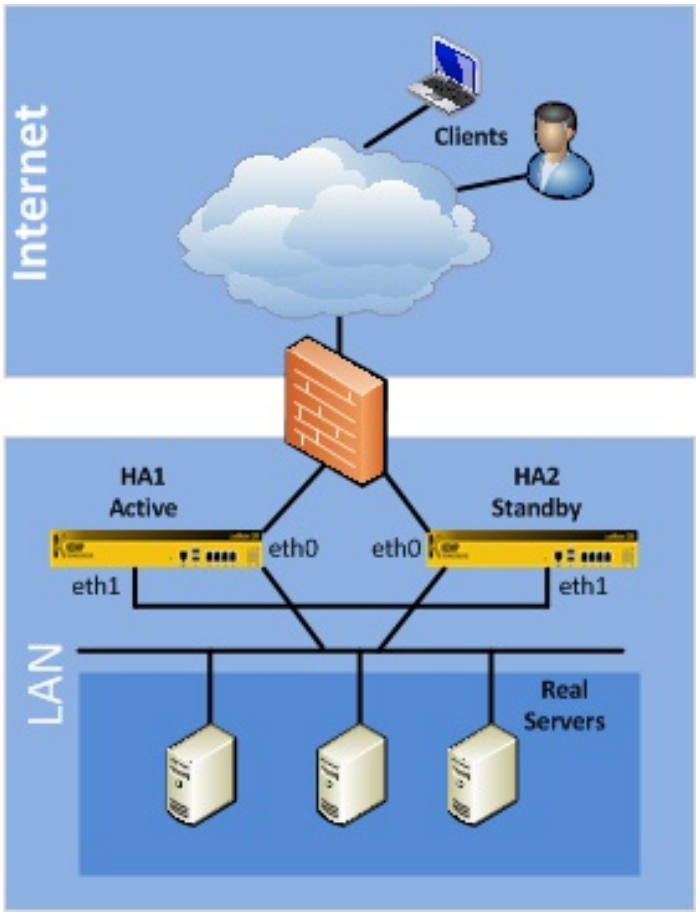


図 2-3：ロードマスターHA、1 アームの構成

ロードマスターHA1 と HA2 は、eth0 を使用してネットワーク（ファイアウォール）とサーバーに接続され、この 2 つのポートは 1 つの共有 IP アドレスを持っています。また、各ユニットの eth1 はパッチケーブルで直接接続されており、増設 HA との間の死活チェック専用ポートとして使用されます（このポートは自動検出機能を持っているため、ストレートケーブルとクロスケーブルのどちらでも使用できます）。なお、eth0 上の HA チェックが何らかの理由で中断されたときに 2 台ともマスターになるのを防ぐため、eth1 を直接接続するようにしてください。

HA 構成での 2 アームトポロジは次のようになります：

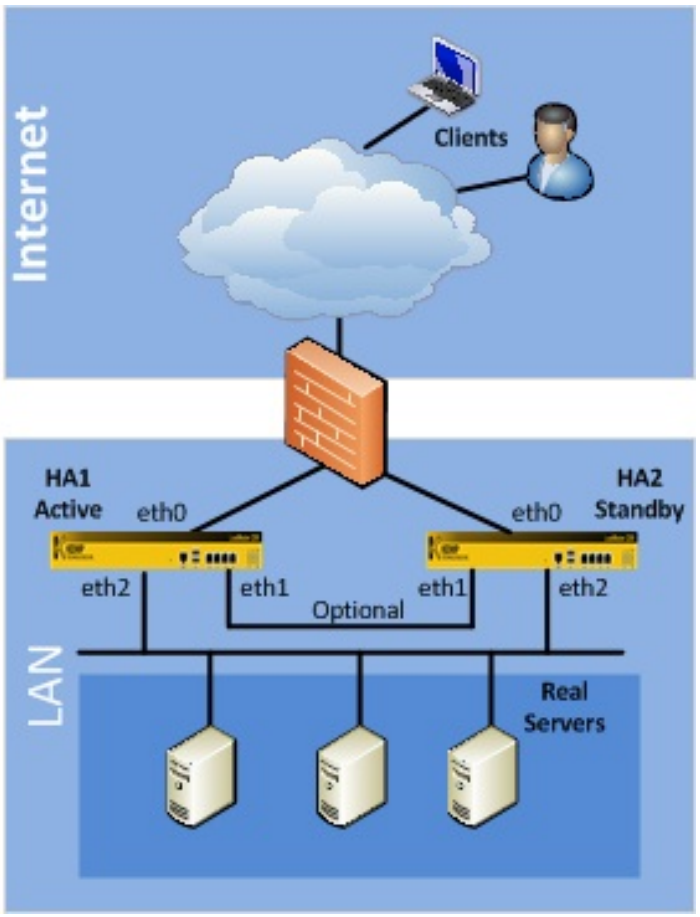


図 2-4：ロードマスターHA、2 アームの構成

HA1 と HA2 の両方とも、ネットワークに接続するために eth0（ファイアウォール）とサーバーへの接続用に eth2 を使用します。両方の eth0 のポートは、個別の IP アドレスと 1 つの共有 IP アドレスを持ち、両方の eth2 ポートは異なる個別の IP アドレスと異なる共有 IP アドレスを持っています。システムは、両方の eth ポートを使用して、2 ユニット間の死活チェックを行います。既に、HA ペアの間に 2 つのヘルスチェックのルートがあるので不要ですが、追加的な必要性に応じて、各ユニットの eth1 を直接パッチケーブルを介して接続することができます。

> HA1 と HA2 の両方は、同じ物理サイト内に配置されて同じサブネット上になければなりません。死活チェックや、共通アドレスを使用するためにイントラサイト内リンクで区切られてはならず、トラフィックを正しく返すために同じゲートウェイを使用する必要があります。

HA は、物理的に離れたサイトの複数のサブネットをまたいでの構成は組めません。複数のサイトを利用したトラフィックの分散が必要な場合は、サイトの死活チェックができる KEMP の DNS ベースのアプライアンスである GEO ロードマスターが正しい解決策となるでしょう。

2.4 ダイレクト・サーバー・リターン ダイレクト・サーバー・リターン- DSR 構成例

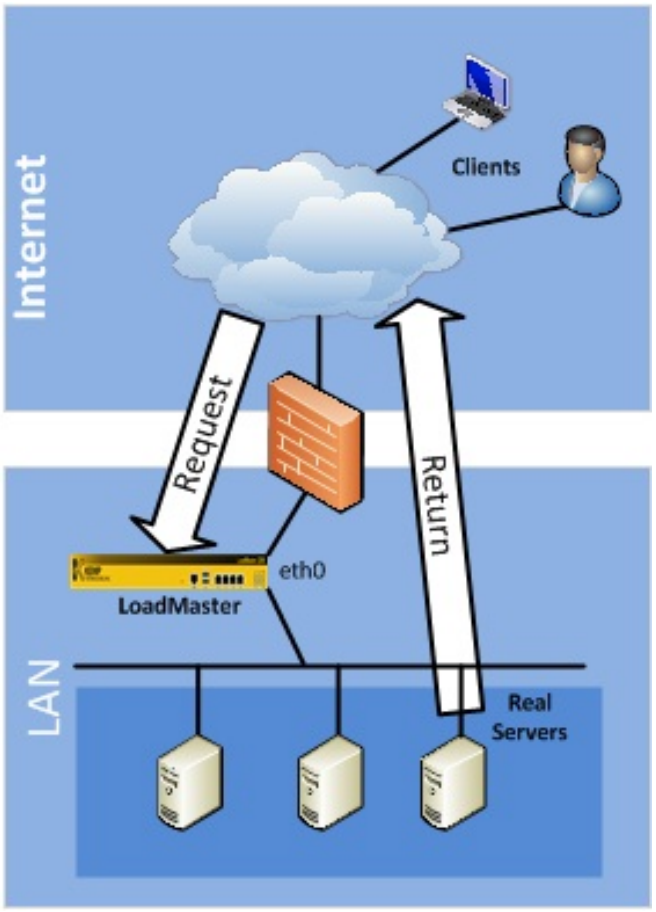


図 2-5：単一のロードマスターDSR、1 アームの構成

1 – ロードマスターが、クライアントからリクエストを受信

2 – 実サーバー1 へとルーティング

3 – 実サーバー1 よりレスポンスを送信

4 – レスポンスは、ロードマスターを介さずにクライアントに直接返信

この機能は、実サーバーがロードマスターを介さずに、直接クライアントにレスポンスを返す必要があるときにだけ設定してください。この構成では、実サーバーはクライアントへの直接パス（例えば、ロードマスターと併設されたルータを介した）を持っていなければなりません。

DSR 構成時には、パーシステンシー 構成時には、パーシステンシー（セッション維持）はソース （セッション維持）はソース IP オプションだけが指定可能です。また、仮 オプションだけが指定可能です。また、仮想サービス（VS）の設定は、L4 の透過モードにしなければなりません。非透過モード(L7 のみ)では、クライアントのソース IP アドレスが RS に送られないので、この機能は動作しません。

DSR には、MAT（MAC アドレス・トランスレーション）と実サーバー（RS）設定変更のコンビネーションが使われます。RS には、通常の IP アドレスを設定しますが、VS 用の IP アドレス（VIP）も設定する必要があります。通常では、VIP アドレスはロードマスター以外の機器に重複して設定することはできません。この問題を解決するためには、実サーバーへ設定する VIP アドレスが、ARP リクエストに対してレスポンスを返さないようにする必要があります。現状でカーネル 2.6 バージョンをもつ Linux では、ループバック・インターフェイス上に IP エリアスとして VIP アドレスを設定することで対応が可能です。

サーバー（Linux と Windows の両方）を設定する方法の詳細については、**DSR 用実サーバーの設定　テクニカルノート**を参照してください。

3 負荷分散方式（Scheduling Method）

ロードマスターには、“スケジューリング・ルール（Scheduring Rules）”もしくは、“アルゴリズム”として一般的に知られている分散方式が多種備わっています。

3.1 ラウンドロビン（Round Robin）

この方式では、入ってくるリクエストはサーバーファーム群のなかの可用なサーバーへ順番に分配されます。

もし、全てのサーバーが同等のリソースを持っていて、サービスへの同じような負担を抱えているのであればこの方式を選択してください。このような前提条件ならば、ラウンドロビンはシンプルで効果的な分配方式です。

しかしながら、もしサーバーが異なるリソースを持っているならば、ラウンドロビン方式を使うことにより非力なサーバーが現在の処理を終了する前に次の要求を受けるようになってしまいます。これは、非力なサーバーがオーバーロードとなる原因になります。

3.2 重み付けラウンドロビン（Weighted Round Robin）

この方式は、シンプルなラウンドロビンの弱みを補ってくれます。入ってきたリクエストは、前もってサーバーごとにアサインした静的重みを計算しながら、サーバー群の各サーバーに順番に配分されます。

管理者は、サーバーの重みをサーバーのリソースに合わせて容易に設定できます。はるかに能力が劣るサーバーB の重みを“50”とすると同時に、最も能力の高いサーバーA には、例えば重み“100”を与えます。これは、サーバーB が最初のリクエストを受け取る前に、サーバーA が 2 つ続けてリクエストを受け付けることになります。そしてこのパターンを繰り返します。

3.3 最小接続（Least Connection）

前述のラウンドロビン方式は、一定時間内に幾つの接続が持続されているかの統計結果を配分計算に取り入れません。それにより、サーバーA より少ないリクエストを受け取っているサーバーB がオーバーロードになることがあります。なぜならば、サーバーB へ配分されたユーザーが、接続を長く持続している場合があるからです。持続している接続数が多いとサーバーへのリクエストが多くなり負荷も増加します。

この潜在的な問題は、最小接続方式により防げます。この方式では、リクエストは全てのサーバーが現在持続している接続数を基に計算されて配分されるからです。クラスター内のサーバーで、アクティブな接続数が一番少ないサーバーが、次のリクエストを必然的に受け取ることになります。パフォーマンスに対しては、基本的には単純なラウンドロビンと同じ原理です。従って、この方式に関係するサーバーは、同じようなパフォーマンスのリソースを持つことが理想的です。

なお、トラフィックレートが低い構成の場合、負荷分散は行われずに最初のサーバーが選択されます。なぜなら、全てのサーバーの条件が等しい場合は、最初のサーバーが選択されるからです。最初のサーバーでアクティブなトラフィックが継続的に処理されるようになるまで、常に最初のサーバーが選択されます。

3.3.1 最小接続方式のスロースタートタイム

最小接続方式と重み付け最小接続方式のスケジューリングでは、実サーバーが最初にオンラインとなったときに、接続可能数を初めは制限しておいて徐々に増やしていくように、時間を設定することができます。これにより実サーバーの「起動時間」が確保され、起動時に接続が殺到してサーバーが過負荷になるのを防ぐことができます。

この値は L7 の設定画面で設定します。

3.4 重み付け最小接続（Weighted Least Connection）

もしサーバーが、異なるパフォーマンスのリソースを持っている場合、重み付け最小接続方式（“weighted least connection”）は最も適切な方法です。アクティブな接続数と管理者によって設定された個別の重みとの組み合わせは、最小接続と重み付けの両方の長所を採用することで、一般的にサーバー負荷が平準化された結果をもたらします。

概して、この方式は接続数とサーバーの重み付けの混合比率を使用するので、正当な配分方法といえます。ファーム内の最低比率を持ったサーバーが自動的に次のリクエストを受け取ることになります。

なお、この方式についても、最小接続方式の低負荷レート警告が適用されます。

3.5 エージェント・ベースのアダプティブ配分（Adaptive）

上記の方式の他に、ロードマスターは一定期間ごとにサーバーの状態をチェックし、動的に重み付けを行うことができる適応性の高い方式であるアダプティブ配分をサポートしています。

極めて強力なエージェント・ベースのアダプティブ配分方式は、バランサが周期的にファーム内、全サーバーのシステム負荷をチェックします。各サーバーマシンは、自分自身の実際の負荷を 0 から 102 までの数値（0＝アイドル、100＝オーバーロード、101＝失敗、102＝管理的に使用負荷）で表すファイルを用意する必要があります。バランサは、このファイルを HTTP GET により取得します。実際の負荷値を格納した ASCII ファイルを用意してロードマスターに返すのはサーバーの役割です。サーバーがどのようにこの情報を査定するかについては、必須条件はありません。

この方式がシステムに問題を発生させないために、“Rules & Checking”サブメニューの“Check Parameters”内にある“Min. Control Variable Value(%)”を調整することを推奨します。

“Min. Control Variable Value(%)”（最低制御変化値）を変更する場合は、“Min. Control Variable Value (%)”の矢印をクリックし、リストの中から適切な値を選択します。このパラメータは、負荷分散対象の各実サーバーの重みの割り当てを、パフォーマンスエージ

ェントが読み込んだパフォーマンス値に従わせるのを開始するための閾値です。仮想サービスにアサインされている全ての実サーバーのパフォーマンス値がこの閾値を超えない限りは、実サーバーの重みに従ったトラフィックの割り当ては、静的に設定されている値を使用して行われます。この場合の負荷分散方式は、静的分散方式である重み付けラウンドロビン方式が使用されます。デフォルトの閾値は 5%です。

アダプティブ・バランシングに関する詳細については、**エージェントベースのアダプティブ・バランシング用 API　テクニカルノート**を参照してください。

3.6　固定重み付け配分（Fixed Weighted）

この方式では、重み付けが一番高い実サーバーのみが使用されます。もし、一番重み付けの高いサーバーが使用不可となった場合は、次に重み付けの高いサーバーがクライアントからのリクエストを処理し応答します。全ての実サーバーは、どのサーバーが優先的にクライアントからのリクエストを処理するかの順番に従って異なる重み付けをする必要があります。

3.7　重み付けレスポンスタイム（Weighted response time)

この方式では、重み付けラウンドロビン方式にてスケジューリングされます。ラウンドロビン方式で使用する重みは、ヘルスチェック要求からのレスポンスタイムで計算されます。

各ヘルスチェック要求に対し、応答に要する時間が測定されます。なお、ヘルスチェックの応答速度は、マシンの速度に応じて変わります（ただし、そうならない場合もあります）。

仮想サービス上にある全ての実サーバーのトータルのレスポンスタイムが加算され、その結果に基づき個々の実サーバーの重みが計算されます。

重みは約 15 秒ごとに計算されます。

3.8　ソース IP ハッシュ（Source IP Hash）

送信元 IP アドレスのハッシュ値が生成され、適切な実サーバーを見つけるために使用されます。これは、同じ IP アドレスを持つホストには、常に同じ実サーバーが使用されることを意味します。
このスケジューリング方式では、ソース IP パーシステンシーの選択を必要としません。

この方式では、実サーバーの負荷不均衡を引き起こすことがあります。

4 パーシステンス（Persistence）

4.1 パーシステンシー入門

アフィニティ、サーバーアフィニティ、もしくはサーバースティッキーとも呼ばれるパーシステンスオプションは、個々のクライアントからのリクエストをサーバーファームの同じサーバーに送るようにする機能です。パーシステンシーは、デフォルトでは設定されていませんが、各仮想サービスを作成するときに設定可能なオプションです。

パーシステンシーなしでは、ロードマスターはラウンドロビン方式や、重み付けラウンドロビン方式などの負荷分散アルゴリズムに従ってトラフィックをサーバーに導きます。(図 4-1)

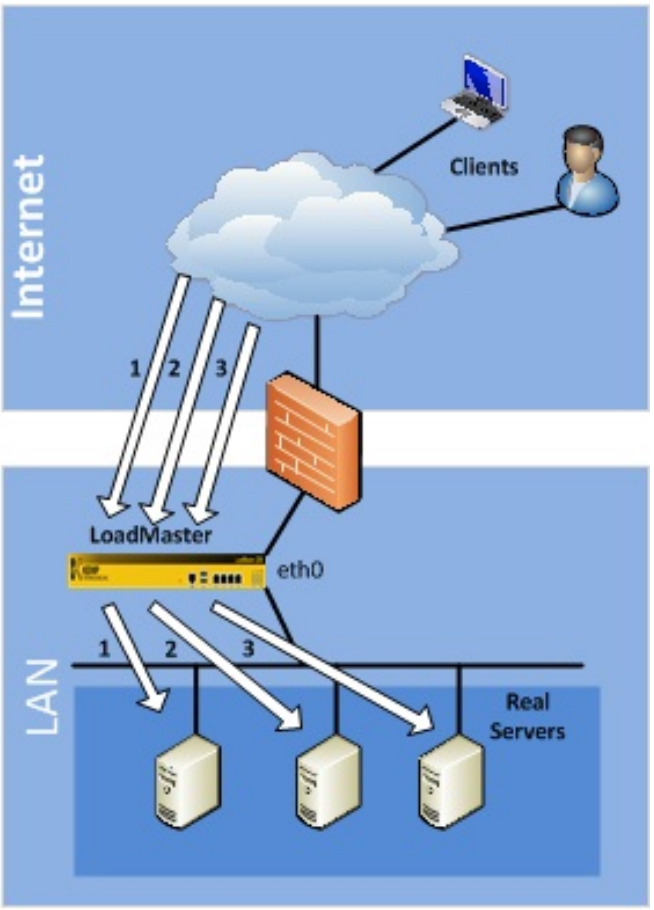


図 4-1：パーシステンスせずに負荷分散

パーシステンシーを利用すると、ロードマスターは新しいリクエストを負荷分散アルゴリズムにより特定のサーバーへと導きますが、次のリクエストは前回と同じサーバーへ導きます。(図 4-2)

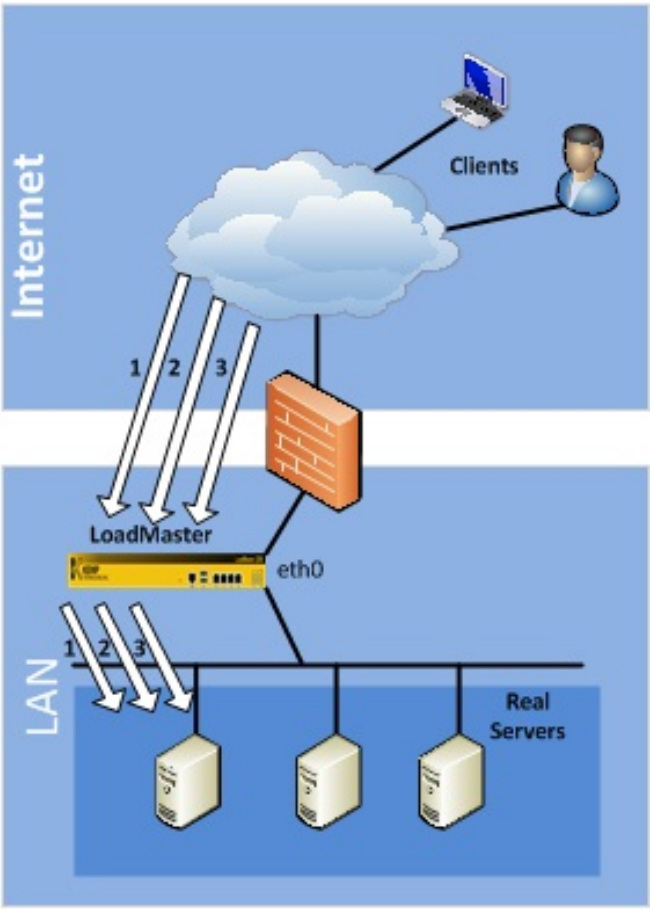


図 4-2：パーシステンス性を持つロードバランシング

4.2 パーシステンシーの必要性

稼動中のサイトがインタラクティブなサイトであればパーシステンシーの必要性が高まります。ログインを求めてくるサイトですと殆ど必要です。もし、静的なテキストやイメージだけを提供するサイトであれば、パーシステンスの必要性はないかも知れません。ほとんどの場合、必要がないとしてもパーシステンスが悪い影響を与えることはありません。

ASP や PHP 等の多数のウェブサイト用プログラム言語のセッションをハンドルするメカニズムは、ステートフル（状態保持）として知られ、ユーザーのためにユニークなセッションを張り、その状態を同一のサーバーに保存します。ログイン時のユーザー証明からショッピングカートの中身まで含んだこのステートフル（状態保持）情報は、一般的にサーバー間では共有しません。よって、複数のサーバーを使用する場合は、各ユーザーがインタラクティブにサーバーとのやり取りを行っている間は、特定のサーバーとの接続を保持することが重要で、パーシステンスは正にこのためにあります。

4.3 タイムアウト（Timeout）

各パーシステンシー・モードには、各ユーザーにどれだけのセッション維持時間が与えられるかを指定する、1 分から 7 日間までの選択可能なタイムアウト値があります。

このタイムアウトの時間は、直近のアクティブとなった接続の開始時間よりカウントされます。もし、クライアントがタイムアウト時間内に何度も仮想サービスにリクエストをした場合は、確実にセッションが同じサーバーに維持されます。

例えば、もし仮想サービスのタイムアウト値を 10 分とし、そしてユーザーが幾つかのリクエストを 20 分内で行ったとしても、各リクエストの間隔がいつも 10 分以内であればパーシステンスは有効です。もし、ユーザーが 20 分間のアイドルを取った場合、次の接続は新しいセッションとしてカウントされ、リクエストは前回とは違うサーバーへ送られるかもしれません。このようにタイムアウト値が十分な時間でない場合は、もっと長い値をセットする必要があります。基本的には、アプリケーション側の Timeout 値と同じにすることを推奨します。

4.4 レイヤ 7 パーシステンス方式

IP アドレス、ポート以外に、HTTP プロトコルでは色々な情報をセッション維持のために使用する方法があります。

4.4.1 サーバー・クッキー・パーシステンス

サーバー・クッキー・オプションは、どのサーバーに HTTP リクエストを送るかを決定する際に、サーバーが作成した既存のクッキーを使うレイヤ 7 機能の 1 つです。この方式は、パッシブクッキーとも呼ばれ、ロードマスターはクッキーの作成や管理をしないで、単に HTTP パケットストリームの中の指定されたクッキーをモニターします。

サーバー・クッキー・パーシステンス方式では、ロードマスターがどのクッキーを参照すればよいかを知るために、クッキー名オプション（図-6）を設定する必要があります。サーバー・クッキー・パーシステンスが問題なく働くためには、サーバーによって作り出されるクッキーが、個々のユーザーのためにユニークな値を持っている必要があります。

4.4.2 アクティブ・クッキー・パーシステンス（Active Cookie Persistence）

アクティブ・クッキー・パーシステンス方式は、サーバー・クッキー・オプション方式と同じようにクッキーを使用するレイヤ 7 機能の 1 つですが、アクティブ・クッキーはサーバーではなく、ロードマスターによりクッキーが作り出されます。

アクティブ・クッキー・パーシステンス方式を設定した仮想サービスに接続要求があった時、ロードマスターは特定のクッキーを見つけ出そうとします。もし、そのクッキーがない場合は、サーバーからのレスポンスをクライアントに返す時に、HTTP パケット内に Set-Cookie ディレクティブとしてクッキーを挿入します。既にレスポンス内にサーバ

一からのクッキーが存在した場合でも、そのクッキーの破棄、改ざん等は行わずに新たにクッキーを追加します。

アクティブ・クッキーの値は、ロードマスターがユーザーを識別するためにユーザーごとにユニークです。

この方式の長所は、サーバーでクッキーを作成、管理する必要がなくサーバー設定の負担を軽減できることです。

共通のプロキシサーバーなどを経由してクライアントからの HTTP セッションが張られる場合は、違うユーザーでも同じクッキーが使用されて負荷が正常に分散されません。この場合は、各セッションごとにアサインされるポート番号をクッキーに挿入させる“Add Port to Active Cookie”機能をオンにしてください。

4.4.3 サーバー・クッキー、もしくはソース IP パーシステンス（Server Cookie or Source IP Persistence）

サーバー・クッキー、もしくはソース IP のセッティングは、サーバー・クッキー・パーシステンスと同じです。もし、何らかの理由で期待していたクッキーが検出できなかった時（例えばユーザーがクッキーの使用を許可していない時に起こり得ます）、パーシステンスの決定にソース IP アドレスが使用されます。

4.4.4 アクティブ・クッキー、もしくはソース IP パーシステンス（Active Cookie or Source IP Persistence）

アクティブ・クッキー、もしくはソース IP のセッティングは、アクティブ・クッキー・パーシステンスと同じです。もし、何らかの理由で期待していたクッキーが検出できなかった時、パーシステンスの決定にソース IP アドレスが使用されます。

もし、特別な条件が無く、レイヤ 7 のパーシステンスの使用を意図するならばこの方式を推奨します。サーバーでの設定は必要ありませんし、ロードマスターがクッキー関連の全ての管理を行うことと、クライアントがクッキーを許可しない設定を行っている場合、ソース IP アドレスを使用することが可能だからです。

4.4.5 ハッシュ全クッキー・パーシステンス（Hash All Cookies Persistence）

ハッシュ全クッキー方式は、HTTP ストリームの中の全クッキーの値を用いてハッシュを作り出します。もしこの値が異なったら、まったく新しい接続として扱います。そして、リクエストは負荷分散アルゴリズムに従ってサーバーへと配分されます。

4.4.6 ハッシュ全クッキー、もしくはソース IP パーシステンス（Hash All Cookies or Source IP Persistence）

ハッシュ全クッキー、もしくはソース IP は、ハッシュ全クッキーと同じですが、HTTP リクエスト内にクッキーがなかった場合にパーシステンスにソース IP アドレスが使用されます。

4.4.7 ソース IP アドレス・パーシステンス

ソース IP アドレス・パーシステンスは、入ってくるリクエストにあるソース IP アドレスをユーザーの識別に使用します。これは、パーシステンシーの一番シンプルな方式で、HTTP に関連しないものも含めて、全ての TCP プロトコルで働きます。

ソース IP アドレス・パーシステンスは、コンテント・スイッチおよびダイレクト・サーバー・リターンと一緒に使用できる唯一のパーシステンスのオプションです。

4.4.7.1 ソース IP アドレスの欠点

ソース IP パーシステンスは、パーシステンスを正しく維持するためには望ましくない、もしくは有効でない状態があります。それらの状態に含まれるのは:

- 多くの（または全ての）ユーザーが単一の IP アドレスを使う場合
- ユーザーが自身の IP アドレスを切り替える場合

最初のケースは、しばしば、多数のユーザーが単一のプロキシーを経由してリクエストしてきて、あたかもシングル IP から来たような状況に遭遇するものです。ソース IP パーシステンスでは、全てこれらのユーザーがシングル・ユーザーに見えてしまいます。他でも同じようなことが起こるケースとしては、インターネットを経由して 1 つのオフィスから全てのクライアントのリクエストが来る場合です。オフィスで使用しているルータは、一般に全てのオフィスのシステムを 1 つの IP アドレスに NAT してしまいます。そして全てのリクエストがシングル・ユーザーからのように見えてしまいます。これは、新しいユーザーセッションが来ても、全てを分散しないで同じ実サーバーへと導き、偏った負荷分散の結果を招いてしまいます。

2 つ目のケースは、歴史的に大きな憂慮点であるメガ-ISP（例えば Nifty や Biglobe）のいくつかでプロキシサーバーを使っている場合です。このような場合、全てではないと思われますが、使用しているプロキシーの設定によって、もしくはネットワークの問題によって時々IP アドレスをスイッチするケースが発生します。IP アドレスが変更されてしまうと、ソース IP パーシステンスでは、同じユーザーが違ったユーザーに見えてしまいます。

これらの各ケースでは、どのような IP アドレスから来ても異なったユーザーごとにユニークなクッキー値を使うレイヤ 7 パーシステンスにより問題を解決できます。しかしながら、これは HTTP プロトコルのみに働きます（HTTPS/SSL プロトコルで、セッションをロードマスターで終端した場合も）。

4.4.8 スーパーHTTP

ロードマスターで HTTP/HTTPS サービスのパーシステンスを実現する場合、スーパーHTTP 方式を推奨します。この方式では、クライアント・ブラウザーのユニークなフィンガープリントを作成し、そのフィンガープリントを使用して正しい実サーバーとの接続を維持します。このフィンガープリントは、“User-Agent”フィールドの値（および利用

可能であれば“Authorization”ヘッダーの値）を組み合わせて作成されます。同じヘッダーの組み合わせを持つ接続では、同じ実サーバーにデータが返送されます。

4.4.9 URL ハッシュ

URL ハッシュパーシステンス方式を用いると、ロードマスターは同じ URL のリクエストを同じサーバーへ送ります。

4.4.10 HTTP ホスト・ヘッダー

HTTP ホスト・ヘッダー・パーシステンス方式を用いると、ロードマスターは“HTTP Host:”ヘッダーに同じ値を含む全てのリクエストを同じサーバーへ送ります。

4.4.11 ハッシュ HTTP クエリ項目

この方式は、ネーム項目の代わりに URL のクエリ文内のクエリ項目を判別します。同じクエリ項目値を持った全てのクエリは、同じサーバーへと送られます。

4.4.12 指定ヘッダー

指定ヘッダー・パーシステンス方式を用いると、指定されたヘッダーに同じ値を含む全てのリクエストを同じサーバーへ送ります。

4.4.13 SSL セッション ID

SSL セッション ID とは、SSL サービスで使用されるパーシステンス方式で、SSL がオフロードでなくても使用されます。この方式では、同じ SSL セッション ID を維持しているクライアントに対し、ユーザーセッションが完全に維持されます。なお、全てのブラウザーでこの方式がサポートされているとは限らないため、HTTPS サービスではこの方式を使用しないようにしてください。このパーシステンス方式を使用するには、サービスタイプを汎用（Generic）に設定する必要があります。

4.5 HTTPS/SSL のパーシステンシー

HTTPS/SSL では、幾つかの考慮点があります。もし、SSL アクセラレーション機能を使用しない（SSL セッションをロードマスターで終端しない）場合、選択できるオプションはソース IP アドレスかセッション ID（あまり効果が期待できない）のみとなってしまいます。これは、SSL セッションを終端しない事によりパケットが暗号化されたままであり、ロードマスターは HTTP ヘッダー、もしくはレイヤ 7 情報を見ることができないためです。

もし、ロードマスターで SSL アクセラレーション機能により HTTPS/SSL を終端するならば、ロードマスターがサポートしているどのパーシステンスのオプションでも使用することが可能です。HTTP/SSL セッションが終端されると、ロードマスターは復号化された全てのトラフィックを見ることが可能で、もちろん HTTP ストリームも見ることができます。これは、HTTPS/SSL セッションを一旦ロードマスターで終端し、再度実サーバーとの間で SSL セッションを確立する SSL リエンクリプトの場合も同様です。

4.6 ポートフォローイング（Port Following）

ユーザーが商品を選択、またはリストに追加するショッピングカートを使用する時は、一般には HTTP 用仮想サービスにより行われますので、上記のどのパーシステンス方式でも使用可能です。ユーザーがそれらの商品に対して購入を決定した後、クレジットカードなどによる支払い処理では、一般的にはセキュアな SSL（https）用仮想サービスに切り替わり実行されます。仮想サービスが、HTTP 用から HTTPS 用に切り替わる時に、2 つのサービス間で同じ実サーバーに接続を継続させる機能がポートフォローウィングです。ポートフォローウィングがオンになっていれば、ショッピングカートに入れた商品を購入しようとしてクレジットカードなどによる支払い処理のために、SSL セッションに切り替わっても引き続き処理が継続されるはずです。もし、ポートフォローウィング機能が HTTP 用と HTTPS 用仮想サービス間でオンになっていなければ、サービスが切り替わった時に今までのショッピングカートの商品リストの情報を保持した実サーバー以外のサーバーに接続され、支払い処理時その情報が取得できないという問題が発生する場合があります。

ポートフォローウィングをオンにした接続試験例として、オンラインショッビングサイト“www.onlineshop.com”の為に HTTP と HTTPS 用仮想サービスを設定しているとします。最初に URL‘http://www.onlineshop.com’に HTTP サービスのアクセスを行います。その後、今度は‘https://www.onlineshop.com’に HTTPS による SSL 接続を行います。SSL セッションは初めの HTTP サービスを提供した同じサーバーと接続されるはずです。

5 アプリケーション・ロントエンド（AFE）

アプリケーション・ロントエンド（AFE）は、ウェブアプリのデータ配信とネットワークの効率を高めるためのグループ機能です。ロードマスターは、AFE を新たに実装することにより、既に実装済みの容易な管理、透明的な高パフォーマンスの負荷分散機能を損なわずに、より一層高いスループットとサーバーのパフォーマンス向上という誰もが求める基本的な要求を満たします。ロードマスターの AFE サービスは、下記の機能を含んでいます。

- ネットワーク侵入防止システム（IPS）
- キャッシング
- データ圧縮

各機能は、仮想サービスごとに設定することが可能です。

注: AFE 機能は、ライセンスで制御されます。もし LM2000、およびそれ以上のモデルでこの機能が使えないならば、弊社代理店までご連絡ください。新しいライセンスキーを発行します。

5.1 ネットワーク侵入防止システム（IPS）

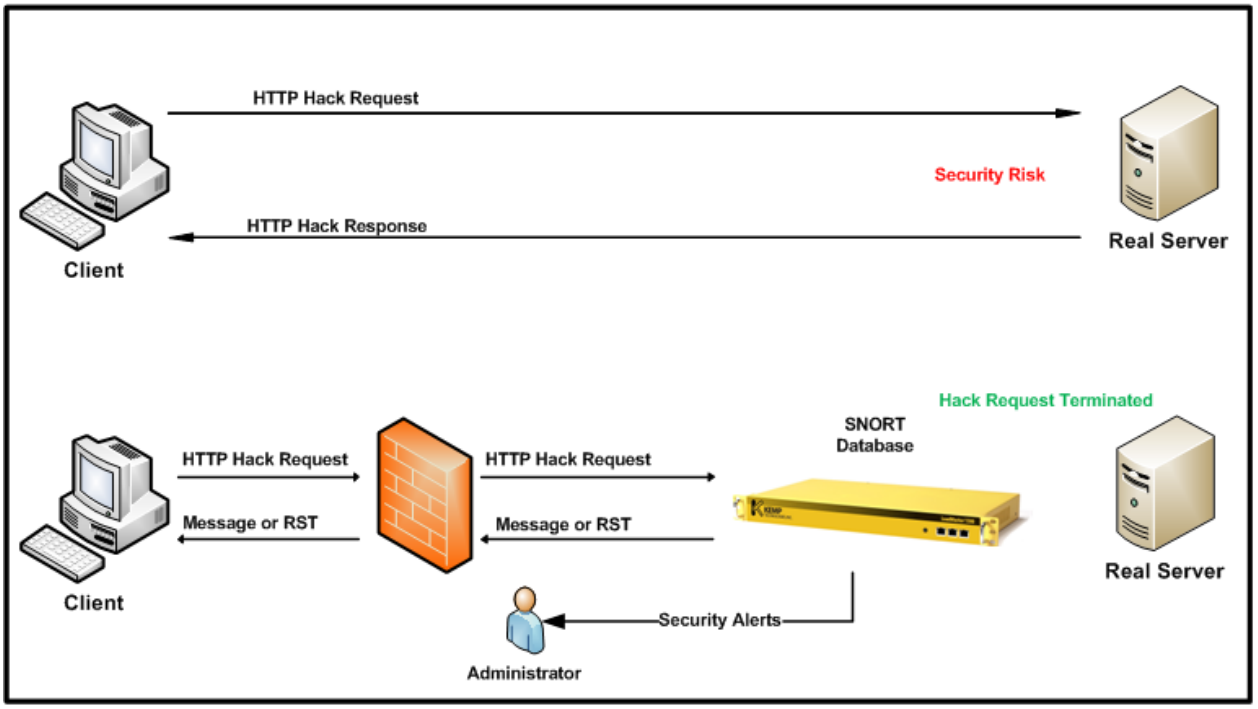


図 5-1：侵入防止

ロードマスターは、この HTTP 侵入防止機能を有効にすることで一層強固なインターネット装置となります。従来の SSL に、この IPS が持つ DoS 攻撃防御が追加されることで、リアルタイムに攻撃を軽減するだけではなく、クリティカルな攻撃には実サーバーを切

り離すことで守ります。侵入防止システムは、業界標準である SNORT データベースをベースにしており、侵入が検知されたらリアルタイムで警告を発します。

> ロードマスターは、Snort ルールのバージョン 2.8、もしくはそれ以前のバージョンをインストールして出荷しています。最新版のルールは、ユーザー自身が http://www.snort.org よりダウンロードしてアップデートをする必要があります。

PS は、 HTTP 仮想サービスごとに有効にすることができます。HTTPS 仮想サービスで使用する場合は、SSL オフロードを有効にしなければなりません。

5.1.1 侵入の扱い

“SNORT”ルールにマッチしたリクエストの扱いには、2 つのオプションがあります。‘Drop Connection’か‘Send Reject’です。両オプションとも、RS（実サーバー）への到達を許さず、侵入を試みたクライアントに対してレスポンスを返すか否かを設定します。

5.1.1.1 Drop Connection による扱い

“SNORT”ルールにマッチした場合、HTTP レスポンスを返しません。TCP 接続は切断され、結果的に HTML コンテントのクライアントへの返信はありません。

5.1.1.2 Send Reject による扱い

“SNORT”ルールにマッチした場合は、ロードマスターは侵入を試みたクライアントへ HTTP 400“Invalid Request"と、マッチした内容を示すメッセージを HTML 形式で返信します。参考例を以下に示します。

サンプルリクエスト： http://<VIP>/modules/articles/index.php?cat_id=SQL

サンプルレスポンス： <html><head><title>400 Invalid Request</title></head><body>Invalid Request: COMMUNITY WEB-PHP Xoops module Articles SQL Injection Exploit</body>

5.1.2 Detection level （検出レベル）

ルールがマッチングするレベルを、システムとして下記のようなレベルに設定変更が可能です。詳細につきましては、‘http://www.snort.org/docs/snort_manual/node220.html’を参照ください。

- **Low**=拒絶なしで記録（ログ出力）のみ行います。
- **Default**=高セキュリティのルールにマッチしたリクエストをブロックし、記録します。
- **High**=高、および中セキュリティのルールにマッチしたリクエストをブロックし、記録します。
- **Paranoid**=全てのセキュリティレベルにマッチしたルールをブロックし、記録します。

5.1.3 警告

侵入防止機能は、悪意のあるアクセスと判断した接続を切断しますが、しかしながら幾つかのものは明確には判断できない場合があります。これらに対しては、デフォルトではブロックせず記録も残しませんが、“WARNING”オプションを有効にすればログに記録します。

SNORT のルールファイルの中で、これらのマイナーなアクティビティとして指定されている、危険でないオペレーションリクエストの例を下記に示します。

Uri: "/OvCgi/OpenView5.exe?Context=Snmp&Action=Snmp&Host=&Oid="

which is described as "WEB-MISC HP OpenView Manager DOS" and is only suspicious.

5.1.4 侵入警告

全ての侵入警告は、“System”と“Warning”ログの中に記録されます。また、警告通知は、Syslog サーバー、および EMail として SMTP サーバーに、最低レベル“Notice”として送信可能です。侵入警告は、重要警告として記録維持のために Syslog サーバーによって記録されることを推奨します。

5.1.5 IPS ルールの更新

新しいルールは"www.snort.org"でダウンロードできます。新しいルールセットを取得、もしくは作成したら、WUI の"System Configuration" -> "Miscellaneous Options" -> "AFE Configuration"を使ってシステムに取り込めます。"Browse"ボタンをクリックして、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ます。コミュニティルールファイルは、"Tar"、もしくは"Gzip"でエンコードされたもので"tar.gz"の拡張子を持ち、"community-rules"のディレクトリー下にファイルが存在しなければなりません。ロードマスターはこのファイルを解凍し、新しいルールとしてリロードします（拡張子.tar.gz は、www.snort.org からダウンロードしたルールファイルの標準形式です）。新しいルールファイルをインストールすると、現在のルールが新しいルールに置き換えられます。ロードマスターの出荷時は、GPL に準拠した共通ルールをインストールしています。

5.2キャッシング

ロードマスターの持つ先進的なキャッシング用エンジンは、実サーバーの貴重な処理能力とネットワーク帯域使用を節約し、クリティカルなコアビジネス用アプリケーションだけに威力を発揮できるように専念させます。キャッシング機能は、際立ったサーバーのパフォーマンス向上をもたらすことに貢献します。クライアントとサーバーが頻繁に相互通信をする HTTP のようなプロトコルでは、静的なリソースをフェッチするために、ネットワークと実サーバー上の不必要なリソース使用を抑えるために接続と切断がひっきりなしに繰り返されます。一般的に、アプリケーションの威力をより発揮させるために、キャッシング機能を有効にし、ネットワーク帯域とそれに関連するリソースの使用を適正化します。ロードマスターでは、キャッシング機能を利用することで、実サーバ

一へのウェブ用トラフィックを減少させ、結果的に実サーバー接続の帯域とサーバー上のリソース使用を節約し、アプリケーションの処理能力を向上させます。

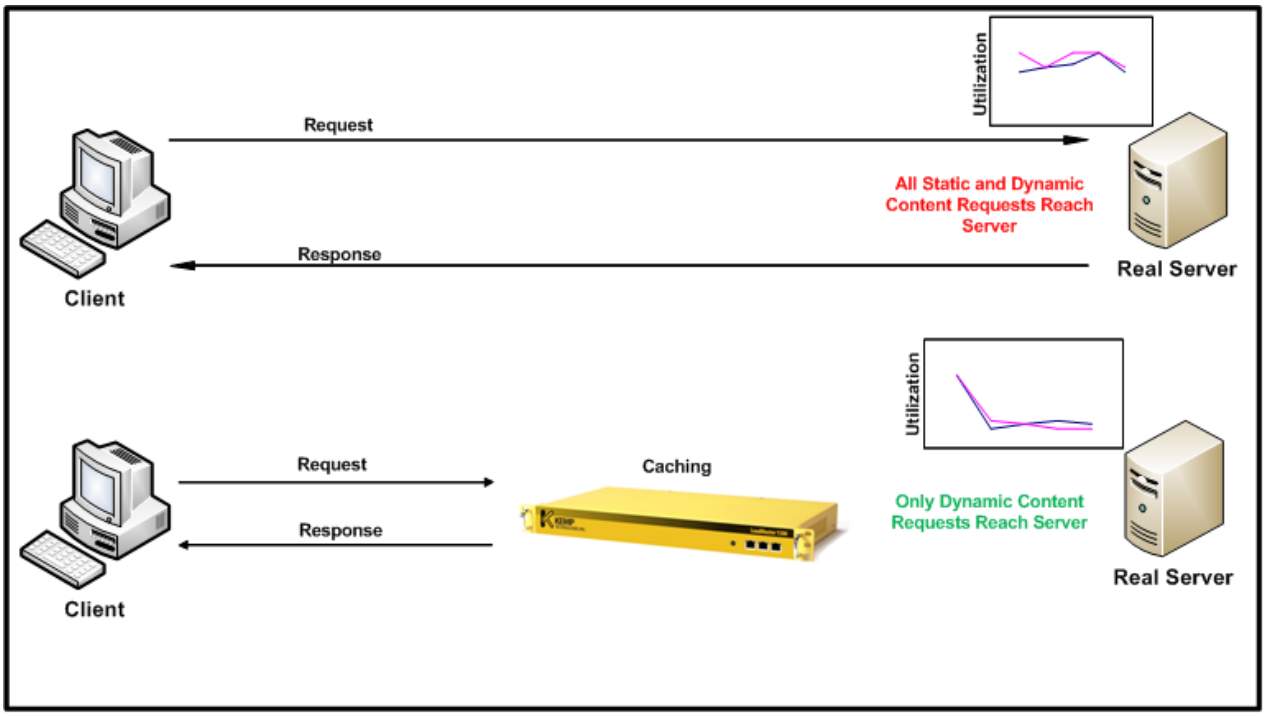


図 5-2：キャッシング

キャッシング機能は、HTTP と SSL オフローディング用 HTTPS の仮想サービスで有効にできます。

注：“no-cache”ヘッダーを持つ HTTP/HTTPS リクエストは、RFC 2616 に準拠してキャッシング機能をバイパスします。キャッシュ処理は、メモリーへの蓄積を行うのに少し時間を必要としますので、静的なコンテンツが正しくキャッシュされるまで 2-3 秒間待つ必要があります。

注：RFC 2616 に従い、クエリ文字列（"?"を rel_path 部分に含むもの）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ング

ロードマスターは、実サーバーのファイルが更新されるのをモニターしていません。よって、もしファイルが更新されても、キャッシュメモリー内にストアされている内容を自動的に更新しません。内容を更新させるためには、この機能を一旦無効にしてから再度有効にしてメモリーのフラッシングを行わせる必要があります。また、ほとんどのブラウザーでは、左 Shift キーを押しながらリロード（または F5 キーを押す）をクリックして非キャッシュ指定を行うことでキャッシュされたオブジェクトをリロードすること

ができます。キャッシュされたファイルは、もし期限が限定されていなければ 1 時間で消去されます。

5.2.2 Maximum Cache Size（最大キャッシュサイズ）

システム全体で使用できるキャッシュ用メモリーサイズの最大値を設定します。この値は、実際実装されているメモリーサイズに連動しています（基本的な最大設定値は、システムが実装しているメモリーサイズの 5 分の一です）。WUI の“System Configuration”-> “Miscellaneous Options” -> “L7 Configuration”から設定可能です。

5.3データ圧縮

ロードマスターのデータ圧縮機能は、一般的なブラウザーで利用できる“gzip”圧縮を使用することで、転送する HTTP オブジェクトのデータ量を減らします。Lempel-Ziv(LZ)と HTTP/1.1 GNU zip (gzip)のコンテンツ圧縮/エンコーディングにより、Text ファイル（HTML、CSS、JavaScript）を高圧縮することでネットワークの使用帯域を減少させます。

データ圧縮は、圧縮する内容の品質を落とすことなく、アプリケーションのリクエストパケットごとのペイロードを圧縮することが可能なために、その結果、ネットワークの使用帯域を少なくし、ユーザーのレスポンスに対する満足度を向上させます。圧縮率は、ファイルの種類により変化します。

サイズが 100MB 以上のファイルは圧縮しないようにしてください。

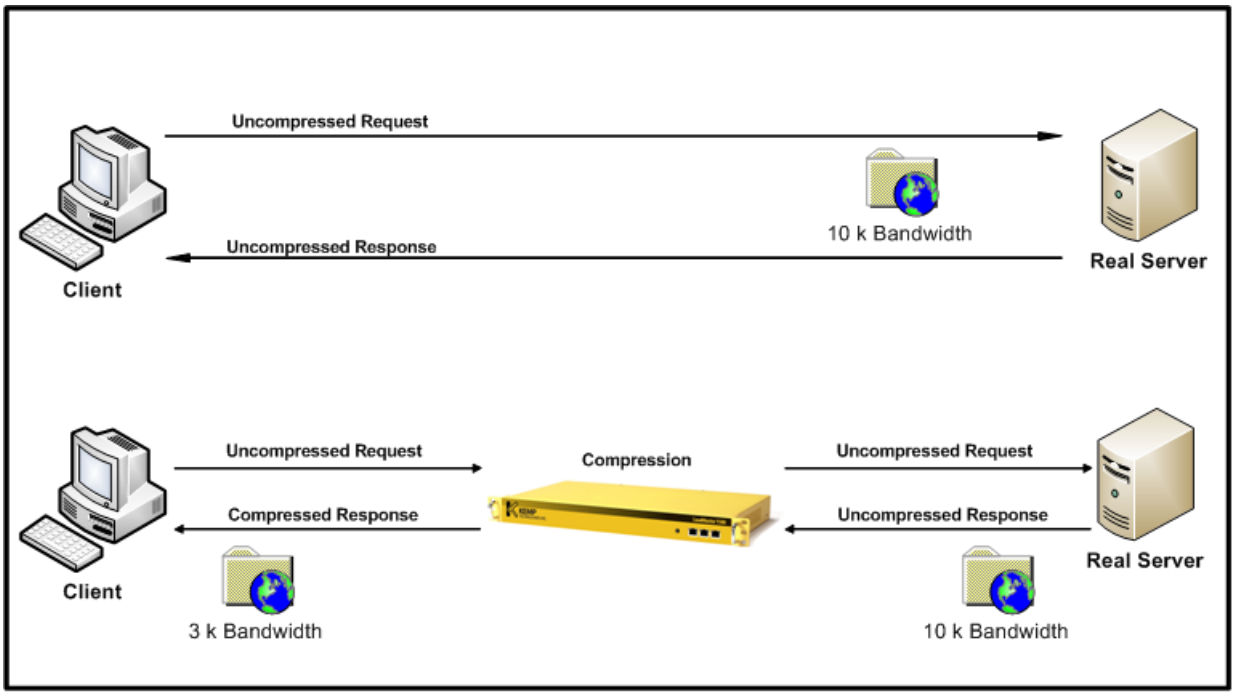


図 5-3：データ圧縮

圧縮は、ファイルを一旦ロードマスターで完全に受け取った後で処理を行うために、リアルタイム処理に遅延が出る可能性があります。実サーバーからのファイル受信処理を減少させるキャッシュ機能を併用して使用することで、圧縮機能がサービスのスループットのボトルネックになるのを防げます。

データ圧縮は、HTTP、および HTTPS（SSL オフローディングを有効にした）用仮想サービスで有効にできます。

圧縮は、ブラウザー側で“gzip”をサポートしているかどうかによります。ブラウザーとロードマスター間で圧縮が行われているかどうかは、HTTP トラフィックをトレースすることで確認ができます。ロードマスターからのパケットに **Content-encoding:gzip** ヘッダーが含まれている場合、クライアントからロードマスターにはデータが圧縮されて送られます。

6 SSL アクセラレーション/オフロード

ロードマスターシリーズは、仮想サービスの SSL のアクセラレーション/オフロードを提供します。 SSL アクセラレーションを使用すると、SSL セッションがロードマスターで終端されます。

SSL アクセラレーションには、下記の 2 つの主な利点があります：

- ロードマスターは、実サーバーの SSL 処理をオフロードします（ハードウェア・アクセラレーションにより処理が格段に加速されます）。
- ロードマスターは、レイヤ 7 機能であるクッキーパーシステンシーやコンテンツスイッチングを実行することができます。

ロードマスターでは、SSL セッションを終端せずにヘッダーとコンテンツを読み取ることができないので、パーシステンシーを行うことはできません。SSL セッションがロードマスターで終端されていない時に、唯一利用可能な信頼性の高いパーシステンシーはソース IP アドレス方式だけです。別の選択可能な SSL セッション ID 方式は、多くのブラウザーが SSL セッション ID を 2 分ごとにネゴシエートして更新させている為に、実行可能なパーシステンス方法ではなくなったからです。

ロードマスターは、SSL アクセラレーション処理に、SSL 複合化／暗号化機能を実行する専用プロセッサを使用しています。この SSL アクセラレータハードウェアを使用すると、ロードマスターは、あたかも非 SSL セッションを処理するように SSL 接続を高速に処理することができます。

ロードマスターファミリーの全モデルは、SSL アクセラレーション／オフロードを実行する機能を持っています。SSL アクセラレーション／オフロード機能には、下記の 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

機能的には、SSL ハードウェアとソフトウェアは同じです。違いは、SSL の操作に関連付けられた実際の暗号化／複合化処理をロードマスターのどの部分が行うかです。

ソフトウェア SSL を使用したロードマスターでは、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、そのようなロード･バランシング、ヘルスチェック、およびその他の管理タスクなどのロードマスターが実行する他のタスクと共有されます。SSL 処理は、CPU 集中型操作によるため、ソフトウェア SSL は低レベルの SSL トラフィックのためには十分でも、高 SSL トラフィックには不十分です。ソフトウェア SSL に頼るロードマスターの一部モデルでは、SSL の高い接続率がシステム全体のパフォーマンスを低下させるかも知れません。

ハードウェア SSL を使用したロードマスターモデルでは、すべての SSL 機能を処理する独立した専用プロセッサを持っています。SSL トラフィックの高低に関係なく、汎用プロセッサは SSL 処理の負担を負いません。 この特殊なハードウェアは、SSL 処理のみを

目的として構築されており、非常に高い SSL トラフィックの接続率（TPS）を扱うことができます。

7 エッジ・セキュリティ・パック（ESP）

KEMP エッジ・セキュリティ・パック（ESP）は、Microsoft の脅威管理ゲートウェイを導入して Microsoft アプリケーションのパブリッシュを行っているお客様向けに、KEMP ロードマスターシリーズのロードバランサを採用したソリューションを提供します。

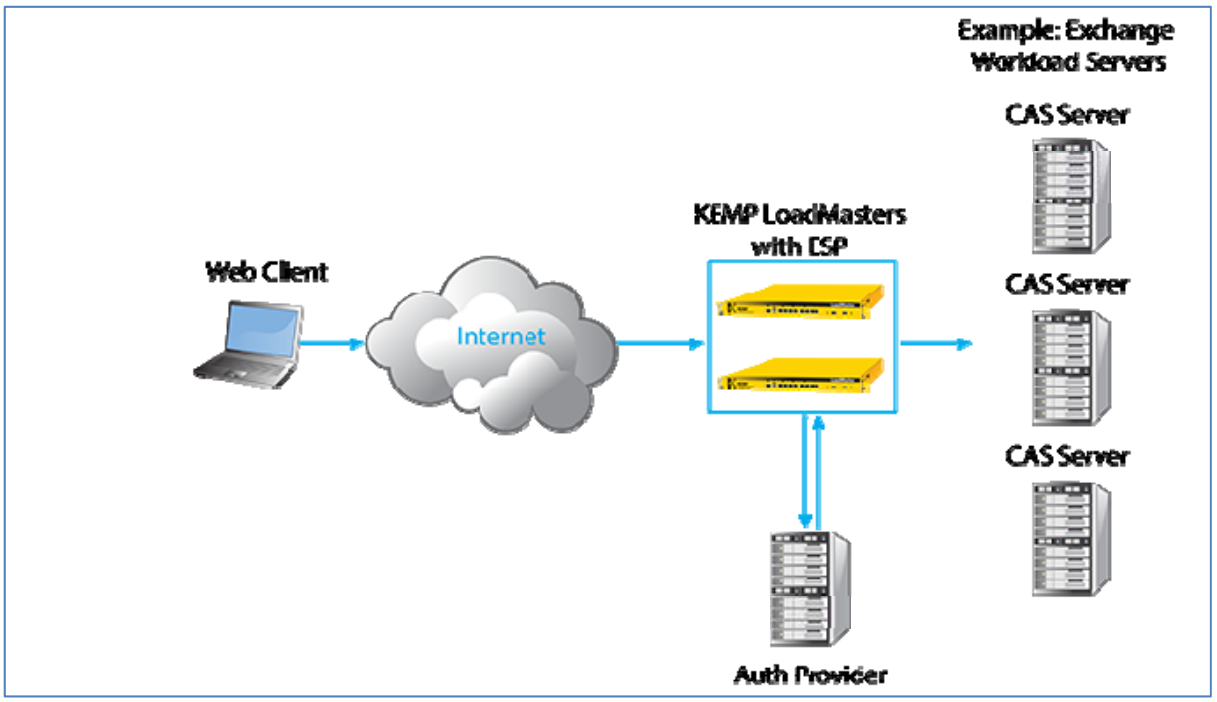


図 6-7-1 ESP を導入したロードマスターによって簡素化されたアプリケーションの展開

KEMP ESP は、次のような特長を備えています。

- Pre-Auth 用のエンドポイント認証
- ユーザーログ記録用の永続的なログ記録およびレポート機能
- 仮想サービス全体でのシングル・サイン・オン（SSO）
- ロードマスターから Active Directory への LDAP 認証
- クライアントからロードマスターへの NTLM および Basic 認証通信

7.1 Pre-Auth 用のエンドポイント認証

ロードマスター上の仮想サービスにアクセスするクライアントは、認証情報を提供する必要があります。このクライアントの認証情報に基づいて、ESP はサービスへのアクセス権限を検証します。認証に問題がなければ、クライアントはサービスへのアクセスを許可されます。認証に問題があれば、クライアントは有効な資格情報を提供しない限り、アクセスを拒否されます。

7.2 ユーザーログ記録用の永続的なログ記録およびレポート機能

クライアントがサービスにアクセスしようとすると、その情報がロードマスター上で ESP の機能によってログに記録されます。この情報に基づいて、管理者によるユーザーの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（SSO）

ロードマスターは複数の仮想サービスを処理して、固有のワークロードをサポートできるよう設計されています。この一連の仮想サービスは、シングル・サイン・オンのグループとしてまとめることが可能です。ESP の機能により、クライアントは最初の仮想サービスで認証情報を 1 回入力するだけで済みます。シングル・サイン・オンのグループ内の他のサービスにアクセスする場合には、この入力情報がそのまま使用されます。したがって、Exchange にアクセスしたクライアントは、SharePoint やその他のワークロード（シングル・サイン・オンのグループとして設定されている場合）にもアクセスできます。

7.4 ロードマスターから Active Directory への LDAP 認証

Active Directory は、Microsoft のワークロード向けの標準認証プロバイダです。ロードマスターは、ロードマスターと Active Directory の間での主要な接続タイプをサポートしています。

7.5 クライアントからロードマスターへの NTLM および Basic 認証通信

ESP を導入したロードマスターはクライアントとロードマスターの間での主要な認証タイプ（Basic や NTLM など）をサポートしており、お客様にとって最適な認証を実現します。

規模を問わず、多くの企業は、増え続けるビジネス要件をサポートするため、さまざまなインターネット利用アプリケーションを導入しています。この結果、サーバー数が急増すると同時に、高いスケーラビリティと信頼性が求められています。とりわけ、サーバーやサービスへのアクセスは、セキュリティで保護する必要があります。ESP の追加によって、ロードマスターは、TMG の存在しない環境でも、インターネット利用アプリケーションに対するお客様のセキュリティ要件に対処すると同時に、多機能かつ費用対効果に優れたスケーラビリティと信頼性に対する要件への取り組みを継続します。

8 サブ仮想サービス（サブ VS）

仮想サービスの範囲内で、1 つまたは複数のサブ仮想サービス（サブ VS）を作成できます。サブ VS はその'親'の仮想サービスにリンクすると同時に、親の仮想サービスの IP アドレスを使用します。サブ VS には、その親の仮想サービスや別のサブ VS と異なる設定（ヘルスチェック方式やコンテンツルールなど）を保持できます。この結果、関連する仮想サービスのグループ全体で同じ IP アドレスを使用することが可能になります。一般に、複数の仮想サービスで構成される Exchange や Lync といった複雑な構成では、この機能が特に役立ちます。

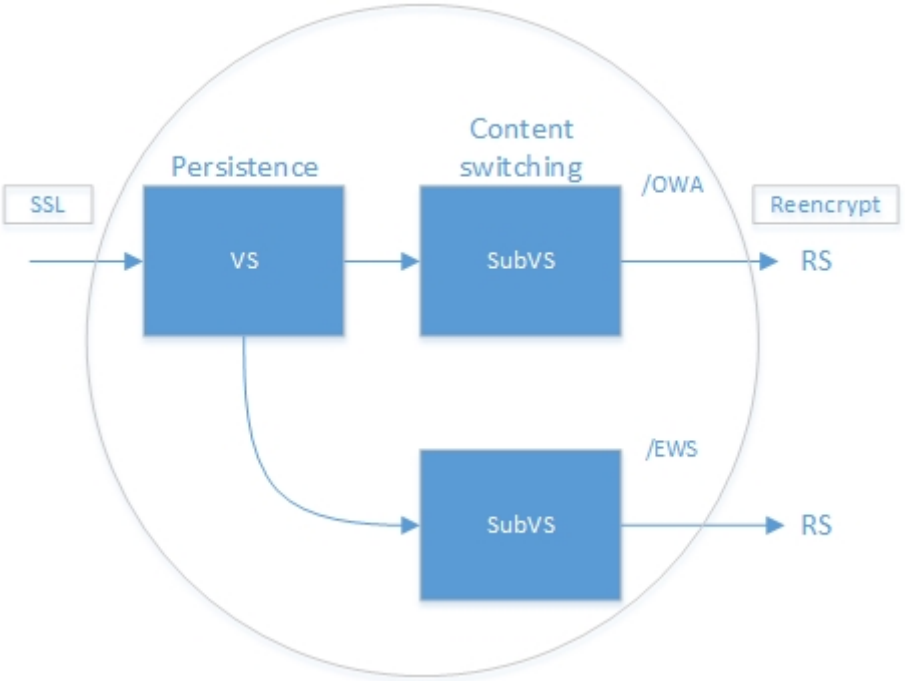


図 8-1: サブ VS の図例

サブ VS の使用には、次のように、さまざまな利点があります。

- サブ VS はその'親'の仮想サービスにリンクすると同時に、親の仮想サービスの IP アドレスを使用します。
- サブ VS を使用すると、Lync や Exchange といったアプリケーションで必要な IP アドレスの数が減少します。
- サブ VS は、非透過性を必要としません。
- サブ VS には、その親の仮想サービスや別のサブ VS と異なる設定（コンテンツルールなど）を保持できます。
- サブ VS を使用すると、同じ VS に対するコンテンツスイッチング機能や持続性機能を利用できます。

- サブ VS を使用すると、同じ VS に対する複数のヘルスチェックの実行機能を利用できます。
- サブ VS は ESP と適切に連携しますが、ESP が必須というわけではありません。

8.1 セルフサイン対 CA サイン証明書

SSL 証明書は、全ての SSL トランザクションのために必要ですので、SSL アクセラレーションを必要とする仮想サービスには証明書のインストールが必要です。ロードマスターでは、二つのタイプの SSL 証明書が使用できます。一つは、セルフサインで、もう一つは Verisign や Thawte などの証明書発行機関（CA）がサインしたものです。

SSL アクセラレーション用仮想サービスを作成すると、ロードマスターはビルトインしてあるセルフサイン証明書を自動的にインストールします。

一般的に、セルフ・サイン証明書はパブリックに公開されているウェブサイトに使用すべきではありません。

下記のようなシナリオで使用するためならば、容認されるかも知れません。

- イントラネット用サイト
- 一般公開される前の QA 試験で使うサイト

8.2 証明書の基本

セルフサインも CA がサインした証明書もトラフィックを暗号化します。しかし、CA サインの証明書は、どのようなサイトであるかをレポートし、詐欺目的のウェブサイトでないことなどの一定の保障を提供します。

8.3 操作性の違い

セルフサイン証明書と CA 証明書間の主要な違いは、セルフサインを使用するとブラウザーが CA から発行された証明書ではないことのエラーや警告を出すことです。インターネットエクスプローラー7.0 で、この証明書に対するエラーが表示された例を図 6-1 に示します。

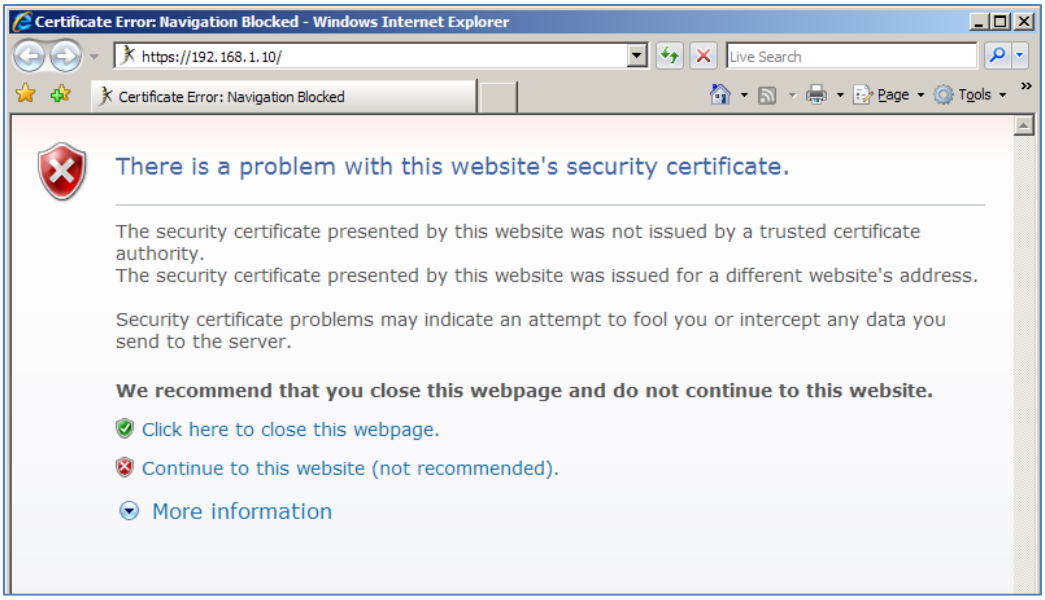


図 8-2 : 自己署名証明書のエラー

これは、同じセルフサイン証明書を使用することから、管理用 WUI に接続したときにも同じ警告メッセージが表示されます。一般的に、この警告は ブラウザーセッションごとに一回だけ出力されます。

9 ルールベースのコンテント・スイッチ

ロードマスターシリーズでは、一般的に URL スイッチングと呼ばれるコンテント・スイッチをサポートしています。これは、リクエストされた URL の内容を基に、ロードマスターが特定のリクエストを特定の実サーバーへ導くものです。

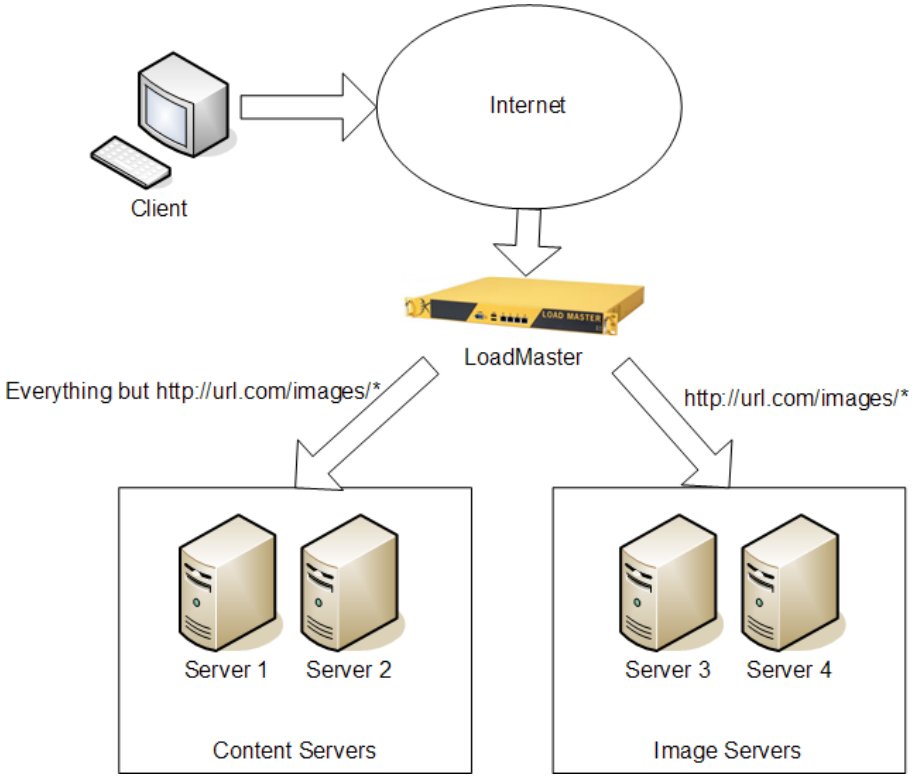


図 9-1：ルールベースのコンテンツスイッチング

例えば、1 つのグループはイメージだけ提供するサーバー群で、他のグループはそれ以外の全ての内容を提供する 2 つのグループのサーバー群を持っていたとすると、2 つの種類のリクエストを分けるためのコンテントルールを作成することができます（図 7-1）。

/images を含んだ URL、例えば“http://url.com/images/party.jpg” や http://url.com/images/dogs.jpg は、サーバー3 と 4 に導かれ、他はサーバー1 と 2 に導かれるようにします。

これは、アプリケーション・サーバー、スタティック・コンテンツ・サーバー、マッピング・サーバーや特定コンテンツ作成サーバーなどの、同じホストネーム下（例えば www.websitename.co.jp）で異なる機能のサーバーを持っている時に役立ちます。

9.1 用語

注意：コンテント・スイッチの用語は、レイヤ 2 スイッチが絡むプロセスを表したものではありません。それよりも、異なるサーバー間でリクエストされたコンテントに応じてトラフィックをスイッチするといった方が良いでしょう。

9.2 コンテント・スイッチの使用

コンテント・スイッチを設定するためには、コンテンツルールと仮想サービスの 2 つの設定箇所があります。コンテンツルールは、ロードマスター上でシステム規模で設定します。そして、仮想サービス下の特定実サーバーへそれらのルールを適用します。最初に行わなければならないのはルールの作成です。

10 ヘルスチェック

10.1 概要

ロードマスターは、レイヤ 3、レイヤ 4、およびレイヤ 7 のヘルスチェックを実サーバーと仮想サービスの可用性確認のために使用します。1 つのサーバーがヘルスチェックの応答を定義された時間間隔とリトライ回数以内に返さない場合は、サーバーの重みがゼロに設定されます。この重みゼロは、実サーバーがオンラインに戻ったことが確認されるまで、仮想サービス設定から外されることを意味します。

ロードマスターが使うこれらのレイヤ 3、レイヤ 4、レイヤ 7 のヘルスチェックの設定は、WUI もしくはコンソールの CLI を介して行うことができます。ロードマスターは、下記のポートに対して最も可能性の高いヘルスチェック方式を、デフォルトとして仮想サービスに関連付けます。

サービス	ポート番号	プロトコル
FTP	21	TCP
TELNET	23	TCP
SMTP	25	TCP
HTTP	80	TCP
HTTPS	443	TCP
POP3	110	TCP
NNTP	119	TCP
IMAP	143	TCP
DNS	53	UDP

仮想サービスを作成する際に、汎用（Generic）以外のサービスタイプを選択する場合は、追加的なヘルスチェックのプロトコルが用意されています。（例）サービスタイプとしてリモートターミナルを選択すると、リモートターミナルプロトコルの使用が追加されます。

リモートターミナルプロトコルでは、ネットワークレベルの認証が可能です。

これ以外のポートに対しては、ロードマスターは TCP サービスならばレイヤ 4 ヘルスチェック、UDP サービスであればレイヤ 3 のヘルスチェックを使用します。ヘルスチェッ

クのセッティングは、仮想サービスのプロパティでデフォルトからスタンダードでない設定へと調整できます。例えば、HTTP サービスがポート 80 ではなく 8080 で稼動している場合、デフォルトのレイヤ 4 ヘルスチェック方式より HTTP に変更できます。

ヘルスチェックのタイムアウト、リトライ回数の設定は、システム全体の共通のものでサーバーごとに違う値の設定はできません。

ロードマスターでは、仮想サービスを定義するときに、必ず 1 つのサービスチェックのオプションを使用するようにしなければなりません。

10.2 サービス、ノンサービス・ベースのヘルスチェック

レイヤ 3 ヘルスチェックは、実サーバーをネットワークを通してチェックするために ICMP ベースのエコーリクエスト（ping）を使います。レイヤ 3 チェック方式は、仮想サービスに頼らないもので、これが失敗すると該当する実サーバーは、そのサーバーを定義している全ての仮想サービスから外されます。

サービスベースのヘルスチェック方式は、レイヤ 3 ヘルスチェックと対照に、レイヤ 4、レイヤ 7 の両方の方式で仮想サービスに関連付けされています。実サーバーがそのようなサービスチェックに失敗した場合は、該当する仮想サービスのみ外され、その他の仮想サービスでは同じ実サーバーでも影響を受けません。

タイプ	詳細
ICMP	ロードマスターは、実サーバーに ICMP エコーリクエスト（ping）を送ります。実サーバーは、設定してあるリトライ回数内でタイムアウト時間内に ICMP エコーレスポンスを返さないとチェックに失敗します。
TCP	ロードマスターは、設定されている実サーバーのサービスポートに TCP 接続を開きます。サーバーの設定ポートに TCP SYN パケットを送付します。サーバーが、TCP SYN ACK を設定してあるリトライ回数内でタイムアウト時間内に返すとチェックはパスします。この場合は、ロードマスターは TCP RESET パケットを送り接続を閉じます。もし、時間内にレスポンスがないとチェックが失敗し、サーバーはダウンしているものとみなします。
FTP	ロードマスターは、実サーバーのサービスポート（ポート 21）上に TCP 接続を開きます。もしサーバーが、ステータス・コード 220 と一緒にグリーティング・メッセージを返すと、ロードマスターは QUIT コマンドをサーバーに送り接続を閉じて、サーバーをアクティブとします。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。

タイプ	詳細
TELNET	ロードマスターは、実サーバーのサービスポート（ポート 23）に TCP 接続を開きます。もし、サーバーが char '0xff'で始まるコマンド文字を返すと、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ます。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うコマンド文字が返すとサーバーはダウンしているものとみなします。
SMTP	ロードマスターは、実サーバーのサービスポート（ポート 25）に TCP 接続を開きます。もしサーバーが、ステータス・コード 220 と一緒にグリーティング・メッセージを受け取ると、ロードマスターは QUIT コマンドをサーバーに送り接続を閉じて、サーバーをアクティブとします。 もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。
HTTP	ロードマスターは、実サーバーのサービスポート（ポート 80）に TCP 接続を開きます。ロードマスターは、ページ "/"に HTTP/1.0 HEAD リクエストを送付します。もし、サーバーが HTTP レスポンスをステータス・コード 2xx（200-299）、301,302 もしくは 401 と共に返すと、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ます。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。
HTTPS	ロードマスターは、SSL 接続を実サーバーのサービスポート（ポート 443）に開きます。ロードマスターは、ページ "/"に HTTP/1.0 HEAD リクエストを送付します。 もし、サーバーが HTTP レスポンスをステータス・コード 2xx（200-299）、301,302 もしくは 401 と共に返すと、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ます。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。
POP3	ロードマスターは、実サーバーのサービスポート（ポート 110）に TCP 接続を開きます。もしサーバーが、"+OK"で始まるグリーティング・メッセージを返すと、ロードマスターは QUIT コマンドをサーバーに送り接続を閉じて、サーバーをアクティブとします。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。
NNTP	ロードマスターは、実サーバーのサービスポート（ポート 119）上に TCP 接続を開きます。もしサーバーが、ステータス・コード 200、201 と一緒にグリーティング・メッセージを返すと、ロードマスターは QUIT コマンドをサーバーに送り接続を閉じて、サーバーをアクティブとします。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。

タイプ	詳細
IMAP	ロードマスターは、実サーバーのサービスポート（ポート 143）に TCP 接続を開きます。もしサーバーが、“+OK”か“*OK”で始まるグリーティング・メッセージを返すと、ロードマスターは LOGOUT コマンドをサーバーに送り接続を閉じて、サーバーをアクティブとします。もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバーはダウンしているものとみなします。
DNS	ロードマスターは、実サーバーのサービスポート（ポート 53／UDP）に Source-of-Authority (SOA)リクエストを送ります。サーバーが SOA リクエストに対して成功裏にレスポンスを返すと、ロードマスターはサーバーをアクティブとします。 もし、サーバーが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないとサーバーはダウンしているものとみなします。
RDP	ロードマスターは、実サーバーに RDP のルーティングトークンを送信します。 RDP のヘルスチェックでは、ネットワークレベルの認証が可能です。
None	ロードマスターは、実サーバーに対してヘルスチェックを行いません。結果として常時サーバーがアップとみなしてトラフィックを転送します。

11 SNMP サポート

Simple Network Management Protocol （SNMP）は、リモート管理ステーション（SNMP マネージャー）よりネットワークを介して多くのネットワーク構成品を管理するのを可能にするプロトコルです。

管理ステーション（SNMP マネージャー）は、被管理ステーション（SNMP エージェント）にデータをリクエストしたり、エージェントのデータを変更できます。

SNMP エージェントは、ユニットのフェイルオーバー等の予め定義してあるイベントに対して警告を出すようにセットアップできます。警報メカニズムには、イベントトラップを用います。

現在のバージョンは、SNMPv3 であり、以前のバージョンでは、SNMPv1 および SNMPv2c（コミュニティベースの SNMPv2）を使用していました。

ロードマスターの SNMP は SNMPv3 をベースにしていますが、上記の 2 つのバージョンも使用できます。しかしながら、SNMPv1 はロードマスターが使用している 64 ビット値をサポートしていないために、SNMv2c、もしくは SNMPv3 の使用を推奨します。MsgSecurity は、SNMP v1 および v2c でのみサポートされています。

注：HA 構成をモニターする場合は、シェアード IP アドレスではなく必ず各ユニットに与えられた個別の IP アドレスを使用してください。

全てのロードマスター特定データオブジェクトに関しての情報は、下記の 3 つのエンタープライズ特定 MIBs（Management Information Base)に用意されています。

ONE4NET-MIB.txt	エンタープライズ id
IPVS-MIB.txt	仮想サービス状態
B-100-MIB.txt	ロードマスター設定情報

これらの MIB ファイルは（www.kemptechnologies.com からダウンロードできます）、SNMP エージェントを介してロードマスターの performance-/config-data を要求できるようにするために、SNMP マネージャマシンにインストールする必要があります。

SNMP は、IPv4/IPv6 仮想サービスのレイヤ 4 とレイヤ 7 でサポートされています。

SNMP サポートは、デフォルトでは無効となっています。

12 ロードマスターのソフトウェア・アップグレード

12.1 オンラインによるアップグレード

ロードマスターは、ソフトウェアのアップデートとアップグレードを、オンラインで行う機能をサポートしています。パッチは、KEMP テクノロジーにより作成されます。これらのパッチは、一旦ローカルディスクへダウンロードした後に、WUI からインストールできます。また、コンソールを使って、FTP, HTTP、もしくは SSH デーモンをサポートしているマシンからインストールする事も可能です。どちらの場合も、一旦ロードマスターをリブートして、ダウンロードするメモリーのスペースを作ってから行うべきです。また、設定ファイルのバックアップをとってから行うことも重要です。

パッチは、チェックサム（MD5）と暗号化でデータ破壊と改ざんに対してプロテクトされています。

パッチは 2 つの方法で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）を使う

- “Configuration”メニューを開きます
- **“Utilities > Software Upgrade”**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、解凍と整合性チェックが行われます。

もし、パッチが正当ならばバージョンが表示され、ユーザーはこのパッチをインストールするかどうかが問われます。パッチが問題なくインストールされたならば、ロードマスターは新しいバージョンをアクティブするためにリブートされなければなりません。

WUI を使う

1. “**System Administration** > **Software Update**”オプションを選択します
2. “**Browse**”ボタンをクリックし、パッチが格納されている場所を選択します
3. “**Update Machine**”ボタンをクリックします

パッチが問題なくインストールされたならば、ロードマスターは新しいバージョンをアクティブにするためにリブートされなければなりません。

もし、何らかの理由でパッチが要求通りに動作しなかった場合には、設定メニューまたは WUI から以前のバージョンへのロールバックを行えます。

ライセンスキーのアップデートは、**ウェブユーザーインターフェイス（WUI） インターフェイスマニュアル**に書かれている方法で、WUI にて実施可能です。

新しいキーにアップデートしてもロードマスターのリブートは必要ありません。

パッチを当てるためのファームウェアの更新は、ライセンスにより期限が限られています。

注意

“Update not permitted”のメッセージが表示された場合、ライセンスの更新のために、システムを購入した販売店にお問い合せください。

13 ユーザー管理

ロードマスターは、異なるアクセスレベルのログインが可能な複数の管理ユーザーをサポートしています。ユーザー管理は、WUI の“System Administration”サブメニューの“User Management”オプションから行います。追加する各ユーザー名は、3 文字以上で 10 文字以下でなければなりません。パスワードは、半角文字で 8 文字から 16 文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めてください。

パスワード指定例

・英小文字のみ ：9 文字以上 ancdefghi

・英小文字と数字の混在 ：8 文字以上 1abcdefg

・英大文字と英小文の混在 ：8 文字以上 Abcdefgh

・英小文字、記号、数字の混在 ：8 文字以上 ab!12345

・数字のみ ：13 文字以上 0123456789012

ユーザーの追加は、WUI からしか許可されていませんので、SSH 通信でのコンソールの設定ユーティリティでは行えません。

認証プロセスにおいて、RADIUS サーバーを使ってロードマスターの設定が行えます。

13.1 ロール/権限（Roles/Permission）

デフォルトの出荷時設定では、管理者ユーザー名は“bal”でパスワードは“1fourall”です。このユーザーは、最高レベルのアクセスが行える権利を有しています。追加できるユーザーには、この“bal”のサブセットとなるアクセス権利を与えることが可能です。各ユーザーのロールの変更は、リアルタイムで有効となります。ロールは、複数を結合できますが互いのロールは干渉し合いません。

新しく作成するユーザーのデフォルトのアクセス権限は、WUI への“read”のみ、SSL 証明書用 CSR 作成、ログファイルの読む込み、および基本的なデバッギング機能の実行だけです。

13.1.1 Real Servers

このロールは、実サーバーの“Enable”と“Disable”を行う権限を持ちます。

実サーバーの権限を持つユーザーは、サブ VS を追加できません。

13.1.2 Virtual Services

このロールは、仮想サービスの管理権限を持ちます。これには、サブ VS が含まれます。仮想サービスの変更、追加、削除、およびサブネットの変更が可能です。

13.1.3 Rules

このロールは、ルールの管理権限を持ちます。ルールの変更、追加、削除が可能です。

13.1.4 Certificate Creation

このロールは、SSL 証明書の管理権限を持ちます。SSL 証明書のインストール、削除が可能です。

13.1.5 Intermediate Certificates

このロールは、インターミディエート証明書（中間証明書）の管理権限を持ちます。インターミディエート証明書の追加および削除が可能です。

13.1.6 Certificate Backup

このロールは、第三者が証明書をエクスポート/インポートするのを許可します。

13.1.7 User Administration

このロールは、“**System Administration > User Management**”画面の全ての機能を使うことを許可します。

13.1.8 All Permissions

このロールは、すべての権限を持ちます。このロールを持ったユーザーはデフォルトユーザーの**‘bal’**と同じ権限が与えられます。

13.1.9 GEO

このロールは、ロードマスターGEO の製品でのみ使用されます。

14 ボンディングと VLAN

14.1 概要

ロードマスターのボンディング／VLAN タギングは、この機能を使用するために必要とされる規格に合っているならば WUI より簡単に設定が行えます。このガイドは、ロードマスター上のインターフェイスのボンディングと VLAN 設定を行うためにデザインされたものです。ボンディングのサポートは、全てのネットワークモデュールで利用可能です。

14.2 必要とする規格 （スイッチ側） （スイッチ側）

- VLAN タギング
- IEEE 802.1Q
- ボンディング（Bonding）/チーミング（Teaming）（802.3ad/Active-Backup）
- IEEE 802.1AX/IEEE 802.3ad/LACP

14.2.1 スイッチ側の設定

ボンディング機能の内、Active/Backup モードでの設定には、スイッチ側でのボンディング／チーミングの設定は必要ありません。単に、一般のポートをロードマスターに接続するだけで OK です。しかし、802.3ad ボンディングモードを使用するには、スイッチ側のポートが 802.1AX（802.3ad）に準拠していて、尚且つそれらのポートをボンディング／チーミングに設定する必要があります。スイッチがこの仕様に準拠しているかどうかは、スイッチ側の仕様を確認してください。各ベンダーでこの機能名が違うかもしれませんので、“リンク・アグリゲーション（link aggregation）”、“イーサネットトランク（Ethernet trunk）”, “NIC チーミング（NIC teaming）”, “ポートチャンネル（port channel）”, “ポートチーミング（port teaming）”, “ポートトランキング（port Trunking）”, “リンクバンドリング（link bundling）”, “イーサネットチャンネル（EtherChanne）”, “マルチーリンクトランキング（MultiLink Trunking 「MLT」）”, “NIC ボンディング（NIC bonding）”, “ネットワーク・フォルトトーレランス（Network Fault Tolerance 「NFT」)”、“LAG”などでチェックしてみてください。

スイッチ側の VLAN トランキング機能を可能にする時は、スイッチの各ポートが一般、アクセス、トランキングの各専用モードをサポートしているか確認ください。

- 一般モード： ポートを VLAN に属させ、タグあり、タグなしの設定が可能です（802.1Q フルモード）。
- アクセスモード： シングルのタグなし VLAN に属させます。
- トランクモード： ポートを全てのポートがタグありの VLAN に属させます。

14.3 ボンディング／チーミング (802.3ad/Active-Backup)

ボンディング機能を設定するためのキーポイントを下記します。

- ボンディングをするポートは、親ポートより高い番号のポートでなければなりません。例えば、ボンディングをポート#10 より始める場合、追加するポートは #11、もしくはそれより高い番号のポートでなければなりません。
- ボンディングと VLAN タギングを併用する場合は、ボンディングを設定し終えてから VLAN タギングを設定しなければなりません。
- ボンディングされたインターフェイスにリンクを追加するには、まず始めに、追加するリンクから IP アドレスを削除する必要があります。
- 通常、“Active-Backup” モードを有効にする際にスイッチ側の設定は必要ありません。
- eth0 と eth1 をボンディングすると深刻な問題が生じるおそれがあるため、それらをボンディングすることはできません。

ボンディングに使用するポートは、スイッチ側、ロードマスター側両方で全て同じスピード、Duplex モードである必要があります。

ポート#0 をボンディングとして設定した場合、WUI 接続が切れてしまいます。再接続をするためには、システムを一旦リブートする必要があります。もし、他のポートにアクセス可能ならば、WUI よりリブートを可能にするためにそのポートに WUI を仮に移すことを推奨します。

14.4 VLAN タギング

VLAN を設定するに当たり、下記を考慮しておいてください。

- VLAN タギングを設定する場合は、スイッチ側の設定を先に済ませておいてください。
- ボンディング／チーミングを VLAN タギングと併用する場合は、ロードマスター側では先ずボンディングの設定を行った上で VLAN タギングの設定を行ってください。
- VLAN タグは、一般の物理ポート、もしくはボンディングポートの両方で設定可能です。

15 その他

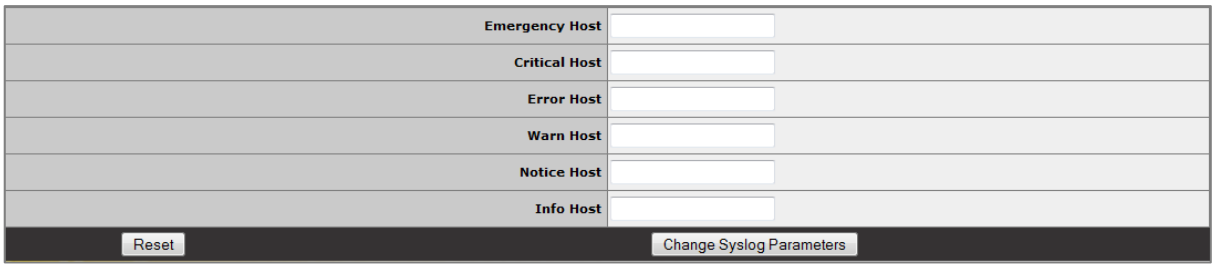
15.1 IPv6 のサポート

ロードマスターのこのソフトウェアバージョンでは、IPv6 をサポートしています。ネットワーク·アドレスを割り当てる前に、どれを IPv4 のままとし、どれを IPv6 に変換するかを考慮してください。ロードマスターは、これらの異なるネットワーク間のアドレス変換をサポートします。従って、例えば IPv6 を持っている内部ネットワークと、IPv4 の外部ネットワーク間を相互接続することが可能です。

レイヤ 4 における IPv6 の FTP はサポートしていません。

15.2 リモート Syslog サポート

ロードマスターは、syslog プロトコルを使い、色々な警告とエラーメッセージを出力できます。これらのメッセージは、通常ローカルメモリーに蓄積され、WUI の“System Configuration”メニューの”logging Options”下の”log Files”からか、コンソールの診断メニューを介して表示することができます。また、ロードマスターがこれらのエラーメッセージをリモート syslog サーバーへ送信するように設定することも可能です。6 つの異なるレベルのエラーメッセージが定義されています。各レベルのメッセージを、異なるサーバーへと送れます。



メッセージは、情報が送られるだけです。Emergency メッセージは、通常早急なアクションを必要とします。

リモート Linux サーバーで、ロードマスターの syslog メッセージを受けられるように syslog プロセスを有効にするためには、syslog を“-r”フラッグを立てて起動しなければなりません。

15.3 ライセンスの入手方法

リブート後、ログイン用プロンプトが現れますので、’bal’（パスワード‘1fourall’）でログインします。

ロードマスターのソフトウェアをアンロックするためには、ライセンスキーが必要です。ライセンスキーは、各単一ロードマスター・インスタンスにハードウェア依存のアクセスコードを結合させて、個々に生成します。

ロードマスター用に入手できるライセンスは、下記の 3 種類です。

1. 評価用(仮)ライセンス。これは最長 30 日間有効なフル機能用ライセンスです。
2. 期限なし（フル）のスタンドアローン用ライセンス。
3. 期限なし（フル）の HA クラスター構成用ライセンス。HA-1 と HA-2 に分かれています。

評価用ライセンスは、フルのスタンドアローンか HA 用にアップグレードができます。

ライセンス情報は、Web ユーザーインターフェイスの **System Configuration** > **System Administration** > **Update License** で更新できます。HA システムの場合は、2 番目のロードマスターにも同じプロセスを繰り返します。

仮想ロードマスターのライセンスを初めて設定する際には、KEMP ID が必要です。KEMP ID がない場合は、その設定手順について、**ライセンス　機能説明**を参照してください。KEMP ID がある場合は、用意されている WUI のオプションで、仮想ロードマスターのライセンスを設定できます。

ハードウェアロードマスターには、事前にインストール済みのライセンスが付属しています。このライセンスをアップグレードする必要がある場合は、KEMP にご連絡ください。

15.4　バックアップとリストア

ロードマスターの設定は、ネットワークを介してリモート PC、もしくはサーバーへセーブできます。完全な設定（仮想サービス設定とシステムのベース設定）が、統計データとともに、1 つのシングルファイルとして PC、もしくはサーバーへセーブされます。SSL 証明書は、このバックアップには含まれませんので気をつけてください。なお、サーバーにて FTP デーモン（または SSH デーモン）が実行され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。

設定をリストアする時、下記のどのポーションをリストアするか問われます。

- The Virtual Service Configuration only（仮想サービス設定関連のみ）
- The LoadMaster “base” Configuration only（システム基本設定のみ）
- The Virtual Service + the LoadMaster “base” Configuration（SSL 証明書を除く全ての設定）

“LoadMaster base Configuration”は、ロードマスターの IP アドレス等の全てのインターフェイス情報や基本的な設定が含まれます。

“Virtual Service Configuration”は、仮想サービスと実サーバーの全ての設定情報が含まれています。

注意： HA クラスターのスタンバイマシンに設定をリストアした場合は、LM 情報だけがリストアされます。仮想サービスの設定はアクティブ側から提供されます。

1 日 1 回または 1 週間に 1 回、自動的にバックアップするよう設定することもできます。

バックアップ/リストアに関する各種オプションの詳細については、**ウェブユーザーインターフェイス（WUI） インターフェイスマニュアル**を参照してください。

15.5 WUI へのアクセス禁止/許可

状況によっては、ロードマスターWUI へのアクセスを禁止したい場合があると思います。WUI へのアクセスを禁止するには、“**Remote Access**” 画面の“**Allow Web Administrative Access** ”オプションをオフにします。または、ロードマスターのコンソールにて、以下の手順で WUI へのアクセスを禁止/許可できます。

1. “**3. Local Administration** ”オプションを選択します
2. “**4. Web Address** ”オプションを選択します
3. “**s. Immediately Stop/Start Web Server Access** ”オプションを選択します

WUI へのアクセスを禁止すると、ユーザーはロードマスターの WUI にアクセスできなくなります。セキュリティ等の理由により、WUI へのアクセス禁止が必要となる場合があります。

15.6 L4 と L7 の仮想サービス間の相互可動性

パーシステンス方式を他の方式に変更した場合、全ての VS/RS の統計情報がリセットされます。

バイト用統計値がテラバイトからゼロに変更された時、関連する値（Byte/sec など）をグラフ表示をしていると最大値と最小値が大きくかけ離れていることから表示に影響が出ます。

15.7 ログ情報

ログ情報は、WUI の“System Configuration”サブメニュー下の“Logging Options”オプションの“Log Files”から閲覧可能です。

- Boot.msg File： Linux の一般的なブート情報が含まれています。
- Warning Message File： コアの負荷分散エンジンが出力したイベントを含んでいます。L4 の関連です。
- System Message File ：Linux の OS とコアな負荷分散エンジン（L7）が出力したイベントを含んでいます。

注：ログ情報は、限られたメモリー容量を使用しているため、上書きされてしまいます。また、システムがハングアップしてしまった場合は参照できません。Syslog サーバーや SNMP マネージャーを使用して、イベント情報が残るようにすることを推奨します。

15.8 デバッギング機能

この機能は、WUI の“System Configuration”サブメニュー下の“Logging Optios”オプション内の“Debug Options”の下記を選択することで実施可能です。特定の問題を解決するために、KEMP 社の販売店サポート技術要員の指示により使用することをお勧めします。

15.8.1 Disable All Transparency

全ての仮想サービスのトランスペアレンシーを変更します。KEMP 社の販売店サポート要員の承諾を得た上でオンにしてください。

15.8.2 Enable L7 Debug Traces

“System Messages”内に、追加的な L7 アクセスのデバッグ情報を出力します。

15.8.3 Perform a PS

システムのプロセス状態をレポートします。

15.8.4 Perform a l7adm

L7 の仮想サービスの詳細情報をテーブル形式で表示します。

15.8.5 Ping Host

ICMP をサポートしている IPv4 デバイスへの ICMP エコーリクエスト（PING）を発信します。

15.9 RESTful API インターフェイス

ロードマスターでは、リモートアプリケーションからアクセスするための、シンプルかつ一貫性のあるインターフェイスが用意されています。これは、REST と同様のインターフェイスになっています。REST（Representational State Transfer）とは、分散システムのためのソフトウェアアーキテクチャ様式で、Web サービスの主要な設計モデルの一つです。

ロードマスターの RESTful API は、ユーザー（またはアプリケーション）からロードマスターへの HTTP リクエストを許可することで使用できるようになります。ロードマスターは、そのリクエストに対して XML 形式で応答を返します。

このインターフェイスを有効にする方法の詳細については、**ウェブユーザーインターフェイス（WUI） インターフェイスマニュアル**を参照してください。

RESTful API の詳細については、KEMP テクノロジーのドキュメントページにある **RESTful API　インターフェイスマニュアル**を参照してください。

参考ドキュメント

特に明記されていない限り、以下のドキュメントは、
http://www.kemptechnologies.com/documentation から入手できます。

1. ウェブユーザーインターフェイス（WUI）　インターフェイスマニュアル
2. DSR 用実サーバーの設定　テクニカルノート
3. エージェントベースのアダプティブ・バランシング用 API　テクニカルノート
4. RESTful API　インターフェイスマニュアル
5. Oracle 仮想マシン　インストールガイド
6. Oracle Virtual Box　インストールガイド
7. VMWare Workstation および Player　インストールガイド
8. XEN（並列仮想化）　インストールガイド
9. Cisco UCS B シリーズのブレードサーバー　インストールガイド
10. KVM（並列仮想化）　インストールガイド
11. Hyper-V　インストールガイド
12. VMWare ESX、ESXi、および vSphere　インストールガイド
13. ライセンス　機能説明

Document History

Date	Change	Reason for Change	Ver.	Resp.
May 2013	Initial draft of the document	Reorganization of documentation	1.0	DD
May 2013	Updated copyright	Updated Copyright Notices section	1.1	LB
July 2013	Release updates	Updates based on 7.0-6 release	1.2	LB
Sep 2013	Licensing section added	New licensing process	1.3	LB

