ウェブユーザーインターフェイス（WUI）

設定ガイド

バージョン：10.0
更新：2016 年 7 月

著作権

かなる場合においても、上記の著作権保持者、または貢献者は、損害の可能性について知らされているものも含めて、このソフトウェアの停止によるいかなる直接的、間接的、偶発的、特殊的、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 にあるフリーソフトウェア財団（株）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ならば、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.

このソフトウェアの一部（1995 年発行 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頂ければ感謝します。

2. ソースを変更したバージョンを使用するならば、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。

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、“現状のまま”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。

本製品は、正当な許可を得て、米国特許 6,473,802、6,374,300、8,392,563、8,103,770、7,831,712、7,606,912、7,346,695、7,287,084 および 6,970,933 を使用しています。

目次

1 はじめに

KEMP テクノロジーの製品は、高可用性、高パフォーマンス、柔軟なスケーラビリティ、セキュリティ、および管理のしやすさによって定義された Web およびアプリケーションインフラストラクチャを最適化することができます。KEMP テクノロジーの製品は柔軟で幅広い導入オプションを提供するとともに、Web インフラストラクチャの総所有コスト（TCO）を最小限に抑えます。

1.1 ドキュメントの目的

本ドキュメントでは、KEMP ロードマスターの Web ユーザーインターフェイス（WUI）について説明します。本ドキュメントでは、WUI を使って KEMP ロードマスターの各種機能を設定する方法について詳しく説明します。

ロードマスターで使用可能なメニューオプションは、本ドキュメントで説明しているものと異なる場合があります。ロードマスターで使用可能な機能は、有効になっているライセンスの種類によって異なります。ライセンスをアップグレードされる場合は、KEMP テクノロジーの担当窓口までご連絡ください。

1.2 対象読者

本ドキュメントは、WUI を使って KEMP ロードマスターを設定するユーザーを対象としています。

2 ホーム

“Home”メニューオプションをクリックすると、ホームページが表示されます。このページには、ロードマスターに関する基本情報のリストが表示されます。

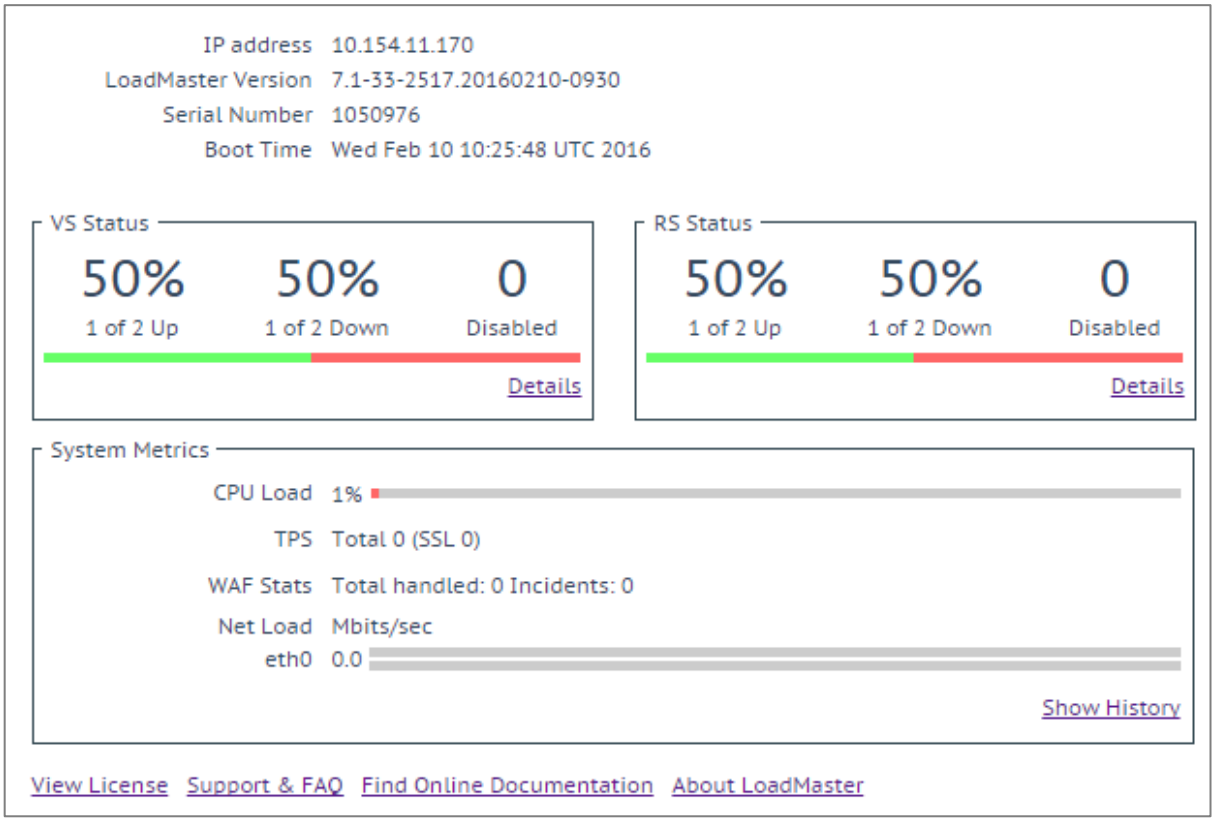

図 2-1:ロードマスターのホーム画面

2.1一般情報

Last Login（最終ログイン）:セッション管理が有効になっている場合、最後にログインした日付と時刻が表示されます。セッション管理についての詳細は、**セクション 9.8** を参照してください。

IP address（IP アドレス）:ロードマスターの IP アドレス

LoadMaster Version（ロードマスターのバージョン）:ロードマスターのファームウェアバージョン

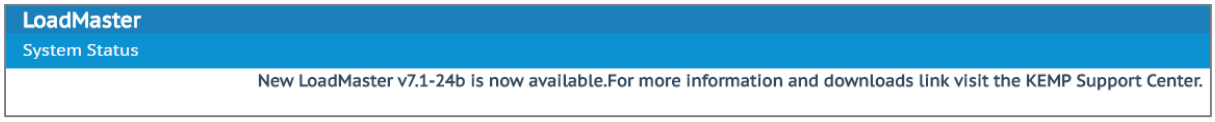

図 2-2:新しいソフトウェアが利用可能

"Allow Update Checks"（更新のチェックを許可する）機能が有効になっている場合、ロードマスターの新しいバージョンのファームウェアが利用可能になると、**"Home"**画面のトップに通知メッセージが表示されます。自動チェック機能を有効にするには、**" Certificates & Security" > "Remote Access"**を選択します。詳細は**セクション 9.6.1** を参照してください。

Serial Number（シリアル番号）:ロードマスターのシリアル番号

Boot Time（ブート時刻）:サーバーを最後にリブートした時刻

2.2仮想サービスと実サーバーの状態

VS Status（VS ステータス）

このセクションには、仮想サービスの監視情報が表示されます（稼働中の仮想サービスの割合、無効になっている仮想サービスの数など）。**"Details"**のリンクをクリックすると、**"View/Modify Services"**画面が表示されます。

1 時間ごとに、仮想サービス、サブ VS、実サーバーの数（稼働/停止中の数など）に関する syslog のメッセージが生成されます。syslog のメッセージは状態が変化したときにも生成されます。

RS Status（RS ステータス）

このセクションには、実サーバーの監視情報が表示されます（稼働中の実サーバーの割合、無効になっている実サーバーの数など）。"Details"のリンクをクリックすると、**"Real Servers"**画面が表示されます。

2.3WAF ステータス

図 2-3:WAF ステータス

Web アプリケーションファイアウォール（WAF）ステータスのセクションには、1 つ以上の仮想サービスで WAF が有効かどうかが表示されます。ここには以下の値が表示されます。

- WAF により処理されたトータルの要求数（ブロックされたかどうかにかかわらず、すべての要求が表示されます）。各接続につき 2 つの要求が記録されます（1 つは受信要求、1 つは送信要求）。
- WAF により処理されたトータルのイベント数（ブロックされた要求）

- 現在の時間内（*xx*.00.00 以降）に発生したイベントの数
- 真夜中（ローカル時刻）以降に発生したイベントの数
- 1 日のうちに、設定された警報しきい値をイベントカウンターが越えた回数例えば、しきい値が 10 に設定されており、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。警報しきい値は、仮想サービス編集画面の**"WAF Options"**にある**"Hourly Alert Notification Threshold"**フィールドに入力することで、仮想サービスごとに設定できます。詳細は**セクション 3.7** を参照してください。

2.4システムメトリックス

CPU Load（CPU 負荷）: ロードマスター機器の CPU 負荷率

TPS [conn/s]:1 秒当たりの総トランザクション数および 1 秒当たりのセキュアソケットレイヤー（SSL）トランザクション数

Net Load（正味負荷）: 設定されたインターフェイスごとのネット負荷（Mbit/秒）**"Net Load"**は、設定済みのインターフェイスについてのみ表示されます。

CPU Temp.: サポートされているハードウェアの CPU の温度を表示します。

CPU 負荷とネット負荷のデータは 5 秒ごとに更新されます。

2.5ライセンス情報

"View License"のリンクをクリックすると、サポートとライセンスの詳細情報が表示されます（ロードマスターライセンスのアクティベーション日や終了日など）。

サポートの有効期限が切れると、**"License Information"**セクションにメッセージが表示されます。サポートを更新される場合は、KEMP までお問い合わせください。

Upgrade（アップグレード）:KEMP 購入ポータルからライセンスを購入することで、ロードマスターをアップグレードします。

2.6その他のリンク

ホームページの下部に、その他のリンクが用意されています。

- **Support & FAQ（サポートと FAQ）**:KEMP サポートサイトへのリンク
- **Find Online Documentation（オンラインドキュメントを検索）**:KEMP のドキュメントページへのリンク
- **About LoadMaster（ロードマスターについて）**:ロードマスターWUI の**"About"**画面へのリンク。

3 Virtual Services（仮想サービス）

これ以降、本ドキュメントでは、ロードマスターの WUI の左側に表示される通常のメインメニューのオプションについて説明します。

3.1新規追加

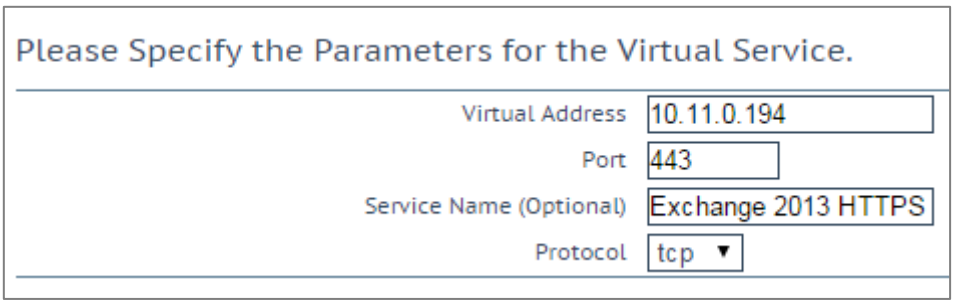

図 3-1:仮想サービスの新規追加画面

ここでは、仮想 IP（VIP）アドレス、ポート、プロトコル、名前を定義できます。新しい仮想サービス作成が行えます。仮想 IP（VIP）アドレス、ポート番号をテキストボックスに手動で入力し、プロトコルタイプをドロップダウンリストから選択します。

お使いのマシンにテンプレートがインストールされている場合、**“Use Template”**プルダウンリストを利用できます。このリストでは、仮想サービスのパラメータ（ポートやプロトコルなど）を設定するためのテンプレートを選択できます。

テンプレートの詳細については、

仮想サービスとテンプレート機能説明ドキュメントを参照してください。

ロードマスターExchange アプライアンスは、仮想サービス作成に 13 の上限があります。

3.2表示/変更（既存の HTTP サービス）

図 3-2:仮想サービスの画面

この画面には、ロードマスター上の仮想サービスのリストが表示されます。各仮想サービスの主なプロパティがまとめられており、サービスの変更や削除、新規作成に対応するオプションが用意されています。

注意

削除すると元に戻すことはできません。**注意して使用してください**。

設定済みの各仮想サービスを変更するには**"Modify"**ボタンをクリックし、削除するには**"Delete"**ボタンをクリックします。

仮想サービスの状態も表示されます。仮想サービス作成時、デフォルトでヘルスチェックが有効になっています。ヘルスチェックについての詳細は、**セクション 3.11** を参照してください。

仮想サービスのステータスは、次のいずれかになります。

- **アップ** - 少なくとも 1 つの実サーバーが利用可能です。
- **ダウン** - 一つの実サーバーも利用できません。
- **Sorry（申し訳ありません）** - すべての実サーバーがダウンしており、ヘルスチェックなしで、（実サーバーの設定に含まれていない）別設定の Sorry サーバーにトラフィックが転送されます。
- **Disabled（無効）** – 仮想サービス編集画面の**"Basic Properties"**セクションの**"Activate or Deactivate Service"**チェックボックスが管理者によりオフにされたため、仮想サービスが無効になっています。
- **リダイレクト** - 固定的なリダイレクトが設定されています。"Advanced Properties"セクションの"Add a Port 80 Redirector VS"オプションを使用すると、リダイレクト仮想サービスを作成できます。詳細は**セクション 3.6** を参照してください。
- **失敗メッセージ** - 固定的なエラーメッセージが設定されています。"Not Available Redirection Handling"オプションを使用すると、固定のエラーメッセージを指定できます。詳細は**セクション 3.6** を参照してください。
- **Unchecked（チェックなし）** – 実サーバーのヘルスチェックが無効になっています。すべての実サーバーが稼働状態であるという前提でアクセスされます。
- **Security Down（セキュリティダウン）** – ロードマスターが認証サーバーにアクセスできません。エッジ・セキュリティ・パック（ESP）が適用されている仮想サービスへのアクセスは、ロードマスターにより拒否されます。
- **WAF Misconfigured（WAF の設定が間違っている）** – 特定の仮想サービスの WAF が正しく設定されていない場合、例えば、ルールファイルに問題がある場合、ステータスが **WAF Misconfigured** に変わり、赤の表示になります。仮想サービスがこの状態にあるとき、すべてのトラフィックがブロックされます。トラブルシュ

ーティングの際は、必要に応じてその仮想サービスの AFP を無効にし、トラフィックがブロックされないようにすることが可能です。

以下の画面は、仮想サービスのプロパティ画面を示しています。この画面は、いくつかのコンポーネントで構成されています。

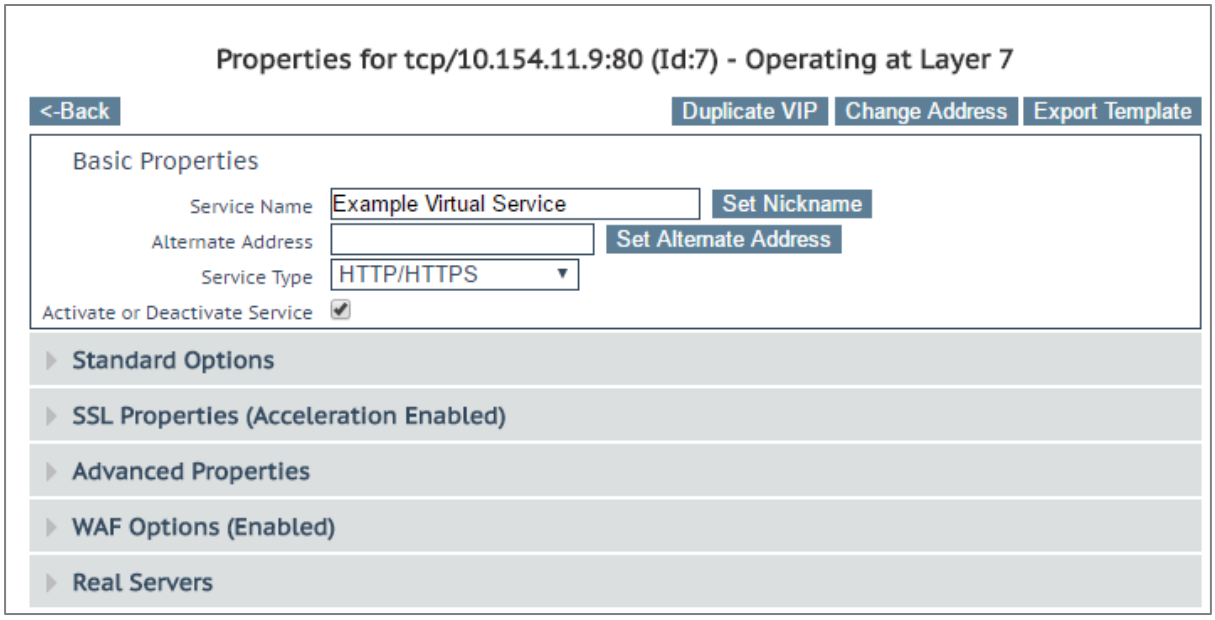

図 3-3:仮想サービスのプロパティの画面

- **Basic Properties（基本プロパティ）** - 最も一般的な属性グループです。
- **Standard Options** –仮想サービスの中で最も広く使われる機能セクションです。
- **SSL Properties（SSL プロパティ）** – SSL アクセラレーションを使用している場合、Acceleration Enabled（アクセラレーション有効）と表示され、SSL 機能を設定する際には、この画面セクションを使用します。
- **Advanced Properties**– 仮想サービスの追加機能セクションです。
- **WAF Options（WAF オプション）** – Web アプリケーションファイアウォール（WAF）に関するオプションを設定できます。
- **ESP Options（ESP オプション）** – ESP に関するオプションを設定します。
- **Real Servers/SubVSs（実サーバー/サブ VS）** – 仮想サーバーに属する実サーバーとサブ VS を割り当てるセクションです。

特定のフィールドとオプションは、サービスタイプ、および機能の有効化または無効化に応じて WUI での非表示/表示が切り替わります。したがって、このドキュメントのスクリーンショットは、すべての構成を網羅していない可能性があります。

3.3Basic Properties

"Basic Properties"ヘッダーの隣に、3 つのボタンが用意されています。

Duplicate VIP（VIP のコピー）

関連するサブ VS を含め、仮想サービスをコピーします。仮想サービスのすべての設定が、複製された仮想サービスにコピーされます。このボタンをクリックすると、コピーした仮想サービスの IP アドレスとポートを指定する画面が表示されます。

Change Address（アドレスの変更）

このボタンをクリックすると、仮想サービスの仮想 IP アドレスとポートを変更する画面が表示されます。

Export Template（テンプレートのエクスポート）

仮想サービスの設定をテンプレートとしてエクスポートします。テンプレートを使用すると、仮想サービスを素早く簡単に作成できます。テンプレートから作成された仮想サービスは、テンプレートの設定に基づきあらかじめ設定されたすべての設定を持っています。仮想サービスの設定は、必要に応じて変更できます。テンプレートについての詳細は、**仮想サービスとテンプレート機能説明**を参照してください。

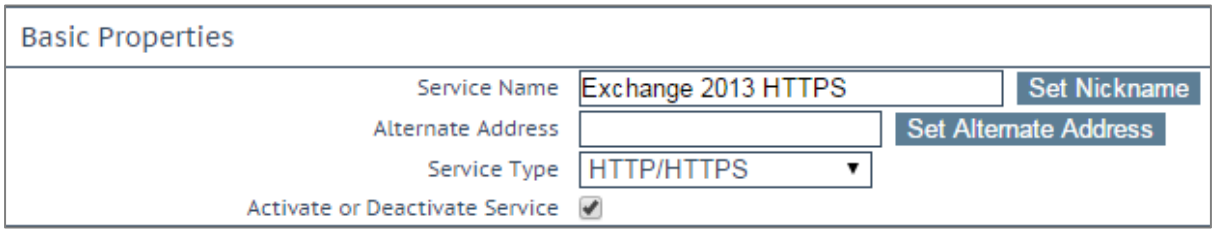

図 3-4:Basic Properties セクション

Service Name

このテキストボックスでは、作成する仮想サービスにニックネームを割り当てたり、既存のニックネームを変更したりすることができます。

サービス名には、通常の英数字のほかに、以下の「特殊」文字が使用できます。

.@ - _

ただし、特殊文字の前に 1 つ以上の英数字がなければなりません。

Alternate Address

必要に応じて、IPv4、もしくは IPv6 どちらかの形式でセカンダリアドレスを指定できます。

Service Type（サービスタイプ）

"Service Type"の設定では、仮想サービス制御の設定オプションを表示し、選択できます。サービスタイプは、負荷分散するアプリケーションの種類に合わせて設定する必要があります。

WebSocket 仮想サービスは**"Generic"**サービスタイプに設定する必要があります。

サービスタイプ **HTTP/2** では、HTTP/2 のトラフィックを使用できます。ただし現在は、アドレス変換以外のレイヤー7 のオプション（透過モード、サブネットからの要求、代替ソース）は用意されていません。

Activate or Deactivate Service（サービスのアクティブ化または非アクティブ化）

このチェックボックスでは、仮想サービスの有効/無効を指定できます。デフォルトでは、有効（active）が選択されています。

3.4Standard Options（標準的なオプション）

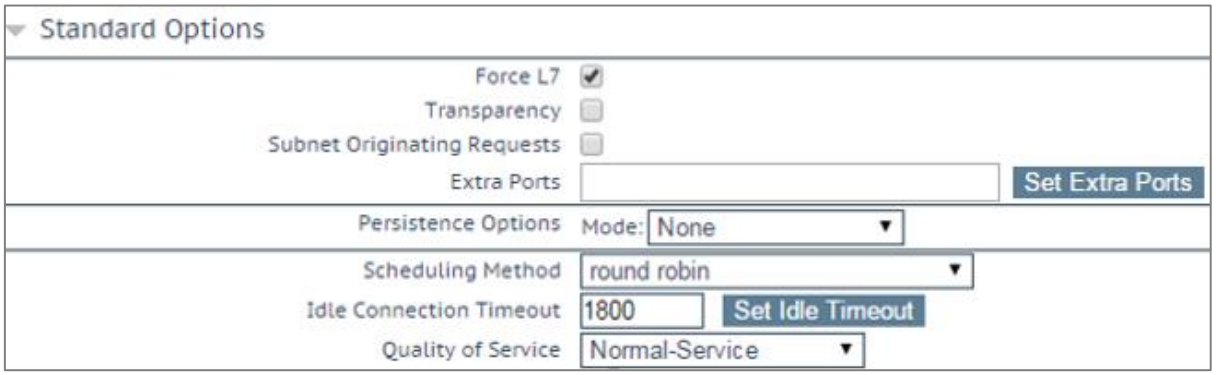

図 3-5:Standard Options セクション

Force L7（L7 を強制）

表示されている場合、**"Force L7"**を選択する必要があります（デフォルト）。選択されていない場合、仮想サービスは強制的にレイヤ 4 に設定されます。

L7 Transparency（レイヤ 7 透過モード）

上記の“Force L7”、もしくは L7 用パーシステンスオプション等を設定した場合のネットワーク透過モードの設定を行います。ただし、クライアントが仮想サービスと実サーバーと同じサブネット上に存在している場合は、送信元 IP は自動的に NAT 変換されます（非透過モードが有効になります）。

"Real Servers considered local"オプションが有効な場合、**"L7 Transparency"**であっても実サーバーは NAT 処理（非透過処理）されます。この動作は、実サーバーが仮想サービスに対する要求送信元である場合（かつ、要求に対して他のクライアントが応答していない場合）のみ発生します。

Subnet Originating Requests（サブネットからの要求）

このオプションは**"Transparency"**が無効のときのみ利用できます。

透過モードが無効の場合、実サーバーへの接続における送信元 IP アドレスは仮想サービスの IP アドレスとなります。透過モードが有効の場合、送信元 IP アドレスは仮想サービスに接続する IP アドレスになります。実サーバーがサブネット上にあり、**"Subnet Originating Requests"（サブネットからのリクエスト）**が有効の場合は、ロードマスターのサブネットアドレスが送信元 IP アドレスとして使用されます。

このスイッチを使用すると、サブネットからの要求を仮想サービスごとに制御できます。グローバルスイッチ（メインメニューの**"System Configuration > Miscellaneous Options > Network Options"**にある**"Subnet Originating Requests"**）が有効の場合、すべての仮想サービスに対して有効になります。

仮想サービスごとに**"Subnet Originating Requests"**オプションを有効にすることを推奨します。

グローバルオプションの詳細については、セクション **10.5.3** を参照してください。

グローバルオプションが無効の場合、仮想サービスごとに制御できます。

SSL の再暗号化が有効な仮想サービスに対してこのスイッチをオンにすると、その仮想サービスを使用しているすべての接続が切断されます。

Extra Ports（追加のポート）

VS がサービスを受け付けるポート番号が複数で尚且つ非連続番号であるならば、このパラメータに追加のポート番号を入力します。ポート番号は、スペースで区切ってフィールドに入力します。入力できるポート数の上限は、510 個です。

ユーザーは、追加のポートを入力できます。追加のポートは、ポート範囲を指定するか、スペース（またはカンマ）で区切って個別に指定できます（ポートの順序は関係ありません）。例えば、'8000-8080, 9002, 80, 8050, 9000'と入力すると、80 番、**8000～8080 番、9000 番、9002 番**のポートが追加されます。

Server Initiating Protocols（サーバー起動プロトコル）

デフォルトでは、クライアントからデータが送信されるまで、ロードマスターは実サーバーに接続しません。そのため、データを送信する前に実サーバーへの接続が必要なプロトコルは、このままでは正しく機能しません。

仮想サーバーがそのようなプロトコルを使用する場合は、プルダウンリストからそのプロトコルを選択し、それらが正しく機能するようにします。

以下のプロトコルの選択が可能です。

- SMTP
- SSH
- IMAP4
- MySQL
- POP3
- Other Server Initiating Protocols（その他のサーバー起動プロトコル）

仮想サービスで **80、8080、443** のポートが指定されている場合、
"Server Initiating Protocol"オプションは表示されません。

Persistence Options （パーシステンスオプション）

パーシステンスは仮想サービスごとに設定されます。このセクションでは、このサービスパーシステンスを有効にするかどうかを選択できます。また、パーシステンスの種類とパーシステンスのタイムアウト時間を設定できます。

もし、パーシステンスが有効になったら、クライアントの接続が特定の実サーバーへ行われるように維持されます。言い換えると、同じクライアントは、同じ実サーバーへと接続されます。タイムアウト値は、ロードマスターがどれぐらいこの特定接続を記憶しておくかを指定するものです。

パーシステンスのタイプは、以下のように、ドロップダウンリストのオプションから選択できます。以下の 3 つです。

- **Source IP Address（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、パーシステンスの一番シンプルな方式で、HTTP に関連しないものも含めて、すべての TCP プロトコルで働きます。

- **Super HTTP（スーパーHTTP）**

  ロードマスターを使用して HTTP および HTTPS のパーシステンスを実現する手法として、スーパーHTTP を推奨します。これは、クライアントブラウザーの一意の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適切な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。

- **Server Cookie（サーバー・クッキー）**

  リクエストの HTTP ヘッダー内に同じクッキーが存在すると、前回と同じサーバーへとリクエストを分配します。このクッキーは、サーバーによって作成される必要があります。

- **Server Cookie or Source IP（サーバークッキー、もしくはソース IP）**

  リクエストの HTTP ヘッダー内に同じクッキー（実サーバーが作成した）が存在すると、前回と同じサーバーへとリクエストを分配します。

- **Active Cookie（アクティブクッキー）**
  アクティブクッキーパーシステンスを使用すると、サーバーではなくロードマスターによりクッキーが生成されます。アクティブクッキーが設定されたロードマスター仮想サービスに接続が行われると、そのロードマスターは特定のクッキーを探します。目的のクッキーが存在しない場合、ロードマスターは HTTP ストリームに Set-Cookie 命令を挿入します。既存のクッキーは影響を受けません。サーバークッキーのパーシステンス方式と同様に、ロードマスターにより生成されたクッキーはユーザーごとに一意の値となるため、ロードマスターは各ユーザーを

識別することができます。この手法には、サーバーがクッキーの管理または生成を行う必要がなく、サーバー設定の負担が軽くなるというメリットがあります。クライアント接続ごとにより効果的に負荷を分散させるには、"L7 Configuration"の"Add Port to Active Cookie"を有効にします。このオプションについての詳細は、**セクション 10.5.2** を参照してください。
アクティブクッキーパーシステンスを使用すると、そのクッキーは、セッションが継続している間またはパーシステンスがタイムアウトするまで有効になります。例えば、パーシステンスタイムアウトが 10 分に設定されたアクティブクッキーパーシステンスを使用しており、クライアントが午後 2 時に接続したとすると、午後 2 時 5 分に切断と再接続が行われます。このとき、パーシステンスタイムアウト値がリセットされます。パーシステンスがタイムアウトした後にクライアントが仮想サービスへの接続を試みた場合、そのクライアントには古いクッキーが提示されます。ロードマスターはパーシステンステーブルをチェックし、有効なエントリが含まれていないことを確認します。すると、ロードマスターは、そのクライアント用に新しいクッキーを生成し、パーシステンステーブルを更新します。

- **Active Cookie or Source IP（アクティブクッキー、もしくはソース IP）**

  リクエストの HTTP ヘッダー内に同じクッキー（ロードマスターが作成した）が存在すると、前回と同じサーバーへとリクエストを配分します。クッキーが存在しない場合には、ソース IP アドレスを使ってパーシステンスを試みます。

- **Hash All Cookies（ハッシュ全クッキー）**

  "Hash All Cookies"（すべてのクッキーをハッシュ化する）は、HTTP ストリームにあるすべてのクッキー値をハッシュ化します。同じ値を持つクッキーは、リクエストを受け取るたびに同じサーバーに送信されます。同じハッシュ値が存在しない場合は、新しい接続とし負荷分散方式に従って実サーバーへとリクエストを転送します。

- **Hash All Cookies or Source IP（ハッシュ全クッキー、もしくはソース IP）**

  リクエストの HTTP ヘッダー内のクッキーより変換した同じハッシュ値が存在すると、前回と同じサーバーへとリクエストを転送します。同じハッシュ値が存在しない場合には、ソース IP アドレスを使ってパーシステンスを試みます。

- **Super HTTP and Source IP Address（スーパーHTTP、もしくはソース IP）**

  先ずは、スーパーHTTP によるハッシュ値によるパーシステンシーを試みます。同じハッシュ値が無い場合は、ソース IP アドレスを使用してパーシステンシーを試みます。

- **URL Hash（URL ハッシュ）**

同じ URL へのリクエストは、同じサーバーへと転送します。

- **HTTP Host Header（HTTP ホストヘッダー）**

  HTTP の Host ヘッダーを使用し、同じホストへのリクエストは、前回と同じサーバーへ転送します。

- **Hash of HTTP Query Item（HTTP クエリ項目ハッシュ）**

  同じクエリ項目を含むリクエストは、前回と同じサーバーへと配分されます。同じクエリ項目値を持つクエリは、すべて同じサーバーに送信されます。

- **Selected Header（指定ヘッダー）**

  特定の HTTP ヘッダーを指定して、そのヘッダーによるパーシステンシーを行います。ヘッダーの値がマッチングしたら前回と同じ RS へ接続します。

- **SSL Session ID（SSL セッション ID）**

  SSL の各セッションには、持続可能な固有のセッション ID が設定されています。

  このオプションをパーシステンス方式として表示するには、仮想サービスの**"Service Type"**を**"Generic"**に設定して、SSL アクセラレーションを無効にする必要があります。

  仮想サービスが SSL サービスに該当し、オフロードされていない場合、ロードマスターはレイヤ 7 のストリームに含まれるデータを有効に操作できません。その理由として、データが暗号化されており、ロードマスターでは復号できないことが挙げられます。

  上記のシナリオで、オフソースの IP に基づいていないパーシステンスモードが必要な場合、これ以外のオプションはありません。SSL セッションが開始されると、接続用のセッション ID が生成されます。このセッション ID を使用して、クライアントを適切なサーバーに永続的に割り当てることが可能になります。

  ただし、この方法には、いくつかのマイナス面があります。最新のブラウザのほとんどは非常に短い間隔でセッション ID を再生成するので、基本的にセッション ID は上書きされ、パーシステンスのタイムアウト間隔を長く設定しても効果がありません。

- **UDP Session Initiation Protocol (SIP)（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 L7"**が有効になっているときに UDP 仮想サービスでのみ利用可能です。SIP は、HTTP と同様のリクエスト/レスポンストランザクションを使用します。最初の INVITE リクエストが送信されますが、この

リクエストにはヘッダーフィールドの数が含まれています。このヘッダーフィールドはパーシステンスで使用可能です。

Timeout（タイムアウト）

パーシステンス方式ごとに、設定可能なタイムアウト値が用意されています。この値は、ユーザーごとにどのくらいの時間パーシステンスを与えるかを決定し、1 分から 7 日の間で選択できます。

このタイムアウトタイマーは、最初に接続が確立されたときに起動します。このタイムアウト時間内にクライアントが再接続を行うと、パーシステンスタイムアウト値が更新されます。例えば、パーシステンスタイムアウトが 1 時間に設定されており、クライアントが午後 2 時に接続した場合、このクライアントが午後 3 時前に切断と再接続を行えば、同じ実サーバーとのパーシステンスが維持されます。また、このクライアントのパーシステンスレコードが更新されてこの操作が反映され、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。

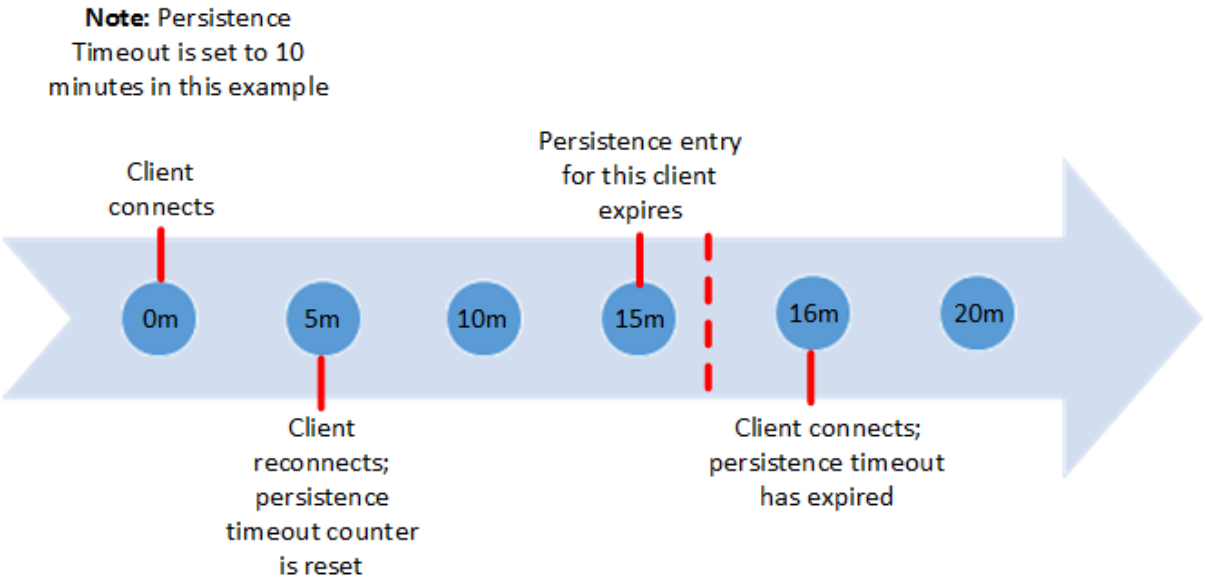

図 3-6:パーシステンスタイムアウトの例

タイムアウト時間内にクライアントが仮想サービスに繰り返し接続を行うと、パーシステンスは無限に与えられます。例として以下のシナリオを考えます。

- パーシステンスタイムアウトが 10 分に設定されている
- ユーザーは、20 分の間に何度かリクエストを行うが、接続間隔は常に 1 分未満である

要求は、利用可能な（ヘルスチェックに合格したサーバー）正しいサーバーに送信する必要があります。

ユーザーが 20 分間何も操作しなかった場合、次の接続は新しいセッションとしてカウントされ、スケジューリング方式に応じて別のサーバーに送信されます。接続が 10 分以上オープンされた状態でクライアントが切断と再接続を行った場合、パーシステンスレコードの有効期限はおそらく切れているでしょう。このとき、ロードマスターによりそのクライアント用のパーシステンスエントリが新たに作成され、そのクライアントは新しい実サーバーに送信されます。これは、接続がクローズされたときではなく、接続が確立されたときにパーシステンスのカウントダウンが開始されるため、そのような動作になります。

パーシステンスの問題が発生する場合、パーシステンスタイムアウト時間が十分長く設定されていないことが原因かもしれません。パーシステンスタイムアウト時間が十分長くない場合、タイムアウトの値をもっと大きく設定する必要があります。一般に、お使いのサーバーのタイムアウト値に合わせてこの値を設定することを推奨します。

Header field name（ヘッダーフィールド名）

LoadMaster において、パーシステンスモードとして**"UDP Session Initiation Protocol"**が選択されている場合、**"Header field 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もととなるヘッダーフィールドをここで入力してください。

Scheduling Methods（負荷分散方式）

このパラメータは、ロードバランサーが特定のサービスのために実サーバーを選択する方式を指定し、負荷の実サーバーへの分散を可能にします。下記の分散方式が選択できます。

- **Round Robin（ラウンドロビン）**

  ラウンドロビンは、最初のセッションを実サーバー1 へ、2 番目を実サーバー 2 へという様に、新しいセッションを順番に実サーバーへフォワードします。この方式では、負荷を特定サーバーに偏らせることはできません。

- **Weighted Round Robin（重み付けラウンドロビン）**

  この方式は、新しいセッションがどの実サーバーにアサインされるべきか、実サーバーの重みによって決定されます。高い重みを持つ実サーバーほど、その重みに比例して多い接続を引き受けさせられます。

- **Least Connection（最小接続）**

この方式では、現状で一番接続数が少ない実サーバーが、新しいセッションにアサインされます。

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

  最小接続と同じですが、重みをバイアスにして計算した結果で実サーバーをアサインします。

- **Resource Based (Adaptive)（アダプティブ）**

  アダプティブ分配方式は、実サーバーの実際の負荷を定期的にモニターしてそのレシオに基づいて実サーバーをアサインします。結果的に非常にバランスの取れた配分ができます。詳細は、3 項の負荷分散方式のセクションを参照ください。

- **Resource Based (SDN Adaptive)（SDN アダプティブ）**
  アダプティブスケジューリング方式を使用している仮想サービスは、（SDN を使用しているかどうかにかかわらず）制御システムとして見えます。これは、実サーバー間で負荷を均等に配分し、コントローラーがそれをもとに誤差を計算するようにするためです（この値は、目的とする負荷均等配分からのずれを表します）。またコントローラーは、誤差が小さくなるように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。
- **Fixed Weighting（固定重み）**

  重みの値が最も大きく、使用可能な状態である実サーバーに、すべてのトラフィックが転送されます。実サーバーには、その作成時点で重みを設定する必要があります。2 つの実サーバーに同じ重みを設定すると、予期しない結果が発生する可能性があるため、このような設定は避けてください

- **Weighted Response Time（加重応答時間）**

  ロードマスターは、15 秒ごとに行うヘルスチェックの応答にかかる時間を測定して、その時間に応じた重みを実サーバーへ付与します。実サーバーの応答時間が早ければ早いほど大きな重みが与えられるので、実サーバーに転送されるトラフィック量が増加します。

- **Source IP Hash（ソース IP ハッシュ）**

  重みやラウンドロビン方式の代わりにソース IP アドレスより生成したハッシュ値を使用して、同じハッシュ値のリクエストはいつも同じ実サーバーへと転送します。これは、同じホストからの実サーバーは常に同じであることを意味します。この方式を使用することで、ソース IP パーシステンシー方式を使用する必要はありません。

この方式はクライアント（ソース）IP アドレスのみに依存し、現在のサーバー負荷を無視するため、この方式を使用すると、特定の実サーバーが過負荷になったり、実サーバー間のトラフィックが不均衡になったりする可能性があります。

Idle Connection Timeout （アイドル接続のタイムアウト時間）（デフォルト 660）

アイドル接続を閉じるまでの秒数を指定します。このフィールドに設定可能な特殊な値が用意されています。

- 0 を設定すると、L7 接続のデフォルトのタイムアウト時間が使用されます。**"Connection Timeout"（接続タイムアウト）**のデフォルトの値は、**"System Configuration" > "Miscellaneous Options" > "Network Options"**で変更できます。
- 1 を設定すると、パケットが最初に転送された後に接続が破棄されます。このとき、レスポンスは期待されず、また、レスポンスの処理も行われません。
- 2 を設定すると、DNS 方式の動作が行われます。応答メッセージ後の接続はドロップされます。

"Idle Connection Timeout"に特殊な値である 1 または 2 を設定すると、UDP 接続におけるパフォーマンスとメモリ効率が向上し、UDP をより効果的に使用できるようになります。

Quality of Service（サービス品質）

"Quality of Service"ドロップダウンリストでは、仮想サービスから送出されるパケットの IP ヘッダーに含まれる Differentiated Services Code Point（DSCP）を設定します。この設定により、次の段階でパケットを処理するデバイスやサービスにトラフィックの処理方法と優先順位の設定方法を指示します。優先順位の高いパケットは、優先順位の低いパケットよりも先にロードマスターから送出されます。

各オプションについて、以下で説明します。

- **Normal-Service（通常サービス）**:特別な優先順位をトラフィックに割り当てない。
- **Minimize-Cost（コスト最小化）**:低コストのリンクでデータを転送する必要がある場合に使用。
- **Maximize-Reliability（信頼性最大化）**:信頼性のあるリンクでデータを宛先に転送して、再転送がほとんど発生しないようにする場合に使用。

- **Maximize-Throughput（スループット最大化）:**リンクの遅延が大きい場合でも、インターバル中に転送されるデータ量が重視される場合に使用。
- **Minimize-Delay（遅延最小化）:**パケットが宛先に到達するまでの所要時間（遅延）を抑制する必要がある場合に使用。このオプションは、**"Quality of Service"**の各オプションで、最も待ち時間が短くなります。

> **"Quality of Service"**機能が有効に機能するのは、レイヤ 7 トラフィックに限定されます。レイヤ 4 トラフィックでは、機能しません。

Use Address for Server NAT（サーバーNAT のアドレスを使用）

ロードマスターが SNAT 実サーバーで使用される場合、デフォルトではロードマスターのソース IP アドレスがインターネットで使用されます。**“Use Address for Server NAT”**オプションを選択すると、仮想サービス上で構成された実サーバーが、仮想サービスのアドレスをソース IP アドレスとして使用できるようになります。

> このオプションは、ロードマスターがパブリックドメイン内にあり、ロードマスターから送られたソースアドレスが送信側の Mail Exchanger（MX）レコードの値と一致するかを確認するために SMTP などのサービスが DNS の逆引きチェックを必要とするとき最も役に立ちます。

このオプションが設定された複数の仮想サービス上で実サーバーが構成されている場合、ポート **80** への接続でのみ、この仮想サービスのアドレスがソース IP アドレスとして使用されます。

> **"Use Address for Server NAT"**オプションは、デフォルトゲートウェイで動作している仮想サービスでのみ有効に機能します。このオプションは、デフォルトゲートウェイでないインターフェイスではサポートされていません。

3.5SSL Properties（SSL のプロパティ）画面

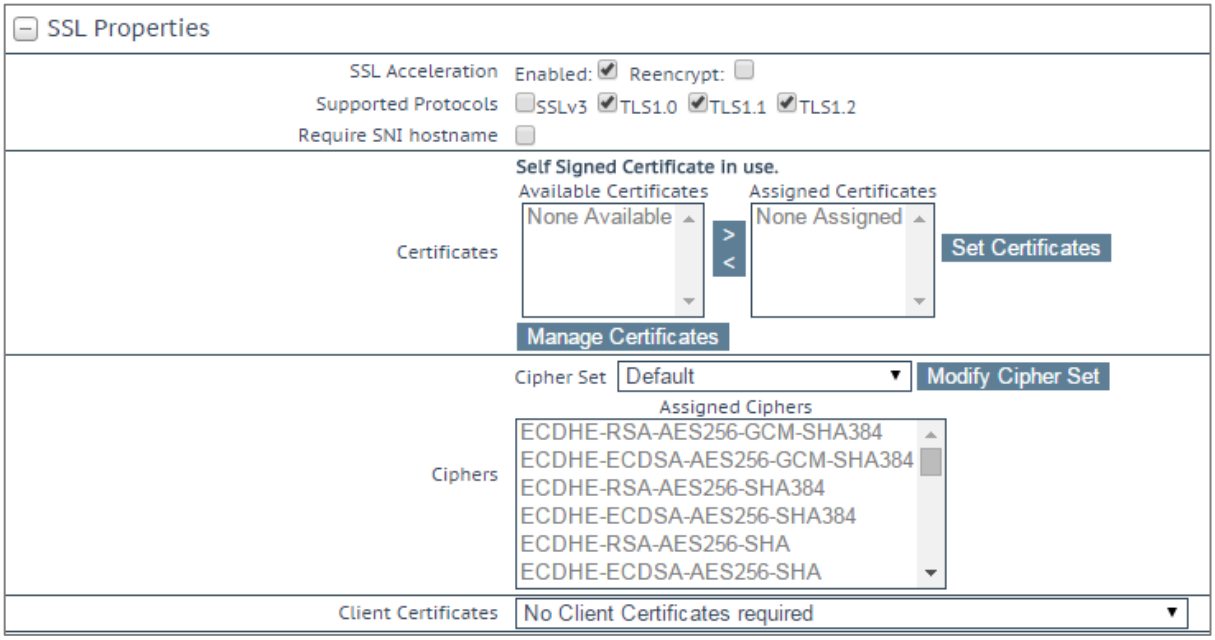

図 3-7:SSL プロパティのセクション

SSL Acceleration（SSL アクセラレーション）

このチェックボックスは、SSL アクセラレーションの基準が満たされていると、SSL アクセラレーションを有効にするために表示されます。

Enabled（有効）:"Enabled"チェックボックスがオンのときに、仮想サービスの証明書が存在しない場合、証明書のインストールを促すメッセージが表示されます。 **"Manage Certificates"**ボタンをクリックして証明書をインポートまたは追加すると、証明書を追加できます。

Reencrypt（再暗号化）:"Reencrypt"チェックボックスをオンにすると、SSL データストリームが実サーバーに送信される前に再暗号化されます。

Reversed（逆方向）:このチェックボックスをオンにすると、ロードマスターから実サーバーへのデータが再暗号化されます。入力ストリームは暗号化する必要がありません。この機能が役に立つのは、SSL トラフィックを復号する個別の仮想サービスとの接続で、この仮想サービスを実サービスとして使用して、データをループバックする場合に限定されます。この方法では、クライアントから実サーバーへのデータパスは送信中、常に暗号化されます。

Supported Protocols（サポートするプロトコル）

"Supported Protocols"（サポートするプロトコル）セクションにあるチェックボックスを使用すると、仮想サービスでサポートされるプロトコルを指定することができます。

デフォルトでは、3 つの TLS プロトコルが有効になっており、SSLv3 が無効になっています。

Require SNI hostname（SNI ホスト名必要）

サーバーネームインディケーション（SNI）が必要な設定を選択した場合、TLS クライアントが送信する Hello メッセージにホスト名を必ず含める必要があります。

"Require SNI hostname"を無効にすると、一致するホストヘッダーが見つからなかった場合に最初の証明書が使用されます。

"Require SNI hostname"を有効にすると、コモンネームが一致する証明書が必要となります。該当する証明書が見つからなかった場合はエラーが発生します。SNI ではワイルドカード証明書もサポートされています。

Subject Alternative Name（SAN）証明書を使用した場合、代替ソース名とホストヘッダーとの照合は行われません。

ワイルドカード証明書をサポートしていますが、ルートドメイン名は RFC 2459 のとおりに照合されません。ドットの左側の部分のみ照合されます。ルートドメイン名を照合するには、別途証明書を追加する必要があります。例えば、www.kemptechnologies.com は、*.kemptechnologies.com のワイルドカードの部分まで照合されます。kemptechnologies.com は照合されません。

HTTPS のヘルスチェックにて SNI ホスト情報を送信するには、該当する仮想サービスの**"Real Servers"**セクションにある**"Use HTTP/1.1"**を有効にし、ホストヘッダーを指定してください。この設定を行わない場合、実サーバーの IP アドレスが使用されます。

Certificates（証明書）

左側の**"Available Certificates"**選択リストに、利用可能な証明書が表示されます。証明書の割り当てまたは割り当て解除を行うには、目的の証明書を選択して左右の矢印ボタンをクリックし、**"Set Certificates"**をクリックします。次に、**"Set Certificates"**をクリックします。キーボードの **Ctrl** を押しながら必要な証明書をクリックすると、複数の証明書を選択できます。

"Manage Certificates"ボタンをクリックすると、**セクション 9.1** で説明している画面に移動します。

Reencryption Client Certificate（クライアント証明書の再暗号化）

SSL 接続を行った場合、ロードマスターはクライアントから証明書を取得し、サーバーからも証明書を取得します。ロードマスターは、クライアント証明書をヘッダーに転記し、そのデータをサーバーに送信します。このとき、サーバーはさらに証明書が送信されることを期待します。そのため、認証済みの証明書をロードマスターにインストールすることを推奨します。

Reencryption SNI Hostname（SNI ホスト名の再暗号化）

実サーバーに接続するときに使用するサーバーネームインジケーション（SNI）ホスト名を指定します。

このフィールドは SSL の再暗号化が有効な場合のみ表示されます。

Cipher Set（暗号セット）

暗号化方式とは、暗号化/復号化を行うアルゴリズムのことです。

各仮想サービス（**"SSL Acceleration"（SSL アクセラレーション）**が有効になっている仮想サービス）には、暗号セットが割り当てられています。暗号化セットには、システム定義の暗号セット、またはカスタム暗号セットのいずれかを使用できます。システム定義の暗号セットを使用すると、暗号セットを素早く簡単に選択でき、目的の暗号を素早く簡単に適用できます。カスタム暗号セットの作成と編集を行うには、**"Modify Cipher Set"**をクリックします。

デフォルトの暗号セットの説明、およびカスタム暗号セットの設定方法については、**セクション 9.5** を参照してください。

暗号

"Ciphers"リストは読み取り専用です。このリストには、現在割り当てられている暗号の一覧が表示されます。**"Modify Cipher Set"**ボタンをクリックすると、**"Cipher Set Management"**画面が表示されます。この画面では、カスタム暗号セットの新規作成、および既存のカスタム暗号セットの編集を行うことができます。詳細は**セクション 9.5** を参照してください。

Client Certificates（クライアント証明書）

- **No Client Certificates required（クライアント証明書不要）**：有効にすることにより、全クライアントからの HTTPS リクエストを受け入れるようにします。これは、デフォルトで推奨オプションです。

デフォルトでは、ロードマスターはすべてのクライアントからの HTTPS リクエストを受け入れます。以下のいずれかの値を選択した場合、すべてのクライアントは有効なクライアント証明書を提示する必要があります。またロードマスターは、証明書に関する情報をアプリケーションに渡すこともできます。

このオプションは、一般的にデフォルトの**"No Client Certificates required"（クライアント証明書不要）**から変更する必要はありません。このサービスにアクセスするすべてのクライアントが有効なクライアント証明書を持っているのを確認できた場合のみ、デフォルトを任意のオプションに変更してください。

- **Client Certificates required（クライアント証明書必要）**:すべてのクライアントは、HTTPS アクセスに対して有効なクライアント証明書を提示する必要があります。
- **Client Certificates and add Headers（クライアント証明書 と追加ヘッダー）**：すべてのクライアントは、HTTPS アクセスに対して有効なクライアント証明書を提示する必要があります。ロードマスターは 、ヘッダーを追加することによって、このクライアント証明書情報を転送します。追加するヘッダーの詳細については、**コンテンツルール機能説明**を参照してください。
- 以下のオプションを選択すると、証明書はオリジナルのまま無加工の状態で送信されます。各種オプションを選択して、証明書の送信形式を指定できます。
  - **Client Certificates and pass DER through as SSL-CLIENT-CERT（SSL-CLIENT-CERT としてクライアント証明書に DER を適用）**
  - **Client Certificates and pass DER through as X-CLIENT-CERT（X-CLIENT-CERT としてクライアント証明書に DER を適用）**
  - **Client Certificates and pass PEM through as SSL-CLIENT-CERT（SSL-CLIENT-CERT としてクライアント証明書に PEM を適用）**
  - **Client Certificates and pass PEM through as X-CLIENT-CERT（X-CLIENT-CERT としてクライアント証明書に PEM を適用）**

Verify Client using OCSP（OCSP によるクライアントの検証）

（オンライン証明書ステータスプロトコル（OCSP）を使用して）クライアントの証明書が有効かどうかを検証します。

このオプションは ESP が有効な場合のみ表示されます。

3.6Advanced Properties（高度なプロパティ）

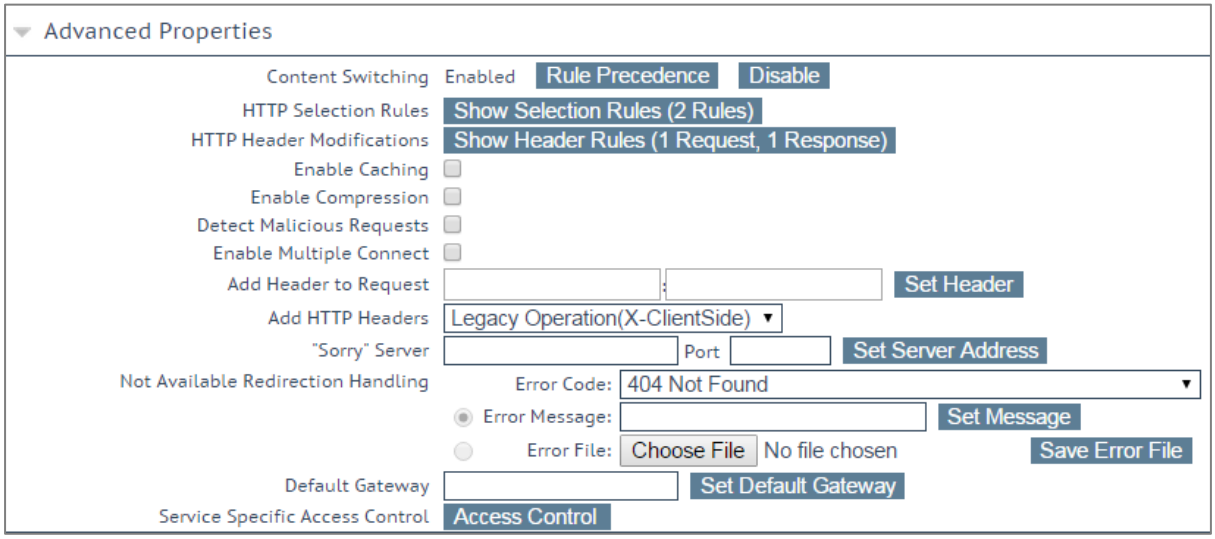

図 3-8:Advanced Properties セクション

Content Switching（コンテンツスイッチ）

"Enable"ボタンをクリックすると、この仮想サービスでルールベースのコンテンツスイッチ機能が有効になります。有効にした場合、該当する実サーバーにルールを割り当てる必要があります。ルールを実サーバーに割り当てるには、実サーバーの隣にある**"None"**ボタンをクリックします。ルールが実サーバーに割り当てられると、割り当てられたルールのカウントが表示されます。

Rules Precedence（ルールの優先順位）

“Rules Precedence”ボタンをクリックすると、コンテントスイッチ用ルールが適用されます。このオプションは、コンテンツスイッチが有効になっており、実サーバーにルールが割り当てられている場合のみ表示されます。

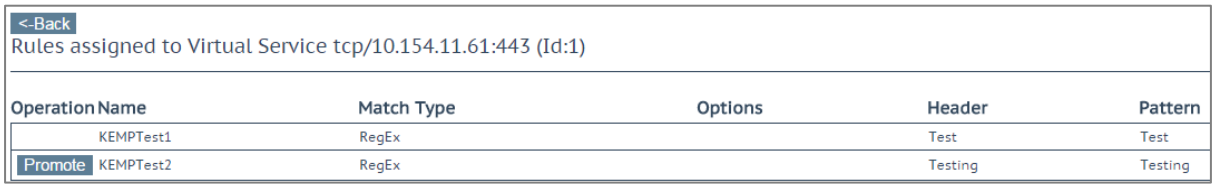

図 3-9:要求ルール

この画面には、仮想サービスの実サーバーに割り当てられたコンテントスイッチ用ルールが表示されます（ルールが適用された順に表示）。ルールの優先順位を上げるには、各ルールの**"Promote"**ボタンをクリックします。

HTTP Selection Rules（HTTP 選択ルール）

仮想サービスに割り当てられている選択ルールを表示します。

HTTP Header Modifications （HTTP ヘッダーの変更）

"Show Header Rules"（ヘッダールールの表示）ボタンをクリックすると、ヘッダー編集ルールが実装されている順序が表示されます。ルールの数（リクエストタイプおよびレスポンスタイプのルールの数）が実際のボタンに表示されます。

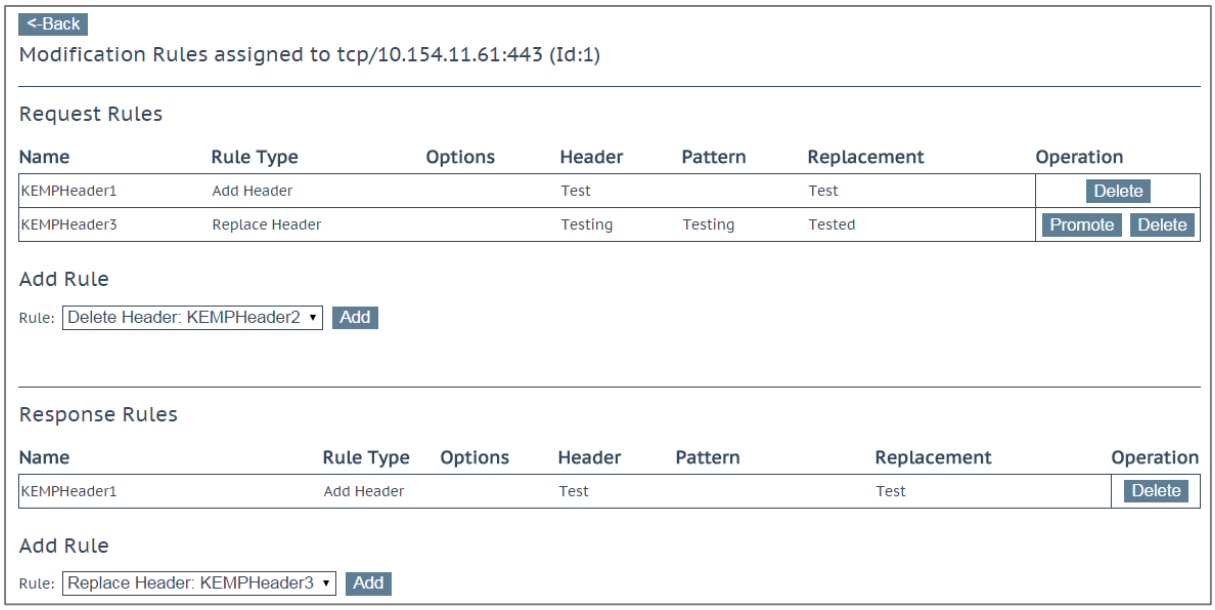

図 3-10:変更ルール

この画面では、ヘッダー変更ルールを**追加/削除**できます。ルールの適用順序を変更するには、**“Promote”**ボタンをクリックします。

Enable Caching（キャッシング有効化）

このオプションを使用すると、静的コンテンツをキャッシングできます。これにより、貴重な実サーバー処理パワーと帯域幅が節約されます。キャッシングは、HTTP、もしくはオフロード用 HTTPS 仮想サービスごとに有効にできます。

キャッシング可能なファイルの種類は、**"Systems Configuration > Miscellaneous Options"**メニューの AFE 設定で定義できます。

Maximum Cache Usage（最大使用キャッシュ）

このオプションは、仮想サービスごとのキャッシュメモリのサイズを制限します。例えば、2 つの仮想サービスに 50%ずつを割り当てているならば、システム全体のキャッシュ用メモリーは、この 2 つの仮想サービスだけですべてを使用します。デフォルトは **“制限なし”**です。しかしながら、キャッシュメモリの不平等な使用を防ぐために、各仮想サービスごとにキャッシュサイズを制限することをお勧めします。 キャッシュの最大使用量は、各仮想サービスで使用するキャッシュ割り当てのトータル値が 100%を超えないようにしてください。キャッシュに割り当てる残りのメモリースペースがない場合、仮想サービスのキャッシュを有効にしても、そのサービスはコンテンツをキャッシュしません。

Enable Compression（圧縮の有効化）

ロードマスターから送られたファイルは Gzip で圧縮されます。

> 圧縮がキャッシュなしで有効になっている場合は、ロードマスターのパフォーマンスが低下する可能性があります。仮想サービスにて圧縮とキャッシングが有効になっている場合、キャッシュされたエントリに対してのみ圧縮が適用されます（エントリがキャッシュされる場合）。最初の要求は圧縮されません。これはキャッシュを充填するのに使用されます。システムは、キャッシュの充填または要求の圧縮のいずれかのみ実行できます。これらを同時に行うことはできません。

圧縮可能なファイルの種類は、ロードマスターの WUI の**"Systems Configuration > Miscellaneous"**セクションの AFE 設定で定義できます。

> 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。
>
> より大きなファイルを圧縮するには、ハイパーバイザーを介して仮想ロードマスターにより多くの RAM を追加する必要があります。

Detect Malicious Requests（IDS 機能の追加）

侵入防御システム（IPS）サービスは、攻撃に対してリアルタイムに攻撃を緩和し、実サーバーの分離を行うことで、実サーバーのインライン保護を提供します。検出には米国 Snort 社の Snort データベースを使用しています。悪意のあるパケットは Reject、もしくは Drop を指定できます。また、これらのパケットの検出をリアルタイムにログに出力する事も可能です。

ルールの更新やカスタマイズを行うには、SNORT の Web サイト（https://www.snort.org/）を参照してください。https://www.snort.org/.

"Detect Malicious Requests"チェックボックスをオンにすると、HTTP およびオフロードされた HTTPS 仮想サービスごとに IPS が有効になります。“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。すなわち、**"Drop Connection"**（一致するルールにより HTTP レスポンスは生成されない）、または**"Send Reject"**（一致するルールによりクライアントへの HTTP 400 "Invalid Request"応答が生成される）のいずれかを選択できます。どちらのオプションを選択した場合も、リクエストは実サーバーに到達しません。

Enable Multiple Connect（複数の接続を有効にする）

このオプションを有効にすると、ロードマスターと実サーバーとの間の接続処理をロードマスターで管理できるようになります。複数のクライアントからのリクエストは、同じ TCP 接続を介して送信されます。

マルチプレクシングは単純な HTTP GET 操作でのみ機能します。**"Enable Multiple Connect"**チェックボックスは、WAF、ESP、SSL アクセラレーションが有効になっている場合など、一部の状況では利用できません。

Port Following（ポートフォローウィング）

ポートフォローウィングは、HTTP／HTTPS から HTTPS（SSL）／HTTP 接続へスイッチする時に、同じ実サーバーへの接続維持（パーシステンス）を提供します。ポートフォローウィングは、UDP 接続と TCP 接続との間で可能です。

ポートフォローウィングを有効にするには、以下の条件が成立している必要があります。

- ポートフォローウィングを有効にする仮想サービスは、HTTPS サービスでなければならない
- HTTP サービスが存在していなければならない
- これらの仮想サービスは、いずれも同じ L7 レイヤーのパーシステンスモード（**Super HTTP パーシステンス**または **Source IP Address パーシステンス**）が選択されていなければならない。

サブ VS 上ではポートフォローウィングは利用できません。

詳細については、**SSL アクセラレーションサービス　機能説明**を参照してください。

Add Header to Request（リクエストにヘッダーを追加）

実サーバーに送信されるすべてのリクエストに挿入する追加ヘッダーのキーと値を入力します。

この機能を使用するには、**“Set Header”**ボタンをクリックします。

Add HTTP Headers（HTTP ヘッダーの追加）

> **"Add HTTP Headers"** ドロップダウンリストは、SSL オフローディング（**SSL アクセラレーション**）が有効になっているときのみ利用できます。

HTTP ストリームに追加するヘッダーを選択できます。以下のオプションの利用が可能です。

- **Legacy Operation(X)（従来の操作（X））**
- **None（なし）**
- **X-Forwarded-For (+ Via)X-Forwarded-For (No Via)（X-フォワーディングされる（Via あり）X-フォワーディングされる（Via なし））**
- **X-ClientSide（X-クライアントサイド（Via あり））**
- **X-ClientSide（X-クライアントサイド（Via なし））**
- **Via Only（Via のみ）**

レガシー動作では、システムが HTTP カーネルモードで動作しているときにヘッダーが追加されます（それ以外の場合は何も行われません）。それ以外の場合は何も行いません。他の動作方式の場合、システムが強制的に HTTP カーネルモードになってから、指定した動作が行われます。

Sorry Server（Sorry サーバー）

該当するフィールドに IP アドレスとポート番号を入力します。ロードマスターは、利用可能な実サーバーがない場合、何もチェックを行わずに指定した場所にリダイレクトします。Sorry サーバーの IP アドレスは、ロードマスターで定義されているネットワーク上またはサブネット上になければなりません。

> レイヤ 4 仮想サービスを使用する場合、Sorry サーバーは実サーバーと同じサブネット上に存在する必要があります。

レイヤ 7 仮想サービスを使用する場合、Sorry サーバーは任意のローカルネットワークに置くことができます。また、ローカルネットワーク上にない Sorry サーバーも追加できます。ローカルネットワーク上にない Sorry サーバーを追加するには、**"Transparency"**を無効にする必要があります。また、Sorry サーバーへの経路が存在し、**"Enable Non-Local Real Servers"**オプションが有効になっている必要があります（**"System Configuration" > "Miscellaneous Options" > "Network Options"**）。

SSL 再暗号化を使用している場合、**Sorry サーバー**機能は正しく動作しません。

Not Available Redirection Handling（利用不可時のリダイレクション処理）

要求を処理するための実サーバーが利用できない場合に、クライアントが受信すべきエラーコードと URL を定義できます。

- **Error Code（エラーコード）**:実サーバーが利用できない場合、ロードマスターは HTTP エラーコードに従って接続を終端できます。適切なエラーコードを選択してください。
- **Redirect URL（リダイレクトする URL）**:実サーバーが利用できず、クライアントにエラーレスポンスを返す必要がある場合、リダイレクトする URL を指定できます。このテキストボックスに文字列を入力する場合、**http://**または **https://**を含めないでください。or **https://**この文字列は現在の場所からの相対位置として扱われます。そのため、リダイレクト時にホスト名がこの文字列に追加されます。このフィールドでは、要求されたホスト名を表す**"%h"**や、ユニフォームリソースアイデンティファイヤー（URI）を表す**"%s"**などのワイルドカードも使用できます。
- **Error Message（エラーメッセージ）**:実サーバーが利用できない場合に、エラーレスポンスをクライアントに返すとき、指定したエラーメッセージがそのレスポンスに追加されます。

  セキュリティ上の理由から、**"Document has moved"**の文字だけを含む HTML ページが返送されます（要求に含まれる情報は返送されません）。要求により提供された情報は返されません。
- **Error File（エラーファイル）**:実サーバーが利用できない場合に、エラーレスポンスをクライアントに返すとき、指定したファイルがそのレスポンスに追加されます。これにより、指定したエラーに対するレスポンスとして、簡単なエラー情報を含む HTML ページを送信できます。

  エラーページの最大サイズは 16KB です。

Not Available Server/Port（利用不可時のサーバー/ポート）

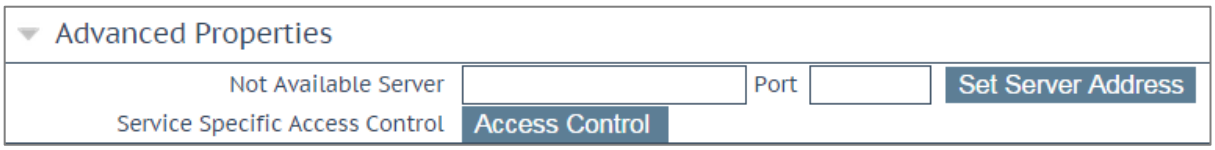

図 3-11:Not Available Server（利用不可時のサーバー）

UDP の仮想サービスでは、**Not Available Server（利用不可時のサーバー）**と **Port（ポート）**を指定できます。このオプションは、要求を処理可能な実サーバーが存在しないときにクライアントが受信する URL を設定します。

> UDP の **Not Available Server** の値は、サービスが **Not Available Server** を使用していない場合のみ変更できます。

Add a Port 80 Redirector VS（ポート 80 リダイレクター仮想サービスの追加）

ポート 80 仮想サービスが設定されていない場合、その作成が行えます。このサービスを作成すると、**“Redirection URL:”**フィールドで指定した URL にクライアントがリダイレクトされます。 field.

このリダイレクターを使用するには、**“Add HTTP Redirector”**ボタンをクリックします。

> **"Add HTTP Redirector"**ボタンをクリックすると、リダイレクター仮想サービスが作成され、関連する仮想サービスからこの WUI オプションが表示されなくなります。

Default Gateway（デフォルト・ゲートウェイ）

クライアントにレスポンスを返信するための仮想サービス固有のゲートウェイを指定します。デフォルトゲートウェイが設定されていない場合、グローバルのデフォルトゲートウェイが使用されます。

デフォルト・ゲートウェイを使用するには、**“Set Default Gateway”**ボタンをクリックします。仮想サービスの**デフォルトゲートウェイ**は、その仮想サービスでのみ使用されます。

> **"System Configuration > Miscellaneous Options > Network Options"**にてグローバルの**"Use Default Route Only"（デフォルトルートのみ使用）**オプションが設定されている場合、**"Default Gateway"（デフォルトゲートウェイ）**が設定されている仮想サービスからのトラフィック

のみ、仮想サービスのデフォルトルートが設定されているインターフェイスに転送されます。これにより、隣接するインターフェイスを使用してトラフィックを直接返送することなく、ロードマスターをクライアントネットワークに直接接続できます。

Alternate Source Addresses（代替ソースアドレス）

アドレスのリストが指定されていない場合、ロードマスターは仮想サービスの IP アドレスをローカルアドレスとして使用します。アドレスのリストを指定すると、ロードマスターはそのリストのアドレスを使用します。

代替ソースアドレスを使用するには、**“Set Alternate Source Addresses”**ボタンをクリックします。

このオプションは、**“L7 Configuration”**画面の**“Allow connection scaling over 64K Connections”**オプションが有効になっている場合のみ利用可能です。

Service Specific Access Control（サービス固有のアクセス・コントロール）

仮想サービス固有のアクセス・コントロール・リストを変更できます。

"Access Control Lists"オプションが有効になっている場合、"Extra Ports"オプションは正しく機能しません。

3.7ウェブアプリケーションファイアウォール（WAF）のオプション

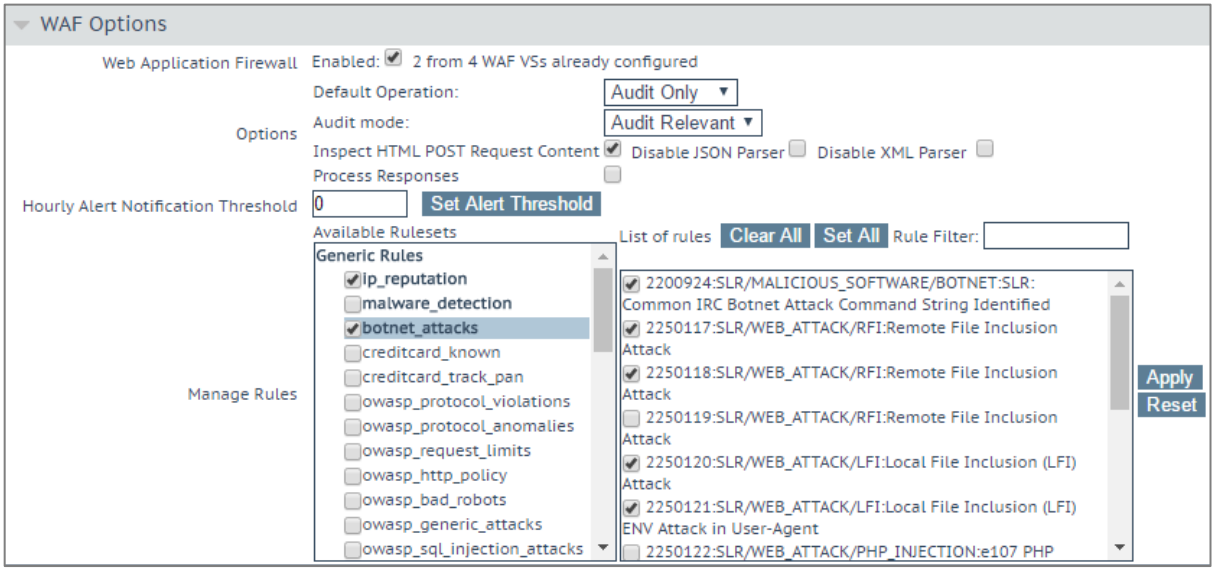

図 3-12:WAF のオプション

これらのオプションを設定する前に、WAF 機能を有効にする必要があります。

図 3-13:WAF の有効化

WAF を有効にするには、**"Enabled"**チェックボックスをオンにします。すると、**"Enabled"**チェックボックスの隣に、WAF が有効な仮想サービスがいくつ存在するかと、WAF が有効な仮想サービスが最大いくつまで存在できるかを示すメッセージが表示されます。WAF が有効な仮想サービスが最大数に達すると、**"Enabled"**チェックボックスがグレー表示になります。

WAF を使用すると、ロードマスターの構成においてパフォーマンスが大きく影響を受けます。適切なリソースが割り当てられていることを確認してください。

仮想およびベアメタル型のロードマスターインスタンスの場合、AFP を動作させるには 2GB 以上の RAM を割り当てる必要があります。バージョン 7.1-22 以前のロードマスターの OS では、仮想およびベアメタル型のロードマスターインスタンスのデフォルトのメモリ割り当ては 1GB となっています。このデフォルトの割り当てを変更して

いない場合は、AFP の設定を行う前に、メモリの設定を変更してください。

Default Operation（デフォルト動作）

WAF のデフォルト動作を選択します。

- **Audit Only（監査のみ）**:監査専用モード – ログが作成されますが、リクエストや応答はブロックされません。
- **Block Mode（ブロックモード）**:リクエストや応答がブロックされます。

Audit mode（監査モード）

どのログを記録するかを選択します。

- **No Audit（監査なし）**:データは記録されません。
- **Audit Relevant（該当するものを監査）**:警告レベル以上のデータを記録します。これは、この設定のデフォルトオプションです。
- **Audit All（すべて監査）**:仮想サービス経由のすべてのデータを記録します。

"Audit All"を選択すると、大量のログデータが作成されます。通常動作に対して**"Audit All"**を選択することは推奨しません。ただし、特定の問題を解決する場合は**"Audit All"**が役に立ちます。

Inspect HTML POST Request Content（HTML POST 要求の内容を検査する）

このオプションを有効にすると、POST リスエストで与えらえたデータも処理されます。

2 つの追加オプション（**"Disable JSON Parser"**および**"Disable XML Parser"**）は、**"Inspect HTML Post Request Content"**が有効な場合のみ利用できます。

Disable JSON Parser（JSON パーサーを無効にする）

Java スクリプトオブジェクト表記法（JSON）リクエストの処理を無効にします。

Disable XML Parser（XML パーサーを無効にする）

XML リクエストの処理を無効にします。

Process Responses（応答を処理する）

このオプションを有効にすると、実サーバーからの応答が検証されます。

このオプションは CPU とメモリを著しく消費します。

実サーバーが gzip エンコーディングの場合、**"Process Responses"**が有効であっても WAF はそのトラフィックをチェックしません。

Hourly Alert Notification Threshold（1 時間当たりのアラート通知しきい値）

アラートが送信されるまでの 1 時間当たりのインシデントのしきい値です。**0** を設定するとアラートが無効になります。このしきい値は、WUI ホームページに表示される **"Events over Limit Today"**の値にも関連しています。例えば、しきい値が 10 に設定されており、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。

Rules（ルール）

カスタム、アプリケーション固有、アプリケーション汎用、汎用のルールを、仮想サービスに割り当てる（または仮想サービスから解除する）ことができます。

アプリケーション固有またはアプリケーション汎用のルールを同じ仮想サービスに割り当てることはできません。

必要に応じて、各ルールセット内の個々のルールを有効/無効にできます。ルールセットを有効にするには、目的のチェックボックスをオンにします。過去にルールセットを有効/無効にしたことがない場合、デフォルトで右側のボックスにあるすべてのルールが有効になっています。その仮想サービスにおいて過去にルールセットを有効/無効にしたことがある場合、ルールは前回の設定が維持されています。

左側にある目的のルールセットのチェックをオンにし、右側にあるルールのチェックをオン/オフすることで、必要に応じて個々のルールを有効/無効にできます。

ルールまたはルールセットによっては、他のルールと依存関係にある場合があります。ロードマスターは、ルールを無効にしたときに依存関係のチェックは行いません。ルールを無効にする前に、ルールの連鎖または依存関係に注意してください。

変更が完了したら、**"Apply"**ボタンをクリックします。

"Clear All"ボタンをクリックすると、選択したすべてのルールが無効になります。

"Set All"ボタンをクリックすると、選択したすべてのルールが有効になります。

"Rule Filter"テキストボックスにテキストを入力すると、フィルターで抽出したいテキストを含むルールのみ表示できます。

"Reset"をクリックすると、ルールとルールセットがすべて無効になります。

3.8エッジセキュリティパック（ESP）のオプション

各オプションを設定する前に、ESP 機能を有効にする必要があります。ESP 機能を有効にするには、**"Enable ESP"**チェックボックスをオンにします。

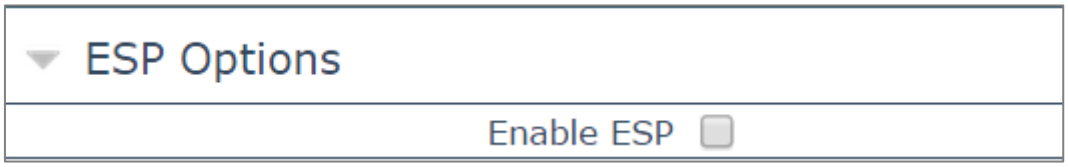

図 3-14:SP オプションの選択

すると、**“ESP Options”**画面が表示され、ESP のすべてのオプションが表示されます。

ESP 機能は、仮想サービスが HTTP、HTTPS、SMTP の仮想サービスである場合のみ有効にできます。

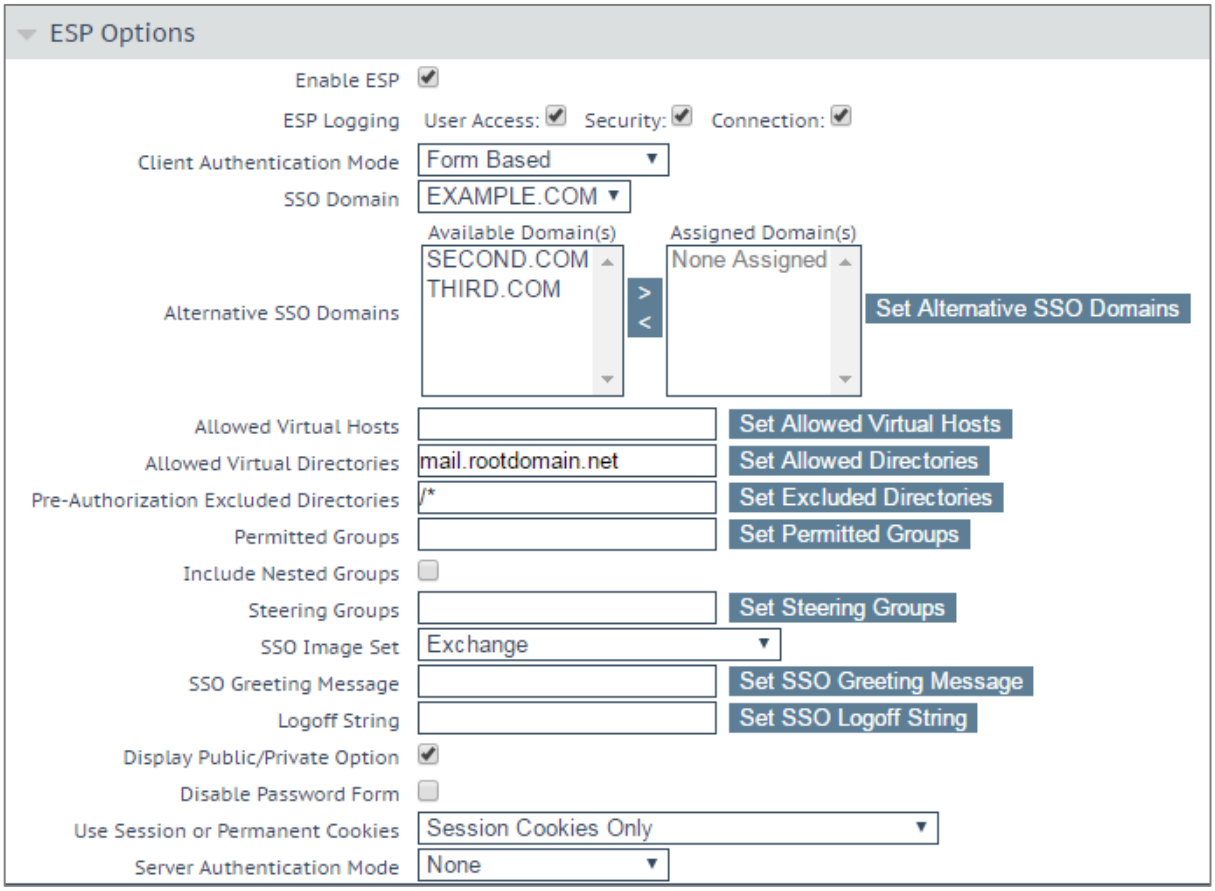

図 3-15:ESP オプション

Enable ESP（ESP の有効化）

ESP 機能を有効/無効にするには、**"Enable ESP"**チェックボックスをオン/オフにします。

ESP Logging（ESP のログ作成）

ESP 機能に関して 3 種類のログが記録されます。チェックボックスをオン/オフすることで、それぞれのログを有効/無効にできます。以下のログが記録されます。

- **User Access（ユーザーアクセス）**:全ユーザーのログイン情報を記録
- **Security（セキュリティ）**: すべてのセキュリティ警告を記録
- **Connection（接続）**:各接続状態を記録

ログは永久保存が可能で、ロードマスターのリブート後もアクセスできます。ログの詳細については、 **セクション 10.4.2** を参照してください。

Client Authentication Mode（クライアント認証モード）

ロードマスターに接続を試みるクライアントをどのように認証するかを指定します。以下に示すタイプの方法が利用可能です。

- **Delegate to Server:** 認証はサーバーに委任される
- **Basic Authentication:** 標準の基本認証を使用
- **フォームベース**クライアントは、ロードマスターで認証を受けるためのユーザー情報をフォームに入力する必要がある
- **Client Certificates（クライアント証明書）**クライアントは、発行機関で証明された証明書を提出する必要がある
- **NTLM:**NTLM 証明書は、対話形式のログオン処理で得られたデータに基づき作成され、ドメイン名とユーザー名が含まれます。

"ESP Options"セクションの残りのフィールドは、選択された**"Client Authentication Mode"**に基づき変更されます。

SSO Domain（SSO ドメイン）

仮想サービスが属するシングルサインオン（SSO）ドメインを選択します。

SSO ドメインの設定方法についての詳細は、**セクション 3.13** を参照してください。ESP 機能を正しく設定するには、SSO ドメインを設定する必要があります。

"Configuration type"で**"Inbound Configuration"**が設定された SSO ドメインのみ、この**"SSO Domain"**フィールドにオプションとして表示されます。

Alternative SSO Domains（代替 SSO ドメイン）

多くの組織では、顧客やパートナーと情報を共有するため、エクストラネットを使用しています。エクストラネットのポータルは、複数のアクティブディレクトリドメインからのユーザーを持つ可能性があります。個々のドメインからのユーザーを同時に認証するのではなく、**"Alternative SSO Domains"（代替 SSO ドメイン）**を割り当てることで、1 つの仮想サービスを使用して複数のドメインからのユーザーを同時に認証できます。

このオプションは、複数のドメインが設定されており、SSO ドメインの**"Authentication Protocol "**が**"LDAP"**に設定されている場合のみ表示されます。

SSO ドメインの設定方法についての詳細は、**セクション 3.13** を参照してください。

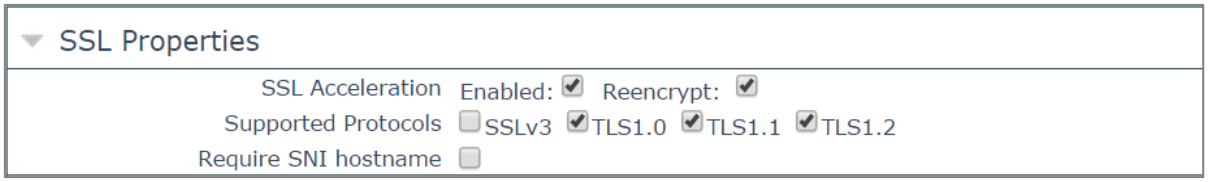

図 3-16:"Enabled"および"Reencrypt"チェックボックスが選択された様子

"Alternative SSO Domains"（代替 SSO ドメイン）を使用するため、**"SSL Properties"**セクションにて**"ESP Options"（ESP オプション）**を設定する前に、**"Enabled"（有効）**および**"Reencrypt"（再暗号化）**のチェックボックスがオンになっていることを確認してください。

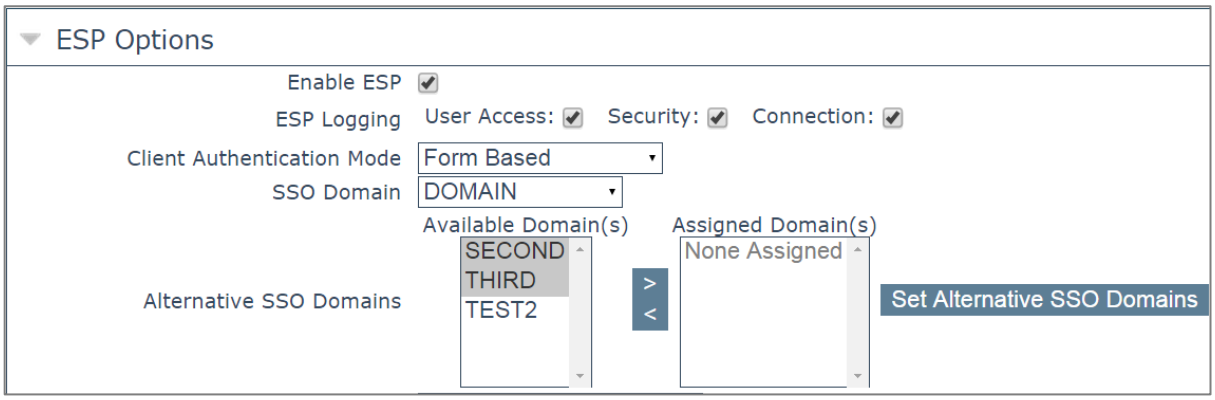

図 3-17:利用可能なドメイン

"SSO Domain"（SSO ドメイン）ドロップダウンリストに表示されるドメイン名は、デフォルトドメインの名前です。またこれは、ドメインが 1 つだけ設定されている場合に使用されるドメインです。

以前に設定したドメインは、**"Available Domain(s)"（利用可能なドメイン）**リストに表示されます。

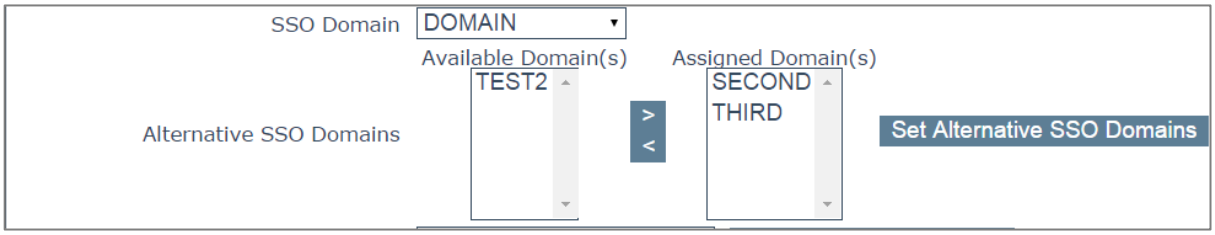

図 3-18:仮想サービスに割り当てられた代替ドメイン（2 次および 3 次ドメイン）

代替ドメインを割り当てるには以下のようにします。

1. 割り当てたいドメインを反転表示させ、">"ボタンをクリックします。

割り当てられたドメインは、特定の仮想サービスを使用して認証できます。

利用可能なドメインとして表示されたドメインは、すべて仮想サービスに割り当てることができます。

2. **"Set Alternative SSO Domains"（代替 SSO ドメインを設定する）**ボタンをクリックし、割り当てられたドメインの最新のリストを確定します。
3. **"Server Authentication Mode"（サーバー認証モード）**ドロップダウンリストから **"Basic Authentication"（基本認証）**を選択します。

代替ドメインにアクセスする必要がある場合、ESP フォームを使用してドメインにログインする際に SSO ドメイン名を入力する必要があります。ユーザー名の欄にドメイン名を入力しない場合、通常、"Default SSO Domain"（デフォルト SSO ドメイン）ドロップダウンリストで選択したドメインにログオンされます。

仮想サービスの状態を見るには、メインメニューの**"Virtual Services"（仮想サービス）**をクリックし、**"View/Modify Services"（サービスの表示/編集）**をクリックします。

"Virtual Services"（仮想サービス）リストには、各サービスの現在の状態が表示されます。

代替ドメインが割り当てられており、特定のドメインに問題がある場合、影響を受けるドメイン名が**"Status"（ステータス）**列に表示されます。

Allowed Virtual Hosts（許可された仮想ホスト）

仮想サービスは、指定した仮想ホストにのみアクセスできます。指定されていない仮想ホストはブロックされます。

アクセスを許可する仮想ホストを指定するには、**“Allowed Virtual Hosts”**フィールドに仮想ホスト名を入力し、**“Set Allowed Virtual Hosts”**ボタンをクリックします。

このフィールドでは複数のドメインを指定できます。これにより、シングルサインオンドメインに複数のドメインを関連付けることができます。

このフィールドでは正規表現を使用できます。

このフィールドが空欄の場合、仮想サービスはブロックされます。

Allowed Virtual Directories（許可された仮想ディレクトリ）

仮想サービスは、アクセスが許可された仮想ホスト内の指定された仮想ディレクトリにのみアクセスできます（指定されていない仮想ディレクトリはブロックされます）。指定されていない仮想ディレクトリはブロックされます。

アクセスを許可する仮想ディレクトリを指定するには、**“Allowed Virtual Directories”**フィールドに仮想ディレクトリ名を入力し、**“Set Allowed Virtual Directories”**ボタンをクリックします。

このフィールドでは正規表現を使用できます。

Pre-Authorization Excluded Directories（事前認証対象外ディレクトリ）

このフィールドで指定した仮想ディレクトリは、この仮想サービスで事前認証されず、関連する実サーバーに直接渡されます。

Permitted Groups（許可グループ）

この仮想サービスへのアクセスを許可するグループを指定します。許可グループを設定した場合、この仮想サービスにより発行されたユーザーがログインするには、そのユーザーは指定したグループのいずれか 1 つ以上に属していなければなりません。1 つの仮想サービスにつき 10 個のグループまでサポートします。入力するグループ数が増えると、パフォーマンスに影響が出ます。このフィールドで入力したグループは、LDAP クエリにより有効になります。

このフィールドに関するガイドラインを以下に示します。

- 指定したグループは、仮想サービスに関連付けられた SSO ドメインのアクティブディレクトリで有効なグループでなければなりません。ロードマスターにおける SSO ドメインはこのグループのディレクトリに設定する必要があります。例えば、ロードマスターにおける SSO ドメインが webmail.example に設定されており、webmail がそのグループのディレクトリでない場合、正しく機能しません。この場合、SSO ドメインは.example.com に設定する必要があります。
- リスト入力するグループはセミコロンで区切る必要があります。

> 多くのグループ名はスペースを含むため（例: **"Domain Users"**）、スペースで区切られたリストは正しく機能しません。

- 許可グループ名には以下の文字は使用できません。
  / :+ *
- SSO ドメインの認証プロトコルは LDAP でなければなりません。
- グループは完全名ではなく名前で指定する必要があります。

Include Nested Groups（ネストされたグループを含める）

このフィールドは、**"Permitted Groups"**の設定と関係しています。認証の際にネストされたグループを含める場合は、このオプションを有効にします。このオプションを無効にすると、最上位レベルのグループに属するユーザーのみアクセスが許可されます。このオプションを有効にすると、最上位レベルおよび最初の下位レベルのグループに属するユーザーのアクセスが許可されます。

SSO Image Set（SSO の画像設定）

このオプションは、クライアント認証モードとして**“Form Based”**が選択されている場合のみ利用できます。Username と Password の入力に使用するフォームを選択できます。ここでは、**"Exchange"**、**"Blank"（ブランク）**、**"Dual Factor Authentication"（2 要素認証）**の 3 つのオプションが用意されています。フォームとエラーメッセージを他の言語で表示するオプションもあります。

- **Exchange フォーム**

図 3-19:Exchange フォーム

“Exchange Form”には KEMP のロゴが表示されます。

- **ブランクフォーム**

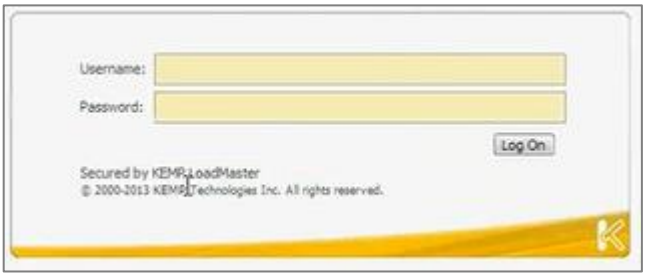

図 3-20:ブランクフォーム

“Blank Form”には KEMP のロゴは表示されません。

- **2 要素認証**

図 3-21:2 要素認証フォーム

"Dual Factor Authentication"（2 要素認証）フォームには、4 つのフィールドが用意されています。そのうち 2 つはリモート証明書に関するもので、他の 2 つは内部証明書に関するものです。

"Remote Credentials"（リモート証明書）は、アクティブディレクトリなどのドメインサーバーで認証する前に、RADIUS などのリモート認証サーバーで認証するための証明書です。

"Internal Credentials"（内部証明書）は、アクティブディレクトリなどの内部ドメインサーバーで認証するための証明書です。

関連する**"SSO Domain"（SSO ドメイン）**の**"Authentication Protocol"（認証プロトコル）**が**"RADIUS and LDAP"（RADIUS および LDAP）**に設定されている場合、**SSO Image Set（SSO の画像設定）**を**"Dual Factor Authentication"（2 要素認証）**に設定する必要があります。

SSO Greeting Message（SSO のあいさつメッセージ）

このオプションは、**クライアント認証モード**として**“Form Based”**が選択されている場合のみ利用できます。ログインフォームは、テキストを追加してさらにカスタマイズが行えます。ログインフォームにテキストを追加するには、**“SSO Greeting Message”**フィールドに表示したいテキストを入力し、**“Set SSO Greeting Message”**ボタンをクリックします。メッセージは最大 255 文字まで入力できます。

"SSO Greeting Message"フィールドには HTML コードを入力できるので、必要に応じて画像を挿入できます。

> アクサングラーブ（`）はサポートしていません。SSO のあいさつメッセージでこの文字を入力しても、出力には表示されません。例えば、**a`b`c** は **abc** となります。

Logoff String（ログオフ文字列）

このオプションは、**クライアント認証モード**として**“Form Based”**が選択されている場合のみ利用できます。通常、このフィールドは空白のままにしてください。OWA 仮想サービスの場合は、**"Logoff String"**を**"/owa/logoff.owa"**に設定してください。カスタマイズされた環境では、変更後のログオフ文字列をこのテキストボックスで指定してください。複数のログオフ文字列を入力するには、スペース区切りのリストを使用します。

> 照合される URL において、指定した文字列の前にサブディレクトリが含まれている場合、ログオフ文字列は照合されません。この場合、ロードマスターはユーザーをログオフしません。

Display Public/Private Option（パブリック/プライベート表示オプション）

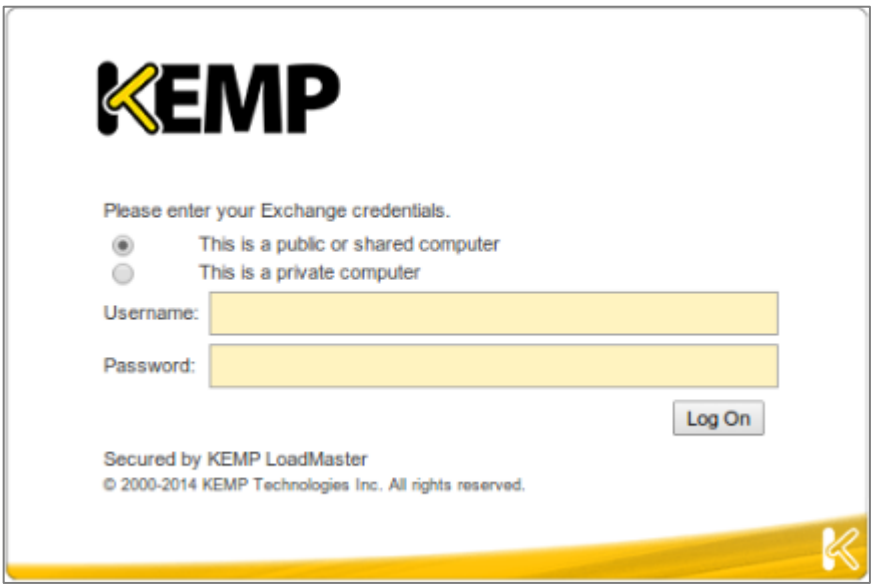

図 3-22:パブリック/プライベートオプション

このチェックボックスをオンにすると、ESP ログインページにパブリック/プライベートオプションが表示されます。**Session timeout** の値は、ログインフォームにてユーザーが選択したオプションに基づいて、**"Manage SSO Domain"**画面で指定したパブリック/プライベートの値に設定されます。ユーザーがプライベートを選択した場合、そのセッションにてユーザー名が保存されます。これらのフィールドの詳細については、**セクション 3.13** を参照してください。

Disable Password Form（パスワードフォームを無効にする）

このオプションを有効にすると、ログインページからパスワードフィールドが削除されます。このオプションは、RSA SecurID 認証のみを使用している場合など、パスワードの検証が不要な場合に必要となります。デフォルトでは、このオプションは無効になっています。

Use Session or Permanent Cookies（セッションクッキーまたはパーマネントクッキーを使う）

このフィールドでは 3 つのオプションを選択できます。

- **Session Cookies Only（セッションクッキーのみ使用）**:これはデフォルトの設定です。最も安全なオプションです。

- **Permanent Cookies only on Private Computers（プライベートコンピューターでのみパーマネントクッキーを使用）**:パブリックコンピューターにセッションクッキーを送信します。
- **Permanent Cookies Always（常にパーマネントクッキーを使用）**:すべての状況においてパーマネントクッキーを送信します。

ログイン時にユーザーのブラウザーにセッションクッキーまたはパーマネントクッキーを送信する必要がある場合は、このオプションを指定してください。

パーマネントクッキーは、複数のアプリケーションにわたるセッションを持つサービス（SharePoint など）にシングルサインオンする場合のみ使用してください。

Server Authentication Mode（サーバー認証モード）

このフィールドは、**"Client Authentication Mode"**が**"Form Based"**に設定されているときのみ更新できます。

実サーバーによりロードマスターがどのように認証されるかを指定します。3 種類の方法が利用可能です。

- **None:** クライアント認証は必要ない
- **Basic Authentication:** 標準の基本認証を使用
- **KCD:**KCD 認証を使用

"Client Authentication Mode"として**"Delegate to Server"**を選択した場合、**"Server Authentication mode"**として**"None"**が自動的に選択されます。同様に、**"Client Authentication Mode"**として**"Basic Authentication"**または**"Form Based"**を選択した場合、**"Server Authentication mode"**として**"Basic Authentication"**が自動的に選択されます。

Server Side configuration（サーバー側設定）

このオプションは、**"Server Authentication mode"**の値が**"KCD"**に設定されているときのみ表示されます。

サーバー側の設定を行うための SSO ドメインを選択します。**"Configuration type"**が**"Outbound Configuration"**に設定されている SSO ドメインのみここに表示されます。

3.8.1 SMTP Virtual Services and ESP（SMTP の仮想サービスと ESP）

SMTP 仮想サービス（ポート番号 **25**）を作成した場合、**“Enable ESP”**チェックボックスをオンにすれば ESP 機能を使用できます（ただし、利用可能なオプションは制限されます）。

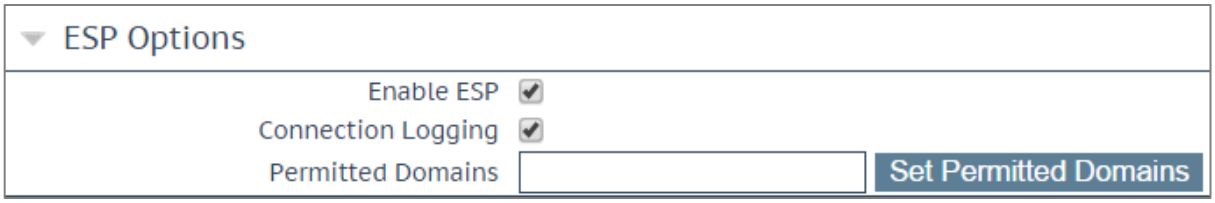

図 3-23:ESP オプション

Enable ESP（ESP の有効化）

ESP 機能を有効/無効にするには、**“Enable ESP”**チェックボックスをオン/オフにします。

Connection Logging（接続ログ）

“Connection Logging”チェックボックスをオン/オフすることで、接続ログを有効/無効にできます。

Permitted Domains（許可ドメイン）

この仮想サービスで受信を許可するすべてのドメインをここで指定します。例えば、仮想サービスにて john@kemp.com からの SMTP トラフィックを受信したい場合は、このフィールドで kemp.com のドメインを指定します。

3.9サブ仮想サービス

仮想サービス内に“サブ仮想サービス”（サブ VS）を作成できます。サブ VS は、親仮想サービスにリンクされ、親仮想サービスの 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。これにより、関連性のある仮想サービスを、同じ IP アドレスでグループ化することが可能となります。これは、Exchange や Lync のように、多くの仮想サービスからなる構成で有効です。

仮想サービスの権限を持つユーザーは、サブ VS を追加できます。

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。

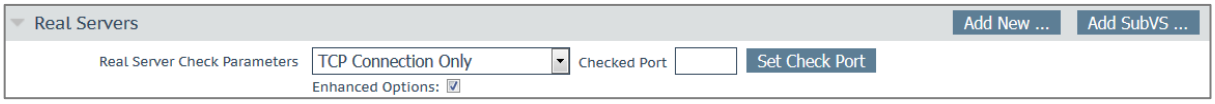

図 3-24:実サーバーのセクション

サブ VS を作成するには、仮想サービス設定画面にて**“Real Servers”**セクションを展開し、**“Add SubVS”**ボタンをクリックします。

図 3-25:SubVS の作成

すると、サブ VS が作成されたことを示すメッセージが表示されます。

実サーバーとサブ VS を同じ仮想サービスに関連付けることはできません。ただし、実サーバーをサブ VS に関連付けることは可能です。

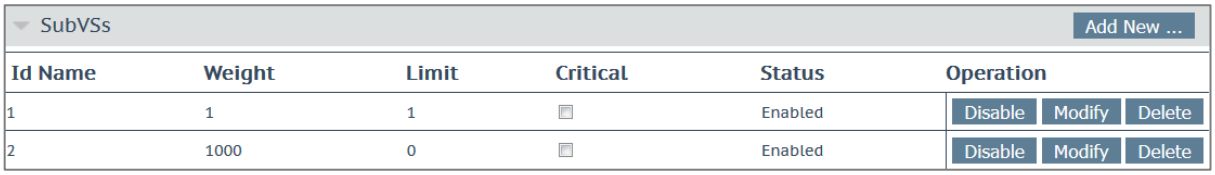

図 3-26:SubVS セクション

サブ VS を作成すると、仮想サービス設定画面の**“Real Servers”**セクションが**“SubVSs”**セクションに変わります。

仮想サービスのすべてのサブ VS が、ここにリスト表示されます。**"Critical"**チェックボックスをオンにすると、仮想サービスが利用可能であると認識されるためにはそのサブ VS が必要であることを示すことができます。重要でないサブ VS が停止しても、仮想サービスは稼働中と報告され、警告が記録されます。重要なサブ VS が停止した場合、重大なログが作成され、その仮想サービスは停止中とマークされます。E メールオプションが設定されている場合、関係する受信者に E メールが送信されます。E メールオプションの詳細については、**セクション 10.4.5** を参照してください。いかなる場合でも、仮想サービスが停止中であると認識され、その仮想サービスが Sorry サーバーを持っている（またはエラーメッセージが設定されている）場合、それらが使用されます。

サブ VS の設定を変更するには、該当するサブ VS の**“Modify”**ボタンをクリックします。すると、サブ VS の設定画面が表示されます。この画面には、通常の仮想サービスで利用可能な設定オプションの一部が表示されます。

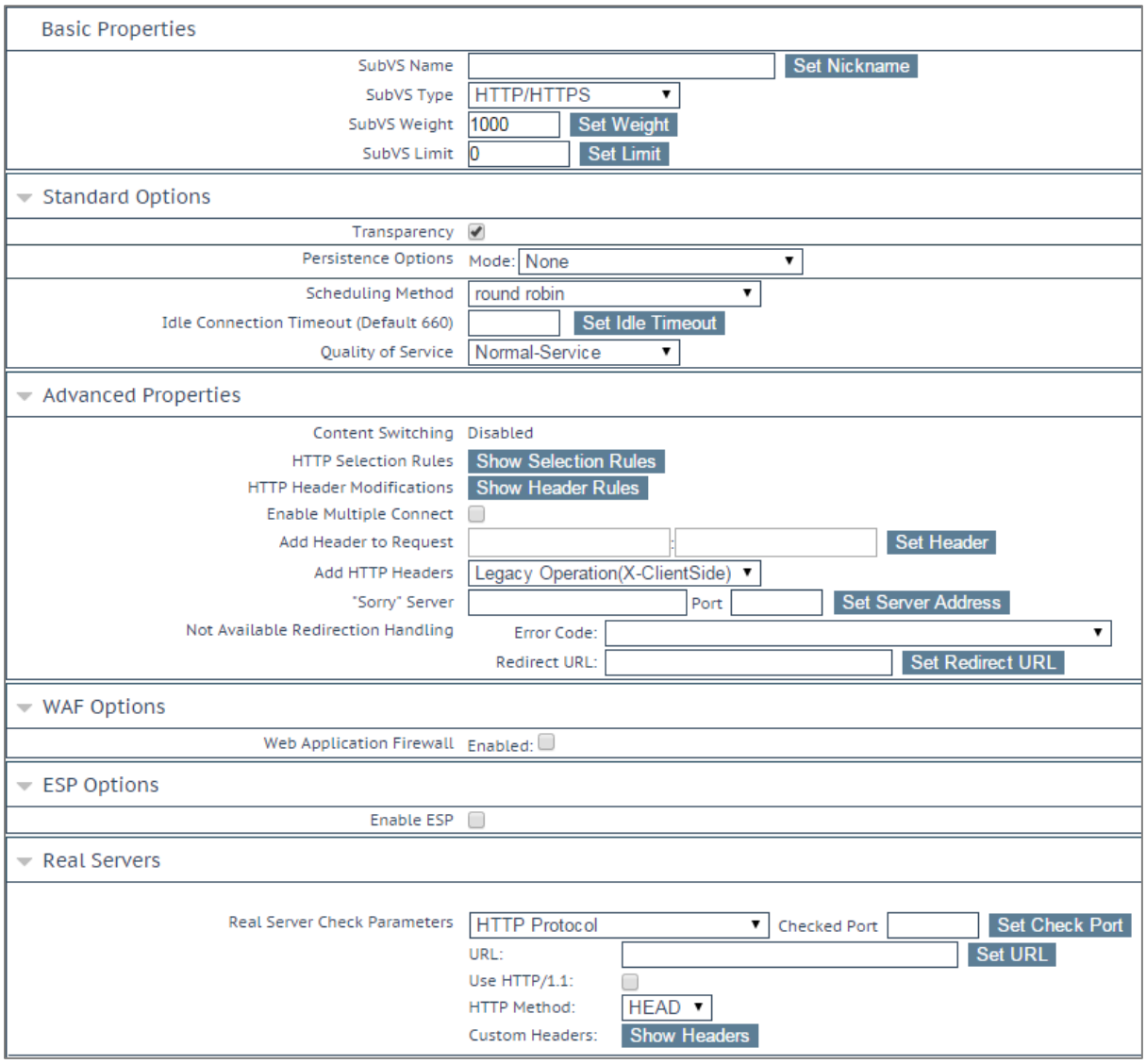

図 3-27:SubVS 編集画面のセクション

またサブ VS は、メインの仮想サービスビューにて該当するサブ VS の**“Modify”**ボタンをクリックしても変更できます。サブ VS を持つ仮想サービスは、仮想 IP アドレスセクションにて異なる色で表示され、そのサブ VS が実サーバーセクションにリスト表示されます。サブ VS の詳細情報を見るには、親仮想サービスをクリックしてビューを展開し、サブ VS の情報をビューに表示します。

サブ VS を含む仮想サービスを削除する場合、メインのサービスを削除する前にサブ VS を削除する必要があります。

サブ VS の ESP オプションは、親仮想サービスとは異なる設定にできますが、親仮想サービスとサブ VS の ESP オプションが矛盾しないように注意してください

3.10 表示/変更（リモート端末サービス）

このセクションは、ロードマスターExchange では関係ありません。

Generic Type といった仮想サービスのプロパティや、リモート端末特有のオプションが用意されています。

Persistence（パーシステンス）

端末サービスがセッションディレクトリをサポートしている場合、ロードマスターは、セッションディレクトリにより提供された「ルーティング」を使用して、接続すべきホストを決定します。ロードマスターのパーシステンシータイムアウト値は、ここでは関係ありません。これはセッションディレクトの機能です。

この機能を動作させるには、セッションディレクトリの設定で"IP address redirection"スイッチを選択しないでください

パーシステンスに関して、ロードマスターでセッションディレクトリを使用するかどうかは必須ではありません。初回要求時にクライアントがユーザー名とパスワードのフィールドに値を入力した場合、その値はロードマスターに保存されます。再接続時にこれらのフィールドに値が入力されると、ロードマスターは名前を照会し、最初の接続時と同じサーバーに再接続します。ロードマスターで情報が保持される時間を制限するため、パーシステンスタイムアウトが使用されます。

"Terminal-Servicec or Source IP"モードを使用しており、これら 2 つのいずれのモードも成功しなかった場合、ソース IP アドレスがパーシステンシーで使用されます。

Service Check for the Virtual Service（仮想サービスのサービスチェック）

"ICMP"、"TCP"、"RDP"の 3 つのオプションのみ利用できます。リモート端末プロトコル（RDP）は、実サーバーのサービスポート（ポート 3389）に対して TCP 接続を開きます。ロードマスターは、サーバーにコード 1110（接続要求）を送信します。サーバーからコード 1110（接続確認）が送信されると、ロードマスターは、接続を閉じてそのサーバーがアクティブであるとしてマーキングします。設定された回数だけ接続を要求しても、設定された応答時間内にサーバーから応答が返されなかった場合、または、他のステータスコードが返された場合、そのサーバーは動作していないとみなされます。

3.11 Real Servers（実サーバーのアサイン）

このセクションは、仮想サービスにアサインされている実サーバーをリストアップします。アサインされていない場合は、追加、また、アサインされている場合は、実サーバー属性の要約が表示され、そして実サーバーの追加、削除、および属性変更が可能です。コンテントスイッチが有効になっていると、各実サーバーへのルールの追加、削除もこのセクションで行えます。

Real Server Check Method（実サーバーチェック方法）

このパラメータで、実サーバーの死活チェックを行う方法を選択します。良く知られるサービスから、下位レベルの TCP/UDP、もしくは ICMP 方式まであります。ここで選択された方式で、実サーバーの可用性がチェックされます。TCP/UDP 方式は、単に接続を試みるだけのチェックを行います。

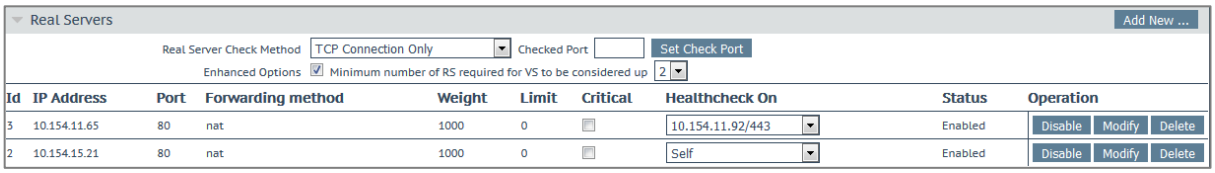

図 3-28:実サーバー

Real Server Check Protocol（実サーバー・チェック用プロトコル）

以下の表では、実サーバーの健全性を確認する場合に使用可能なオプションについて説明しています。実サーバーのヘルスチェック用ポートも指定できます。ここで何も指定しなかった場合、実サーバーのポートがデフォルトのポートになります。

サービスタイプとして**"HTTP/HTTPS"、"Generic"**、および**"STARTTLS protocols"**を選択した場合、以下のヘルスチェックオプションを利用できます。

方式	アクション
ICMP Ping:	Ping を実サーバーへ送信します

方式	アクション
HTTP	HTTP GET／HEAD リクエストを送信します
HTTPS	SSL 通信で HTTP GET／HEAD リクエストを送信します
TCP	TCP 接続を試みます
Mail（メール）	ポート 25（または設定ポート）に TCP 接続を試みます
NNTP	ポート 119（または設定ポート）に TCP 接続を試みます
FTP	ポート 21（または設定ポート）に TCP 接続を試みます
Telnet	ポート 23（または設定ポート）に TCP 接続を試みます
POP3	ポート 110（または設定ポート）に TCP 接続を試みます
IMAP	ポート 143（または設定ポート）に TCP 接続を試みます
Name Service (DNS) Protocol（ネームサービス（DNS）プロトコル）	ネームサービスプロトコルを使用します
Binary Data（バイナリデータ）	送信する 16 進文字列、および応答内でチェックする 16 進文字列を指定します
None（なし）	ヘルスチェックを行いません

サービスタイプとして**"Remote Terminal"**を選択した場合、以下のヘルスチェックオプションを利用できます。

方式	アクション
ICMP Ping:	Ping を実サーバーへ送信します
TCP	TCP 接続を試みます
Remote Terminal Protocol（リモートターミナルプロトコル）	実サーバーに RDP のルーティングトークンが渡されます。 こ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（なし）	ヘルスチェックを行いません

UDP 仮想サービスの場合、**“ICMP Ping”**および**“Name Service (DNS) Protocol”**のみ利用できます。

Enhanced Options（拡張オプション）

"Enhanced Options"チェックボックスをオンにすると、ヘルスチェックに関する追加のオプション**"Minimum number of RS required for VS to be considered up"**が利用できるようになります。**"Enhanced Options"**チェックボックスがオフの場合（デフォルト）、いずれかの実サーバーが利用可能であれば、その仮想サービスは利用可能であるとみなされます。**"Enhanced Options"**チェックボックスがオンの場合、仮想サービスが利用可能であると認識されるのに必要な最低限の実サーバー数を指定することができます。

Minimum number of RS required for VS to be considered up（仮想サービスが稼働中であると認識されるのに必要な最低限の実サーバー数）

このオプションは、**"Enhanced Options"**チェックボックスがオンになっており、複数の実サーバーが存在する場合に表示されます。

仮想サービスが稼働中であると認識されるのに必要な最低限の実サーバー数を選択してください。

利用可能な実サーバーの数が最小数より少ない場合、重大なログが生成されます。一部の実サーバーが停止しているものの、指定された最小数を下回っていない場合は、警告が記録されます。E メールオプションが設定されている場合、関係する受信者に E メールが送信されます。E メールオプションの詳細については、**セクション 10.4.5** を参照してください。

なお、**"Enhanced Options"**が有効で、指定された最小数より多くの実サーバーが利用可能な場合であっても、**"Critical"**とマークされた実サーバーが利用不可能になると、その仮想サービスは停止中であるとマークされます。

いかなる場合でも、仮想サービスが停止中であると認識され、その仮想サービスが Sorry サーバーを持っている（またはエラーメッセージが設定されている）場合、それらが使用されます。

最小数としてトータルの実サーバー数が設定されているとき、実サーバーを 1 つ削除すると、この最小数が自動的に 1 つ減らされます。

サブ VS にてコンテキストルールを使用する場合、必要な実サーバーの最小数が持つ意味は少し異なります。ルールが割り当てられている利用可能な実サーバーの数が下限値以上の場合のみ、そのルールが利用可能とみなされて照合することができます。利用可能な実サーバーの数が下限を下回ると、そのルールは照合されません。そのサブ VS は停止中とマークされ、その旨がログに記録されます。

サブ VS 上の実サーバーが重要であるとマークされている場合、その実サーバーが停止すると、そのサブ VS は停止中であるとマークされます。ただし、サブ VS が重要であるとマークされていない限り、その親の仮想サービスは停止中であるとマークされません。

3.11.1 HTTP または HTTPS プロトコルによるヘルスチェック

“HTTP Protocol”または**“HTTPS Protocol”**を選択した場合、以下の追加オプションを利用できます。

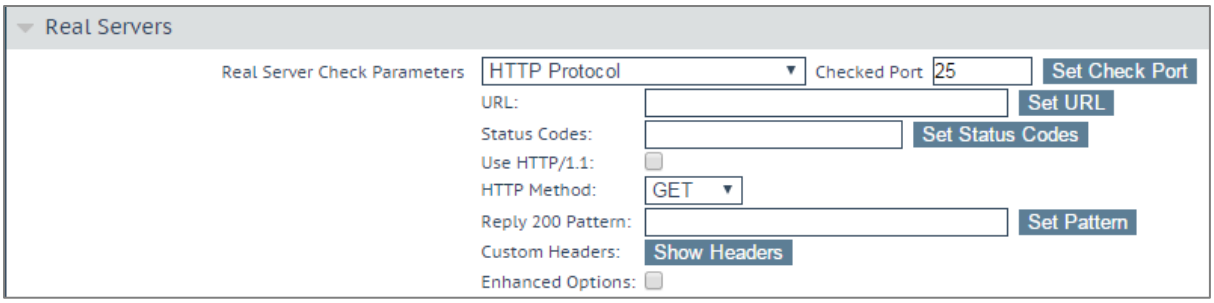

図 3-29:実サーバーのセクション

"post data"オプションが表示されるのは、"HTTP Method"に"POST"を選択した場合に限定されます。

"Reply 200 Pattern"オプションが表示されるのは、"HTTP Method"に"POST"または"GET"を選択した場合に限定されます。

URL

デフォルトでは、ヘルスチェッカーは URL にアクセスして、マシンの利用可否を判断します。別の URL を指定するには、このフィールドに入力します。

Status Codes（ステータスコード）

ヘルスチェックのステータスコードを設定して、デフォルトの動作を上書きできます。**"Status Codes"**を設定しない場合、HTTP ステータスコードが以下の値の場合に稼働中とみなされます。

- 200-299
- 301
- 302
- 401

また、2*xx* のステータスコードが設定されている場合、このコードと応答データとのパターン照合が行われます。その他のコードについては、コードが設定されていてもパターン照合なしで稼働中とみなされます。

カスタムのヘルスチェックコードが設定されている場合、動作は以下のようになります。

- チェックコードには、300～599 の値から成る数字のリストが設定されます。
- チェックコードは、最大 127 文字（32 個の有効なコード）で構成されます。
- リストのいずれのコードも、稼働中を表すヘルスチェックコードであるとみなされます。
- 設定されたコードにより、デフォルトの設定が上書きされます。
  - 2*xx* のコードが設定されている場合、このコードはいかなる場合も常に稼働中とみなされ、パターン照合の対象となります。
  - チェックコードには、300～599 の範囲に入っている限り、公式の HTTP ステータスコード、非公式のコード、またはカスタム定義されたユーザーコードを使用できます。
    - 公式の HTTP ステータスコードについては、下記を参照してください。https://en.wikipedia.org/wiki/List_of_HTTP_status_codes
    - 非公式の HTTP ステータスコードについては、下記を参照してください。https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#Unofficial_codes
  - 小数を用いた Microsoft のサブコードをサポートします。ただし、トップレベルのステータスコードのみサポートします。
    - 小数を用いた Microsoft のサブコードについては、下記を参照してください。https://support.microsoft.com/en-us/kb/943891
    - サブコードは**"Status Codes"**フィールドでは設定できません。3 桁のコードを使用してください。
    - サブコードはトップレベルのコードでグループ化されます。

Use HTTP/1.1（HTTP/1.1 を使う）

デフォルトでは、ロードマスターは HTTP/1.0 を使用します。ただし、より処理効率が高い **HTTP/1.1** を使用できます。HTTP/1.1 を使用する場合、ヘルスチェックは 1 つの接続

にマルチプレックスされます。これは、1 つの接続でより多くのヘルスチェックがサーバーに送信されることを意味します。接続の観点から見ると、これはより効率が高い方法であるといえます（複数の接続ではなく、接続は 1 つだけとなる）。

HTTP/1.1 Host（HTTP/1.1 ホスト）

このフィールドは**"Use HTTP/1.1"**が選択されている場合のみ表示されます。

HTTP/1.1 を使用してチェックする場合、実サーバーに対する各リクエストにホスト名を与える必要があります。何も値を指定しない場合、このフィールドには仮想サービスの IP アドレスが設定されます。

HTTPS のヘルスチェックにて SNI ホスト情報を送信するには、該当する仮想サービスの **"Real Servers"**セクションにある**"Use HTTP/1.1"**を有効にし、ホストヘッダーを指定してください。この設定を行わない場合、実サーバーの IP アドレスが使用されます。

HTTP Method（HTTP メソッド）

ヘルスチェック用 URL にアクセスする際に、システムは **HEAD メソッド、GET メソッド**または **POST メソッド**を使用できます。

Post Data（Post データ）

このフィールドは、**HTTP Method** が **POST** に設定されているときのみ利用できます。**POST** メソッドを使用する場合、最大 2047 文字の POST データをサーバーに渡せます。

Reply 200 Pattern（レスポンス 200 のパターン）

GET メソッドまたは **POST** メソッドを使用すると、返されたレスポンスメッセージの内容をチェックできます。レスポンスメッセージに正規表現で指定された文字列が含まれている場合、マシンが動作していると判断します。このレスポンスには、照合が行われる前に削除された HTML 形式の情報がすべて含まれています。照合に使用されるのは、レスポンスデータの先頭 4K 部分だけです。

ロードマスターは、サーバーからのレスポンスがコード 200 の場合のみ、そのフレーズをチェックします。それ以外の場合はフレーズをチェックせず、ページが停止しているものとしてマークします。ただし、レスポンスがリダイレクト（コード 302）の場合、

そのページが停止しているものとしてマークしません。これは、サービスがダウンしているとみなすとリダイレクトが使い物にならないため、ロードマスターはフレーズが存在しないと仮定するためです。

カラット(^)で始まるパターンの場合、レスポンスのパターンを反転させます。

正規表現と Perl Compatible Regular Expression（PCRE）のどちらでも文字列を指定できます。正規表現と PCRE の詳細については、**コンテンツルール機能説明**ドキュメントを参照してください。

Custom Headers（カスタムヘッダー）

ここでは、ヘルスチェック要求とともに送信される追加のヘッダー/フィールドを最大 4 つまで指定できます。**"Show Headers"**ボタンをクリックすると、入力フィールドが表示されます。最初のフィールドでは、ヘルスチェック要求の一部として送信されるカスタムヘッダーのキーを定義します。2 番目のフィールドには、ヘルスチェック要求の一部として送信されるカスタムヘッダーの値を入力します。それぞれの情報を入力したら、**"Set Header"**ボタンをクリックします。各ヘッダーには最大 20 文字、フィールドには最大 100 文字を設定できます。ただし、4 つのヘッダー/フィールドに入力できる合計の最大文字数は 256 です。

"Custom Headers"（カスタムヘッダー）フィールドでは、以下の特殊文字を使用できます。

; .( ) / + = - _

HTTP/1.1 を指定している場合、Host フィールドは従来どおり RS に送信されます。この処理は、追加のヘッダーセクションで Host エントリを指定することによって無効にできます。User-Agent も同様の方法で無効にできます。実サーバーがアダプティブ負荷分散機能を使用している場合、ヘルスチェックで指定されている追加のヘッダーもアダプティブ情報の取得時に送信されます。

認証されたユーザーを使用してヘルスチェックを行うことができます。**"Use HTTP/1.1"** を有効にし、**"HTTP Method"**として**"HEAD"**を選択し、正しく構築された値を持つ認証ヘッダーを入力してください。認証フィールドは以下のように構築されます。

1. ユーザー名とパスワードは、“ユーザー名:パスワード”という文字列に結合されます。
2. このようにして得られた文字列は、Base64 の RFC2045-MIME バリアントを用いて符号化されます。ただし、76 文字/行の制約はありません。

3. 符号化された文字列の先頭に、認証方式とスペース（すなわち“Basic “）が追加されます。

例えば、ユーザーエージェントが、ユーザー名として'Aladdin'を使用し、パスワードとして'open sesame'を使用している場合、このフィールドは以下のように構築されます。

Authorization:Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

HTTPS のヘルスチェックにて SNI ホスト情報を送信するには、該当する仮想サービスの **"Real Servers"**セクションにある**"Use HTTP/1.1"**を有効にし、ホストヘッダーを指定してください。この設定を行わない場合、実サーバーの IP アドレスが使用されます。

Rules（ルール）

実サーバーにコンテントスイッチ用ルールが割り当てられている場合、実サーバーセクションに**“Rules”**列が表示されます。**“Rules”**列には、実サーバーに割り当てられたルール番号のボタン（ルールが割り当てられていない場合は**“None”**ボタン）が表示されます。

“Rules”列のボタンをクリックすると、**“Rules Management”**画面が表示されます。

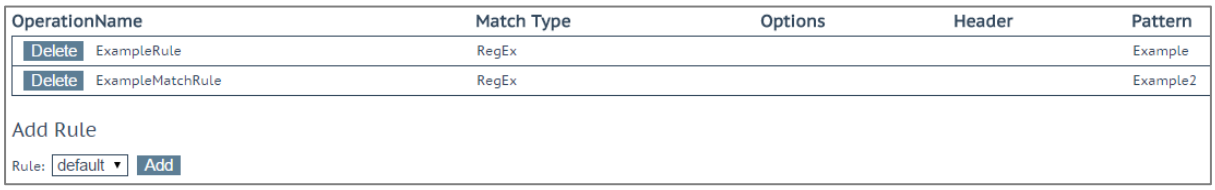

図 3-30:ルール

この画面では、実サーバーに割り当てられたルールを**追加**または**削除**できます。

3.11.2 バイナリデータによるヘルスチェック

ヘルスチェック方式として**"Binari Data"**を選択すると、以下に示す追加のフィールドが利用可能になります。

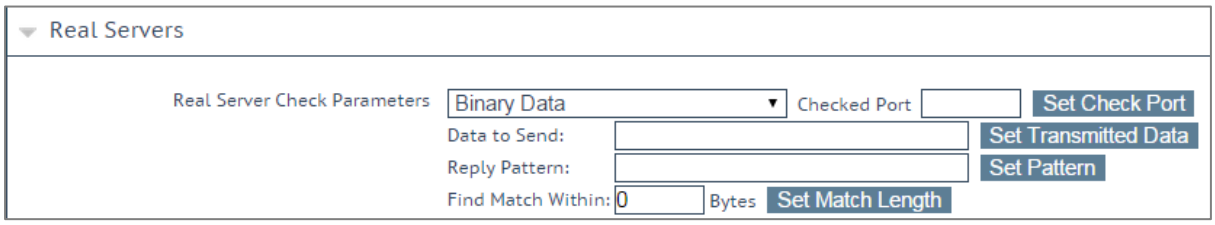

図 3-31:バイナリデータによるヘルスチェック

Data to Send（送信データ）

実サーバーに送信する 16 進文字列を指定します。

この 16 進文字列には偶数個の文字が含まれいてる必要があります。

Reply Pattern（応答パターン）

実サーバーから返信された応答内で検索する 16 進文字列を指定します。応答内にこのパターンが見つかると、ロードマスターはその実サーバーが稼働中であるとみなします。この文字列が見つからなかった場合、実サーバーが停止しているものとしてマークします。

この 16 進文字列には偶数個の文字が含まれいてる必要があります。

Find Match Within（検索バイト数）

応答が返されると、ロードマスターは、**"Reply Pattern"**で指定された文字列をその応答内で検索します。ロードマスターは、このフィールドで指定されたバイト数まで検索します。

このオプションを **0** に設定した場合、最後まで検索が行われます。パターンが一致するまで実サーバーからデータを読み込みます。実サーバーから最大 8KB のデータを読み込みます。

応答文字列の長さより小さい値を設定した場合、**0** に設定した場合と同じ動作になります。すなわち、すべてのパケット（最大 8KB）が検索されます。

3.11.3 Add a Real Server（実サーバーの追加）

[Add New] ボタンをクリックすると、実サーバーのプロパティを設定する次の画面が表示されます。

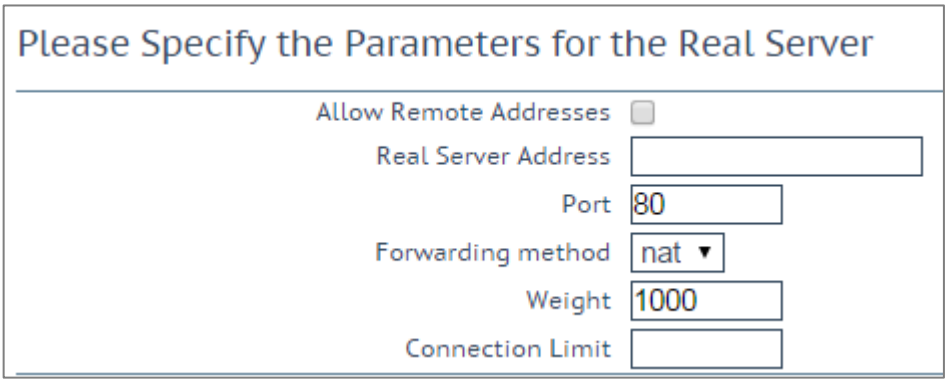

図 3-32:実サーバーのパラメータ

Allow Remote Addresses（リモートアドレスを許可）:デフォルトでは、ローカルネットワーク上の実サーバーのみ仮想サービスに割り当てられます。このオプションを有効に

すると、ローカルネットワーク上にない実サーバーを仮想サービスに割り当てることができます。

"Allow Remote Addresses"オプションを表示するには、**"Enable Non-Local Real Servers"**を選択する必要があります（**"System Configuration" > "Miscellaneous Options" > "Network Options"**）。また、仮想サービスにて**"Transparency"**を無効にする必要があります。

代替ゲートウェイ/非ローカルの実サーバーが設定されている場合、ヘルスチェックはデフォルトゲートウェイを通して転送されます

Real Server Address（実サーバーのアドレス）: 実サーバーのアドレス。実サーバーのアドレスには、IP アドレス、または完全修飾ドメイン名（FQDN）のいずれかを使用できます。実サーバーの変更中に、このフィールドは編集できません。FQDN は、**"Nameserver"**が設定されている場合のみ使用できます。詳細は**セクション 10.1.2** を参照してください。実サーバー追加時に FQDN を使用する場合、FQDN 名はサーバー追加時に解決されます。名前の解決に失敗した場合、実サーバーは作成されず、エラーが発生します。

Port（ポート）:実サーバーのフォワーディングポート。このフィールドは編集できるので、必要に応じて後からポートを変更できます。

Forwarding Method（フォワーディング方式）: Network Address Translation（NAT）または Route（直接）フォワーディング。利用可能なオプションは、サービスに対して選択した他のモードに応じて異なります。

Weight（重み）:実サーバーの重み。これは重み付け負荷分散方式（Weighted Round Robin、Weighted Least Connection、および Adaptive）で使用されます。デフォルトの初期設定値は **1000** で、最高 **65535**、最低 **1** までの値への変更が可能です。これには、実サーバーの処理スピードに比例した値をアサインすると、良いベンチマークになります。例えば、サーバー2 が、サーバー1 と比較して 4 倍の CPU 性能だとすると、サーバー2 を **4000** とし、サーバー1 はデフォルト値の **1000** のままとします。

Connection Limit（接続上限）:ローテーションから取り出される前に、実サーバーが受け入れられるオープン接続の最大数を設定します。これは、レイヤ 7 のトラフィックにの

み適用されます。この上限により、新たな接続の作成が制限されます。ただし、サーバーとの間ですでにパーシステントコネクションが確立しているリクエストは許可されます。パーシステンス接続には、セッションブローカーパーシステンスによる仮想サービスへの接続が含まれます。このセッションブローカーパーシステンスには、接続ブローカーにより設定されたセッションブローカークッキーが含まれます。

実サーバーは、最大 1024 台まで使用できます。これは全体の上限で、実サーバーは既存の仮想サービスに分配されます。例えば、ある仮想サービスが 1000 台の実サーバーを使用している場合、残りの仮想サービスは 24 台の実サーバーしか使用できません。

ロードマスター*Exchange* では、設定できる実サーバーに最大 6 台という制約があります。

"Add This Real Server"ボタンをクリックすると、その実サーバーがプールに追加されます。

Critical（重大）:

このオプションは、**"Enhanced Options"**チェックボックスがオンの場合のみ表示されます。**"Enhanced Options"**チェックボックスの詳細については、**セクション 3.11** を参照してください。

仮想サービス編集画面の実サーバーのセクションには、各実サーバーの**"Critical"**チェックボックスが用意されています。このオプションが有効な場合、仮想サービスが利用可能であると認識されるためにはこの実サーバーが必要であることを意味します。この実サーバーが機能しなくなる（または無効になる）と、この仮想サーバーは停止中であるとマークされます。

サブ VS 上の実サーバーが重要であるとマークされている場合、その実サーバーが停止すると、そのサブ VS は停止中であるとマークされます。ただし、サブ VS が重要であるとマークされていない限り、その親の仮想サービスは停止中であるとマークされません。

このオプションは、**"Minimum number of RS required for VS to be considered up "**フィールドより優先されます。例えば、最小値が 2 に設定されているとき、1 台の実サーバーしか停止していなくても、その実サーバーが重要なサーバーに設定されている場合、その仮想サービスは停止中であるとマークされます。

いかなる場合でも、仮想サービスが停止中であると認識され、その仮想サービスが Sorry サーバーを持っている（またはエラーメッセージが設定されている）場合、それらが使用されます。

Healthcheck On（ヘルスチェックオン）

このオプションは、**"Enhanced Options"**チェックボックスがオンの場合のみ表示されます。**"Enhanced Options"**チェックボックスの詳細については、**セクション 3.11** を参照してください。

仮想サービス編集画面の実サーバーのセクションには、各実サーバーの**"Healthcheck On"**ドロップダウンリストが用意されています。このドロップダウンリストでは、どの実サーバーに基づいてヘルスチェックを行うかを指定できます。このオプションを**"Self"**に設定してこの実サーバーの状態に基づきヘルスチェックを行わせることも、他の実サーバーを選択することもできます。例えば、実サーバー1 が停止している場合、実サーバー1 に基づきヘルスチェックを行っている実サーバーは、それらの実サーバーの状態にかかわらず、すべて停止中であるとマークされます。

以下に、いくつかの注意点を示します。

- 実サーバーは実サーバーのみフォローできます。サブ VS はフォローできません。
- 実サーバーは、第三の実サーバーをフォローしている実サーバーをフォローできます。最初の 2 つの実サーバーの状態は、第三の実サーバーの状態を反映します。
- 実サーバーを連結させることができます。ただし、ループにすることはできません。
- 実サーバー（単体の実サーバーまたは仮想サービスに含まれる実サーバー）が削除された場合、その実サーバーをフォローしているすべての実サーバーが通常動作にリセットされます（仮想サービスのヘルスチェックオプションが使用されます）。
- 仮想サービスに含まれるすべての実サーバーが他の仮想サービスに含まれる実サーバーをフォローしている場合、その仮想サービスのヘルスチェックパラメーターは WUI に表示されません（この設定はどの実サーバーにも影響しないため）。
- **"Enhanced Options"**チェックボックスをオフにすると、その仮想サービスをフォローしているすべての実サーバーのヘルスチェックが無効になります。

3.11.4 Modify a Real Server（実サーバーの設定変更）

実サーバーの"Modify"ボタンをクリックすると、以下のオプションを設定できます。

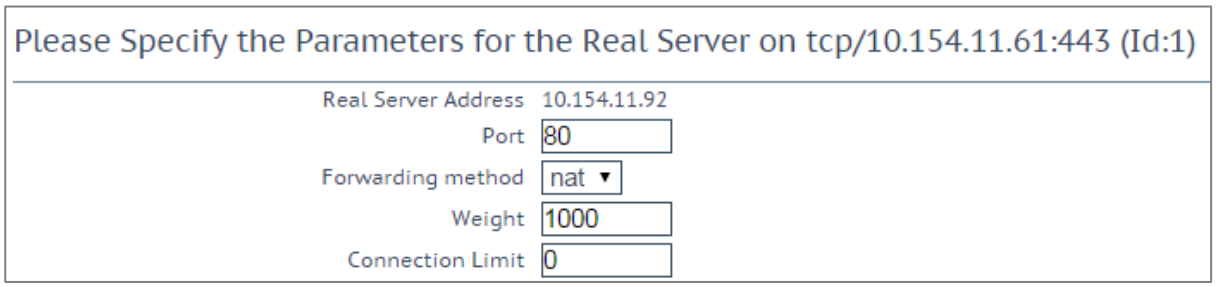

図 3-33:実サーバーのオプション

Real Server Address（実サーバーのアドレス）

このフィールドには、実サーバーのアドレスが表示されます。このフィールドは編集できません。

Port（ポート）

このフィールドには、実サーバーが使用するポートが表示されます。

Forwarding Method（フォワーディング方式）

このフィールドには、実サーバーが使用するフォワーディング方式が表示されます。デフォルトは NAT です。ダイレクト・サーバー・リターンはレイヤ 4 でのみ使用できます。

Weight（重み）

重み付けラウンドロビン方式を使用する場合、サーバーに送信するトラフィックの相対比率は、実サーバーの重みに基づき決定されます。高い値が設定されたサーバーは、より多くのトラフィックを受信します。

Connection Limit（接続上限）

ローテーションから除外されるまでに、実サーバーに送信できるオープン接続の最大数です。上限は 100,000 です。

3.12 Manage Templates（テンプレートの管理）

テンプレートを使用すると、仮想サービスのパラメータが自動的に作成/設定されるため、仮想サービスの設定が容易になります。テンプレートを使って仮想サービスを設定するには、ロードマスターにテンプレートをインポートしてインストールする必要があります。

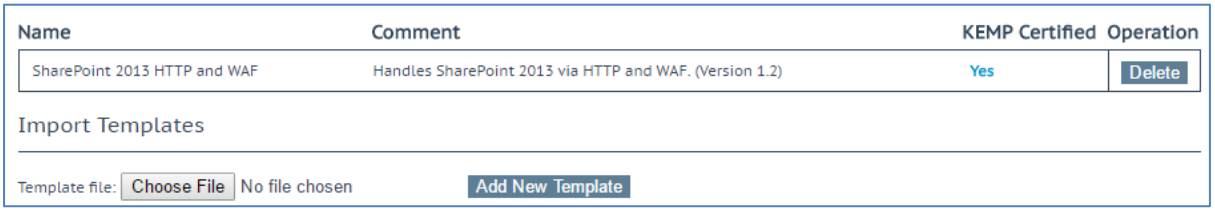

図 3-34:テンプレートの管理

“Choose File”ボタンをクリックしてインストールしたいテンプレートを選択し、**“Add New Template”**ボタンをクリックして選択したテンプレートをインストールします。これで、新たに仮想サーバーを追加したときに、このテンプレートを使用できるようになります。

テンプレートを削除するには、**"Delete"**ボタンをクリックします。

"KEMP Certified"列には、そのテンプレートが KEMP から提供されたかどうかが表示されます。テンプレートが認証されている場合、そのテンプレートは KEMP から提供されたものです。テンプレートが認証されていない場合、そのテンプレートはユーザーにより作成された（仮想サービスからエクスポートされた）可能性があります。

テンプレートに関する詳細（テンプレートを使用して新規仮想サービスの作成と設定を行う方法や、KEMP のテンプレートの入手先など）は、

仮想サービスとテンプレート機能説明ドキュメントを参照してください。

3.13 Manage SSO Domains（SSO ドメインの管理）

エッジ・セキュリティ・パック（ESP）を使用する前に、ユーザーは最初にシングル・サイン・オン（SSO）ドメインをロードマスター上にセットアップする必要があります。SSO ドメインとは、LDAP サーバーによって認証された仮想サービスを論理的にグループ化したものです。

SSO ドメインは最大 128 個まで設定できます。

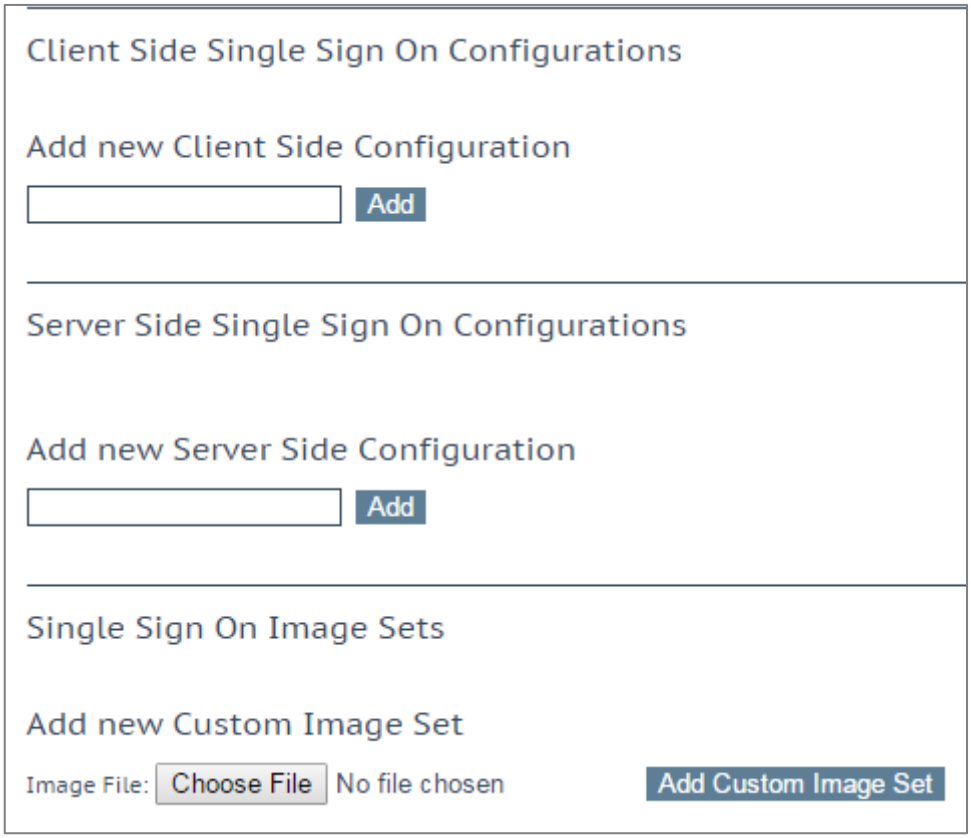

図 3-35:SSO 管理オプション

"Manage SSO Domains"メニューオプションをクリックすると、**"Manage Single Sign On Options"**画面が表示されます。

3.13.1 Single Sign On Domains（SSO ドメイン）

クライアントサイドとサーバーサイドの 2 種類の SSO ドメインを作成できます。

"Client Side"（クライアントサイド）の構成では、**"Authentication Protocol"（認証プロトコル）**を**"LDAP"**、**"RADIUS"**、**"RSA-SecurID"**、**"Certificates"（証明書）**、**"RADIUS and LDAP"（RADIUS および LDAP）**、**"RSA-SecurID and LDAP"（RSA-SecurID および LDAP）**に設定できます。

"Server Side"（サーバーサイド）の構成では、**"Authentication Protocol"**を**"Kerberos Constrained Deletation（KCD）"**に設定できます。

SSO ドメインを新規追加するには、**"Name"**フィールドにドメイン名を入力して**"Add"**ボタンをクリックします。ここで入力する名前は、SSO ドメインでアクセスを許可されたホストと関連している必要はありません。

"ESP Options"にて**"Permitted Groups"**フィールドを使用している場合、ここで設定した SSO ドメインが許可されたグループのディレクトリであることを確認する必要があります。例えば、**"SSO Domain"**が webmail.example に設定されており、webmail が example.com 内で許可されたグループのディレクトリでない場合、正しく機能しません。この場合、**"SSO Domain"**は.example.com に設定する必要があります。この場合、SSO ドメインは.example.com に設定する必要があります。

"Domain/Realm"フィールドが設定されていない場合、SSO ドメインを最初に追加したときに設定した**名前**が**"Domain/Realm"**の名前として使用されます。

3.13.1.1 クライアントサイド（インバウンド）SSO ドメイン

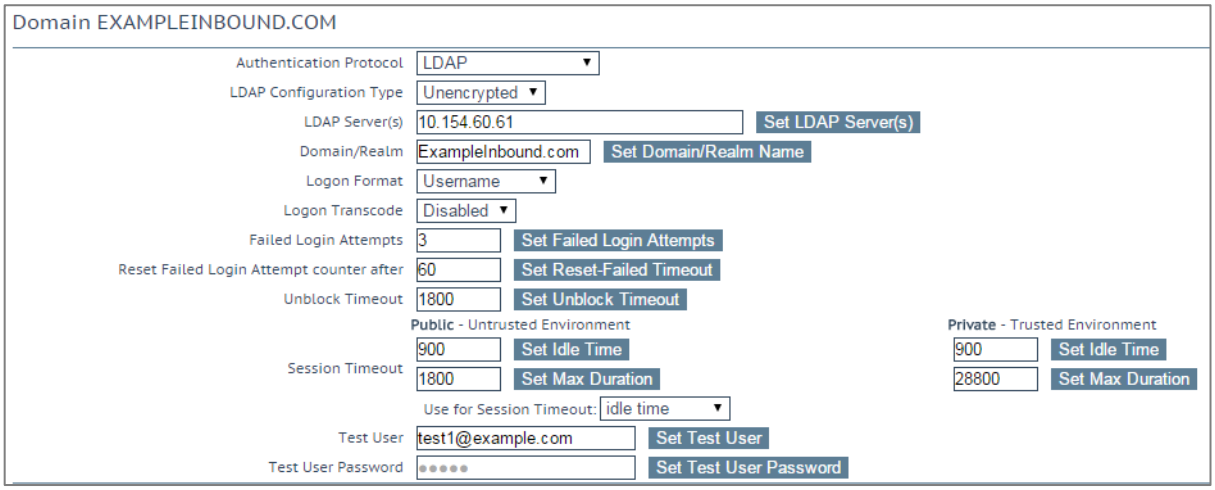

図 3-36:ドメインの管理画面

Authentication Protocol（認証プロトコル）

このドロップダウンリストでは、認証サーバーとの通信で使用する転送プロトコルを選択できます。以下のオプションが利用できます。

- **LDAP**
- **RADIUS**
- **RSA-SecurID**
- **Certificates（証明書）**
- **RADIUS and LDAP（RADIUS および LDAP）**

- **RSA-SecurID and LDAP（RSA-SecurID および LDAP）**

この画面に表示されるフィールドは、"Configuration Type"および"**Authentication protocol**"の選択により変わります。

LDAP Configuration Type（LDAP 設定タイプ）

LDAP の設定タイプを選択します。以下のオプションが利用できます。

- **Unencrypted（暗号化なし）**
- **StartTLS**
- **LDAPS**

このオプションは、"**Authentication Protocol**"が"**LDAP**"に設定されているときのみ利用できます。

RADIUS and LDAP（RADIUS および LDAP の設定タイプ）

RADIUS および LDAP の設定タイプを選択します。以下のオプションが利用できます。

- **RADIUS and Unencrypted LDAP（RADIUS および非暗号化 LDAP）**
- **RADIUS and StartTLS LDAP（RADIUS および StartTLS LDAP）**
- **RADIUS and LDAPS（RADIUS および LDAP）**

このオプションは、"**Authentication Protocol**"（**認証プロトコル**）が"**RADIUS and LDAP**"（**RADIUS および LDAP**）に設定されている場合に限り利用できます。

RSA-SecurID and LDAP Configuration Type（RSA-SecurID および LDAP の設定タイプ）

RSA-SecurID および LDAP の設定タイプを選択します。以下のオプションが利用できます。

- **RSA-SecurID and Unencrypted LDAP（RSA-SecurID および非暗号化 LDAP）**
- **RSA-SecurID and StartTLS LDAP（RSA-SecurID および StartTLS LDAP）**
- **RSA-SecurID and LDAPS（RSA-SecurID および LDAPS）**

このオプションは、"**Authentication Protocol**"（**認証プロトコル**）が"**RSA-SecurID and LDAP**"（**RSA-SecurID および LDAP**）に設定されている場合に限り利用できます。

LDAP/RADIUS/RSA-SecurID Server(s)（LDAP/RADIUS/RSA-SecurID サーバー）

ドメイン認証に使用するサーバーの IP アドレスをサーバーのフィールドに入力し、"Set LDAP server(s)"ボタンをクリックします。

このテキストボックスには複数のサーバーアドレスを入力できます。各入力はスペースで区切ってください。

RADIUS Shared Secret（RADIUS 共有秘密鍵）

この共有秘密鍵は、RADIUS サーバーとロードマスターとの間で使用されます。

このフィールドは、**HTTP Method** が **POST** に設定されているときのみ利用できます。

LDAP Administrator（LDAP 管理者）および LDAP Administrator Password（LDAP 管理者パスワード）

これらのテキストボックスは、**"Authentication Protocol"**が**"Certificates"**に設定されているときのみ表示されます。

これらの情報は、LDAP データベースをチェックして証明書からのユーザーが存在するか判断するのに使用されます。

Check Certificate to User Mapping（証明書とユーザーの対応をチェックする）

このオプションは、**"Authentication Protocol"**が**"Certificates"**に設定されている場合のみ利用できます。このオプションを有効にすると、クライアントの証明書が有効かどうかのチェックに加え、アクティブディレクトリにあるユーザーの altSecurityIdentities（ASI）アトリビュートに基づきクライアント証明書がチェックされます。

このオプションが有効であり、かつチェックに失敗した場合、ログインが失敗します。このオプションが無効の場合、ユーザーの altSecurityIdentities アトリビュートが存在しないか一致しない場合でも、ログイン時に（SubjectAltName（SAN）のユーザー名を持つ）有効なクライアント証明書が必要になります。

詳細は、**Kerberos Constrained Delegation　機能説明**を参照してください。

Allow fallback to check Common Name（フォールバックによるコモンネームのチェックを許可する）

このオプションを有効にすると、SAN を利用できないときに、フォールバックによるコモンネーム（CN）のチェックを許可します。

> このフィールドは、**"Authentication Protocol"**が**"Certificates"**に設定されている場合のみ表示されます。

Domain/Realm（ドメイン/レルム）

使用するログインドメインです。これは、ログインフォーマットとともに使用して正規化されたユーザー名を作成するのにも使用されます。例:

- **Principalname（プリンシパル名）**:<ユーザー名>@<ドメイン>
- **username（ユーザー名）**:<ドメイン>\<ユーザー名>

> **"Domain/Realm"**フィールドが設定されていない場合、SSO ドメインを最初に追加したときに設定した名前が**"Domain/Realm"**の名前として使用されます。

RSA Authentication Manager Config File（RSA 認証マネジャーの設定ファイル）

このフィールドは、RSA 認証マネジャーにエクスポートする必要があります。

> RSA の設定方法等、RSA の認証方式についての詳細は、**RSA の 2 要素認証　機能説明**を参照してください。

RSA Node Secret File（RSA ノード秘密ファイル）

ノード秘密ファイルは、RSA 認証マネジャーにより生成/エクスポートされます。

> RSA 認証マネジャーの設定ファイルをアップロードするまで、RSA ノード秘密ファイルをアップロードできません。ノード秘密ファイルは設定ファイルにより異なります。

Logon Format（ログオンフォーマット）

このドロップダウンリストでは、クライアントに入力を要求するログイン情報のフォーマットを指定できます。

どのオプションが利用できるかは、**"Authentication Protocol"（認証プロトコル）**の選択内容によります。

Not Specified（指定しない）:ユーザー名は正規化されません。入力したとおりに使用されます。

Principalname（プリンシパル名）:このオプションを **Logon format** として選択した場合、クライアントはログインするときにドメイン（**name@domain.com** など）を入力する必要がありません。この場合、該当するテキストボックスに追加した SSO ドメインがドメインとして使用されます。

Authentication protocol（認証プロトコル）として **RADIUS** を使用する場合、この SSO ドメインフィールドの値はログイン情報と完全に同じでなければなりません。大文字と小文字が区別されます。

Username（ユーザー名）:このオプションを **Logon format** として選択した場合、クライアントはログインするときにドメインとユーザー名（**domain\name@domain.com** など）を入力する必要があります。

Username Only（ユーザー名のみ）:このオプションを**"Logon Format"（ログオン形式）**として選択すると、入力したテキストが正規化されてユーザー名のみ使用されます（ドメインは削除されます）。

"Username Only"（ユーザー名のみ）オプションは、**"RADIUS"**および**"RSA-SecurID"**のプロトコルでのみ利用できます。

Logon Format (Phase 2 Real Server)（ログオン形式（フェーズ 2 実サーバー））

実サーバーで認証するためのログオン文字列形式を指定します。

"Logon Format (Phase 2 Real Server)"（ログオン形式（フェーズ 2 実サーバー））フィールドは、**"Authentication Protocol"（認証プロトコル）**に以下のオプションを設定した場合に限り表示されます。

- **RADIUS**
- **RSA-SecurID**

Logon Format (Phase 2 LDAP)（ログオン形式（フェーズ 2 LDAP））

LDAP により認証されるためのログイン文字列の形式を指定します。

"Logon Format (Phase 2 LDAP)"（ログオン形式（フェーズ 2 LDAP））フィールドは、**"Authentication Protocol"（認証プロトコル）**に以下のオプションを設定した場合に限り表示されます。

- **RADIUS and LDAP（RADIUS および LDAP）**
- **RSA-SecurID and LDAP（RSA-SecurID および LDAP）**

Logon Transcode（ログオン時のトランスコード）

ログオン証明書の ISO-8859-1 から UTF-8 へのトランスコード（要求された場合）を有効/無効にします。

このオプションを無効にすると、クライアントにより指定された形式でログインします。このオプションを有効にすると、クライアントが UTF-8 を使用するかチェックします。クライアントが UTF-8 を使用しない場合は ISO-8859-1 を使用します。

Failed Login Attempts（ログイン試行回数）

ユーザーがロックされるまでに連続してログイン失敗可能な最大回数です。有効な値の範囲は **0～99** です。**0** を設定すると、ユーザーはロックされません。

ユーザーがロックされると、そのユーザーによるログイン状態は、
将来行われるログインも含めてすべて終了します。

Reset Failed Login Attempt Counter after（ログイン試行回数のリセット）

認証の試行に失敗した後、（新たに試行が行われないまま）この時間（単位: 秒）が経過すると、試行回数が **0** にリセットされます。このテキストボックスの有効な値の範囲は **60～86400** です。この値は、**Unblock timeout**（タイムアウトの解除）の値より小さくなければなりません。

Unblock timeout（タイムアウトの解除）

ブロックされたアカウントのブロックが解除されるまでの時間、すなわち管理者の操作によらずにブロックがされるまでの時間（単位: 秒）です。このテキストボックスの有効な値の範囲は **60～86400** です。この値は、**Reset Failed Login Attempt Counter after**（ログイン試行回数のリセット）の値より大きくなければなりません。

Session timeout（セッションタイムアウト）

信頼できる環境（プライベート環境）および信頼できない環境（パブリック環境）の **idle time（アイドル時間）** と **max duration（最大継続時間）** の値をここで設定します。使用される値は、ログインフォームにてユーザーがパブリックとプライベートのどちらを選択したかにより異なります。また、**max duration（最大継続時間）** と **idle time（アイドル時間）** のどちらを使用するかを指定できます。

Idle time（アイドル時間）:セッションの最大アイドル時間（アイドルタイムアウト）を秒で指定します。

Max duration（最大継続時間）:セッションの最大継続時間（セッションタイムアウト）を秒で指定します。

これらのフィールドの有効な値な範囲は **60～86400** です。

Use for Session Timeout（セッションタイムアウトで使用）:セッションタイムアウトの動作（**max duration** または **idle time**）を選択します。

ユーザーによる明示的な操作がない場合でも、下層ネットワークトラフィックによりセッションがアクティブのまま維持されます。

Test User（テストユーザー）と Test User Password（テストユーザーパスワード）

この 2 つのフィールドには、SSO ドメイン用のユーザーアカウントの資格情報を入力します。ロードマスターは、この情報に基づいて、認証サーバーのヘルスチェックを実行します。このヘルスチェックは、20 秒間隔で実行されます。

Currently Blocked Users（ブロックされたユーザー）

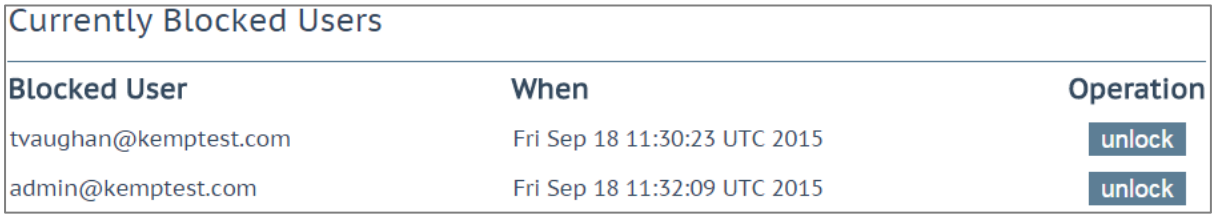

図 3-37:ブロックされたユーザー

このセクションには、現在ブロックされているユーザーおよびそのユーザーがブロックされた日時がリスト表示されます。**"Operation"**ドロップダウンリストにて**"unlock"**ボタンをクリックすると、ブロックを解除できます。

> 1 つのユーザーを異なる形式で表した場合、それらはすべて同じユーザー名として扱われます。例えば、**administrator@kemptech.net**、**kemptech\administrator**、**kemptech.net\administrator** はすべて 1 つのユーザー名として扱われます。

3.13.1.2 サーバーサイド（アウトバウンド）SSO ドメイン

Authentication Protocol（認証プロトコル）

このドロップダウンリストでは、認証サーバーとの通信で使用する転送プロトコルを選択できます。アウトバウンド（サーバーサイド）の構成では**"Kerberos Constrained Delegation"**オプションのみ利用できます。

Kerberos Realm（Kerberos レルム）

Kerberos レルムのアドレスです。

> このフィールドでは、コロン、スラッシュ、2 重引用符は使用できません。
>
> このフィールドは 1 つのアドレスのみサポートします。

Kerberos Key Distribution Center（Kerberos キー配信センター）（KDC）

Kerberos キー配信センターのホスト名または IP アドレスです。KDC は、セッションチケットや一時セッションキーを、アクティブディレクトリドメイン内にあるユーザーやコンピューターに供給するネットワークサービスです。

> このフィールドにはホスト名または IP アドレスのみ入力できます。
> このフィールドでは 2 重引用符や引用符は使用できません。

Kerberos Trusted User Name（Kerberos で信頼されたユーザー名）

ロードマスターを設定する前に、Windows のドメイン（アクティブディレクトリ）にてユーザーを作成して信頼を受ける必要があります。また、このユーザーが委任を使用するよう設定する必要があります。この信頼された管理者ユーザーアカウントは、パスワードが提供されていない場合に、ユーザーやサービスの代わりにチケットを取得するのに使用されます。この信頼されたユーザーのユーザー名を、このフィールドに入力する必要があります。

このフィールドには 2 重引用符や引用符は使用できません。

Kerberos Trusted User Password（Kerberos で信頼されたユーザーパスワード）

Kerberos で信頼されたユーザーのパスワードです。

3.13.2 Single Sign On Image Sets（SSO の画像設定）

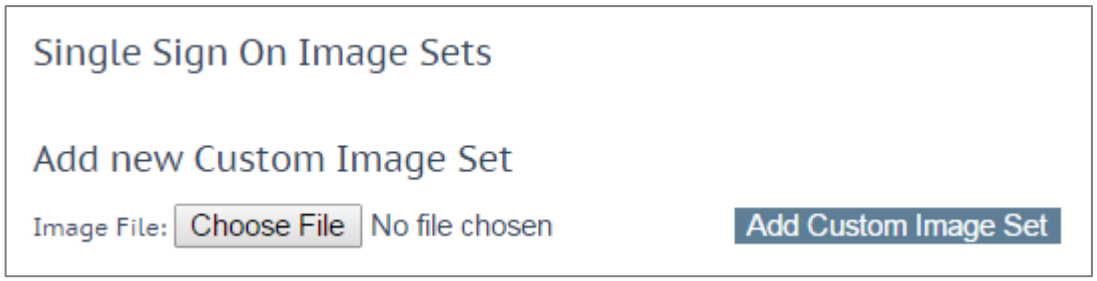

図 3-38:SSO の画像設定

新規画像を設定するには、**"Choose File"**をクリックし、ファイルをブラウズ/選択して**"Add Custom Image Set"**をクリックします。ファイルを追加すると、追加した画像がこのページにリスト表示されます。また、仮想サービス編集画面の**"ESP Options"**セクションにある**"SSO Image Set"**ドロップダウンリストでも選択可能です。

.tar ファイルの作成方法等、SSO の画面設定に関する詳細は、**ポートフォローウィング機能説明**を参照してください。

3.14 WAF の設定

この画面を開くには、ロードマスターWUI のメインメニューで**"Virtual Services" > "WAF Settings"**を選択します。

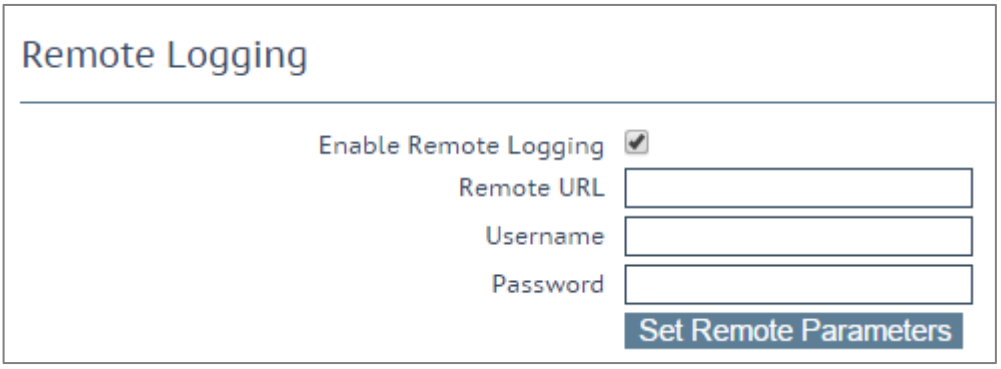

図 3-39:Remote Logging（リモートログの作成）

Enable Remote Logging（リモートログの作成を有効にする）

このチェックボックスを使用すると、WAF のリモートログの作成を有効/無効にできます。

Remote URL（リモート URL）

リモートログサーバーのユニフォームリソースアイデンティファイアー（URI）を指定します。

Username（ユーザー名）

リモートログサーバーのユーザー名を指定します。

Password（パスワード）

リモートログサーバーのパスワードを指定します。

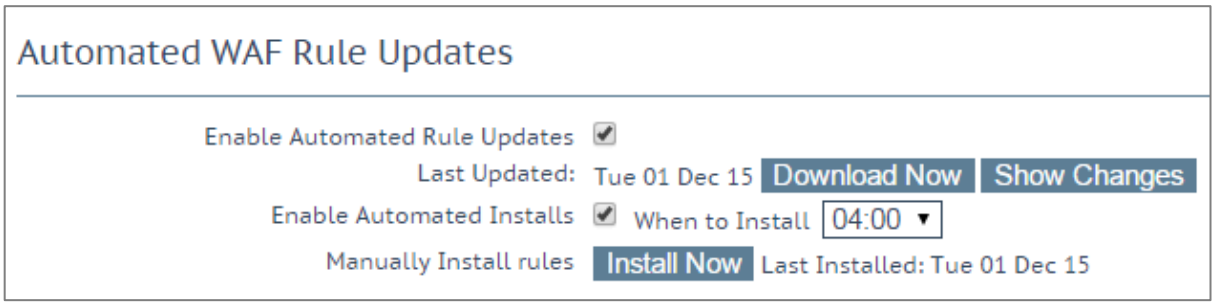

図 3-40:Automated WAF Rule Updates（WAF ルールの自動更新）

AFP のサブスクリプション期限が切れている場合、自動/手動ダウンロードオプションはグレー表示になります。

Enable Automated Rule Updates（ルールの自動更新の有効化）

このチェックボックスをオンにすると、最新の WAF ルールファイルの自動ダウンロードが有効になります。これを有効にすると、毎日ダウンロードが行われます。

Last Updated（最新更新日）

このセクションには、最新のルールがダウンロードされた日が表示されます。このセクションでは、直ちにルールをダウンロードするためのオプションが用意されています。また、過去 7 日間ルールがダウンロードされていない場合、警告が表示されます。ルールをダウンロードすると、**"Show Changes"**ボタンが表示されます。このボタンをクリックすると、KEMP テクノロジーの WAF ルールセットに対して行われた変更のログを取得できます。

Enable Automated Installs（自動インストールの有効化）

このチェックボックスをオンにすると、指定した時刻に最新のルールが毎日自動的にインストールされます。

When to Install（インストール時刻）

毎日何時に最新のルールをインストールするか選択します。

Manually Install rules（ルールを手動インストール）

このボタンを使用すると、最新のルールを自動インストールする代わりに手動でインストールできます。またこのセクションでは、ルールの最終インストール日が表示されます。

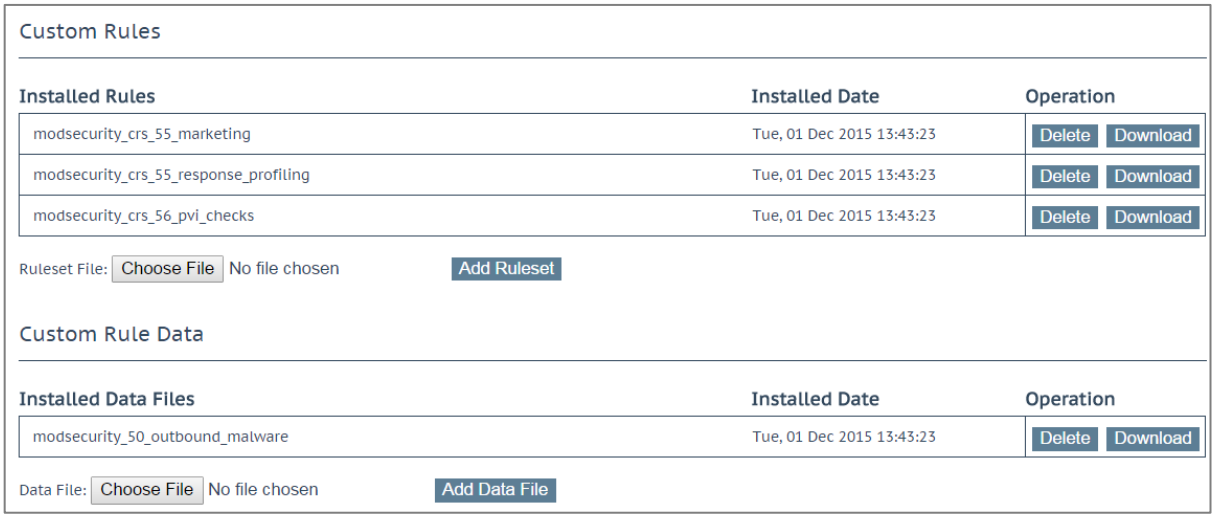

図 3-41:Custom Rules and Custom Rule Data（カスタムルールとカスタムルールデータ）

Custom Rules（カスタムルール）

このセクションでは、カスタムルールおよび関連するデータファイルをアップロードできます。個々のルールを拡張子*.conf* を持つファイルとして読み込むか、ルールのパッケージを Tarball（*.tar.gz*）ファイルで読み込むことができます。Tarball ファイルには、通常、*.conf* ファイルおよび*.data* ファイルが含まれます。

.conf ファイルは、標準の ModSecurity ルールファイル形式でなければなりません。

Custom Rule Data（カスタムルールデータ）

このセクションでは、カスタムルールに関連するデータファイルをアップロードできます。

4 グローバル負荷分散

構成によっては、このメニューオプションを使用できない可能性があります。この機能は GSLB 機能パックに含まれており、ロードマスターに適用されているライセンスに基づいて有効になります。このオプションを利用するには、ライセンスをアップグレードする必要があるので、KEMP にご連絡ください。

4.1Enable/Disable GSLB（GSLB の有効化/無効化）

このメニューオプションをクリックすると、GEO 機能を有効/無効にできます。GEO を有効にすると、**Packet Routing Filter（パケット・ルーティング・フィルター）**がデフォルトで有効になり、変更不可能になります。GEO を無効にすると、**"System Configuration" > "Access Control" > "Packet Filter"の Packet Routing Filter** を有効/無効にできます。

4.2FQDN の管理

絶対ドメイン名とも呼ばれる完全修飾ドメイン名（FQDN）は、ドメイン名システム（DNS）のツリー階層における厳密な場所を指定するドメイン名です。FQDN は、最上位レベルのドメインとルートゾーンを含むすべてのドメインレベルを指定します。完全修飾ドメイン名は、曖昧さがないことが特徴で、一意に解釈されます。DNS のルートドメインには名前がついていおらず、空のラベルで表されます。この場合、FQDN の末尾はドット文字になります。

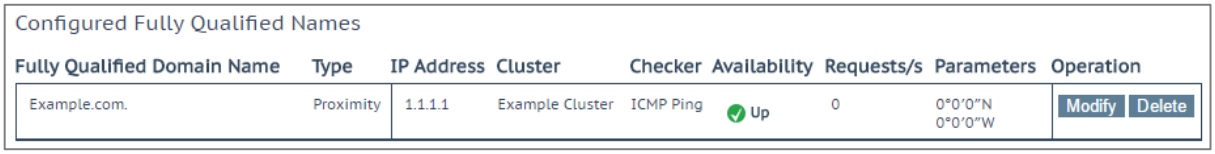

図 4-1:グローバルな完全修飾名

この画面から、FQDN の**"Add"**または**"Modify"**を選択できます。

4.2.1 Add a FQDN（FQDN の追加）

図 4-2:FQDN の追加

New Fully Qualified Domain Name（新規完全修飾ドメイン名）

FQDN 名の例を挙げると、www.example.com のようになります。ワイルドカードをサポートします。例えば、***.example1.com** は、末尾が**.example1.com** で終わるすべての名前と一致します。

4.2.2 Add/Modify an FQDN（FQDN の追加/変更）

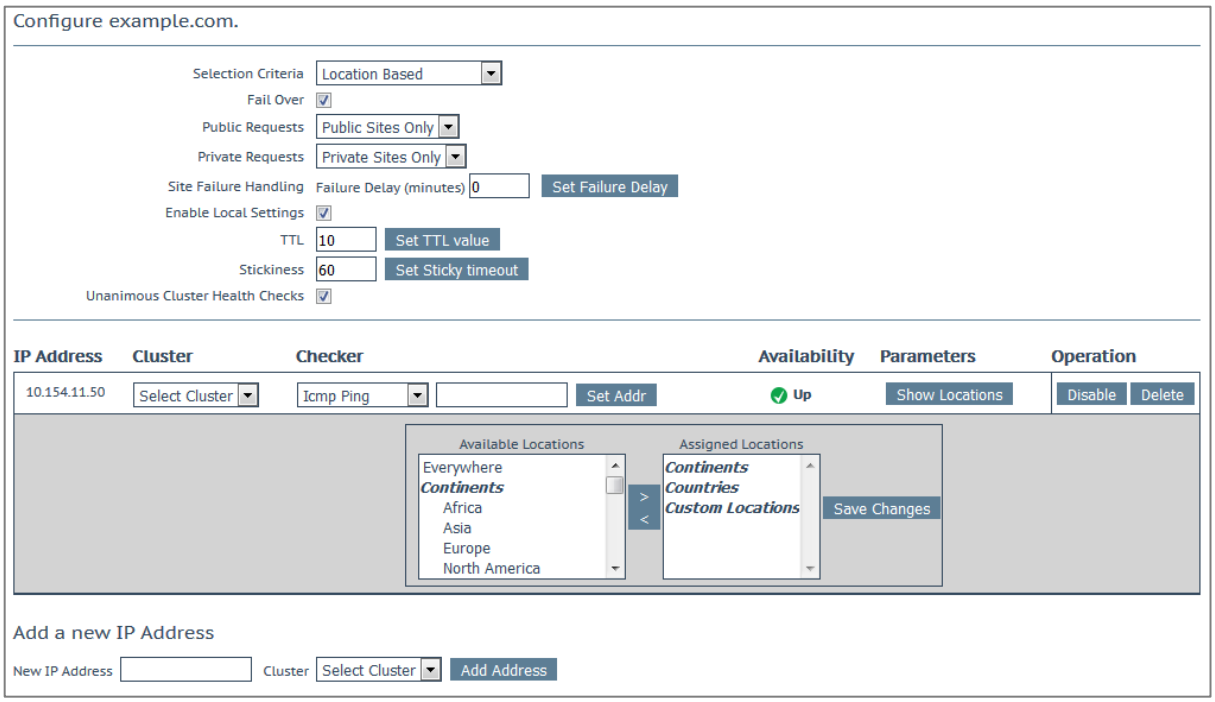

図 4-3:FQDN の設定

Selection Criteria（選択条件）

解決要求を分配する際に使用される選択条件は、このドロップダウンリストから選択できます。利用可能な Selection Criteria は、以下のとおりです。

- **Round Robin（ラウンドロビン）** - トラフィックはサーバーファーム（クラスター。利用可能なサーバーと同義）全体に順番に分配されます。
- **Weighted Round Robin（重み付けラウンドロビン）** – 受信した要求は、サーバー単位に事前に割り当てできる静的な重み付けを考慮して、クラスター全体に順番に分配されます。
- **Fixed Weighting（固定重み）** - 他の実サーバーに小さい重みの値が与えられている場合に限定して、最も重みが大きい実サーバーが使用されます。
- **Real Server Load（実サーバーの負荷）** - ロードマスターに用意されているロジックで、設定済みの重み付けとは無関係に、サーバーの状態を一定の間隔でチェックします。
- **Proximity（近接）** – トラフィックはクライアントに最も近接するサイトに分配されます。**"Proximity"（近接）**スケジューリングを使用する場合、GEO データベー

スに基づき新しいパブリックサイトが地理的座標に自動的にマッピングされます。新しいプライベートサイトは 0º0'0"にマッピングされ、期待どおりに機能します。負荷分散を正しく行うには、この座標を正確な値で上書きする必要があります。クライアントの位置は、そのクライアントの IP アドレスによって判定されます。

- **Location Based（位置ベース）** – トラフィックはクライアントに最も近接するサイトに分配されます。サイトの位置は、セットアップ時にサイトの位置（国名や大陸名）を入力することで設定します。クライアントの位置は、そのクライアントの IP アドレスによって判定されます。同じ国コードを持つ複数のサイトがある場合、リクエストは各サイトにラウンドロビン方式で配信されます。
- **All Available** – A、AAAA、ANY クエリリクエストに対し、健全と思われるすべてのターゲットを返します。返されるリストの内容は、**"Public Requests"**および**"Private Requests"**の設定によっても制御されます。
  - **"Public Sites Only"**を選択すると、パブリックアドレスのみリストに含まれます。同様に、**"Private Sites Only"**を選択すると、プライベートアドレスのみリストに含まれます。
  - **"Prefer Public"**を選択すると、利用できるパブリックアドレスが存在しない場合を除き、パブリックアドレスのみリストに含まれます。利用できるパブリックアドレスが存在しない場合、利用可能なプライベートアドレスが存在すれば、そのプライベートアドレスがリストに含まれます。同様に、**"Prefer Private"**を選択すると、利用できるプライベートアドレスが存在しない場合を除き、プライベートアドレスのみリストに含まれます。利用できるプライベートアドレスが存在しない場合、利用可能なパブリックアドレスが存在すれば、そのパブリックアドレスがリストに含まれます。
  - **"All Sites"**を選択すると、利用可能なすべてのアドレスがリストに含まれます。

  このオプションは、推奨アドレスが利用可能な場合に、そのアドレスのリストを提供するためのものです。推奨アドレスが利用できない場合、可用性を高めるために、フェイルバック手段として非推奨アドレスのリストが提供されます。

Fail Over（フェイルオーバー）

"Fail Over"オプションは、**"Selection Criteria"**が**"Location Based"**に設定されている場合のみ利用できます。**"Fail Over"**オプションが有効な場合に、特定の地域からリクエストが送信されてそのターゲットが停止していると、その接続はフェイルオーバーされ、階層の次のレベルにて応答が行われます。それが不可能な場合は、最も近い（近接の）ターゲットが応答が行います。それが不可能な場合は、最も少ないリクエストを持つターゲットが選択されます。**"Fail Over"**の設定はすべてのターゲットに影響を与えます。

パブリックリクエスト/プライベートリクエスト

バージョン 7.1-30 において、**"Isolate Public/Private Sites"（パブリック/プライベートサイトを隔離する）**の設定が拡張されました。チェックボックスは 2 つの独立したドロップダウンメニューに移行され、DNS の応答をより細かく制御できるようになりました。これまでの動作はそのまま残され、現在の設定がそのまま引き継がれます。そのため、DNS の応答は何も変わりません。

この新しい設定を使用すると、管理者は、設定された FQDN に対する DNS の応答をより細かく制御できます。管理者は、クライアントがパブリック IP とプライベート IP のどちらから来たかに応じて、パブリックとプライベートのいずれかを選択して応答できます。例えば、管理者はプライベートなクライアントのみプライベートなサイトに転送することができます。

以下の表に、各設定と設定可能な値の概要を示します。

設定	値	クライアントの種類	許容されるサイトの種類
パブリックリクエスト	パブリックのみ	パブリック	パブリック
	パブリックを推奨	パブリック	パブリック。パブリックが存在しない場合はプライベート
	プライベートを推奨	パブリック	プライベート。プライベートが存在しない場合はパブリック
	すべてのサイト	パブリック	プライベートおよびパブリック
プライベートリクエスト	プライベートのみ	プライベート	プライベート
	プライベートを推奨	プライベート	プライベート。プライベートが存在しない場合はパブリック
	パブリックを推奨	プライベート	パブリック。パブリックが存在しない場合はプライベート
	すべてのサイト	プライベート	プライベートおよびパブリック

表 4-1:パブリック/プライベートリクエストの設定

この方法によりプライベート IP アドレスの情報を公開で問い合わせると、ネットワークの情報が公開される可能性があります。この設定はご自身の責任において選択してください。

Site Failure Handling（サイト障害時の処理）

デフォルトでは、フェイルオーバーが自動的に実行されます。ただし、複数サイトにまたがる Exchange 2010 構成など、環境によっては、このような処理は最適ではなく、異なる処理が必要になる場合があります。**"Failure Delay"**は分単位で設定します。**"Failure Delay"**を設定すると、**"Site Recovery Mode"**という新しいオプションが利用可能になります。

Site Recovery Mode（サイト復旧モード）

このオプションは、**"Failure Delay"**を設定した場合のみ利用できます。2 つのオプションが用意されています。

- **Automatic（自動）**:復旧すると直ちにサイトの動作が開始されます。
- **Manual（手動）**:サイトに障害が発生するとそのサイトは無効になります。通常動作に復旧するには手動の作業が必要になります。

Enable Local Settings（ローカルの設定を有効にする）

このオプションを選択すると、**"TTL"**と**"Stickiness"**の 2 つのフィールドが新たに表示されます。これらのフィールドは、FQDN 用の設定またはグローバルな設定として指定できます。FQDN 用に設定するには、ローカルの設定を有効にし、必要に応じてローカルの設定を行う必要があります。FQDN 用の設定では、FQDN 作成時にデフォルトでグローバル設定の値が使用されます。

TTL

有効期限（"TTL"）の値は、他の DNS サーバーやクライアントデバイスで GEO ロードマスターからのリプライをキャッシュ可能な期間を規定します。この期間は、秒単位で定義します。この値は、可能な限り小さく設定する必要があります。このフィールドのデフォルト値は 10 です。有効な値の範囲は **1～86400** です。

Stickiness（持続性）

"Stickiness"（持続性。パーシステンス）は、指定した時間が経過するまで、個別のクライアントからのあらゆる名前解決要求を同じリソースに送信可能にするプロパティです。Stickiness（持続性）の詳細については、**パケットトレースガイド　テクニカルノート**を参照してください。

Unanimous Cluster Health Checks（全部一致方式のクラスターヘルスチェック）

このオプションを有効にした場合、いずれかの IP アドレスのヘルスチェックに失敗すると、同じクラスターに属する他の FQDN IP アドレスも停止中であるとマークされます。**"Unanimous Cluster Health Checks"**を有効にすると、特定の FQDN 内にある同じクラスターに属する IP アドレスは、すべて稼働中またはすべて停止中のいずれかになります。例えば、**example.com** が、クラスター**cl58** に属するアドレスとして、172.21.58.101、172.21.58.102、172.21.58.103 を持っていたとします。

- 172.21.58.101 のチェックに失敗すると、全部一致の方針により、172.21.58.102 および 172.21.58.103 も停止中となります。
- 172.21.58.101 が復帰すると、全部一致の方針により、172.21.58.102 および 172.21.58.103 も復帰します。

そのため、常に、3 つのアドレスすべてが利用可能であるか、3 つのアドレスすべてが停止中であるかのいずれかになります。

これと同じ方式が、手動復帰を伴うサイト障害にも適用されます。手動復帰を行うと、チェックに失敗したアドレスが無効になります。これにより、管理者は、問題を修正してからそのアドレスを再度有効にすることができます。**"Unanimous Cluster Health Checks"**を有効にすると、この 3 つのアドレスがすべて無効になります。

全部一致の方針では、無効化されたアドレスは無視されます。そのため、あるアドレスが停止していることが分かっており、何らかの理由でそれと同じクラスターに属する他のアドレスを使用したい場合、障害が発生しているアドレスを停止することで、そのクラスター内にある他のアドレスが全部一致の方針により強制的に停止させられないようにすることができます。

"Unanimous Cluster Health Checks"を有効にすると、設定によっては、FQDN のアドレスが強制的に停止させられたり、バックアップ状態になったりする場合があります。例えば、アドレスが強制的に停止させられ、全部一致の方針が適用されている間にそのアドレスをクラスターから外すと、そのアドレスはバックアップ状態になります。同様に、全部一致の方針が適用されているクラスターにアドレスを追加し、そのクラスターのいずれかのアドレスが停止している場合、新たに追加したアドレスが強制的に停止させら

れます。この状態変化は直ちに発生しない場合がありますが、次のヘルスチェック実行時には発生します。

ヘルスチェックが設定されているアドレスと、**"Checker"**が**"None"**に設定されているアドレスが混在している場合、ヘルスチェックが設定されていないアドレスは強制的に停止させられませんが、**"Site Recovery Mode"**が**"Manual"**に設定されていると強制的に無効になります。例えば、以下の 3 つのアドレスがあったとします。

- **"Checker"**が**"Cluster Checks"**に設定されている 172.21.58.101
- **"Checker"**が**"Cluster Checks"**に設定されている 172.21.58.102
- **"Checker"**が**"None"**に設定されている 172.21.58.103

サイトの障害処理がオフまたは自動の場合、172.21.58.101 に障害が発生すると、172.21.58.102 は強制的に停止させられますが、172.21.58.103 は稼働中のままとなります。その理由は、172.21.58.103 のヘルスチェックを行いたくない場合、このアドレスは稼働中とする必要があるためです。

ただし、**"Site Recovery Mode"**が**"Manual"**に設定されている場合、172.21.58.101 に障害が発生すると、172.21.58.101 とともに 172.21.58.102 と 172.21.58.103 も無効になります。サイト復帰時は、ヘルスチェックが設定されていないアドレスが含まれている場合でも、すべてのアドレスが無効になります。これは、システム管理者が問題を修正するまで、問題のあるデータセンターからトラフィックを遠ざけるためです。この場合、稼働中のアドレスも無効にできるため、ヘルスチェックが設定されていないアドレスが存在しても矛盾は生じません。

Cluster（クラスター）

必要に応じて、IP アドレスを含むクラスターを選択できます。

Checker（チェッカー）

実行するヘルスチェックのタイプを定義します。オプションには、以下の種類があります。

- **None（なし）:**現在の FQDN に関連するマシン（IP アドレス）の健全性をチェックするためのヘルスチェックを行わないことを意味します。
- **ICMP Ping:**IP アドレスに Ping を送信することで健全性をテストします。
- **TCP Connect（TCP 接続）:**指定したポートにて IP アドレスへの接続を試みることで健全性をテストします。
- **Cluster Checks（クラスターチェック）:**このオプションを選択すると、選択したクラスターに関連する手法を用いて健全性がチェックされます。

- **"Slection Criteria"**として**"Real Server Load"**が使用されており、クラスターの**"Type"**が**"Local LM"**または**"Remote LM"**に設定されている場合、**"Mapping Menu"**ドロップダウンリストが表示されます。**"Mapping Menu"**ドロップダウンリストには、そのロードマスターからの仮想サービスの IP アドレスのリストが表示されます。ここには、ポートを持たない各仮想サービスの IP アドレス、および仮想 IP アドレスとポートのすべての組み合わせがリストされます。このマッピングに割り当てられている仮想 IP アドレスを選択してください。
  ポートをもたない仮想サービスを選択した場合、選択したアドレスと同じ IP アドレスをもつすべての仮想サービスがヘルスチェックによりチェックされます。仮想サービスのいずれかが"UP"（稼働中）の状態であった場合、FQDN は"UP"と表示されます。このとき、ポートは考慮されません。
  ポートをもつ仮想サービスを選択した場合、FQDN の健全性を更新するときにその仮想サービスの健全性のみチェックされます。

ヘルスチェックの詳細については、**GEO Sticky DNS　機能説明**を参照してください。

Parameters（パラメータ）

Selection Criteria のパラメータは、このセクションで設定および変更できます。パラメータの種類は、以下で説明するように、使用する **Selection Criteria** に応じて異なります。

- **Round Robin（ラウンドロビン）** – 利用可能なパラメータなし
- **Weighted Round Robin（重み付けラウンドロビン）** – IP アドレスの重みは、"Weight"テキストボックスの値を変更して、**"Set Weight"**ボタンをクリックすることで設定可能
- **Fixed Weighting（固定重み）** – IP アドレスの重みは、**"Weight"**テキストボックスで設定可能
- **Real Server Load（実サーバーの負荷）** – IP アドレスの重みは、**"Weight"**テキストボックスで設定可能であり、測定対象の仮想サービスは**"Mapping"**フィールドから選択可能
- **Proximity （近接）** – IP アドレスの物理的な位置は**"Show Coordinates"（座標を表示）**ボタンをクリックすることで設定可能
- **Location Based（位置ベース）** – IP アドレスに関連付ける位置は**"Show Locations"**ボタンをクリックすることで設定可能

Delete IP address（IP アドレスの削除）

IP アドレスを削除するには、該当する IP アドレスの**"Operation"**列で"Delete"ボタンをクリックします。

Delete FQDN（FQDN の削除）

FQDN を削除するには、**"Modify (Configure) FQDN"**画面の下部にある"Delete"ボタンをクリックします。

4.3クラスターの管理

GEO クラスターは、主にデータセンター内で使用される機能です。FQDN に関連するマシン（IP アドレス）上でヘルスチェックが行われますが、マシンそのものではなく、そのマシンを含むクラスターサーバーを用いてヘルスチェックが行われます。

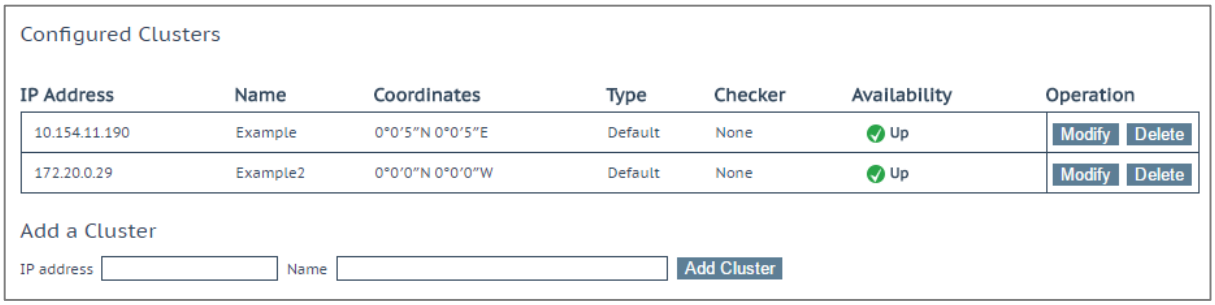

図 4-4:設定済みのクラスター

"Manage Clusters"画面には、クラスターの**"Add"**、**"Modify"**、および**"Delete"**オプションが用意されています。

4.3.1 Add a Cluster（クラスターの追加）

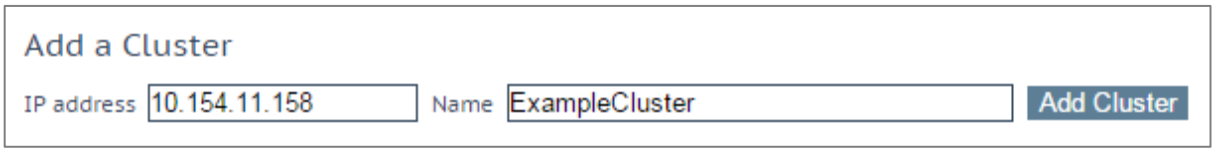

図 4-5:クラスターの追加

クラスターを追加する場合は、以下の 2 つのテキストボックスに入力する必要があります。

- **IP address（IP アドレス）** – クラスターの IP アドレス。
- **Name（名前）** – クラスターの名前。この名前は、他の画面でクラスターを識別する目的で使用できます。

4.3.2 Modify a Cluster（クラスターの変更）

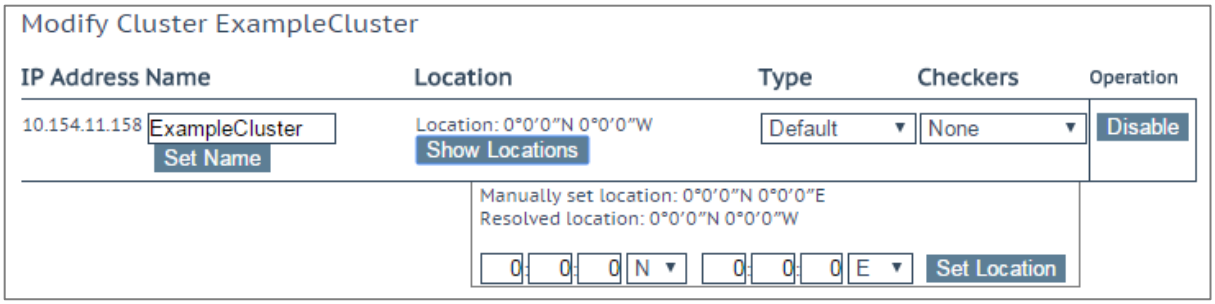

図 4-6:クラスターの変更

Name（名前）

クラスターの名前。

Location（位置）

必要に応じて、**"Show Locations"**ボタンをクリックし、IP アドレスの位置を示す緯度と経度を入力します。

Type（タイプ）

クラスターのタイプとして、**"Default"**、**"Remote LM"**、**または"Local LM"**を選択できます。

- **Default（デフォルト）**:クラスタータイプを"Default"に設定すると、利用可能な以下の 3 つのヘルスチェックのいずれかを使用して、クラスターに対するヘルスチェックが行われます。
  - **None（なし）**:ヘルスチェックは行われません。そのため、マシンは常に稼働中であるように見えます。
  - **ICMP Ping**:クラスターの IP アドレスに Ping を送信することでヘルスチェックが行われます。
  - **TCP Connect（TCP 接続）**:指定したポートにてクラスターの IP アドレスに接続することでヘルスチェックが行われます。
- **Local LM（ローカル LM）**:"Type"として**"Local LM"**を選択すると、**"Checkers"**フィールドは自動的に**"Not Needed"**に設定されます。これは、クラスターがローカルマシンであるため、ヘルスチェックが必要ないためです。
- **Remote LM（リモート LM）**:このタイプのクラスターのヘルスチェックは **"Implicit"（暗黙）**です（ヘルスチェックは SSH により行われます）。

"Remote LM"と**"Local LM"**の唯一の違いは、"Local LM"では TCP 接続に関する情報を TCP 経由ではなくローカルで取得するため、"Local LM"では TCP 接続が保存されるという点にあります。それ以外については両者の機能は同じです。

Checkers（チェッカー）

クラスターのステータスをチェックする目的で使用するヘルスチェック方式。

"Type"が**"Default"**に設定されている場合、利用可能なヘルスチェック方式は、**"ICMP Ping"**および**"TCP Connect"**です。

"Remote LM"または**"Local LM"**が**"Type"**として選択されている場合、"Checkers"ドロップダウンリストは使用できません。

Disable（無効）

必要に応じて、**"Operation"**列の**"Disable"**ボタンをクリックすることで、クラスターを無効にできます。

4.3.3 Delete a Cluster（クラスターの削除）

クラスターを削除するには、該当するクラスターの"Operation"列で"Delete"ボタンをクリックします。

"Delete"機能の使用時は、十分に注意してください。この削除処理を元に戻す方法はありません。

4.3.4 GEO クラスターのアップグレード

GEO クラスターをアップグレードする場合、すべてのノードを同時にアップグレードすることを強く推奨します。GEO クラスターはアクティブ/アクティブモードで動作するため、同時にアップグレードすることで、すべてのノードで整合性のとれた動作が保証されます。

異なるバージョンが混在した GEO クラスターを動作させる場合、最も新しいバージョンからすべての変更を行うようにしてください。これにより、互換性のない設定によって設定が失われてしまうのを防ぎます。また、古いバージョンでは用意されていない設定オプションに変更すると、動作の整合性が失われます。

4.4その他のパラメータ

"Miscellaneous Params"メニューオプションに含まれているセクションおよびフィールドについて、以下で説明します。

4.4.1 Source of Authority（権限ソース）

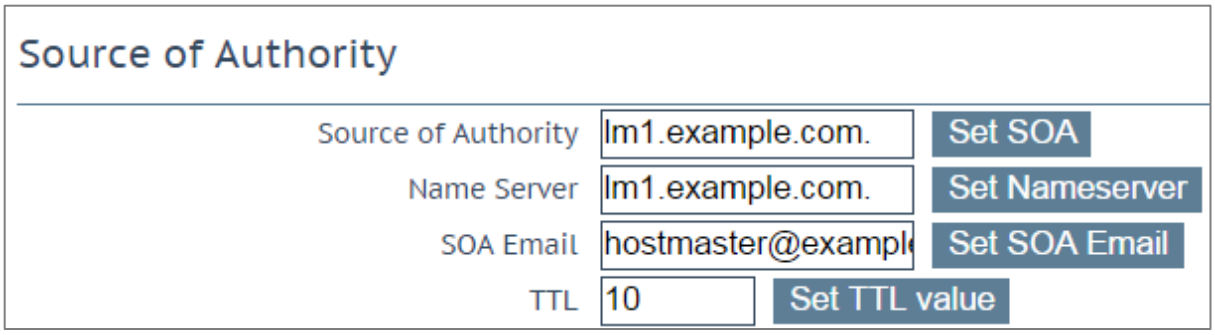

図 4-7:権限ソース

Source of Authority（権限ソース）

この項目は、RFC 1035 で定義されています。SOA は、ゾーン（ドメイン）のグローバルなパラメータを定義します。ゾーンファイルで許可される SOA レコードは 1 つだけです。

Name Server（ネームサーバー）

"Name Server"はトップレベル DNS に設定されるフォワード DNS エントリとして定義され、完全修飾ドメイン名（FQDN と末尾のピリオド。たとえば、**lm1.example.com**）として書き込まれます。

HA 構成の事例のように、複数の Name Server が存在する場合、2 番目の Name Server もスペースで区切ってフィールドに追加する必要があります（たとえば、**lm1.example.com lm2.example.com**）。

SOA Email（SOA Email アドレス）

このテキストボックスは、"@"を"."に変換して、このゾーンを処理するユーザーまたはロールアカウントのメールアドレスを発行する目的で使用します。ベストプラクティスとして、専用のメールエイリアスを定義（および保持）することを推奨します。たとえば、DNS 操作用の"hostmaster" [RFC 2142]の場合、**hostmaster@example.com** です。

TTL

有効期限（"TTL"）の値は、他の DNS サーバーやクライアントデバイスで GEO ロードマスターからのリプライをキャッシュ可能な期間を規定します。この値は、可能な限り小さく設定する必要があります。このフィールドのデフォルト値は 10 です。この期間は、秒単位で定義します。

4.4.2 リソースチェックのパラメータ

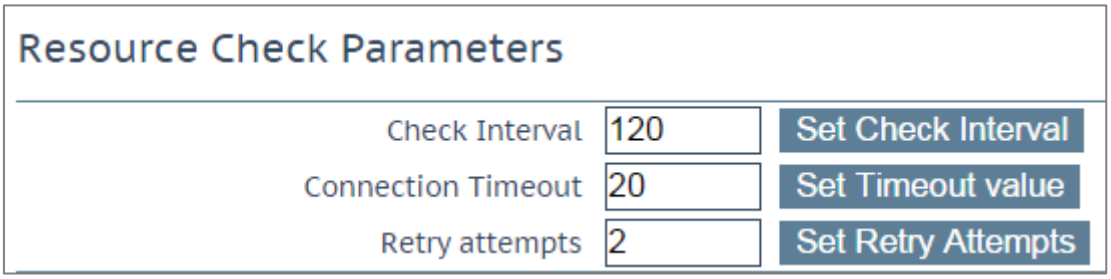

図 4-8:リソースチェックのパラメータ

Check Interval（チェック間隔）

ヘルスチェックの遅延間隔を秒単位で定義します。これには、クラスターと FQDN が含まれます。このフィールドの有効範囲は 9～3600 です。デフォルトは **120** です。

インターバルの値は、タイムアウト値とリトライ値の積より大きくなければなりません（インターバル＞タイムアウト×リトライ＋1）。これは、現在のヘルスチェックが完了する前に次のヘルスチェックが開始されないようにするためです。

タイムアウト値またはリトライ値を増やしてこのルールが破られた場合、インターバルの値が自動的に増やされます。

Connection Timeout（接続タイムアウト）

秒単位で定義します。この値は、ヘルスチェックに対するリプライの最大許容待ち時間です。このフィールドの有効範囲は 4～60 です。デフォルトは **20** です。

Retry Attempts（再試行回数）

ダウン状態として記録され、正常に動作している実サーバーのリストから削除されるまでに許容される、ヘルスチェックの連続失敗回数です。デフォルトの再試行回数は 2 です。

FQDN の障害クラスターの最大検出期間は、 **"Check Interval"** + （**"Connection Timeout"** * （**"Retry attempts"** + 1）） です。概して、最大期間はこの半分です。

以下に、リソース IP が追加または有効化されてから、それが停止して再度復帰するまでのタイムラインの図を示します。

1. リソース IP が有効化/追加されると、ロードマスターにより ICMP 要求がリソース IP へ送信されます。このリソースが応答すると仮定して、このリソースは稼働中とマークされます。
2. 120 秒経過後（**"Check Interval"**のデフォルト値）、ICMP 要求がリソース IP に送信されます。20 秒（**"Connection Timeout"**のデフォルト値）が経過してもこの IP から応答がない場合、ロードマスターは最大 2 回（**"Retry Attempts"**のデフォルト値）までさらに要求を送信し、それぞれ 20 秒間待ちます。これら 3 回の要求に対して何も応答がない場合、このリソースは停止中とマークされ、**"Check Interval "**タイマーがリセットされます。
3. 120 秒経過後、ロードマスターは、このリソース IP への ICMP 要求の送信を試みます。このリソースが復帰し、**"Connection Timeout"**の時間が経過する前に応答が返された場合、ロードマスターはこのリソースを稼働中とマークし、**"Check Interval"**タイマーをリセットします。

図 4-9:リソースチェックのタイミング図

4.4.3 Stickiness（持続性）

図 4-10:スティッキネス

"Stickiness"（持続性。グローバルなパーシステンス）は、指定した時間が経過するまで、個別のクライアントからのあらゆる名前解決要求を同じリソースに送信可能にするプロパティです。**Stickiness（持続性）**の詳細については、**パケットトレースガイド　テクニカルノート**を参照してください。

4.4.4 Location Data Update（位置データ更新）

図 4-11:位置データ更新

位置パッチには、位置データに対して地理的にエンコードされた IP アドレスが含まれています。データファイルは、通常のサポートチャンネル経由で KEMP から直接入手できます。この一連のファイルは、Maxmind の GeoIP データベースを再パッケージしたディストリビューションです。最新のリリースを入手するには、http://www.kemptechnologies.com からサポートにお問い合わせください。

4.5IP 範囲の選択条件

図 4-12:新規 IP アドレスの追加

このセクションでは、新しい IP アドレス範囲を定義できます。

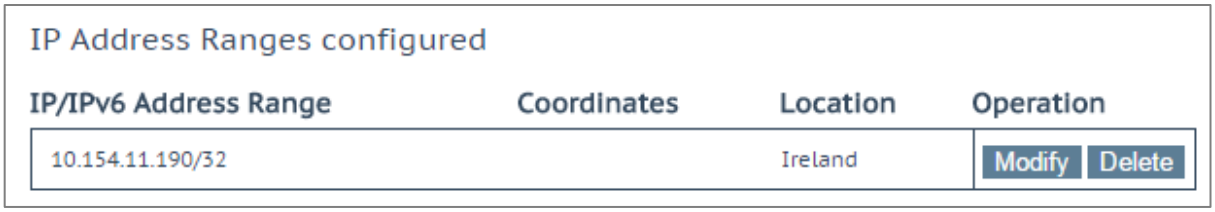

図 4-13:設定された IP アドレス範囲

アドレスを追加後、"Modify"をクリックすると、設定編集画面が表示されます。アドレス範囲を追加後に、そのアドレス範囲を削除することもできます。

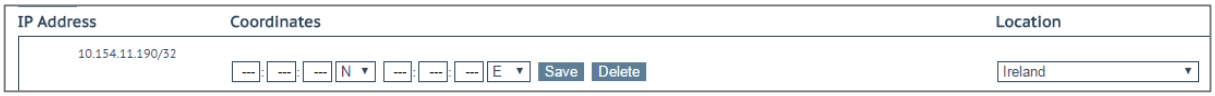

図 4-14:IP 範囲の選択条件

このセクションでは、データセンターごとに最大 64 個の IP 範囲を定義できます。

IP Address（IP アドレス）

IP アドレスまたはネットワークを指定します。ここで有効なエントリは、単一の IP（たとえば、**192.168.0.1**）または Classless Inter-Domain Routing（CIDR）フォーマットのネットワーク（たとえば、**192.168.0.0/24**）です。

Coordinates（座標）

位置を示す緯度と経度を入力します。

Location（位置）

アドレスに割り当てる位置を指定します。

図 4-15:カスタムロケーションの追加

Add Custom Location（カスタムロケーションの追加）

このセクションでは、カスタムロケーションを追加できます。

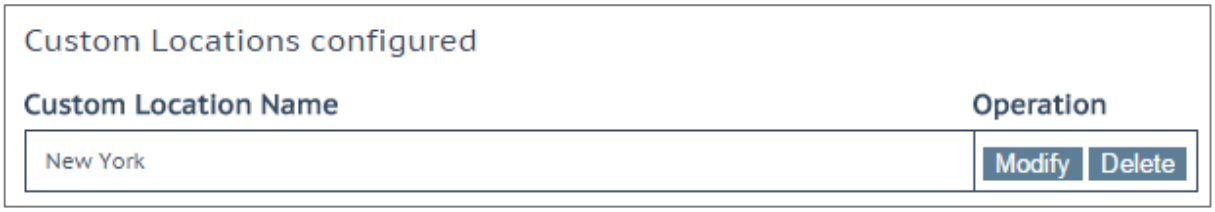

図 4-16:設定されたカスタムロケーション

このセクションでは、カスタムロケーションの編集と削除も行えます。

4.6IP ブラックリストの設定

KEMP からブラックリストをダウンロードして、ブラックリストに登録されている IP アドレスへのアクセスをブロックできます。ホワイトリストは手動で指定できます。ホワイトリストはブラックリストより優先されます。

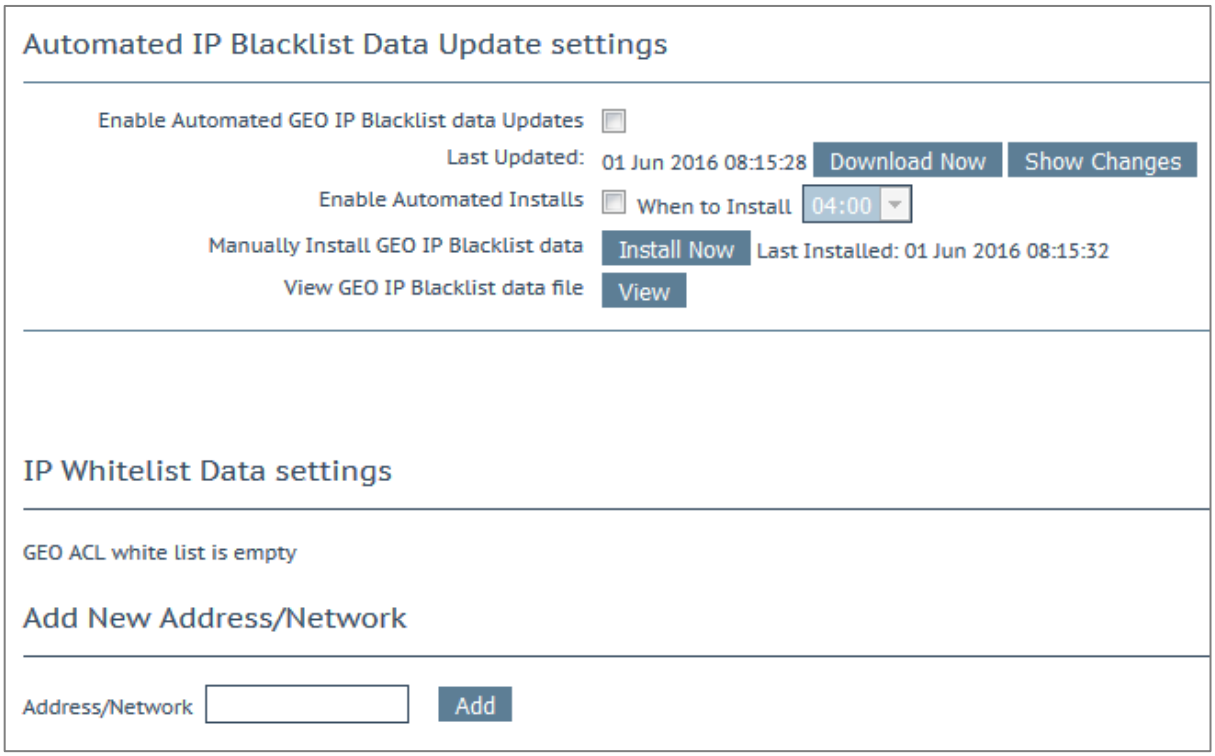

図 4-17:GEO IP ブラックリスト設定の管理

Enable Automated GEO IP Blacklist data Updates（GEO IP ブラックリストデータの自動更新を有効にする）

このオプションを有効にすると、GEO IP ブラックリストに対する更新データが毎日ダウンロードされます。デフォルトでは、このオプションは無効になっています。

Last Updated（最新更新日）

最新の更新データがダウンロードされた日付が表示されます。GEO ブラックリストデータが 7 日より前のものである場合、通知メッセージが表示されます。

Download Now（直ちにダウンロード）

このボタンをクリックすると、更新データが直ちにダウンロードされます。

Enable Automated Installs（自動インストールの有効化）

このチェックボックスをオンにすると、指定した時刻に最新のルールが毎日自動的にインストールされます。

When to Install（インストール時刻）

毎日何時に最新のルールをインストールするか選択します。

Manually Install GEO IP Blacklist data（GEO IP ブラックリストデータの手動インストール）

このボタンを使用すると、更新データを手動でインストールできます。またこのセクションでは、更新データの最終インストール日が表示されます。GEO ブラックリストデータが 7 日以上更新されない場合、通知メッセージが表示されます。

View GEO IP Blacklist data file（GEO IP ブラックリストデータファイルの表示）

"View"ボタンをクリックすると、現在の GEO IP ブラックリストデータファイルが表示されます。

IP Whitelist Data Settings（IP ホワイトリストデータの設定）

このセクションには、ホワイトリストに現在登録されている IP アドレスが表示されます。

Add New Address/Network（アドレス/ネットワークの新規追加）

このセクションでは、新しいアドレスとネットワークをホワイトリストに追加できます。ホワイトリストはブラックリストより優先されます。

5 Statistics（統計情報）

5.1実サーバーの統計情報

システム（**"Global"（グローバル）**）、**"Real Servers"（実サーバー）**、**"Virtual Services"（仮想サービス）**、WAF におけるロードマスターの動作状態を表示します。

5.1.1 Global（システム統計）

図 5-1:統計

Total CPU Activity（合計 CPU アクティビティ）

このグラフは、ロードマスターの以下の CPU 使用率を表示します。

統計	説明
User（ユーザー）	ユーザーモードでの処理に消費された CPU のパーセンテージ
System（システム）	システムモードでの処理に消費された CPU のパーセンテージ
Idle（アイドル）	アイドル状態の CPU のパーセンテージ

統計	説明
I/O Waiting（I/O 待ち）	I/O 処理の完了待ち時に使用された CPU のパーセンテージ

この 4 つのパーセンテージの合計は 100%になります。

Core Temperatures（コア温度）:ロードマスターハードウェア機器の各 CPU コアの温度が表示されます。仮想アプライアンス型ロードマスターの統計画面には CPU 温度は表示されません。

CPU Details（CPU 詳細）:各 CPU の統計情報を取得するには、**"CPU Details"（CPU 詳細）**にて目的の番号ボタンをクリックします。

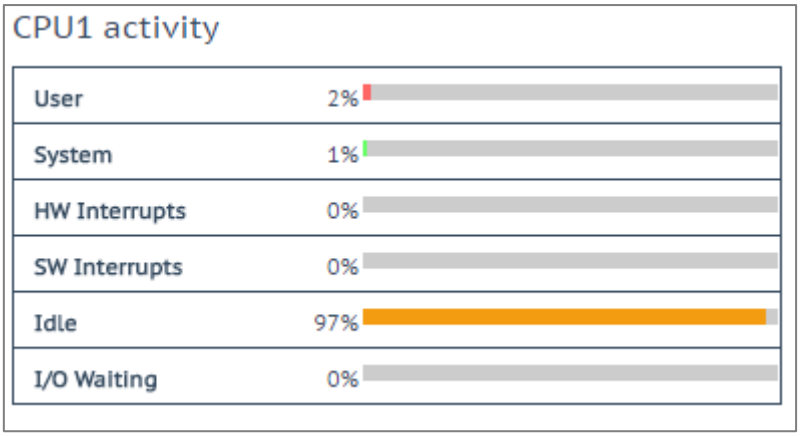

図 5-2:CPU の統計情報

CPU 詳細には、**"HW Interrupts"（ハードウェア割り込み）**と**"SW Interrupts"（ソフトウェア割り込み）**の 2 つの統計情報が追加で表示されます。

Memory usage（メモリ使用率）

この棒グラフには、メモリの使用容量と空き容量が表示されます。

Network activity（ネットワークアクティビティ）

この棒グラフは、各インターフェイスのネットワーク・スループットを示します。

5.1.2 実サーバー

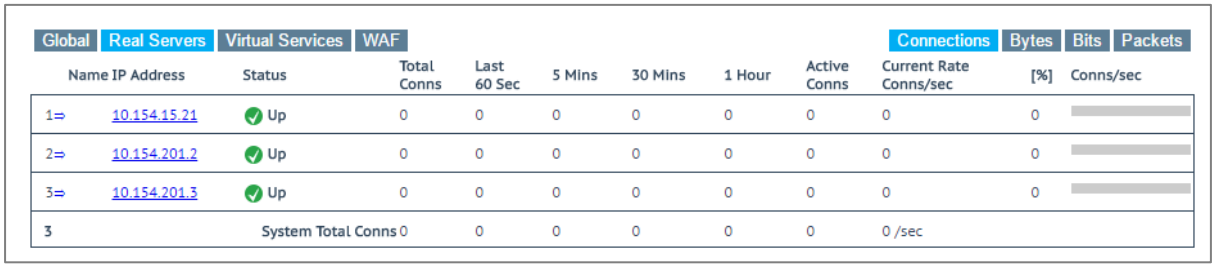

図 5-3:実サーバー統計情報画面のセクション

このグラフには、選択した項目に応じて、接続数、バイト数、ビット数、またはパケット数が表示されます。ページの右上にあるボタンをクリックすると、表示される値が切り替わります。実サーバーに対して表示されている値は、実サーバーにアクセスしているすべての仮想サービスの値を表しています。

実サーバーが複数の仮想サービスに割り当てられている場合、最初の列に表示されている番号の右側にある矢印（⇒）をクリックすると、各実サーバーの統計情報を仮想サービスごとに参照できます。この矢印をクリックするとビューが展開され、その実サーバーが割り当てられている各仮想サービスの統計情報が表示されます。

暗号化されたサービスの実装方式の関係上、暗号化された仮想サービスのパケットに関する統計情報は参照できません。

Name（名前）:"Name"列は DNS ルックアップに基づいて自動的に設定されます。

RS-IP:この列には、実サーバーの IP アドレス、および仮想サービス（列を展開すると表示される）が表示されます。

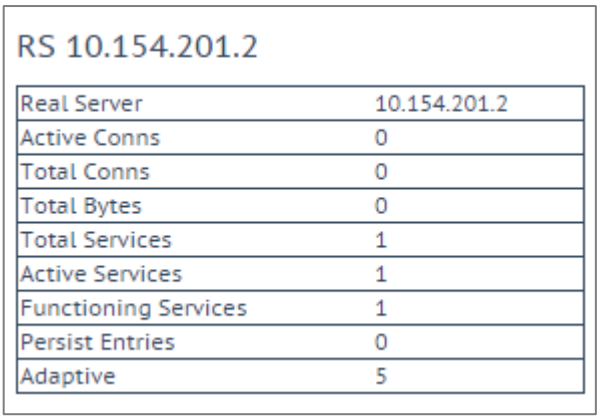

図 5-4:実サーバーの統計情報

"RS-IP"（実サーバーの IP）列のリンクをクリックすると、新たな画面が開き、その実サーバーに関する各種統計情報が表示されます。

Status（ステータス）:実サーバーの状態が表示されます。

Adaptive（アダプティブ）:このオプションは、仮想サービスに対してアダプティブスケジューリング方式が選択されている場合のみ表示されます。この列にはアダプティブ値が表示されます。

Weight（重み）:このオプションは、仮想サービスのスケジューリング方式が**"resource based (SDN adaptive)"（リソースベース（SDN アダプティブ））**に設定されている場合のみ表示されます。コントローラーから収集された情報により、**"Adaptive"（アダプティブ）**値をどのように設定するかが決定されます。アダプティブ値が上昇すると、実サーバーの重みが低下します。すべてのアダプティブ値が同じ場合、重みはすべて同じになります。アダプティブ値が異なる場合、重みは変化します。実サーバーの重みにより、トラフィックをどこに送信するかが決定されます。複数の仮想サービスにて実サーバーが設定されている場合、重みには 2 つの値が表示されます。1 番目の値は、実サーバーが設定されているすべての仮想サービスにおける現在の重みの平均値を表します。2 番目の値は、実サーバーが設定されている仮想サービスの数を表します。例えば、**"Weight"（重み）**が **972/2** の場合、2 つの仮想サーバーにて設定されている実サーバーの重みの平均値が 972 であることを意味します。

Total Conns（トータルの接続数）:トータルの接続数です。

Last 60 Sec（過去 60 秒間）:過去 60 秒間におけるトータルの接続数

5 Mins（5 分間）:過去 5 分間におけるトータルの接続数

30 Mins（30 分間）:過去 30 分間におけるトータルの接続数

1 Hour（1 時間）:過去 1 時間におけるトータルの接続数

Active Conns（アクティブな接続数）:現在アクティブな接続のトータルの数

Current Rate Conns/sec（現在の接続レート（接続数/秒））:1 秒当たりの現在の接続レート

[%]:1 秒当たりの現在の接続率

Conns/sec（接続数/秒）:1 秒当たりの接続数をグラフ表示したもの

System Total Conns（システムのトータルの接続数）:この行には、各列の合計が表示されます。

5.1.3 仮想サービス

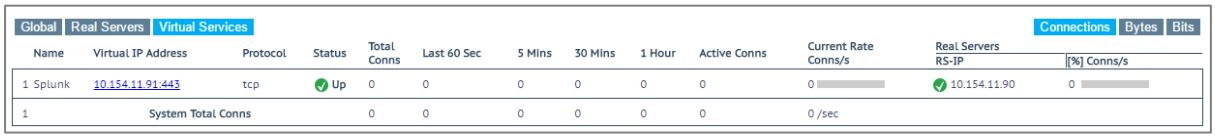

図 5-5:Virtual Services（仮想サービス）

このグラフには、選択した項目に応じて、接続数、バイト数、ビット数、またはパケット数が表示されます。ページの右上にあるボタンをクリックすると、表示される値が切り替わります。仮想サービスの実サーバーに対する分配のパーセンテージが表示されます。

Name（名前）:仮想サービスの名前

Virtual IP Address（仮想 IP アドレス）:仮想サービスの IP アドレスとポート

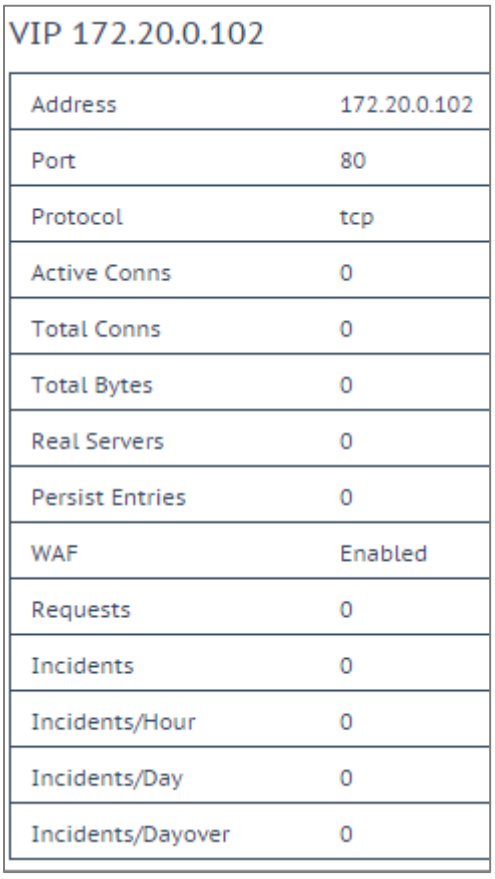

図 5-6:仮想サービスの統計情報

"Virtual IP Address"（仮想 IP アドレス）列のリンクをクリックすると、新たな画面が開き、その仮想サービスに関する各種統計情報が表示されます。

Address（アドレス）:仮想サービスの IP アドレス

Protocol（プロトコル）:仮想サービスのプロトコル **tcp** または **udp** を選択できます。

Active Conns（アクティブな接続数）:現在アクティブな接続のトータルの数

Total Conns（トータルの接続数）:トータルの接続数です。

Total Bytes（トータルのバイト数）:送信されたトータルのバイト数

Real Servers（実サーバー）:この仮想サービスにおけるトータルの実サーバーの数

Persist Entries（パーシステンスエントリ）:入力されたパーシステンスエントリのトータルの数

WAF:仮想サービスで WAF が有効になっている場合、以下に示す他の WAF 統計情報とともに、ステータスが表示されます。

Requests（要求）:WAF により処理されたトータルの要求数（ブロックされたかどうかにかかわらず、すべての要求が表示されます）。各接続につき 2 つの要求が記録されます（1 つは受信要求、1 つは送信要求）。

Incidents（インシデント）:WAF により処理されたトータルのイベント数（ブロックされた要求）

Incidents/Hour（インシデント/時）:現在の時間内（*xx*.00.00 以降）に発生したイベントの数

Incidents/Day（インシデント/日）:真夜中（ローカル時刻）以降に発生したイベントの数

Incidents/Dayover（インシデント/1 日あたりの超過数）:1 日のうちに、設定された警報しきい値をイベントカウンターが越えた回数例えば、しきい値が 10 に設定されており、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。警報しきい値は、仮想サービス編集画面の**"WAF Options"**にある**"Hourly Alert Notification Threshold"**フィールドに入力することで、仮想サービスごとに設定できます。詳細は**セクション 3.7** を参照してください。

System Total Conns（システムのトータルの接続数）:この行には、各列の合計が表示されます。

5.1.4 WAF

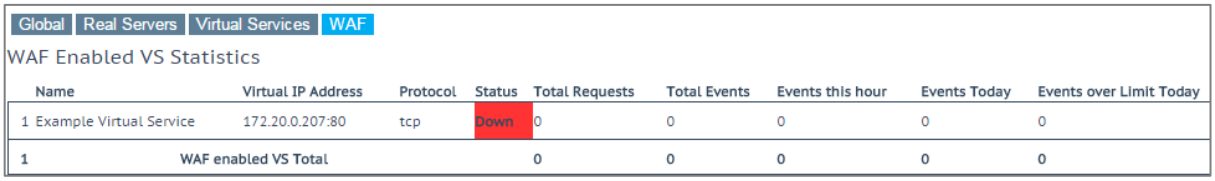

図 5-7:WAF が有効な VS の統計情報

この統計情報は、5～6 秒ごとに更新されます。この画面には、以下の項目が表示されます。

Count（カウント）:一番左の列には、WAF が有効な仮想サービスのトータルの数が表示されます。

Name（名前）:WAF が有効な仮想サービスの名前

Virtual IP Address（仮想 IP アドレス）:仮想サービスの IP アドレスとポート

Protocol（プロトコル）:仮想サービスのプロトコル（TCP または UDP）

Status（ステータス）:仮想サービスの状態取り得るステータスに関する詳細は、**セクション 3.2** を参照してください。

Total Requests（トータルの要求数）:WAF により処理されたトータルの要求数（ブロックされたかどうかにかかわらず、すべての要求が表示されます）。各接続につき 2 つの要求が記録されます（1 つは受信要求、1 つは送信要求）。

Total Events（トータルのイベント数）:WAF により処理されたトータルのイベント数（ブロックされた要求）

Events this hour（現在の時間内のイベント数）:現在の時間内（*xx*.00.00 以降）に発生したイベントの数

Events Today（本日のイベント数）:真夜中（ローカル時刻）以降に発生したイベントの数

Events over Limit Today（上限を超えた本日のイベント数）:1 日のうちに、設定された警報しきい値をイベントカウンターが越えた回数例えば、しきい値が 10 に設定されており、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。警報しきい値は、仮想サービス編集画面の**"WAF Options"**にある**"Hourly Alert Notification Threshold"**フィールドに入力することで、仮想サービスごとに設定できます。詳細は**セクション 3.7** を参照してください。

5.2履歴グラフ

"Historical Graphs"（履歴グラフ）画面には、ロードマスターの統計情報がグラフ表示されます。設定可能なこのグラフには、ロードマスターで処理されているトラフィックの情報が視覚的に表示されます。

各インターフェイスのネットワークアクティビティに関するグラフが用意されています。仮想サービスの全体情報および個別情報に関するグラフや、実サーバーの全体情報および個別情報に関するグラフを表示するオプションも用意されています。

時間の細かさは、**"hour"（時）**、**"day"（日）**、**"month"（月）**、**"quarter"（四半期）**、**"year"（年）**オプションを選択することで指定できます。

インターフェイスのネットワーク活動のグラフでは、**"Packet"（パケット）**、**"Bits"（ビット）**、**"Bytes"（バイト）**オプションを選択することで、使用する測定単位を選択できます。

仮想サービスおよび実サーバーのグラフでは、**"Connections"**、**"Bits"**、**"Bytes"**オプションを選択することで、使用する測定単位の種類を選択できます。

"Virtual Services panel"パネルの設定アイコン  をクリックすると、仮想サービスのどの統計情報を表示するかを設定できます。このアイコンをクリックすると、仮想サービスの設定ウィンドウが表示されます。

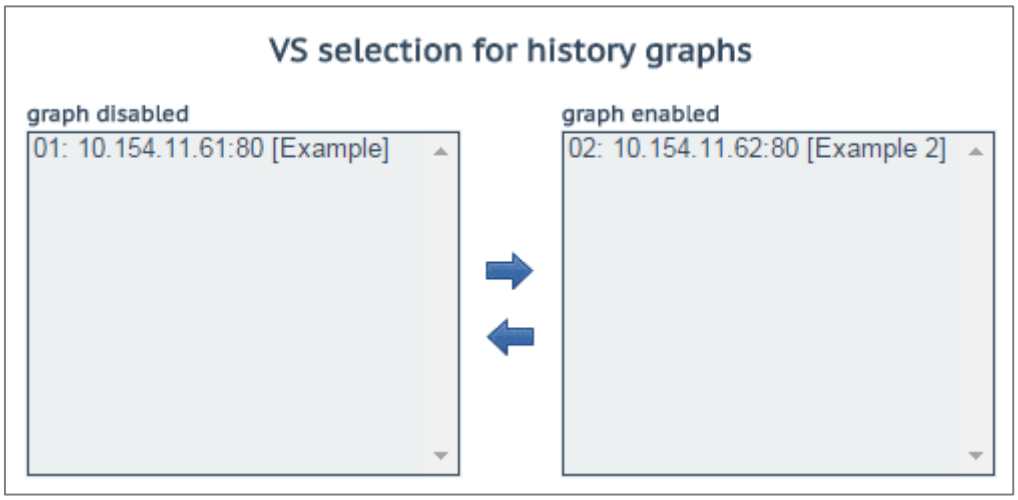

図 5-8:履歴グラフ用の仮想サービス（VS）の選択

このダイアログで、仮想サービスの統計情報表示を追加/削除できます。

"WUI Settings（WUI の設定）"画面の**"Enable Historical Graphs "**チェックボックスをオフにすると、これらのグラフを無効にできます。

最大 5 個の仮想サービスを同時に表示できます。

ダイアログを閉じて変更を適用するには、ウィンドウの✖ボタンをクリックします。

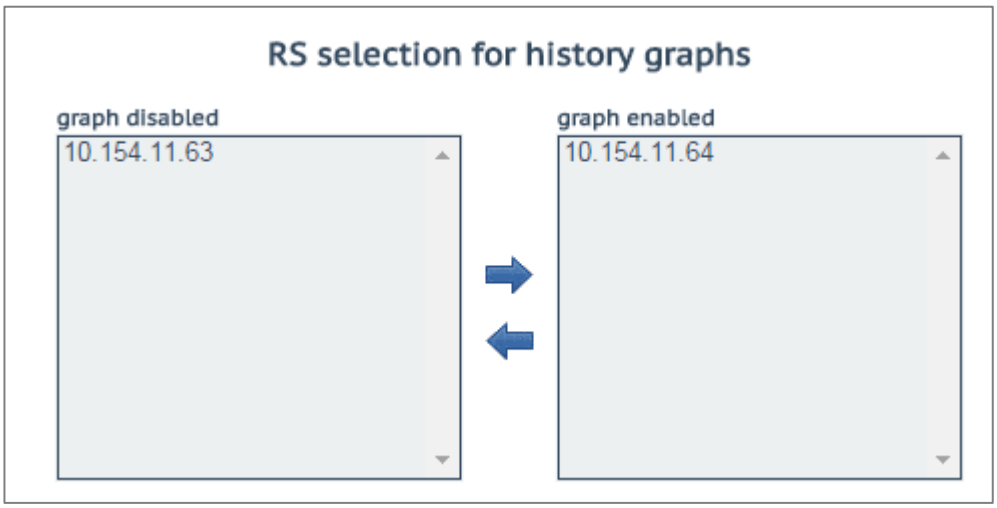

図 5-9:履歴グラフ用の実サーバー（RS）の選択

"Real Servers"パネルの設定アイコン  をクリックすると、どの実サーバーの統計情報を表示するかを設定できます。このアイコンをクリックすると、実サーバー設定ダイアログが別ウインドウで表示されます。

このダイアログで、実サーバーの統計情報表示を追加/削除できます。

最大 5 個の実サーバーを同時に表示できます。

ダイアログを閉じて変更を適用するには、ウィンドウの  ボタンをクリックします。

デフォルトでは、"Statistics"ページに表示されている仮想サービスと実サーバーの統計情報だけが収集および保存されます。仮想サービスと実サーバーの統計情報を表示するには、**"System Configuration > Miscellaneous Options > WUI Settings"**の**"Collect All Statistics"**オプションを有効にします。

> 数多くの仮想サービスや実サーバーの統計情報を収集すると、CPU の使用率が高まるので、このオプションは、デフォルトでは無効になっています。

ロードマスターWUI のグラフは自動的に拡大縮小され、SI 測定単位を用いて表示されます。グラフには、倍率を表す接頭辞が表示されます。そのため、必要に応じて絶対的な値を計算できます。

使用可能な倍率とその接頭辞を以下の表に示します。

記号	接頭辞	倍率
P	ペタ	10^15
T	テラ	10^12
G	ギガ	10^9
M	メガ	10^6
k	キロ	10^3
m	ミリ	10^(-3)
μ	マイクロ	10^(-6)

表 5-1:倍率と接頭辞

絶対的な「実際の」値を計算するには、グラフに表示されている値に倍率を掛けます。

例:

1 秒あたりの接続数のグラフに、倍率"m"とともに 200 という値が表示されています。前記の表に示すように、"m"は「ミリ」を表します。そのため、その時点における 1 秒あたりの接続数の絶対的な値を調べるには、200 という値に倍率 10^(-3)を掛ける必要があります:

- 10^(-3) = 0.001
- 200 x 0.001 = 0.2 コネクション/秒

この計算結果は、1 秒あたりの接続数が 1 未満であることを示しています。接続率が非常に低いため、グラフに絶対的な接続数を表示すると、0 の位置に直線が表示されるだけとなり、有益な情報は何も提供されません。

6 SDN 統計情報

SDN の統計情報を表示するには、ロードマスターWUI メインメニューにて"**Statistics > SDN Statistics**"をクリックします。

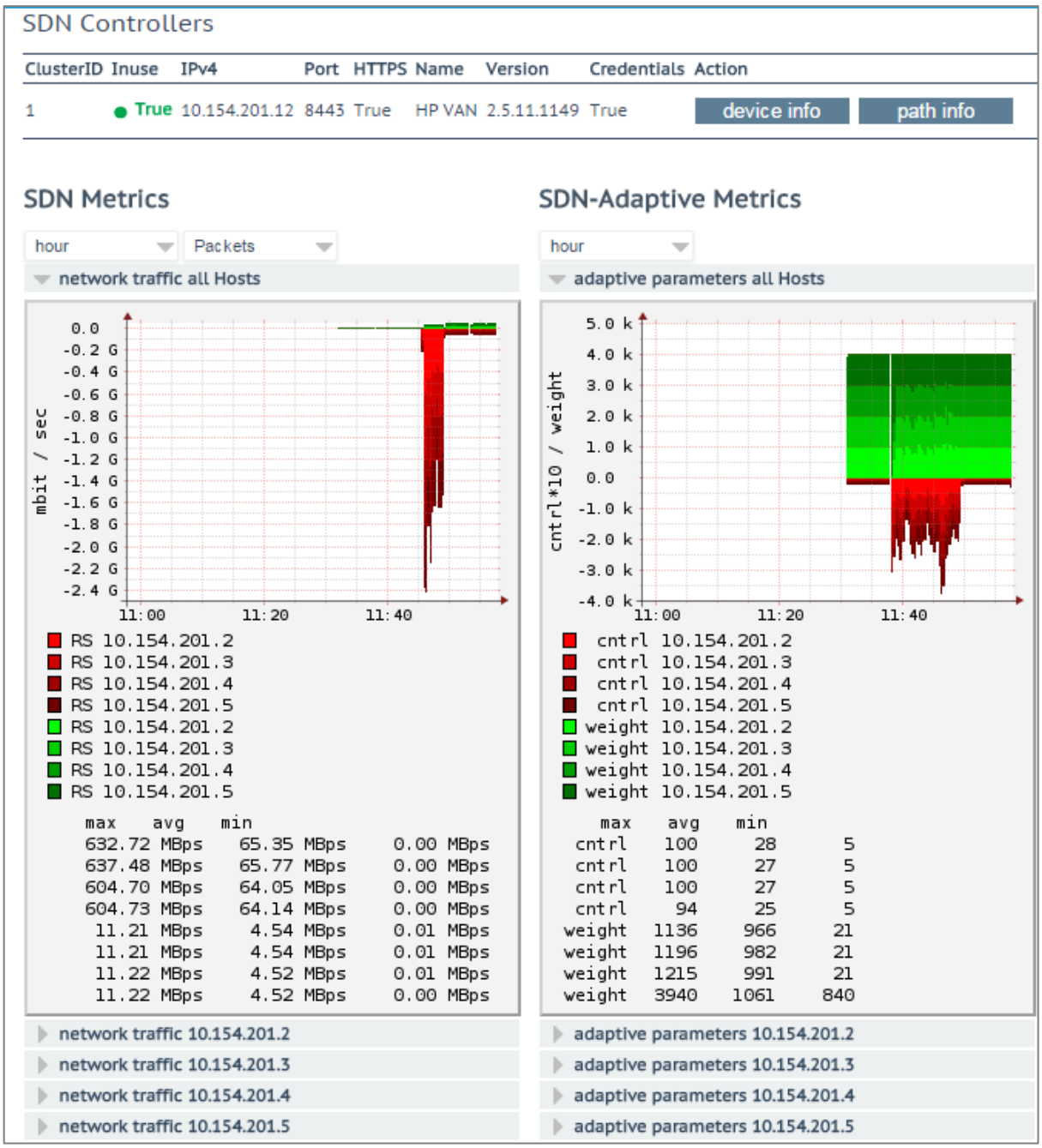

図 6-1:SDN の統計情報

ロードマスターが SDN コントローラーに接続されると、**"Name"（名前）、"Version"（バージョン）、および"Credentials"（証明書）**が表示されます。

Statistics section（統計情報の選択）

SDN コントローラーが追加され、ロードマスターと通信が行われるまで、統計情報は表示されません。**"Name"、"Version"、**および**"Credentials"**が表示されない場合、ロードマスターが SDN コントローラーに接続されていないことを意味します。この場合、設定が間違っているか、SDN コントローラーが停止している可能性があります。

この画面には、ネットワークトラフィックとアダプティブパラメーターの 2 種類の統計情報が表示されます。

- Network traffic（ネットワークトラフィック） - ここには、1 秒あたりに送信されたビット数とバイト数が実サーバーごとに表示されます。1 秒当たりのビット/バイト数の最大値、平均値、最小値が表示されます。
- Adaptive parameters（アダプティブパラメーター） - ここには、アダプティブ値（ctrl）と重みが表示されます。アダプティブ値が上昇すると、実サーバーの重みが低下します。

6.1.1 デバイス情報

UID	Name	Type
00:00:54:9f:35:1c:c5:30	ovsbr0	Default OpenFlow Switch
00:00:66:52:10:5f:fb:45	ovsbr1	Default OpenFlow Switch

図 6-2:デバイス画面のセクション

"device info"（デバイス情報）ボタンをクリックすると、OpenFlow が有効になっているコントローラーのスイッチに関する情報が表示されます。

UID	Name	Type	Vendor	Product
00:00:54:9f:35:1c:c5:30	ovsbr0	Default OpenFlow Switch	Nicira, Inc.	Open vSwitch

	ID	Name	State	Mac
Interface Info	id=0x1	Name:eno1	State:[UP]	Mac:54:9f:35:1c:c5:30
	id=0x4	Name:vnet2	State:[UP]	Mac:fe:54:00:bc:1b:c3
	id=0x7	Name:vnet1	State:[UP]	Mac:fe:54:00:8d:73:9b
	id=0x8	Name:vnet7	State:[UP]	Mac:fe:54:00:b1:4b:3b
	id=0xa	Name:patch-ovsbr0	State:[UP]	Mac:7e:6d:ac:6b:9f:11
	id=0xb	Name:patch-ovsbr3	State:[UP]	Mac:2a:32:8c:e7:4c:5b
	id=0xfffffffe	Name:ovsbr0	State:[UP]	Mac:54:9f:35:1c:c5:30

	ID	VID	Port	Mac
Node Info	10.154.50.25	0	1	00:0c:29:b1:96:46
	10.154.120.62	0	1	00:50:56:b8:13:45
	10.154.190.197	0	1	00:50:56:b8:4d:7d
	10.154.30.80	0	1	00:0c:29:64:83:1b
	10.154.190.104	0	1	00:50:56:b8:e7:31
	10.154.190.172	0	1	00:0c:29:91:e6:9d
	10.154.190.137	0	1	00:0c:29:d7:aa:5e
	10.154.25.30	0	1	00:50:56:b8:b4:5d
	10.154.190.145	0	1	00:50:56:b8:54:d5
	10.154.120.115	0	1	00:50:56:b8:19:67
	10.154.190.111	0	1	00:50:56:b8:e8:08
	10.154.190.120	0	1	00:50:56:b8:ee:39
	10.154.190.157	0	1	00:50:56:b8:97:f6
	10.154.190.126	0	1	80:3f:5d:08:92:d6
	10.154.0.3	0	1	20:0c:c8:49:f6:4c
	10.154.190.152	0	1	00:0c:29:54:e8:2b
	10.154.190.174	0	1	00:50:56:b8:b7:2e
	10.154.190.115	0	1	00:50:56:b8:7e:6b
	10.154.50.61	0	1	00:50:56:b8:a5:00
	10.154.190.151	0	1	00:50:56:b8:1b:67
	10.154.190.118	0	1	00:50:56:b8:b7:5c
	10.154.190.128	0	1	00:50:56:b8:d4:84
	10.154.75.25	0	1	00:50:56:b8:0c:3f
	10.154.25.102	0	1	00:50:56:b8:70:8c
	10.154.190.190	0	1	00:10:f3:38:4a:e4
	10.89.0.44	0	1	00:0c:29:56:ad:2f
	10.154.190.150	0	1	00:0c:29:2b:d7:ac
	10.154.50.167	0	1	00:0c:29:24:2e:49
	10.154.30.81	0	1	00:0c:29:a1:6a:3b

図 6-3:デバイス画面のセクション - 追加の詳細情報

追加の詳細情報を表示するには、プラス（"+"）ボタンをクリックして各デバイスの表示を展開します。

6.1.2 パス情報

Path Info

Dir	Source	Dest	Switch		
			Idx	Name	Dpid
=>	10.231.100.5	10.231.100.12	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
<=	10.231.100.12	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
=>	10.231.100.5	10.231.100.13	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
<=	10.231.100.13	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
=>	10.231.100.5	10.231.100.14	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
<=	10.231.100.14	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
=>	10.231.100.5	10.231.100.15	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
<=	10.231.100.15	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
=>	10.231.100.5	10.231.100.16	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
<=	10.231.100.16	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
=>	10.231.100.5	10.231.100.17	0	Path2	00:64:34:64:a9:b7:04:80
<=	10.231.100.17	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80

図 6-4:パス情報画面のセクション

"path info"（パス情報）ボタンをクリックすると、パス情報が表示されます。

> パス情報を表示するには、ロードマスターと SDN コントローラーを直接接続する必要があります。

パス情報をグラフ表示するには、目的のパスの**"Dir"（ディレクトリ）**列にある"=>"または"<="のアイコンをクリックします。

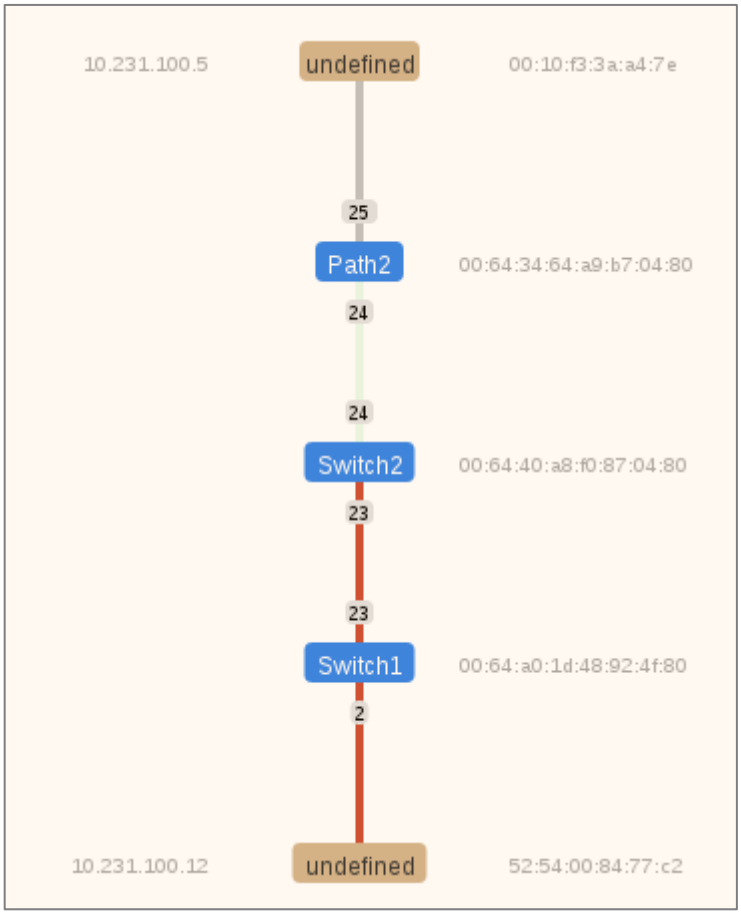

図 6-5:パス情報 - グラフ表示

この画面には、ロードマスター、実サーバー、およびその間にあるスイッチが表示されます。ロードマスターと実サーバーは茶色で表示されます。ロードマスターは上に表示され、実サーバーは下に表示されます。

スイッチは青で表示されます。SDN コントローラーによって検出されたスイッチは青で表示されます。

スイッチの右側に、ネットワーク上にある各スイッチのデータパス ID（DPID）が表示されます。DPIP は、コントローラーが各スイッチをどのように識別するかを規定します。

これらのデバイスの右側に、ロードマスターと実サーバーのメディアアクセス制御（MAC）アドレスが表示されます。また、ロードマスターと実サーバーの IP アドレスが左側に表示されます。

パスの色の意味は以下のとおりです。

- ライトグリーン:トラフィックがアイドル状態で、リンクは正常です。
- 赤:パスのトラフィックが混雑しています。
- グレー:ロードマスターと最初のスイッチとの間のパスはグレーで表示されます。

そのため、上記のスクリーンショットでは、**Path2** と **Switch2** との間のパスは正常ですが、**Switch2**、**Switch**、および実サーバーの間のトラフィックは混雑しています。

パスの混雑具合が変化すると、パスの色が変わります。赤の色はさまざまな段階で表示されます。赤の色が暗くなるほど、パスがより混雑していることを表します。

7 実サーバー

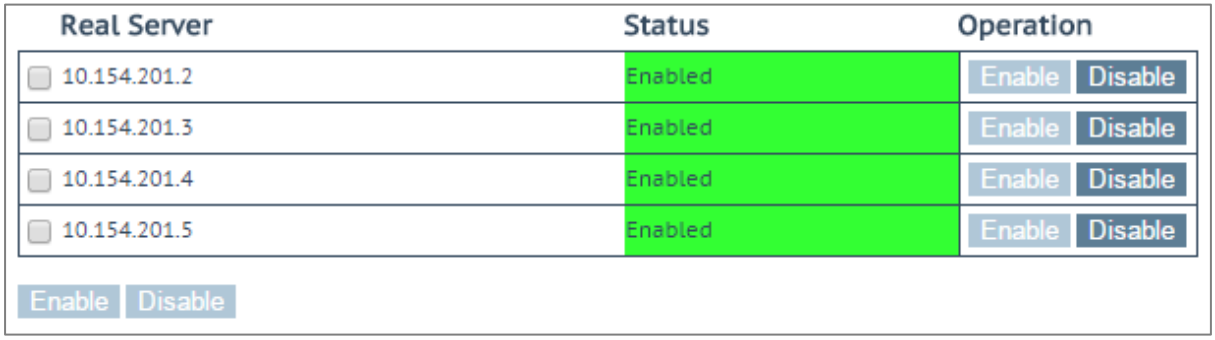

図 7-1:実サーバーの画面

この画面には、実サーバーの現在のステータスが表示されます。また、各実サーバーを**"Disable"**または**"Enable"**に設定するオプションが用意されています。実サーバーごとにボタンが用意されており、一方のボタンを押すと、オンラインになっているサーバーがオフラインになります（もう一方のボタンを押すとその逆の動作になります）。操作する対象の実サーバーを複数選択した状態で、画面の下部にある操作ボタンをクリックすることで、複数の実サーバーを同時に"Enable"または"Disable"に切り替えることができます。サーバーの状態は、Enabled（緑）、Disabled（赤）、Partial（黄）のいずれかで表されます（Partial は、1 つの仮想サービスで実サーバーが有効になっていることを表します）。

注意

実サーバーを無効にすると、その実サーバーを使用するよう設定されていたすべての仮想サービスに対して無効になります。たとえば、利用可能であった唯一の実サーバーを無効にした場合、仮想サービスは事実上、ダウン状態になり、あらゆるトラフィックがブロックされます。

8 Rules & Checking（ルールとチェック）

8.1コンテンツルール

8.1.1 Content Matching Rules（コンテンツマッチング用ルール）

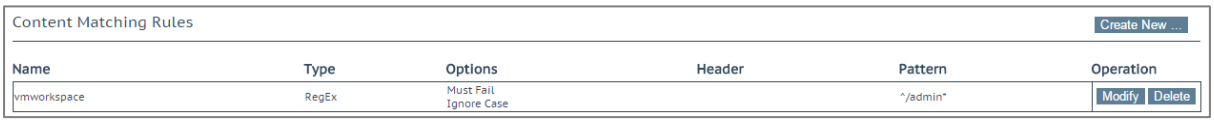

図 8-1:ルール

この画面には、設定されているルールが表示され、ルールを**変更**または**削除**するためのオプションが用意されています。

新しいルールを定義するには、**"Create New"**ボタンをクリックします。定義したルールには、名前を付ける必要があります。

ルール名は、アルファベット文字、数字の組み合わせしか有効ではありません。そしてアルファベットで始める必要があります。注意：ルール名は、ユニークでケースセンシティブです。もし作成したルールが、既存のルール名と重複する場合は上書きされてしまいます。しかし“Rule1”と“rule1”は、別々のルールとして作成されます。コンテンツルールの名前を **default** にすることはできません。

どのオプションが利用できるかは、**“Rule Type”**の選択内容によります。以下のルールを選択できます。下記の分散方式が選択できます。

ルールの種類:

- **Content Matching（コンテンツマッチング）**：ヘッダーまたはボディのコンテンツを照合します。
- **Add Header** – ルールに従ってヘッダーを追加
- **Delete Header（ヘッダーの削除）**–ルールに従ってヘッダーを削除
- **Replace Header** – ルールに従ってヘッダーを置き換え
- **Modify URL** – ルールに従って URL の変更

ルール設定の詳細については、**コンテンツルール機能説明**ドキュメントを参照してください。

8.1.2 Content Matching（コンテンツマッチング）

“Rule Type”で**“Content Matching”** を選択したときのオプションを以下に示します。

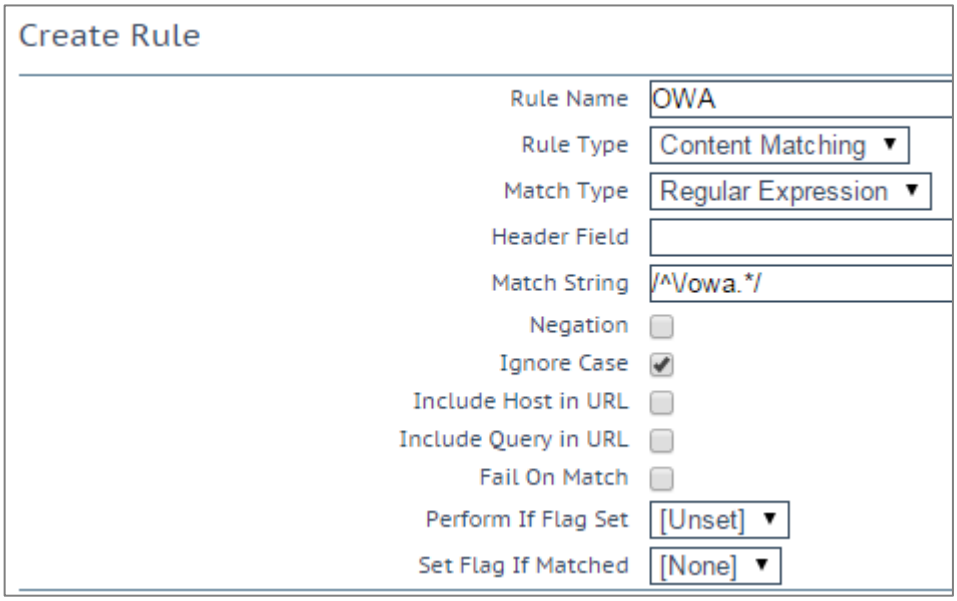

図 8-2:コンテンツマッチング

Rule Name（ルール名）

ルールの名前です。

Match Type（マッチタイプ）:

- **Regular Expression:** ヘッダーをルール文と比較します
- **Prefix:** ルール文に基づいて、ヘッダーのプレフィックスを比較します
- **Postfix:**ルール文に基づいて、ヘッダーのポストフィックスを比較します

Header Field（ヘッダーフィールド）

ヘッダーフィールド名のマッチを行います。ヘッダーフィールド名が設定されていない場合は、URL 内の文字列のマッチが行われます。

"Header Field"テキストボックスに **src-ip** と入力することで、クライアントのソース IP アドレスに基づいてルールのマッチングを実行できます。ヘッダーフィールドは、クライアントのソース IP アドレスによって設定されます。

同様に、使用する HTTP メソッド（GET、POST、HEAD など）に基づいて、ルールのマッチングを実行できます。マッチング条件のメソッドは、大文字で入力する必要があります。

リクエストのボディは、**"Header Field"（ヘッダーフィールド）**テキストボックスに **"body"（ボディ）**と入力することでも照合できます。

Match String（マッチ文字列）

マッチを行うパターンを入力します。正規表現または PCRE を使用できます。最大 250 文字まで入力可能です。

正規表現と PCRE の詳細については、**コンテンツルール機能説明**ドキュメントを参照してください。

Negation（反転）

マッチ文の意味を反転します。

Ignore Case（大文字と小文字を区別しない）

文字列の大文字と小文字を区別しません。

Include Host in URL（URL にホスト名を含める）

ルール文のマッチを行う前に、リクエスト URL の先頭にホスト名を追加します。

Include Query in URL （URL にクエリ文字列を含める）

ルール文のマッチを行う前に、クエリ文字列を URL に追加します。

Fail On Match（マッチ失敗時の処理）

このルール文にマッチした場合、常に接続しません。

Perform If Flag Set（フラグセット時にマッチ実行）

指定したフラグがセットされている場合のみこのルール文が実行されます。

Set Flag If Matched（マッチ時にフラグをセット）

このルール文のマッチに成功すると、指定したフラグがセットされます。

"Perform If Flag Set"および**"Set Flag If Matched"**オプションを使用すると、別のルールがマッチングした場合に限定して特定のルールを実行するというように、相互に依存関係のあるルールを作成できます。ルールの連鎖方法の詳細については、**コンテンツルール機能説明**ドキュメントを参照してください。

8.1.3 Add Header（ヘッダーの追加）

“Rule Type”で**“Add Header”**を選択したときのオプションを以下に示します。

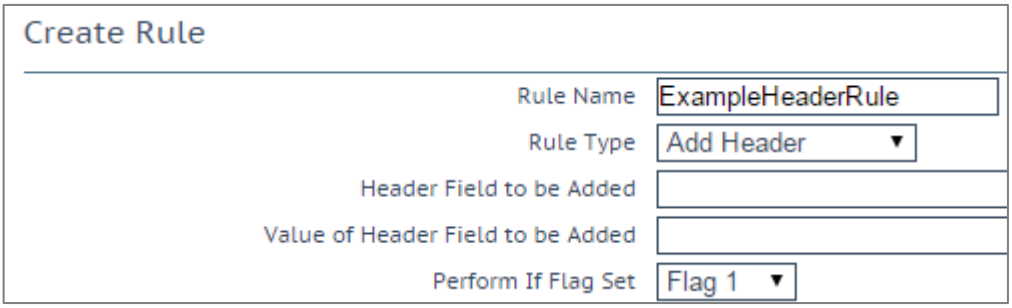

図 8-3:ヘッダーの追加

Rule Name（ルール名）

ルールの名前を入力するためのテキストボックスです。

Header Field to be Added（追加するヘッダーフィールド）

追加するヘッダーフィールドの名前を入力するためのテキストボックスです。

Value of Header Field to be Added（追加するヘッダーフィールドの値）

追加するヘッダーフィールドの値を入力するためのテキストボックスです。

Perform If Flag Set（フラグセット時に実行）

指定したフラグがセットされている場合のみこのルール文が実行されます。

このフラグは、別のルールによってセットされます。フラグの詳細については、**セクション 8.1.2** を参照してください。

8.1.4 Delete Header（ヘッダーの削除）

“Rule Type”で**“Delete Header”**を選択したときのオプションを以下に示します。

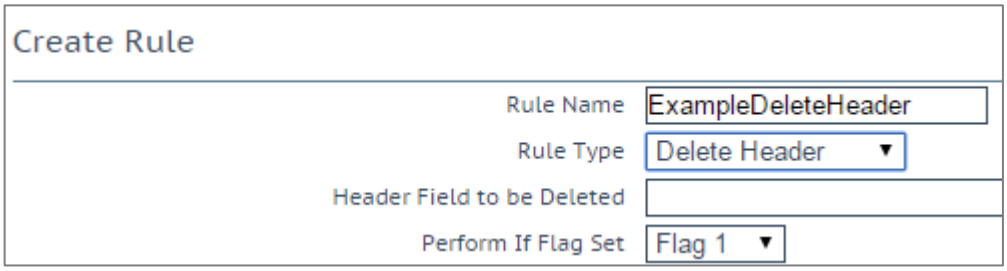

図 8-4:ヘッダーの削除

Rule Name（ルール名）

ルールの名前を入力するためのテキストボックスです。

Header Field to be Deleted（削除するヘッダーフィールド）

削除するヘッダーフィールドの名前を入力するためのテキストボックスです。

Perform If Flag Set（フラグセット時に実行）

指定したフラグがセットされている場合のみこのルール文が実行されます。

このフラグは、別のルールによってセットされます。フラグの詳細については、**セクション 8.1.2** を参照してください。

8.1.5 Replace Header（ヘッダーの置換）

“Rule Type”で**“Replace Header”**を選択したときのオプションを以下に示します。

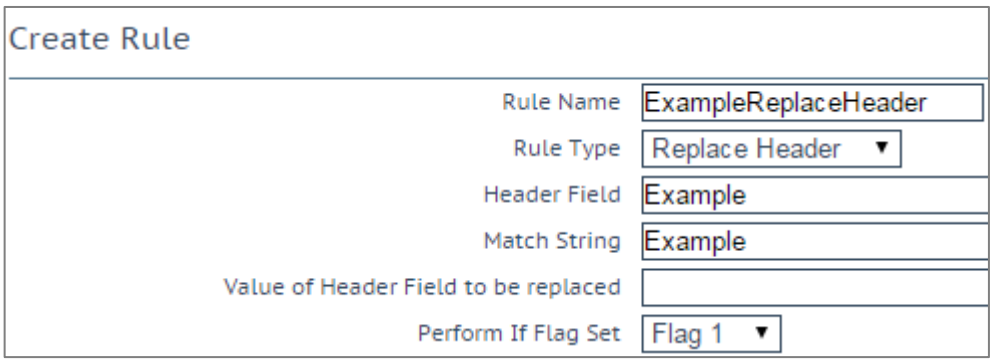

図 8-5:ヘッダーの置換

Rule Name（ルール名）

ルールの名前を入力するためのテキストボックスです。

Header Field（ヘッダーフィールド）

置換するヘッダーフィールドの名前を入力するためのテキストボックスです。

Match String（マッチ文字列）

マッチを行うパターンを入力します。

Value of Header Field to be replaced（置換するヘッダーフィールドの値）

置換するヘッダーフィールドの値を入力するためのテキストボックスです。

Perform If Flag Set（フラグセット時に実行）

指定したフラグがセットされている場合のみこのルール文が実行されます。

このフラグは、別のルールによってセットされます。フラグの詳細については、**セクション 8.1.2** を参照してください。

8.1.6 Modify URL（URL の変更）

“Rule Type”で**“Modify URL”**を選択したときのオプションを以下に示します。

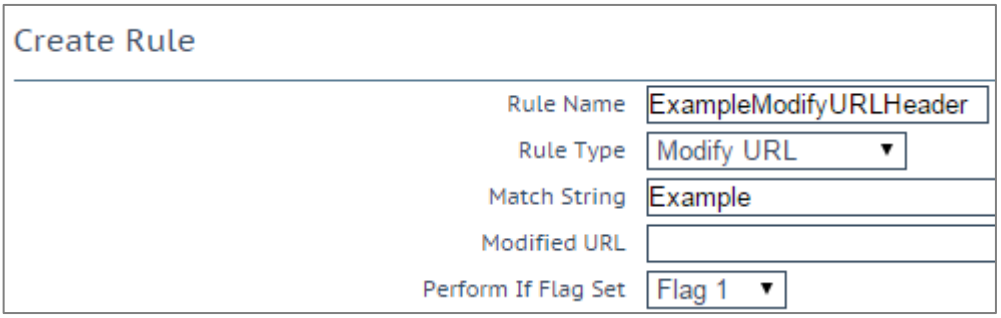

図 8-6:URL の変更

Rule Name（ルール名）

ルールの名前を入力するためのテキストボックスです。

Match String（マッチ文字列）

マッチングするパターンを入力するためのテキストボックスです。

Modified URL（変更後の URL）

変更する URL を入力するためのテキストボックスです。

Perform If Flag Set（フラグセット時に実行）

指定したフラグがセットされている場合のみこのルール文が実行されます。

このフラグは、別のルールによってセットされます。フラグの詳細については、**セクション 8.1.2** を参照してください。

8.1.7 Header Modification（ヘッダーの変更）

ヘッダーの変更の詳細については、**ヘッダー変更ガイド　テクニカルノート**を参照してください。

8.2Check Parameters（チェック用パラメータ）

"Check Parameters"画面にアクセスするには、ロードマスターWUI のメインメニューにて**"Rules & Checking > Check Parameters"**を選択します。**"Check Parameters"**画面には、2 つのセクション、すなわち、**"Service Check Parameters"**セクション、および、仮想サービスで選択した **Scheduling Method** に応じて**"Adaptive Parameters"**または**"SDN Adaptive Parameters"**のいずれかのセクションが表示されます。**Scheduling Method** が **resource based (adaptive)**に設定されている場合、**"Adaptive Parameters"**セクションが表示されます。**Scheduling Method** が **resource based (SDN adaptive)**に設定されている場合、**"SDN Adaptive Parameters"**セクションが表示されます。

詳細は、以下の関連するセクションを参照してください。

8.2.1 Service (Health) Check Parameters（サービス（ヘルス）チェック用パラメータ）

ロードマスターは、実サーバーと仮想サービスの可用性を監視するために、レイヤ 3、レイヤ 4、および Layer 7 のヘルスチェックを利用します。

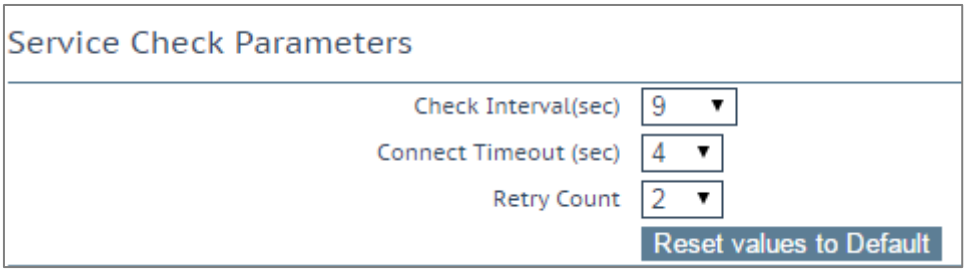

図 8-7:サービスチェック用パラメータ

Check Interval(sec)（チェック周期（秒））

ヘルスチェックの周期時間を変更できます。デフォルト値は 9 秒です。

Connect Timeout (sec)（接続タイムアウト（秒））

RS へのサービスチェックは 2 つのタイプがあります。サーバーと接続を確立させるだけの L4 タイプ（例えば TCP 接続を指定した場合）と、そしてアプリケーションレイヤでアクセスしその応答を促すタイプです（例えば L7 の HTTP/HTTPS を指定した場合）。このタイムアウトは、L4 レイヤでは TCP 接続が確立されるまで、また L7 ではアプリケーションレイヤのアクセスが確立されるまでどれだけ待つかの設定です。デフォルトは **4** 秒に設定してあります。

Retry Count（リトライ回数）

これは、サーバーのヘルスチェックでタイムアウトが発生した時にリトライする回数を指定します。デフォルト値は“**2**”で、それ以下の設定はできません。

8.2.2 アダプティブ負荷分散方式用パラメータ

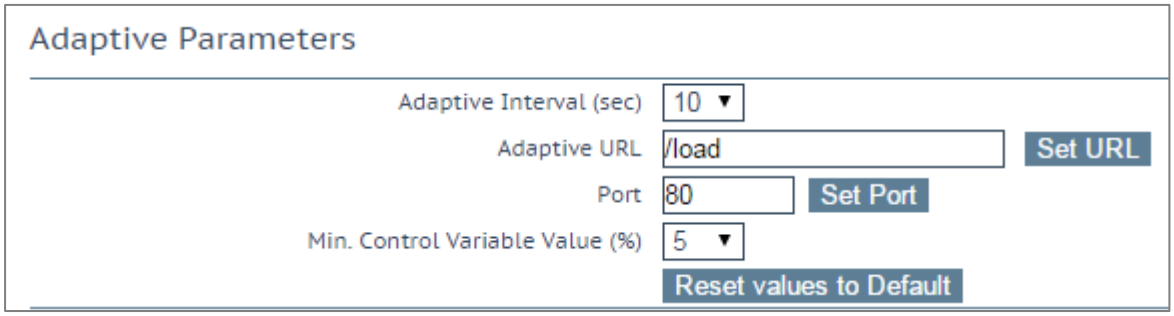

図 8-8:アダプティブ負荷分散方式用パラメータ

Adaptive Interval (sec)（インターバル（秒））

これは、ロードマスターが実サーバーの負荷をチェックする間隔（秒）です。この値が低いほど、ロードマスターは負荷に対して敏感になりますが、ロードマスター自身の負荷が増大します。開始値としては **7** 秒を推奨します。この値を HTTP のチェック間隔より短くしてはなりません。

Adaptive URL（アダプティブ URL）

アダプティブ方式では、HTTP による問い合わせを用いて負荷情報をサーバーから取得します。この URL は、サーバーの負荷情報を保存するリソースを指定します。このリソースは、この情報を配信するファイルまたはプログラムのいずれか（アダプティブエージェントなど）を指定できます。標準の場所は**/load** です。このファイルに ASCII 形式で現在の負荷データを提供する処理は、サーバーが実行します。この処理では、次の点を考慮する必要があります。

先頭行に 0～100 の値を含む ASCII ファイル（0＝アイドル、100＝オーバーロード）。0=idle and 100=overloaded.この値が大きくなると（すなわち、サーバーの負荷が高くなると）、ロードマスターはそのサーバーに渡すトラフィックを減らします。これにより、サーバーの負荷が「適応制御」されます。

サーバーの負荷が 101%または 102%になると、ログにメッセージが追加されます。

ファイルロケーションのデフォルトは“/load”です。

このファイルは HTTP を介してアクセスできます。

ファイルは HTTP 経由でアクセス可能でなければなりません。

> この機能は、HTTP ベースの仮想サービスだけでなく、あらゆるサービスを対象にします。HTTP は単に、実サーバーからアプリケーション固有の負荷情報を抽出するための転送方法として使用されます。

Port（ポート）

ロードマスターが、実サーバーの負荷値を HTTP GET で採取する時のポート番号を指定します。デフォルトは **80** です。

Min. Control Variable Value (%)（アダプティブ開始最低重み値（%））

この値は、ロードバランサーがスケジューリング方式を切り替えるしきい値を規定します。負荷がこのしきい値未満になると、ロードバランサーは静的な重み付けを用いたスケジューリング方式（通常の重み付けラウンドロビン）に切り替わります。この値は、最大負荷に対する割合（0～50）で指定します。デフォルトは **5** です。

8.2.3 SDN のアダプティブ負荷分散方式パラメーター

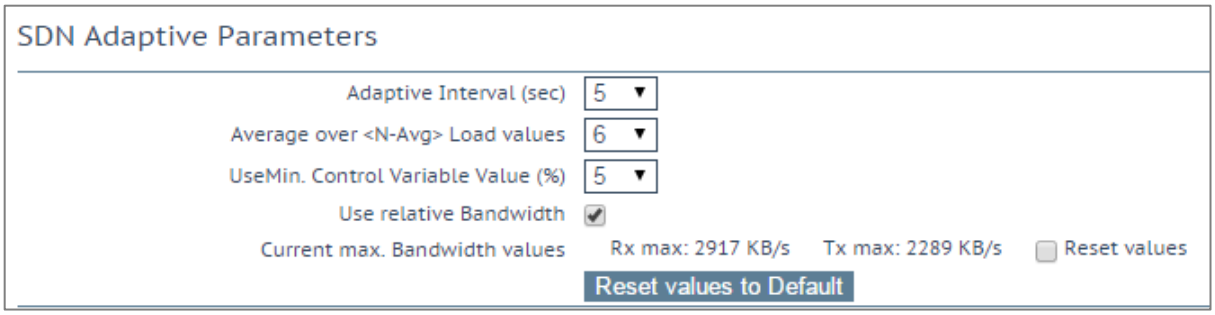

図 8-9:SDN のアダプティブ負荷分散方式パラメーター

Adaptive Interval (sec)（インターバル（秒））

SDN のアダプティブスケジューリングを使用している場合、実サーバーの負荷の値を取得するために、SDN コントローラーがポーリングされます。このフィールドの値は、このポーリングの頻度を指定します。

Average over <N-Avg> Load values（N 個の平均負荷）

システムにおける変動を抑制するにはこの値を使用します。

UseMin, Control Variable Value (%)（アダプティブ開始最低重み値（%）を使用）

ここで設定した値より低いものについてはアイドルトラフィックとみなされ、アダプティブ値に影響を与えません（アダプティブ値は実サーバーの"Statistics"画面に表示されます）。例えば、上記のスクリーンショットでは、5%未満のものはすべてアイドルとみなされます。

User Relative Bandwidth（相対帯域幅を使用）

リンクで観測された最大負荷を帯域幅として使用します。このオプションは有効にすることを推奨します。

Current max. Bandwidth values（現在の最大帯域幅の値）

このセクションには、送受信された現在の最大帯域幅の値が表示されます。

Reset values（値のリセット）

このチェックボックスを使用すると、現在の最大帯域幅の値をリセットできます。

9 証明書とセキュリティ

以下のセクションでは、ロードマスターWUI の"**Certificates & Security**"の各種画面について説明します。

9.1SSL Certificates（SSL 証明書）

SSL 証明書の画面は、ハードウェアセキュリティモジュール（HSM）機能が有効かどうかによって異なります。HSM に関する詳細は、**ハードウェアセキュリティモジュール（HSM）　機能説明**を参照してください。

SSL 証明書の画面に関する詳細は、使用する設定に応じて以下の関連セクションを参照してください。

9.1.1 HSM が有効でない場合

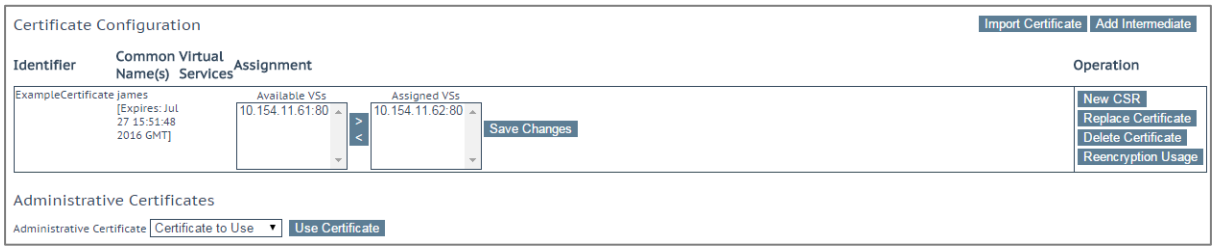

図 9-1:SSL Certificates（SSL 証明書）

上図は、SSL 証明書の管理画面を示します。

Import Certificate（証明書のインポート） – 選択したファイル名を持つ証明書をインポートします。

Add Intermediate – 詳細は**セクション 9.2** を参照してください。

Identifier – 証明書作成時に与えられた証明書名です。

Common Name(s)（共通名） – サイトの完全修飾ドメイン名（FQDN）。

Virtual Services（仮想サービス） – 証明書が関連付けられる仮想サービス。

Assignment（割り当て） – 割り当てられた利用可能な仮想サービスのリスト

Operations（操作） –

- **New CSR（新規 CSR）** – 現在の証明書に基づいて新規の証明書署名要求（CSR）を作成します。

証明書にサブジェクト代替名（SAN）が含まれている場合、この方法で CSR を作成しても SAN は追加されません。この場合は手動で CSR を作成してください。この動作についての詳細は、セクション **9.3** を参照してください。

- **Replace Certificate** – 証明書の更新、もしくはリプレースが行えます。
- **Delete Certificate（証明書の削除）** – 対象となる証明書を削除します。
- **Reencryption Usage（再暗号化の使用）** – 再暗号化時にこの証明書をクライアント証明書として使用している仮想サービスを表示します。

Administrative Certificates – 管理用 WUI へのアクセスで使用する SSL 証明書を選択できます。デフォルトは、KEMP のセルフサイン証明書です。

TPS のパフォーマンスはキーの長さにより変化します。キーが長くなるとパフォーマンスが低下します。

9.1.2 HSM が有効な場合

Private Key Identifier（秘密鍵識別子）

HSM が有効のとき、**"Generate CSR"**オプションは、ロードマスターのメインメニューから**"Manage Certificates"**画面に移動します。

識別可能なロードマスターの秘密鍵名を入力し、**"Generate CSR"**をクリックします。Generate CSR"画面のフィールドは、**"Use 2048 bit key"**がないことを除き、**セクション 9.3** で説明した内容と同じです。

Add Intermediate – 詳細は**セクション 9.2** を参照してください。

Private Key（秘密鍵） - この列には秘密鍵名が表示されます。

Common Name(s)（コモンネーム） – サイトの FQDN（完全修飾ドメイン名）。

Virtual Services（仮想サービス） – 証明書が関連付けられる仮想サービス。

Assignment（割り当て） – 割り当てられた利用可能な仮想サービスのリスト

Operations（操作） –

- **Import Certificate（証明書のインポート）** – このキーに関連付けられた証明書をインポートします。
- **Delete Key（鍵の削除）** – 秘密鍵または証明書を削除します。
- **Show Reencrypt Certs（再暗号化された証明書）** – 再暗号化された証明書を表示します。

9.2Intermediate Certificates（インターミディエート証明書）

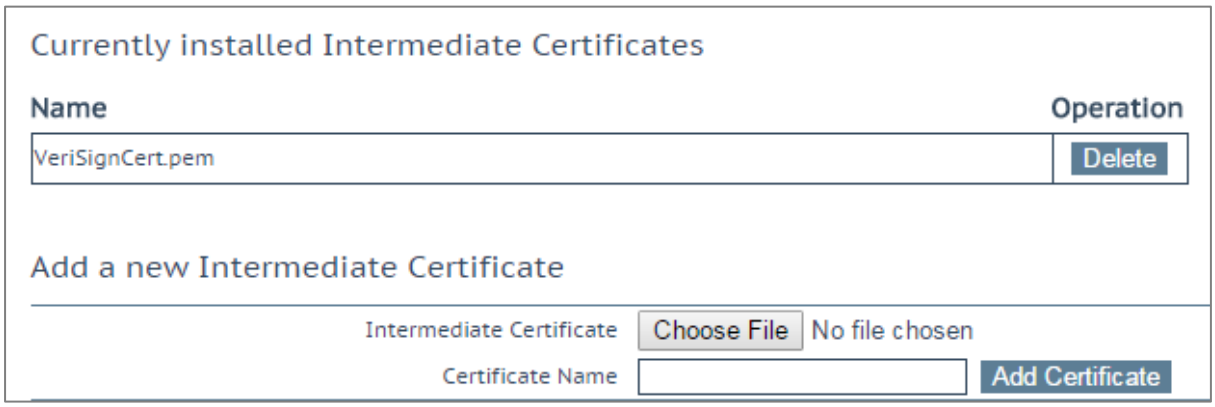

図 9-2:インターミディエート証明書

この画面には、インストールされている中間証明書と、その中間証明書に割り当てられている名前のリストが表示されます。

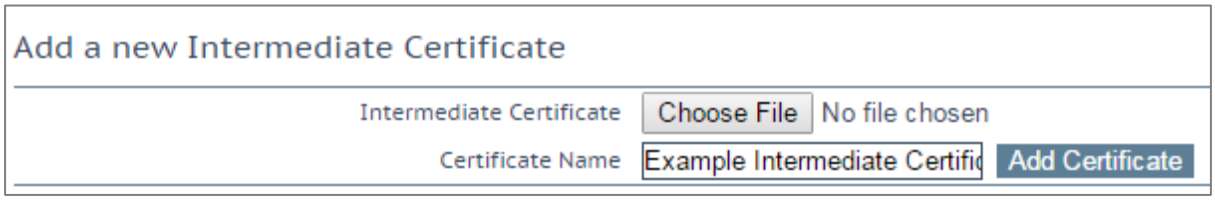

図 9-3:中間証明書のインストール

すでに証明書を持っている場合、または CSR からすでに証明書を受け取っている場合、**"Choose File"（ファイルを選択）**をクリックして証明書をインストールできます。証明書を選択して、**"Certificate Name"（証明書名）**に目的の名前を入力します。この名前には、アルファベット文字しか使用できません。また、最大 32 文字という制限があります。

GoDaddy の証明書などのように、1 つのテキスト文にて複数の連続したインターミディエート証明書をアップロードできます。アップロードしたファイルは、個々の証明書に分割されます。

9.3Generate CSR (Certificate Signing Request)（CSR（証明書署名要求）の作成）

証明書が存在しない場合は、証明書署名要求（CSR）フォームに入力して、**"Create CSR"**ボタンをクリックします。ロードマスターによって生成される CSR は SHA256 を使用します。

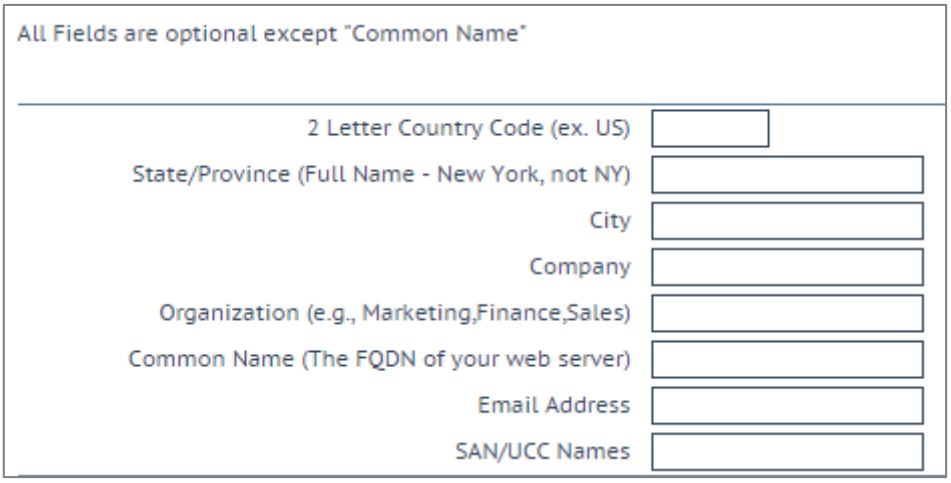

図 9-4:CSR の作成

2 Letter Country Code (ex. US)（2 文字国コード（例: US））

証明書に含める 2 文字国コードです。例えば、米国であれば US と入力します。

State/Province （州/行政区）（名前を入力 – NY ではなく New York と入力）

証明書に含める州です。ここではフルネームを入力します。例えば、NY ではなく **New York** と入力します。

City（都市）

証明書に含める都市名です。

Company（企業）

証明書に含める企業名です。

Organization (e.g., Marketing,Finance,Sales)（組織（例: マーケティング、財務、販売））

証明書に含める部門または組織単位です。

Common Name（コモンネーム）

お使いの Web ブラウザーの完全修飾ドメイン名（FQDN）です。

Email Address（E メールアドレス）

この証明書に関する問い合わせ先の担当者または組織の E メールアドレスです。

SAN/UCC Names（SAN/UCC 名）

スペースで区切られた代替名のリストです。

[Create CSR] ボタンをクリックすると、次の画面が表示されます。

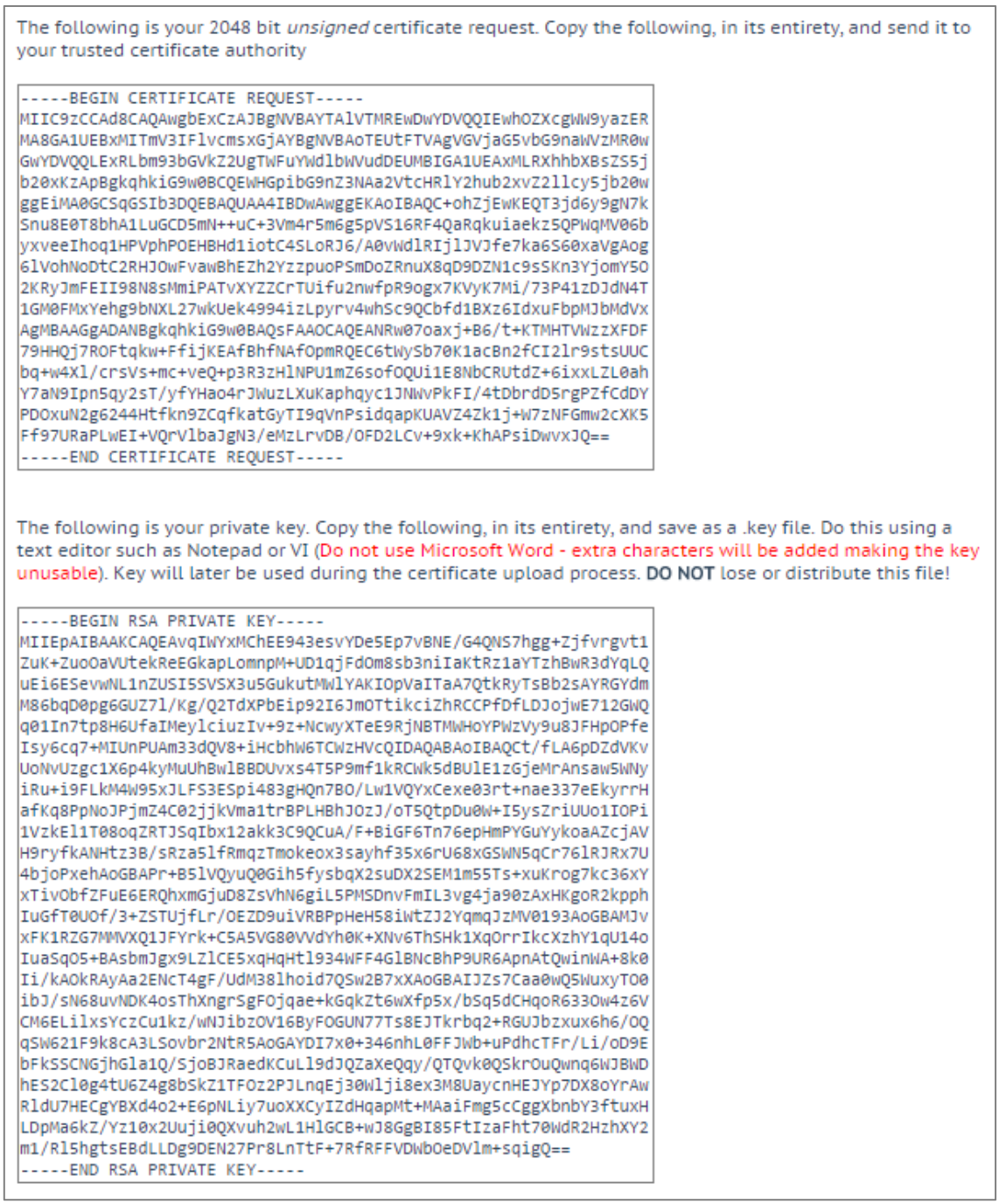

図 9-5:CSR 未署名の証明書と秘密鍵

図 8 6: CSR 未署名の証明書と秘密鍵

画面上部の CSR は、プレーンテキストファイルに貼り付けて、認証局（CA）に送信する必要があります。認証局は情報を検証して、検証済みの証明書を返します。

画面下部は、秘密鍵であり、安全な場所に保管する必要があります。秘密鍵は、認証局より送られてくる証明書とペアで使用する必要がありますが、このキーは誰にも渡すべきではありません。秘密鍵をコピーし、プレーンテキストファイルに貼り付けて（Microsoft Word など、アプリケーションは使用しないこと）、安全な場所で保管します。

9.4Backup/Restore Certificates（証明書のバックアップ/復元）

この画面は、HSM が有効かどうかにより異なります。ロードマスターの設定に応じて、以下の関連するセクションを参照してください。

9.4.1 HSM が有効でない場合

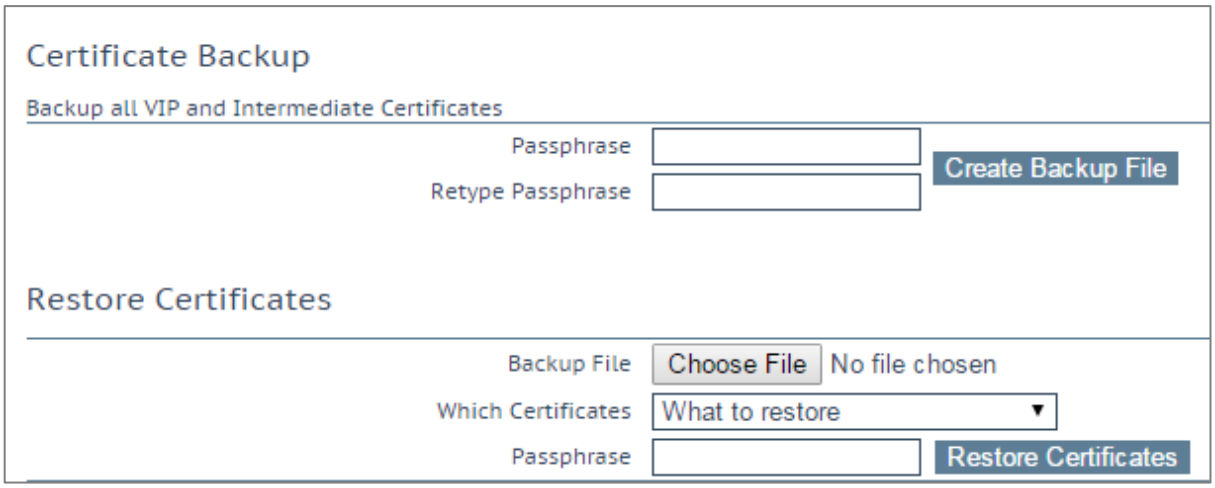

図 9-6:証明書のバックアップ/復元 - HSM が無効な場合

Backup all VIP and Intermediate Certificates（VIP および中間証明書をすべてバックアップ）：証明書をバックアップするときに、必須のパスフレーズ（パスワード）を 2 回入力するよう求めるプロンプトが表示されます。パスフレーズのパラメータには、英数字しか使用できません。また、大文字と小文字が区別され、最大 64 文字という制限があります。

注意

パスフレーズは、証明書を復元するために必須です。パスフレーズがないと証明書を復元できません。パスフレーズを忘れた場合は、証明書を復元する方法はありません。

Backup File（バックアップファイル）:証明書のバックアップファイルを選択します

Which Certificates（証明書）：リストアする証明書を選択します

Passphrase（パスフレーズ）: 証明書のバックアップファイルに関連付けられているパスフレーズを入力します

9.4.2 HSM が有効な場合

Backup Intermediate Certificates（中間証明書をバックアップ）:証明書をバックアップするときに、必須のパスフレーズ（パスワード）を 2 回入力してください。パスフレーズのパラメータには、英数字しか使用できません。また、大文字と小文字が区別され、最大 64 文字という制限があります。

> **注意**
>
> パスフレーズは、証明書を復元するために必須です。パスフレーズがないと証明書を復元できません。パスフレーズを忘れた場合は、証明書を復元する方法はありません。

Intermediate Certificate Backup File（中間証明書のバックアップファイル）:中間証明書のバックアップファイルを選択します

Passphrase（パスフレーズ）: 証明書のバックアップファイルに関連付けられているパスフレーズを入力します

9.5Cipher Set（暗号セット）

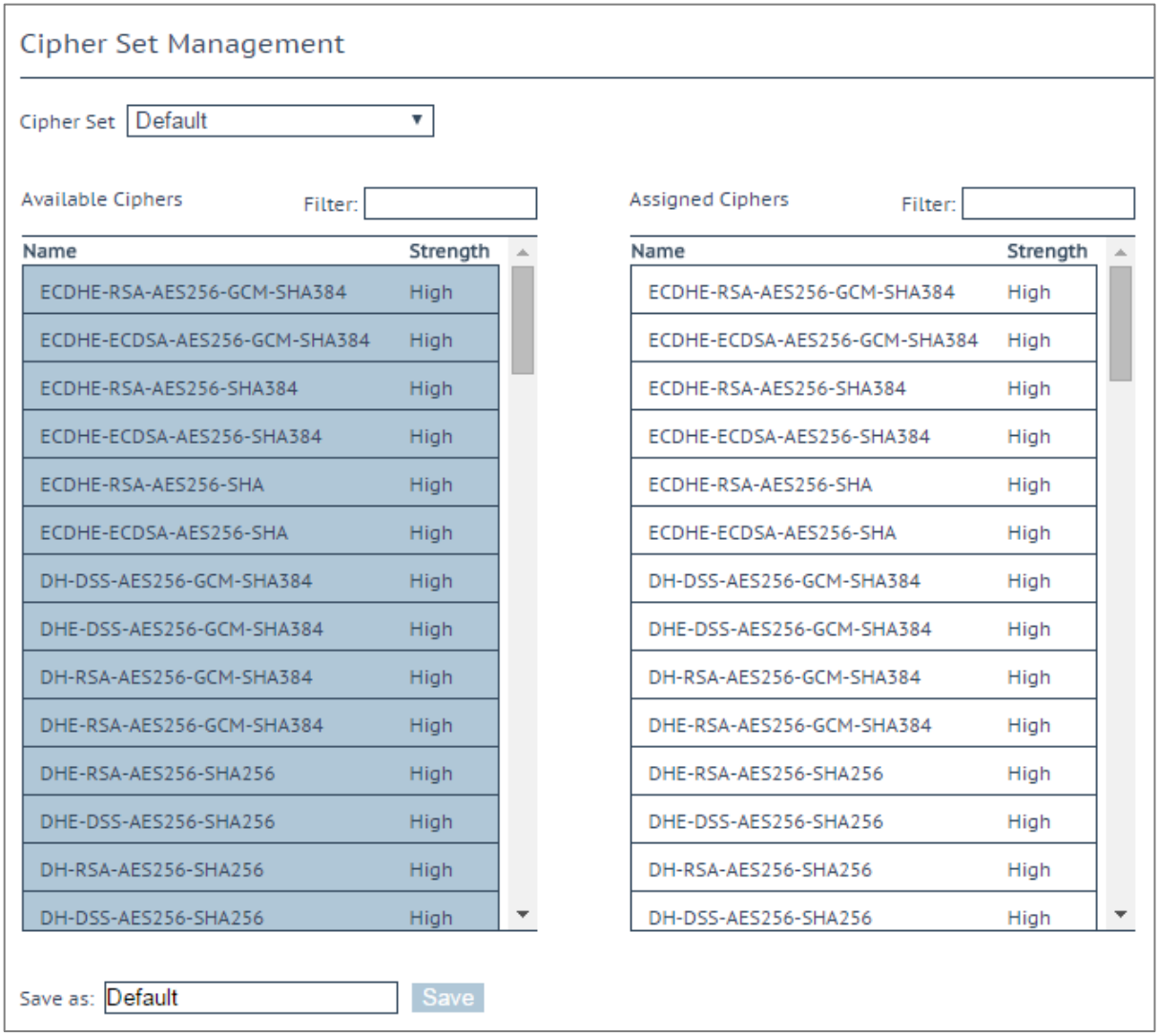

図 9-7:暗号セットの管理

Cipher Set（暗号セット）

表示/編集する暗号セットを選択します。

以下に示すシステム定義の暗号セットが用意されています。

- **Default（デフォルト）**:現在のデフォルトの暗号セットは LoadMaster です。
- **Default_NoRc4:**Default_NoRc4 の暗号にはデフォルトの暗号セットと同じ暗号が含まれますが、RC4 暗号は含まれません（RC4 は安全ではないとみなされています）。

- **BestPractices:**これは推奨の暗号セットです。この暗号セットは、後方互換性が必要ないサービスで使用します。この暗号は、高いレベルのセキュリティを提供します。この設定は、Firefox 27、Chrome 22、IE 11、Opera 14、Safari 7 に対応しています。
- **Intermediate_compatibility:**古いクライアント（多くの場合、Windows XP）との互換性が必要ないものの、幅広いクライアントをサポートする必要があるサービスについては、この設定を推奨します。この設定は、Firefox 1、Chrome 1、IE 7、Opera 5、Safari 1 に対応しています。
- **Backward_compatibility:**これは古い暗号セットで、Windows XP/IE6 のクライアントで動作します。これは最後の手段として使用してください。
- **WUI:**WUI の暗号セットとして使うことを推奨された暗号セットです。WUI の暗号セットは、**"Admin WUI Access"**画面で選択できます。詳細は**セクション 9.7** を参照してください。
- **FIPS:**FIPS（連邦情報処理規格）に準拠した暗号です。
- **Legacy:**これは、OpenSSL が更新される前の古いロードマスターのファームウェア（v7.0～10）で使用されていた暗号セットです。

ロードマスターでサポートされている暗号の一覧、およびシステム定義の暗号セットでどの暗号が使用されているかについては、**アプリケーションファイアウォールパック（AFP）カスタムルール**を参照してください。

KEMP テクノロジーでは、利用可能な最良の情報に基づいて、必要に応じてこれらの暗号セットの内容を変更することができます。

"Available Ciphers"（利用可能な暗号）と**"Assigned Ciphers"（割り当てられた暗号）**の 2 つのリストが表示されます。画面に表示される**"Filter"**テキストボックスに文字を入力すると、これらのリストをフィルターできます。**"Filter"**テキストボックスでは、暗号名に含まれる有効な文字のみ入力できます（例: **ECDHE**）。無効な文字を入力すると、その文字が赤くなり、無効な文字が削除されます。

必要に応じて、**"Available"**リストおよび**"Assigned"**リストに（またはこれらのリストから）暗号をドラッグアンドドロップできます。既に割り当てられている暗号は、**"Available Ciphers"**リストにおいてグレーで表示されます。

設定済みの暗号セットに対する変更は行えません。ただし、設定済みの暗号セットをベースにして必要な変更を行い、その暗号セットを新しいカスタム名で保存することができます。**"Save as"**テキストボックスに新しい名前を入力し、**"Save"**ボタンをクリックします。カスタム暗号セットは、複数の仮想サービスで使用することができます。また、WUI の暗号セットとして割り当てることができます。

設定済みの暗号セットは削除できません。ただし、目的のカスタム暗号セットを選択して"**Delete Cipher set**"ボタンをクリックすると、カスタム暗号セットを削除することができます。

9.6Remote Access（リモートアクセス）

以下のセクションでは、ロードマスターWUI の"**Remote Access**"画面の各種エリアについて説明します。

9.6.1 管理者アクセス

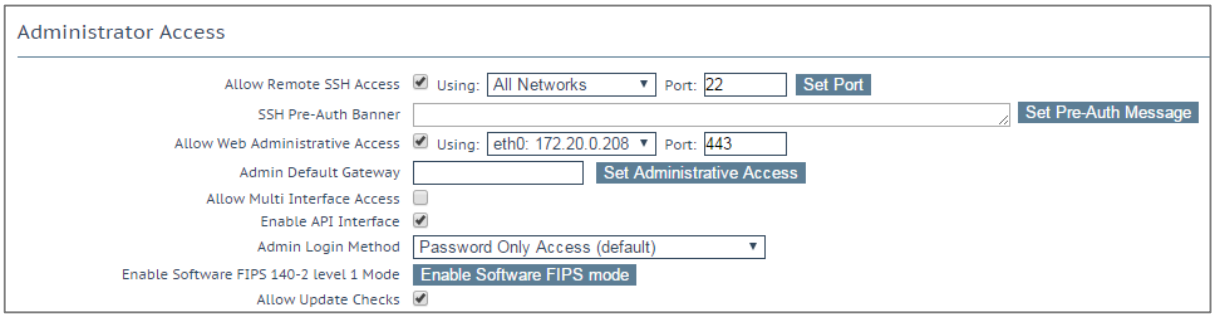

図 10-37:管理者アクセス

Allow Remote SSH Access（SSH アクセスの許可／禁止）

このオプションは、SSH 接続を介したロードマスターへのアクセスを許可／禁止します。もし、このオプションが禁止されていると、設定メニューへのアクセスはコンソールだけから可能となります。'bal'ユーザーのパスワードが設定されていない場合は、SSH 接続を介したログインはできません。

Using（使用）

リモートからロードマスターへの管理用 SSH アクセスにおいて、どのアドレスを許可するかを指定します。

Port（ポート）

SSH プロトコルにてどのポートを使用してロードマスターにアクセスするかを指定します。

SSH 事前認証バナー

SSH 事前認証バナーを設定します。これは、SSH でログインする際に、ログインプロンプトの前に表示されます。このフィールドには 5,000 文字まで入力できます。

Allow Web Administrative Access（WUI へのリモートアクセス許可／禁止）

このチェックボックスをオンにすると、ロードマスターへの管理用 Web アクセスが可能となります。このオプションを無効にすると、次に再起動したときにアクセスが停止します。このフィールドに変更を適用するには、**"Set Administrative Access"（管理用アクセスの設定）**をクリックします。

Web アクセスを無効にすることは推奨しません。

Using0

管理用 Web アクセスを許可するアドレスを指定します。このフィールドに変更を適用するには、**"Set Administrative Access"（管理用アクセスの設定）**をクリックします。

Port（ポート）

管理用 Web インターフェイスにアクセスするためのポートを指定します。このフィールドに変更を適用するには、**"Set Administrative Access"（管理用アクセスの設定）**をクリックします。

管理用デフォルトゲートウェイ

WUI のための特定ゲートウェイ装置を設定して、システムのグローバルゲートウェイとは違うルーティングを行わせることが可能です。WUI 以外のアクセスでは、この設定は使用されません。このフィールドに変更を適用するには、**"Set Administrative Access"（管理用アクセスの設定）**をクリックします。

Allow Multi Interface Access（マルチインターフェイスアクセスの許可/禁止）

このオプションを有効にすると、複数のインターフェイスから WUI にアクセスできます。このオプションが有効のとき、各インターフェイスの画面（**"System Configuration > eth<n>"**）に **Allow Administrative WUI Access** という新しいオプションが表示されます。これらのオプションを 2 つとも有効にすると、該当するインターフェイスの IP アドレスと、そのインターフェイスに設定された**"Additional addresses"（追加アドレス）**から WUI にアクセスできます。このフィールドに変更を適用するには、**"Set Administrative Access"（管理用アクセスの設定）**をクリックします。

WUI との接続にデフォルトで使用される証明書では、最初の WUI の IP アドレスが指定されています。そのため、この証明書は、他のインターフェイスにおける WUI との接続では機能しません。複数のインターフェイスの WUI を有効にするには、その WUI のワイルドカード証明書をインストールする必要があります。証明書についての詳細は、**アプリケーションファイアウォールパック（AFP）カスタムルール**を参照してください。

複数のインターフェイスの WUI を有効にすると、システムのパフォーマンスが影響を受けます。最大 64 個のネットワークインターフェイスを追跡できます。システムは、トータルで最大 1024 個のアドレスをリッスンします。

RADIUS Server（RADIUS サーバー）

ここでは、ロードマスターへのユーザーアクセスの認証に使用する RADIUS サーバーのアドレスを入力できます。RADIUS サーバーを使用するには、**"Shared Secret"**を指定する必要があります。

共有秘密鍵とは、ロードマスターと RADIUS サーバーとの間のパスワードとして使用される文字列のことです。

“Revalidation Interval”にて、RADIUS サーバーがユーザーを再認証する頻度を指定します。

RADIUS Server Configuration（RADIUS サーバーの設定）

ロードマスターとともに RADIUS が正しく機能するよう設定するには、RADIUS サーバーにて認証情報を設定し、RADIUS の応答メッセージをロードマスターの権限に対応させる必要があります。

応答メッセージの値は、ロードマスターの権限と**表 9-1** のように対応しています。

応答メッセージ	ロードマスターの権限
real	実サーバー
vs	Virtual Services（仮想サービス）
rules	Rules（ルール）
backup	システムバックアップ
certs	証明書の作成
cert3	Intermediate Certificates（インターミディエート証明書）
certbackup	証明書のバックアップ
users	ユーザの管理

応答メッセージ	ロードマスターの権限
geo	OCSP の設定

表 9-1:応答メッセージ/ロードマスターの権限

応答メッセージの値は、"All Permissions"（すべて許可）を除き、図 119 のように WUI のユーザー権限のページと対応させる必要があります。

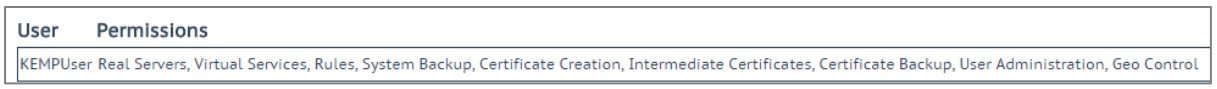

図 9-8:ユーザー権限のセクション

Windows 版の RADIUS を設定するには、KEMP の Web サイトにある **RADIUS の認証と権限設定　テクニカルノート**を参照してください。

Linux 版の FreeRADIUS サーバーを設定する場合、/etc/freeradius/users の指定されたセクションに、以下のテキストを挿入してください。以下に、"LMUSER"ユーザーの権限を設定する例を示します。

LMUSER Cleartext-Password := "1fourall"

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

また、/etc/freeradius/clients.conf を設定してロードマスターの IP アドレスを含める必要があります。このファイルには、RADIUS に接続可能な IP アドレスの一覧が記述されています。

> セッション管理が有効になっている場合、この画面で“RADIUS Server”オプションは使用できません。セッション管理が有効なときに RADIUS サーバーを設定する方法については、**Section9.6.4** を参照してください。

Enable API Interface（API インターフェイスを有効にする）

RESTful アプリケーション・プログラム・インターフェイス（API）を有効/無効にします。

Admin Login Method（ログイン方式の管理）

> このオプションは、セッション管理が有効な場合のみ表示されます。セッション管理についての詳細は、**セクション 9.7** または***ユーザー管理　機能説明***を参照してください。

ロードマスターWUI にアクセスするためのログインオプションを指定します。以下のオプションが利用可能です。

- **Password Only Access (default)（パスワードのみのアクセス（デフォルト））**:このオプションを選択すると、ユーザー名とパスワードを用いたアクセスのみ可能になります。クライアント証明書によるアクセスはできません。
- **Password or Client certificate（パスワードまたはクライアント証明書）**:ユーザーは、ユーザー名/パスワードまたは有効なクライアント証明書を用いてログインできます。有効なクライアント証明書が存在する場合、ユーザー名とパスワードは必要ありません。
  クライアントは、証明書を提供するよう求められます。クライアント証明書が提供されると、ロードマスターはその証明書が一致するかチェックします。ロードマスターは、提供された証明書がローカルに保存されている証明書と一致するかチェックします。または、提供された証明書のサブジェクト代替名（SAN）もしくはコモンネーム（CN）が一致するかチェックします。照合を行う際、CN よりも SAN が優先的に使用されます。一致するものがあった場合、ユーザーはそのロードマスターへのアクセスを許可されます。この動作は、API とユーザーインターフェイスのどちらでも機能します。
  証明書が無効な場合はアクセスは許可されません。
  クライアント証明書が提供されない場合、ロードマスターは、ユーザー名とパスワードが提供されることを期待します（API を使用する場合）。または、標準の WUI ログインページからパスワードを入力するようユーザーに要求します。
- **Client certificate required（クライアント証明書が必要）**:クライアント証明書を用いたアクセスのみ許可します。ユーザー名とパスワードによるアクセスはできません。SSH のアクセスは、このオプションによる影響を受けません（**bal** ユーザーのみ SSH 経由でログイン可能）。
- **Client certificate required (Verify via OCSP)（クライアント証明書が必要（OCSP 経由で照合））**:これは**"Client certificate required"**オプションと同じですが、クライアント証明書は OCSP サービス経由で照合されます。このオプションが機能するには、OCSP サーバーを設定する必要があります。OCSP サーバーの設定に関する詳細は、**セクション 9.5** を参照してください。

クライアント証明書を用いた方式に関して、以下の点に注意する必要があります。

- **bal** ユーザーはクライアント証明書を持っていません。そのため、**"Client certificate required"**方式を用いて **bal** としてロードマスターにログインすることはできません。ただし、**bal** 以外のユーザーを作成し、そのユーザーに**"All Permissions"**の権限を与えることができます。これにより、**bal** ユーザーと同じ機能を実現することができます。

- クライアント証明書でログインした場合、ログアウトすることはできないため（ログアウトしても次回アクセス時に自動的に再度ログインされる）、クライアント証明書でログインしたユーザーに対するログアウトオプションはありません。ページを閉じるかブラウザーを再起動すると、セッションが終了します。

クライアント証明書による WUI 認証に関する詳細（ステップバイステップの設定方法など）は、***ユーザー管理　機能説明***を参照してください。

Enable Software FIPS 140-2 level 1 Mode（ソフトウェア FIPS 140-2 レベル 1 モードを有効にする）

> セッション管理が無効な場合、FIPS モードを有効にできません。セッション管理についての詳細は、**セクション 9.7** を参照してください。

このロードマスターを FIPS 140-2 レベル 1 で認定されたモードに切り替えます。有効にするにはロードマスターを再起動する必要があります。

> FIPS を有効にする前に、数多くの警告が表示されます。ロードマスターで FIPS を有効にすると、FIPS を簡単には無効にできません。ロードマスターで有効になっている FIPS を無効にしたい場合は、KEMP のサポートにお問い合わせください。

図 9-9:FIPS-1 モード

ロードマスターが FIPS レベル 1 モードになっている場合、ロードマスターWUI の右上に **"FIPS-1"**と表示されます。

FIPS レベル 1 では、非 FIPS ロードマスターとは異なる暗号セットを持っています。**"Default"（デフォルト）**の暗号セットが用意されていますが、これ以外のシステム定義の暗号セットを選択することはできません。

Allow Update Checks（アップデートのチェックを許可する）

KEMP の Web サイトにソフトウェアの新しいバージョンがあるかどうかをロードマスターが定期的にチェックするのを許可します。

9.6.2 GEO の設定

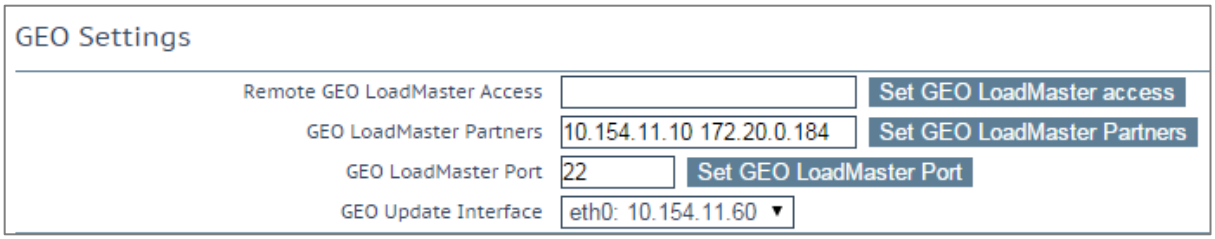

図 10-38:GEO の設定

Remote GEO LoadMaster Access（GEO ロードマスターのリモートアクセス）

LoadMaster-GEO, LoadMaster-DR、もしくは VLM-DR と併用して使用する時に、状態監視を受け付けるために相手の IP アドレスを設定します。アドレスはスペースで区切ります。HA モードにある場合、共有アドレスの入力のみ必要です。

GEO LoadMaster Partners（GEO ロードマスターパートナー）ロードマスターの分散パートナー

> GEO 機能は GSLB 機能パックに含まれており、ロードマスターに適用されているライセンスに基づいて有効になります。GSLB 機能パックを利用するには、ライセンスをアップグレードする必要があるので、KEMP にご連絡ください。

パートナーGEO ロードマスターのアドレスを設定します。アドレスはスペースで区切ります。この GEO ロードマスターは、DNS の設定をシンクに保持しています。

> GEO ロードマスターのパートナーを設定する前に、正しい設定/推奨設定を持つ該当する GEO ロードマスターのバックアップを作成する必要があります。そして、このバックアップを、オリジナルのロードマスターのパートナーとなるロードマスターに保存する必要があります。詳細および手順については、**GEO　製品概要**を参照してください。
>
> 最大 64 個の GEO HA パートナーのアドレスを追加できます。選択基準の詳細については、を参照してください。

GEO LoadMaster Port（GEO ロードマスターのポート）

上記“Remote GEO LoadMaster Access”のポート番号を設定します。SSH プロトコルが使用されますので、通常ポート番号 22 を使用します。

GEO update interface（GEO 更新インターフェイス）

SH パートナートンネルを作成する GEO インターフェイスを指定します。このインターフェイスを介して、GEO パートナーは情報をやり取りします。

9.6.3 GEO パートナーのステータス

このセクションは GEO パートナーが設定されている場合のみ表示されます。

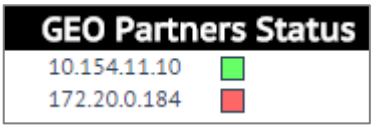

図 10-39:GEO パートナーのステータス

GEO パートナーの**緑**のステータスは、2 つのパートナーがお互いに見える状態にあることを示しています。

GEO パートナーの**赤**のステータスは、ロードマスターが通信できないことを示しています。その原因のひとつとして、いずれかのパートナーの電源がオフになっていることが考えられます。この場合、停電が発生しているか、ケーブルが接続されていない可能性があります。

GEO パートナーの更新に失敗すると、そのパートナーに対する GEO の更新が失敗したことを示すエラーメッセージがログに表示されます。このメッセージには、そのパートナーの IP アドレスが表示されます。

9.6.4 WUI Authentication and Authorization（WUI による認証と権限設定）

WUI Authorization Options（WUI の権限設定オプション）

"Remote Access"（リモートアクセス）画面の**"WUI Authorization Options"（WUI 認証オプション）**ボタンをクリックすると、**"WUI Authentication and Authorization"（WUI による認証と権限設定）**画面が表示されます。このオプションは、セッション管理が有効になっているときのみ表示されます。

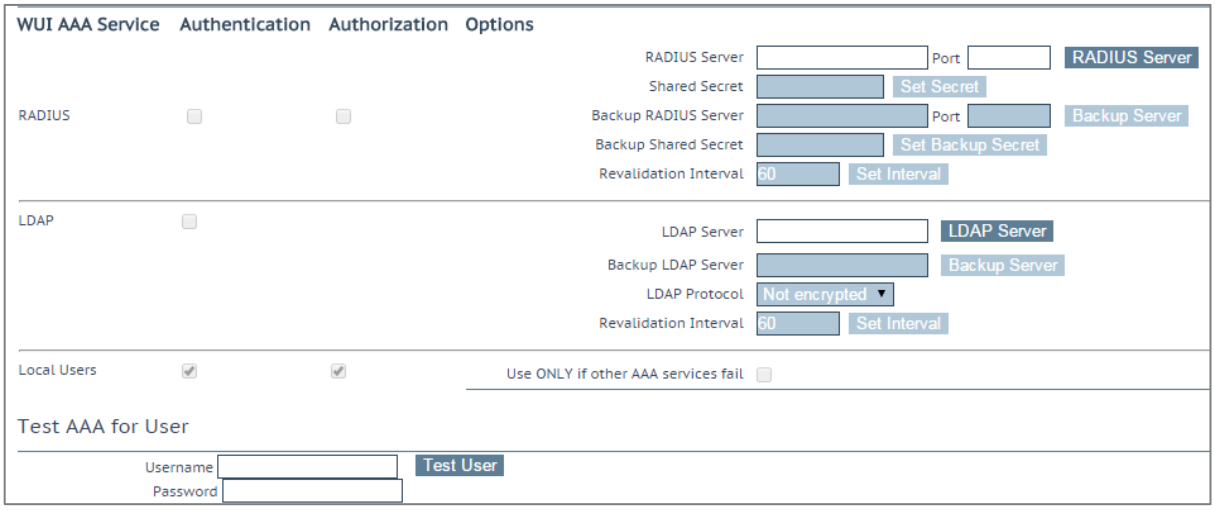

図 9-10:WUI の認証および承認

WUI による認証と権限設定画面では、認証（ログイン）と権限設定（権限の許可）に関するオプションを管理できます。

Authentication（認証）

ユーザーは、ロードマスターにログインする前に認証を受ける必要があります。ロードマスターでは、ローカルユーザーの認証方式の他に、RADIUS および LDAP による認証方式を用いてユーザー認証を行えます。

すべての認証方式が選択されている場合、ロードマスターは以下の順序でユーザー認証を試みます。

1. RADIUS
2. LDAP
3. ローカルユーザー

例えば、RADIUS サーバーを利用できない場合、LDAP サーバーが使用されます。LDAP サーバーも利用できない場合は、ローカルユーザーの認証方式が使用されます。

RADIUS による認証方式も LDAP による認証方式も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の認証方式が選択されます。

Authorization（権限設定）

ロードマスターでは、RADIUS を用いて（またはローカルで）ユーザーに権限を設定できます。ユーザー権限の設定では、ユーザーがロードマスターのどの機能をどのレベルまで使用できるかを設定できます。

RADIUS による認証方式を使用している場合、RADIUS による権限設定のみ行えます。

権限設定方式が両方とも選択されている場合、ロードマスターは、まず始めに RADIUS による権限設定を試みます。RADIUS による権限設定を利用できない場合、ロードマスターは、ローカルユーザーの権限設定方式を使用します。なお、LDAP による権限設定はサポートしていません。

RADIUS による権限設定方式が選択されていない場合は、デフォルトでローカルの権限設定方式が選択されます

以下に示すのは、RADIUS サーバーによる認証が適切に機能する上で必要な設定の例です。

以下の例は、Linux 専用です。

"Reply-Message"には、許可する権限の種類をそのまま指定する必要があります。具体的には、"All Permissions"を除く、WUI のユーザー権限のページに対応させる必要があります。

LMUSER Cleartext-Password := "1fourall"

Reply-Message = "real,vs,rules,backup,certs,cert3,certbackup,users" bal
ユーザーは常に、ローカルユーザーの認証および承認方式に基づいて認証および承認されます。

RADIUS Server Configuration（RADIUS サーバーの設定）

RADIUS Server（RADIUS サーバー）

WUI からロードマスターへアクセスするユーザーの認証に使う RADIUS サーバーのアドレスとポート番号を入力します。

Shared Secret（共有秘密鍵）

RADIUS サーバーの共有秘密鍵を入力します。

共有秘密鍵とは、ロードマスターと RADIUS サーバーとの間のパスワードとして使用される文字列のことです。

Backup RADIUS Server（バックアップ用 RADIUS サーバー）

WUI からロードマスターへアクセスするユーザーの認証に使うバックアップ用 RADIUS サーバーのアドレスとポート番号を入力します。このサーバーは、メインの RADIUS サーバーが故障したときに使用されます。

Backup Shared Secret（バックアップ用共有秘密鍵）

このテキストボックスには、バックアップ RADUS サーバーの共有秘密鍵を入力します。

Revalidation Interval（再認証間隔）

RADIUS サーバーがユーザーを再認証する頻度を指定します。

LDAP Server Configuration（LDAP サーバーの設定）

LDAP Server（LDAP サーバー）

WUI からロードマスターへアクセスするユーザーの認証に使う LDAP サーバーのアドレスとポート番号を入力します。

Backup LDAP Server（バックアップ用 LDAP サーバー）

WUI からロードマスターへアクセスするユーザーの認証に使うバックアップ用 LDAP サーバーのアドレスとポート番号を入力します。このサーバーは、メインの LDAP サーバーが故障したときに使用されます。

LDAP Protocol（LDAP プロトコル）

LDAP サーバーとの通信で使用する転送プロトコルを選択します。

“Not encrypted”、“StartTLS”、“LDAPS”のオプションを選択できます。

Revalidation Interval（再認証間隔）

LDAP サーバーがユーザーを再認証する頻度を指定します。

Local Users Configuration（ローカルユーザーの設定）

Use ONLY if other AAA services fail（AAA サービスが失敗したときのみ使用）

このオプションを選択すると、RADIUS および LDAP による認証/権限設定方式に失敗したときのみ、ローカルユーザーの認証/権限設定方式が使用されます。

Test AAA for User（ユーザーの AAA をテスト）

ユーザーの資格情報をテストするには、**"Username"**および**"Password"**フィールドにそのユーザーのユーザー名とパスワードを入力して、**"Test User"**ボタンをクリックします。

これで、そのユーザーの認証に成功したかどうかを示すメッセージが表示されます。この機能を使用すると、ログイン/ログアウトを必要とせずに、ユーザーの認証情報をチェックできます。

9.7管理用 WUI へのアクセス

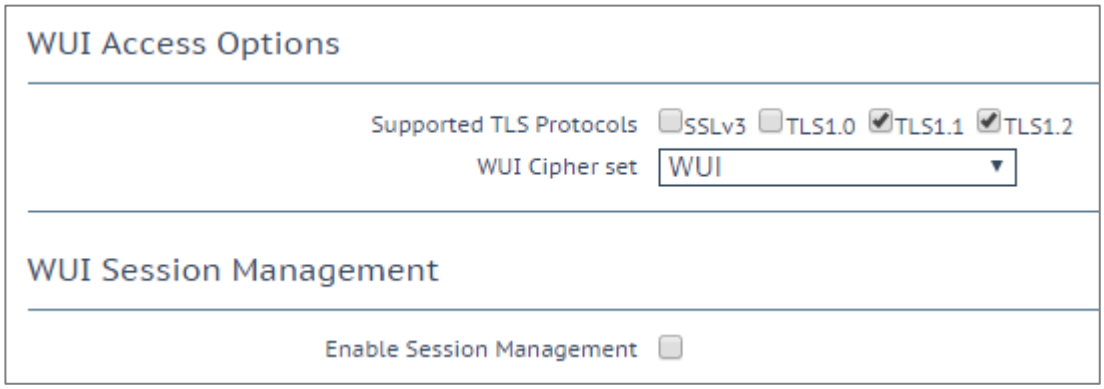

図 9-11:管理用 WUI への設定

Supported TLS Protocols（サポートされている TLS プロトコル）

ここでは、SSLv3、TLS1.0、TLS1.1、TLS1.2 のプロトコルを用いてロードマスターに接続できるかどうかを指定するためのチェックボックスが用意されています。TLS1.1 と TLS1.2 はデフォルトで有効になっています。SSLv3 は一部の古いブラウザーでしかサポートされていないため、SSLv3 だけを選択することは推奨されません。Web ブラウザーから WUI に接続する場合、ブラウザーと WUI の両方で相互にサポートされている最もセキュリティの高いプロトコルが使用されます。

FIPS モードが有効な場合、TLS1.1 および TLS1.2 のみ選択可能です。

WUI Cipher set（WUI 暗号セット）

WUI へのアクセスに使用する暗号セットを選択します。利用可能な暗号セットについては、**セクション 9.5** を参照してください。

WUI Session Management（WUI セッション管理）

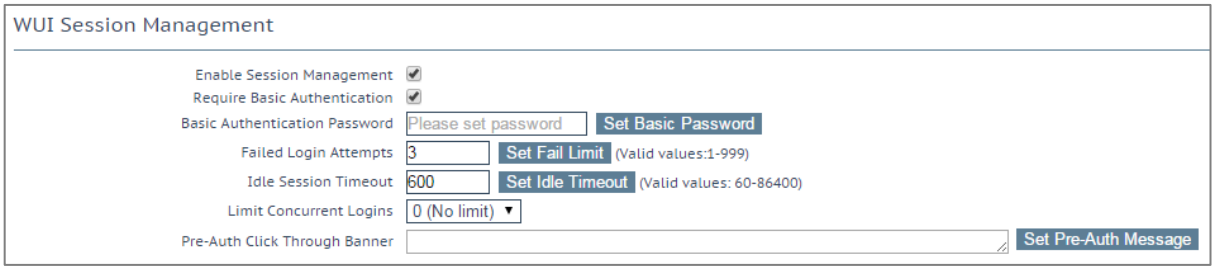

図 9-12:WUI セッション管理（bal ユーザー）

ファームウェアバージョン 7.1.35 以降のロードマスターは、展開された初期状態において、デフォルトでセッション管理が有効になっています。

ユーザー権限のレベルに応じて、WUI のどのセッション管理フィールドが表示・編集可になるかが決まります。権限の詳細については以下の表を参照してください。

制御	Bal ユーザー	'All Permissions'（すべての権限）を持つユーザー	'User Administration'（ユーザー管理）の権限を持つユーザー	その他のすべてのユーザー
セッション管理	Modify（変更）	表示	表示	None（なし）
Require Basic Authentication（基本認証が必要）	Modify（変更）	表示	表示	None（なし）
Basic Authentication Password（基本認証パスワード）	Modify（変更）	表示	表示	None（なし）
Failed Login Attempts（ログイン試行回数）	Modify（変更）	Modify（変更）	表示	None（なし）
Idle Session Timeout（アイドルセッションのタイムアウト）	Modify（変更）	Modify（変更）	表示	None（なし）
Limit Concurrent Logins（同時ログインを制限する）	Modify（変更）	Modify（変更）	表示	
Pre-Auth Click Through Banner（事前認証クリックスルーバナー）	Modify（変更）	Modify（変更）	表示	None（なし）
Currently Active Users（現在アクティブなユーザー）	Modify（変更）	Modify（変更）	表示	None（なし）

制御	Bal ユーザー	'All Permissions'（すべての権限）を持つユーザー	'User Administration'（ユーザー管理）の権限を持つユーザー	その他のすべてのユーザー
Currently Blocked Users（ブロックされたユーザー）	Modify（変更）	Modify（変更）	表示	None（なし）

表 9-2:WUI セッション管理の権限

WUI セッション管理を使用する場合、1 段階認証または 2 段階認証を使用できます。

"Enable Session Management"（セッション管理を有効にする）チェックボックスがオンになっており、**"Require Basic Authentication"（基本認証が必要）**が無効になっている場合、ユーザーはローカルのユーザー名とパスワードだけでログインできます。**"bal"**または**"user"**を使用してのログインは求められません。

"Enable Session Management"（セッション管理を有効にする）と**"Require Basic Authentication"（基本認証が必要）**のチェックボックスが両方ともオンになっている場合、ロードマスターWUI にアクセスするには 2 段階認証が必要です。最初の段階は基本認証で、**"bal"**または**"user"**でログインします（これらはシステムで定義されたデフォルトのユーザー名です）。

user ユーザーが用意されているのは、管理者が **bal** ユーザーの証明書ではなく **user** ユーザーの証明書を提供できるようにするためです。**user** ユーザーのパスワードを設定するには、**"Basic Authentication Password"**テキストボックスを設定します。**"Basic Authentication Password"**は **bal** ユーザーのみ設定できます。

基本認証でログインしたら、ローカルのユーザー名とパスワードでログインしてセッションを開始します。

Enable Session Management（セッション管理の有効化）

"Enable Session Management"チェックボックスをオンにすると、WUI セッション管理機能が有効になります。このとき、すべてのユーザーは通常の証明書を使用してセッションにログインする必要があります。

このチェックボックスをオンにした場合、ユーザーは、引き続きロードマスターを使用するためにログインする必要があります。

LDAP ユーザーは、ログイン時に完全なドメイン名を入力する必要があります。例えば、LDAP のユーザー名として、**test** ではなく **test@kemp.com** と入力する必要があります。

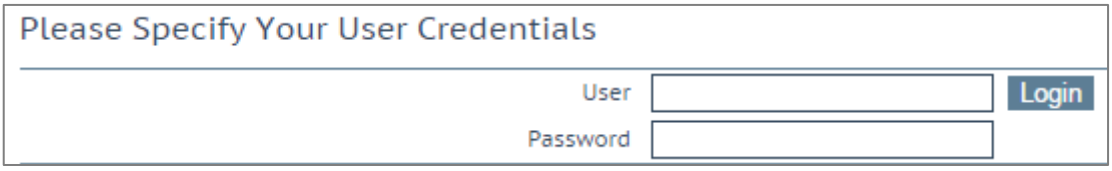

図 9-13:ユーザー資格情報

ログインしたユーザーは、画面の右上隅にある"Logout"ボタン  をクリックしてログアウトできます。

WUI のセッション管理機能を有効にすると、WUI のセッション管理オプションがすべて表示されます。

Require Basic Authentication（基本認証が必要）

WUI セッション管理と基本認証が両方とも有効になっている場合、ロードマスターにアクセスするには 2 段階認証が必要です。最初の段階は基本認証で、**“bal”**または**“user”**でログインします（これらはシステムで定義されたデフォルトのユーザー名です）。

基本認証でログインしたら、ローカルのユーザー名とパスワードでログインしてセッションを開始します。

Basic Authentication Password（基本認証パスワード）

"user"ログイン用の基本認証パスワードを設定するには、**"Basic Authentication Password"**テキストボックスにパスワードを入力して、**"Set Basic Password"**ボタンをクリックします。

パスワードは、アルファベットと数字を組み合わせ、8 文字以上になるように設定してください。パスワードが弱すぎると判断された場合、新たにパスワードを入力するよう求めるメッセージが表示されます。

“bal”ユーザーのみ、基本認証パスワードを設定できます。

Failed Login Attempts（ログイン試行回数）

このテキストボックスでは、ログインの失敗回数を指定して、この回数を上回ってログインに失敗したユーザーをブロックするよう設定できます。入力できる値の範囲は、**1** から **999** までです。

ユーザーがブロックされた場合、**“bal”**ユーザーまたは**“All Permissions”**の権限が設定されたユーザーのみ、ブロックされたユーザーのブロックを解除できます。

“bal”ユーザーがブロックされた場合、**“bal”**ユーザーが再度ログインできるようになるまで 10 分間の“クールダウン”期間が設けられています。

Idle Session Timeout（アイドルセッションのタイムアウト）

ユーザーがセッションからログアウトされる前に、ユーザーがアイドル状態（何も操作が記録されない状態）でいられる期間を秒で指定します。**60〜86400**（1 分〜24 時間）の値を入力できます。

Limit Concurrent Logins（同時ログインを制限する）

ロードマスターの管理者は、このオプションを使用して、1 人のユーザーがロードマスターWUI に 1 度にログインできる数を制限できます。

この値は 0〜9 の範囲で選択できます。

値を 0 にすると、ログイン数が制限されなくなります。

入力した値はトータルのログイン数を表します。この値には**"bal"**ユーザーのログインが含まれます。

Pre-Auth Click Through Banner（事前認証クリックスルーバナー）

ロードマスターの WUI ログインページの前に表示される事前認証クリックスルーバナーを設定します。このフィールドにはプレインテキストまたは HTML コードを入力できます。このフィールドには Java スクリプトは入力できません。このフィールドには 5,000 文字まで入力できます。

Active and Blocked Users（アクティブなユーザーおよびブロックされたユーザー）

“bal”ユーザーまたは“All Permissions”の権限が設定されたユーザーのみ、この機能を使用できます。“User Administration”の権限が設定されたユーザーの場合、画面上のボタンや入力フィールドはすべてグレー表示になります。その他のユーザーの場合、この部分は画面上に表示されません。

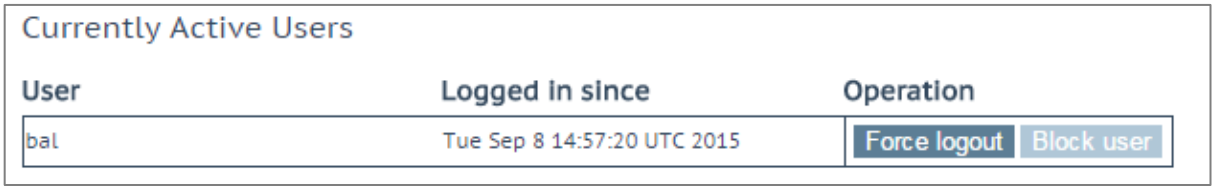

図 9-14:現在アクティブなユーザー

Currently Active Users（アクティブなユーザー）

このセクションには、ロードマスターにログインしている全ユーザーのユーザー名とログイン時刻がリスト表示されます。

ユーザーを直ちにログアウトさせ、システムに再度ログインするよう強制するには、**"Force logout"**ボタンをクリックします。

ユーザーを直ちにログアウトさせ、システムにログインできないようそのユーザーをブロックするには、**"Block user"**ボタンをクリックします。ブロックされたユーザーは、ブロックが解除されるか、ロードマスターが再起動するまで、システムに再度ログインできません。**"Block user"**ボタンをクリックしても、そのユーザーを強制的にログオフできません。この場合、**"Force logout"**ボタンをクリックする必要があります。

ユーザーがログオフせずにブラウザを終了した場合、そのセッションは、タイムアウトになるまでアクティブなユーザーのリストでオープンになったままとなります。その後、タイムアウトになる前にそのユーザーが再度ログインすると、そのユーザーは別のセッションでログインされます。

Currently Blocked Users（ブロックされたユーザー）

このセクションには、ユーザーがブロックされた時点でのユーザー名とログイン時刻がリスト表示されます。

ブロックされたユーザーのブロックを解除して、再度システムにログインできるようにするには、**"Unblock"**ボタンをクリックします。

9.8OCSP の設定

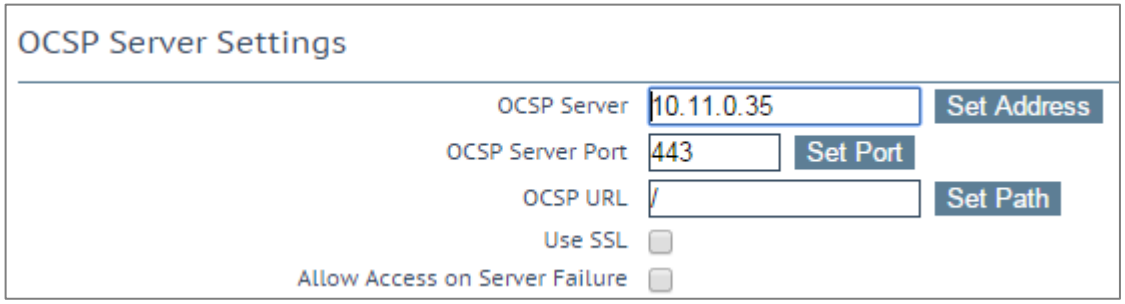

図 9-15:OCSP サーバーの設定

OCSP Server（OCSP サーバー）

OCSP サーバーのアドレスです。

OCSP Server Port（OCSP サーバーポート）

OCSP サーバーのポートです。

OCSP URL

OCSP サーバーにアクセスするための URL です。

Use SSL（SSL を使用する）

SSL を使用して OCSP サーバーに接続する場合はこのオプションを選択します。

Allow Access on Server Failure（サーバー障害発生時のアクセスを許可する）

OCSP サーバーが有効な応答を返したものとして（クライアント証明書が有効であるものとして）OCSP サーバー接続障害またはタイムアウトを処理します。

9.9HSM の設定

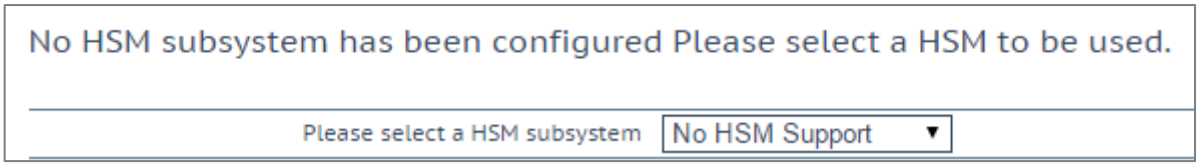

図 9-16:HSM をサポートしない場合

Please select a HSM subsystem（HSM サブシステムを選択してください）

このドロップダウンメニューでは 2 つのオプションが用意されています。

- **No HSM Support（HSM をサポートしない）**
- **Safenet Luna HSM**

HSM を使用するには、**"Safenet Luna HSM"**を選択して設定を行ってください。

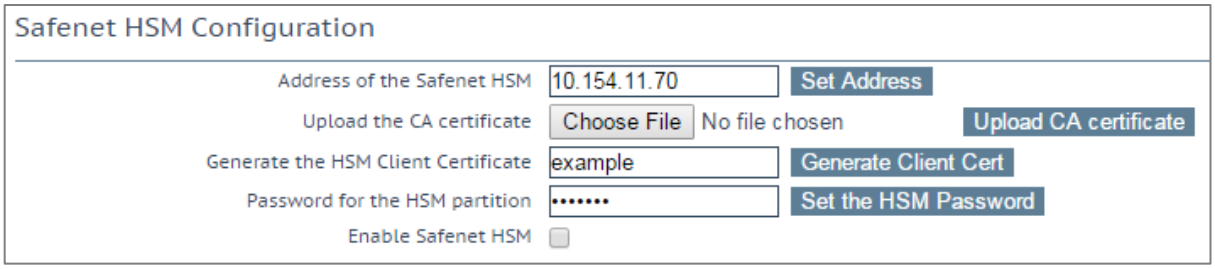

図 9-17:Safenet HSM の設定

Address of the Safenet HSM（Safenet HSM のアドレス）

使用する Safenet ユニットの IP アドレスを入力します。

Upload the CA certificate（CA 証明書のアップロード）

HSM からダウンロードした証明書をアップロードします。

Generate the HSM Client Certificate（HSM クライアント証明書の生成）

HSM にアップロードするローカルクライアントの証明書を生成します。ここで指定する名前は、ロードマスターの FQDN 名である必要があります。この名前は、HSM の **client register** コマンドで使用されます。

Password for the HSM partition（HSM パーティションのパスワード）

ロードマスターが HSM にアクセスできるように、HSM におけるパーティションのパスワードを指定します。

証明書を生成するまで、パーティションのパスワードは指定できません。

Enable Safenet HSM（Safenet HSM を有効にする）

このチェックボックスを使用すると、HSM を有効/無効にできます。

HSM の起動には時間がかかる場合があります。

HSM を無効にすると、新たに HSM が追加されるか証明書の設定が変更されるまで、ロードマスターが新たな SSL（HTTPS）接続を作成できなくなり、既存の接続が直ちにドロップされます。

アクティブな SSL 接続が存在しない場合のみ HSM の設定を変更することを強く推奨します。

10 System Configuration（システム用設定）

10.1 ネットワークの設定

10.1.1 Interfaces（インターフェイス）

外部ネットワークと内部ネットワークのインターフェイスについて規定します。この画面には、**eth0** および **eth1** イーサネットポートで同じ情報が用意されています。以下の例は、非高可用性（HA）ユニットの **eth0** の場合です。

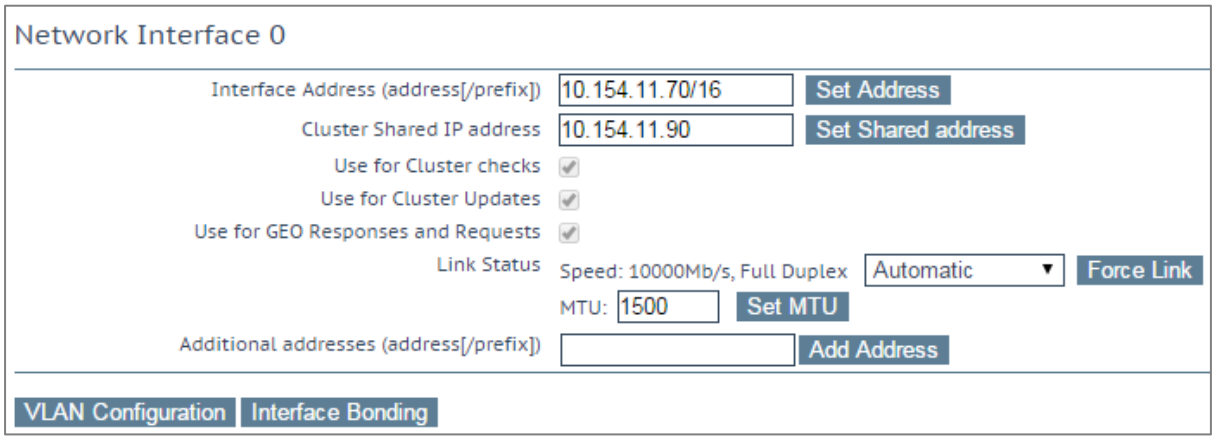

図 10-1:ネットワークインターフェイスのオプション

Interface Address（インターフェイスアドレス）

"Interface Address (address[/prefix])"テキストボックスにて、このインターフェイスのインターネットアドレスを指定できます。

Cluster Shared IP address（クラスターの共有 IP アドレス）

クラスターへのアクセスに使用できる共有 IP アドレスを指定します。これは、サーバーの NAT を使用する際のデフォルトのソースアドレスとしても使用されます。

"Clustering"のオプションは、ロードマスターにクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMP の担当者にお問い合わせください。クラスタリングについての詳細は、**ロードマスターのクラスタリング　機能説明**を参照してください。

Use for Cluster checks（クラスターのチェックで使用）

このオプションを使用すると、ノード間でクラスターのヘルスチェックを行うことができます。少なくとも 1 つのインターフェイスを有効にする必要があります。

Use for Cluster Updates（クラスターの更新で使用）

これは、クラスターの同期動作のためのインターフェイスです。

Speed（速度）

デフォルトでは、リンクの **Speed（速度）**は自動的に検出されます。構成によってはこの速度は適切でない場合があるため、値を指定する必要があります。

Use for Default Gateway（デフォルトゲートウェイで使用）

"Use for Default Gateway"チェックボックスを使用できるのは、**"Network Options"**画面で**"Enable Alternate GW support"**が選択されている場合に限定されます。表示対象の設定がデフォルトのインターフェイス用である場合、このオプションは灰色表示で選択されている状態です。このオプションを別のインターフェイスで有効にするには、左側にあるメインメニューでインターフェイスをクリックし、そのインターフェイスに移動します。これで、このオプションを選択できる状態になります。

Allow Administrative WUI Access（管理用 WUI へのアクセスを許可）

このオプションは、**"Miscellaneous Options > Remote Access"**の**"Allow Multi Interface Access"**チェックボックスがオンの場合のみ利用できます。

これらのオプションを 2 つとも有効にすると、該当するインターフェイスの IP アドレスと、そのインターフェイスに設定された**"Additional addresses"（追加アドレス）**から WUI にアクセスできます。

> これらの全アドレスに対して 1 つのインターフェイスのみ割り当てられます。そのため、ワイルドカード証明書以外の証明書を使用すると問題が生じるおそれがあります。証明書についての詳細は、**アプリケーションファイアウォールパック（AFP）カスタムルール**を参照してください。

最大 64 個のネットワークインターフェイスを追跡できます。また、トータルで最大 1024 個のアドレスがシステムによりリッスンされます。

Use for GEO Responses and Requests（GEO の応答/要求に使用）

デフォルトでは、デフォルトゲートウェイを使用して DNS 要求をリッスンして応答を返します。このフィールドを使用すると、他のインターフェイスでもリッスンできるようになります。

このオプションは、デフォルトゲートウェイを含むインターフェイスでは無効にできません。デフォルトでは eth0 に設定されています。

このオプションを有効にすると、GEO はそのインターフェイスで設定された**"Additional addresses"**でもリッスンします。

MTU

“MTU”フィールドでは、このインターフェイスから送信されるイーサネットフレームの最大サイズを指定できます。有効範囲は 512～9216 です。

VLM の場合、VLM が実行されているハードウェアによって有効範囲が決まるため、**512～9126** の範囲が必ず適用されるとは限りません。ハードウェアによる制約をチェックするようにしてください。

Additional addresses（追加アドレス）

"Additional addresses"フィールドを使用すると、ロードマスターから複数のアドレスを各インターフェイスにエイリアスとして提供できます。この機能は、「ルーター・オン・ア・スティック」と呼ばれることがあります。この機能では、標準 IP+CIDR 形式の IPv4 アドレスと IPv6 アドレスの両方が使用できるので、同じインターフェイス上で IPv4 アドレスと IPv6 アドレスが混在するモードも実現できます。ここで追加したサブネットはすべて、仮想 IP アドレスと実サーバーIP アドレスの両方で使用できます。

HA

ユニットが HA 構成の一部である場合、いずれかのインターフェイスをクリックすると、次の画面が表示されます。

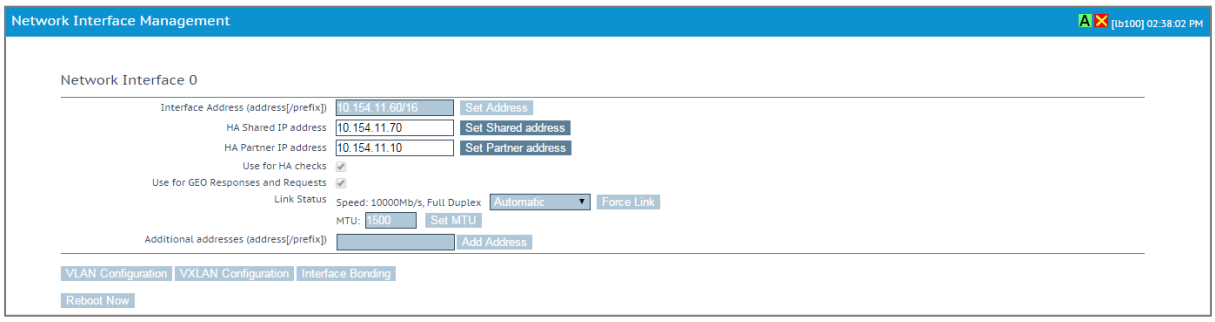

図 10-2:ネットワークインターフェイスの管理 - HA

この画面では、ユーザーに下記を示唆します。

- これはペアの**マスター**マシン（画面の左上）です。
- このシステムは アップ状態であり、ペアを組む相手マシンはダウンしています（緑と赤のアイコン）。
- このインターフェイスアドレスは、このユニット自身の IP アドレスです。
- **"HA Shared IP address"**。ペアを組む相手マシンの IP アドレスです。
- ペアマシンの IP アドレス
- このインターフェイスは、HA ヘルスチェックが有効になっています。
- このインターフェイスは、デフォルトゲートウェイとして使用されています。
- リンクの速度が自動的に検出されています（Link Status）。
- このインターフェイスの代替アドレスは登録されていません（Additional addresses）

ボンディング/チーミングの設定

ボンディングインターフェイスを作成する前に、以下の点に注意してください。

- 親より大きい番号のボンディングインターフェイスのみ作成できます。例えば、ポート 10 から始まるように指定した場合、ポート 11 以降のインターフェイスのみ作成できます。
- VLAN タギングが必要な場合、まず始めにリンクをボンディングし、ボンディングの設定が終わった後に VLAN を追加してください。
- 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発生する可能性があるので、このボンディングは許可されていません。

"Interface Bonding"ボタンをクリックし、ボンディングを要求します。

"Create a bonded interface"ボタンをクリックし、ボンディングの作成を実行します。

警告ダイアログを確認します。

ウェブユーザーインターフェイス（WUI）を使用して、**“System Configuration > Interfaces > bndx”**メニューオプションを選択します。

"bndX"インターフェイスが表示されない場合、ブラウザの表示を更新し、ボンディングインターフェイスを選択して、**"Bonded Devices"**ボタンをクリックします。

目的のボンディングモードを選択します。

ボンディングにインターフェイスを追加します。

ボンディングインターフェイスの IP アドレスとサブネットマスクを設定します。

ボンディング／チーミングの解除

ボンディングポートに VLAN が設定されている場合は、まずこれらの設定を削除します。これらを削除しないとボンディングを解除したポートの最初の親ポートにこれらの設定が残ります。

"System Configuration > Interfaces > bndx"メニューオプションを選択します。**"bndX"**インターフェイスが表示されない場合、ブラウザの表示を更新し、ボンディングインターフェイスを選択して、**"Bonded Devices"**ボタンをクリックします。

ポートのボンディングを解除するには、**“Unbind Port”**ボタンをクリックします（すべてのポートのボンディングが解除されるまでこの作業を繰り返します）。

子ポートのボンディングをすべて解除したら、**“Unbond this interface”**ボタンをクリックして親ポートのボンディングを解除できます。

Adding a VLAN（VLAN の追加）

インターフェイスを選択し、**“VLAN Configuration”**ボタンをクリックします。

図 10-3:VLAN Id

“VLAN Id”に値を入力し、“Add New VLAN”メニューオプションを選択します。

必要に応じて、手順を繰り返します。VLAN を表示するには、**"System Configuration" > "Network Setup"**メニューオプションを選択してドロップダウンリストを展開します。

Removing a VLAN（VLAN の削除）

VLAN を削除する前に、インターフェイスが他の用途（マルチキャストインターフェイス、WUI インターフェイス、SSH インターフェイス、GEO インターフェイスなど）で使用されていないことを確認してください。

VLAN を削除するには、**"System Configuration" > "Network Setup"**メニューオプションを選択し、プルダウンリストから目的の VLAN ID を選択します。

VLAN ID を選択したら、IP アドレスを削除して、**"Set Address"**をクリックします。IP アドレスが削除されたら、**"Delete this VLAN"**ボタンをクリックし、VLAN を削除します。

必要に応じて、手順を繰り返します。VLAN を表示するには、**"System Configuration > Interfaces"**メニューオプションを選択して、ドロップダウンリストから目的の VLAN ID を選択します。

Adding a VXLAN（VXLAN の追加）

目的のインターフェイスを選択し、**"VXLAN Configuration"（VXLAN の設定）**ボタンをクリックします。

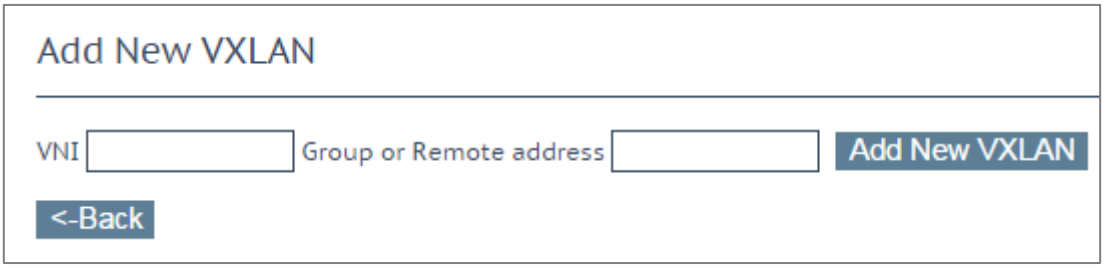

図 10-4:VXLAN の新規追加

"VNI"テキストボックスに、新しい VXLAN ネットワーク識別子（VNI）を入力します。**"Group or Remote address"（グループまたはリモートアドレス）**テキストボックスに、マルチキャストグループまたはリモートアドレスを入力します。**"Add New VXLAN"（VXLAN の新規追加）**をクリックします。

VXLAN を編集するには、**"System Configuration > Interfaces"**を選択して、ドロップダウンリストから目的の VXLAN を選択します。

図 10-5:VXLAN の編集

この画面では、VXLAN のインターフェイスアドレスを指定できます。また、この画面では VXLAN の削除も行えます。

HA が有効になっている場合、VXLAN にて HA パラメーターの設定が行えます。

- **"HA Shared IP address"**。これは、HA ペアの設定で使用される IP アドレスです。
- パートナーマシンの IP アドレス
- このインターフェイスを HA ヘルスチェックで使用するかどうかを指定します。

10.1.2 ホストと DNS の設定

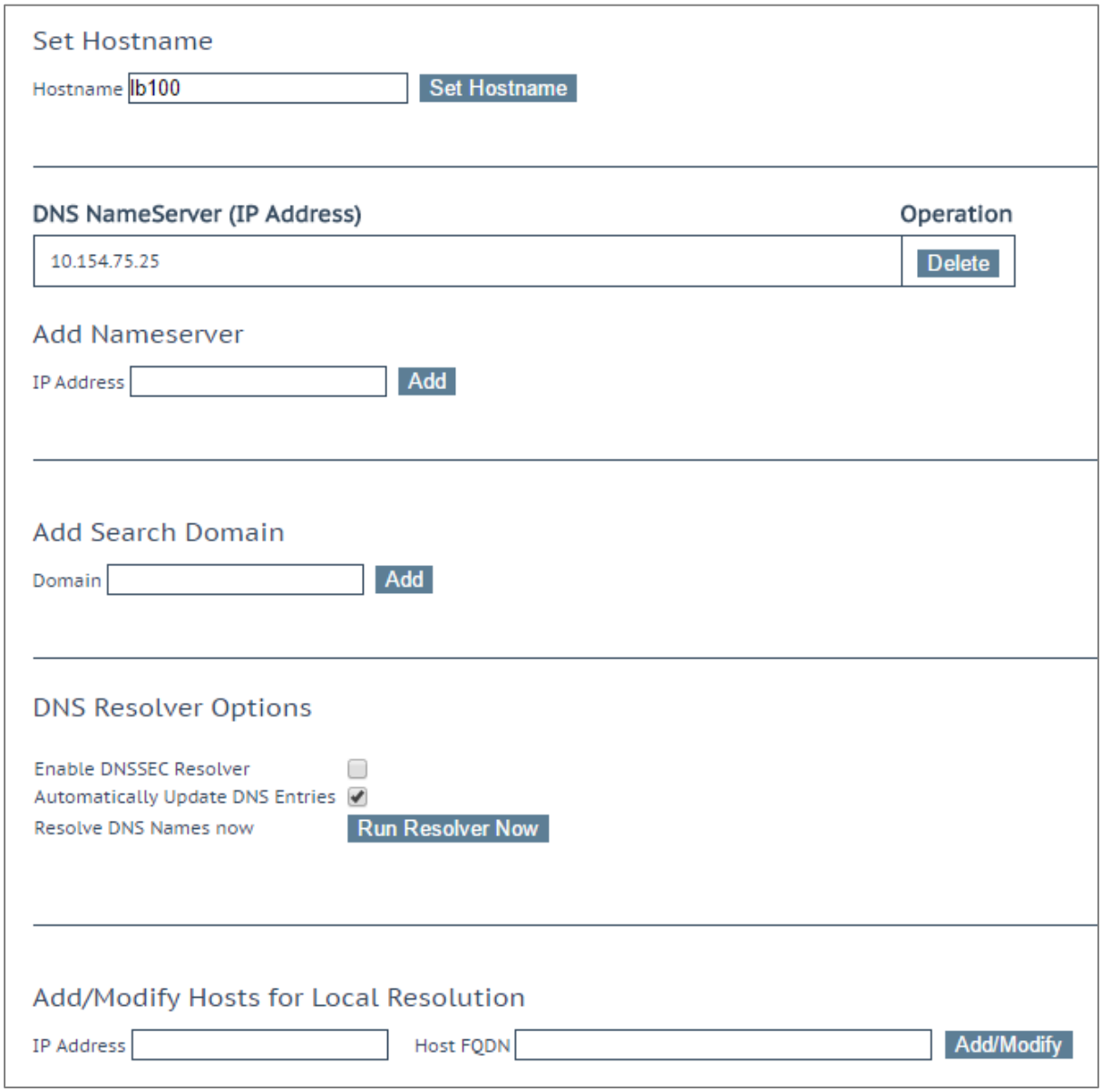

図 10-6:ホスト名と DNS の設定

ホスト名の設定

"Hostname"（ホスト名）テキストボックスにホスト名を入力し、**"Set Hostname"（ホスト名の設定）**ボタンをクリックして、ローカルマシンのホスト名を設定します。使用できるのは、英数字だけです。

Add NameServer (IP Address)（ネームサーバーの追加（IP アドレス））

ロードマスターにてローカルに名前解決する DNS サーバーの IP アドレスを入力し、**"Add"**ボタンをクリックします。最大 3 つまで DNS サーバーを指定できます。

DNSSEC が有効な場合、最後に残ったネームサーバーを削除することはできません。DNSSEC クライアントは、**"Host & DNS Configuration"** 画面で無効にできます。

Add Search Domain（検索ドメインの追加）

DNS ネームサーバーへのリクエストの先頭に追加するドメイン名を入力し、**"Add"**ボタンをクリックします。最大 6 つまで検索ドメインを指定できます。

Add/Modify Hosts for Local Resolution（ローカル名前解決ホストの追加/編集）

このフィールドを使用すると、ロードマスターからホストファイルを操作できます。IP アドレスとホスト FQDN を指定してください。

Enable DNSSEC Resolver（DNSSEC レゾルバを有効にする）

デフォルトでは、ロードマスターの DNSSEC クライアントは無効になっています。必要な場合のみこのオプションを有効にしてください。DNSSEC の検証は、失敗するまで非常に時間がかかることがあります。これにより、ロードマスターがフリーズまたはハングするおそれがあります。

このオプションを有効にすると、ロードマスターで DNSSEC 機能が有効になります。DNSSEC を有効にするには、**ネームサーバー**を 1 つ以上追加する必要があります。この機能を有効/無効にするには、DNSSEC オプションを変更後にロードマスターを再起動する必要があります。1 度設定を変更すると、ロードマスターを再起動するまで設定を再度変更できません。

HA を使用している場合、両方の機器で個別に DNSSEC オプションを設定する必要があります。

DNSSEC は、ロードマスターの以下のユーティリティで機能します。

- Vipdump
- Ping および ping6
- Syslog
- SNMP

- Wget
- NTP
- SMTP
- 実サーバー

Automatically Update DNS Entries（DNS エントリの自動更新）

このオプションを有効にすると、ロードマスターにより 1 時間おきに DNS 名の解決が試みられます。

- アドレスが見つからない場合、または、アドレスが前回と同じであった場合、何も行いません（ログエントリの作成を除く）。
- アドレスが前回と異なる場合、実サーバーのエントリが新しいアドレスで更新されます。
- 何らかの理由によりアドレスが無効であった場合、例えば、そのアドレスがローカルのアドレスではなく、**"Enable Non-Local Real Servers"**オプションが無効であった場合、何も変更されずにログが作成されます。

Resolve DNS Names now（DNS 名を直ちに解決する）

"Run Resolver Now"ボタンをクリックすると、DNS 名が直ちに解決されます。この動作は、**"Automatically Update DNS Entries"**オプションと同じですが、手動チェック（自動ではない）である点が異なります。

10.1.3 デフォルト・ゲートウェイ

ロードマスターでは、インターネットに接続するためのデフォルト・ゲートウェイを設定する必要があります。

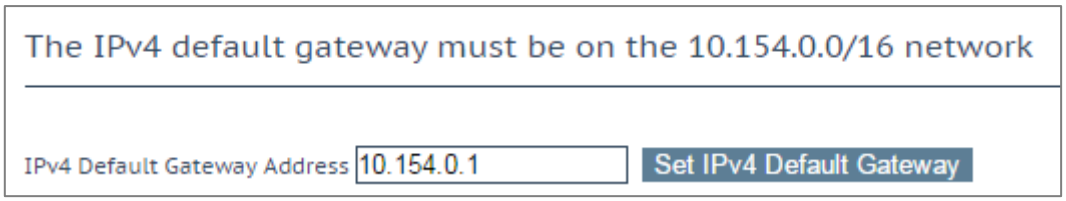

図 10-7:デフォルト・ゲートウェイ

ロードマスターで IPv4 と IPv6 を使用する場合、IPv4 と IPv6 のデフォルト・ゲートウェイ・アドレスを指定する必要があります。

IPv4 および IPv6 のデフォルトゲートウェイは、同じインターフェイス上に存在している必要があります。

10.1.4 追加ルート

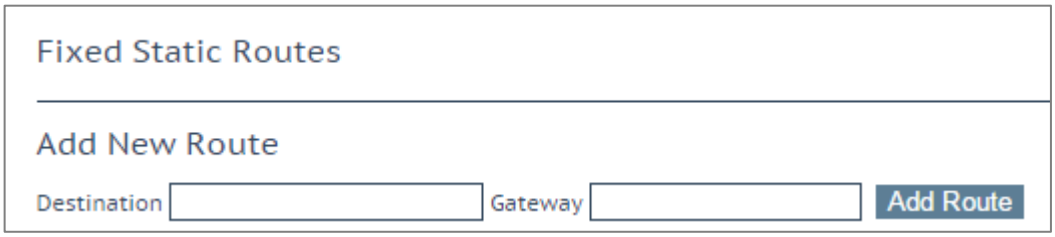

図 10-8:追加ルート

追加のルートを設定できます。これは静的ルーティングであるため、ゲートウェイはロードマスターと同じネットワーク上になければなりません。なお、仮想サービスレベルのデフォルト・ゲートウェイを使用してトラフィックを分割することもできます。

10.1.5 Packet Routing Filter（パケット・ルーティング・フィルター）

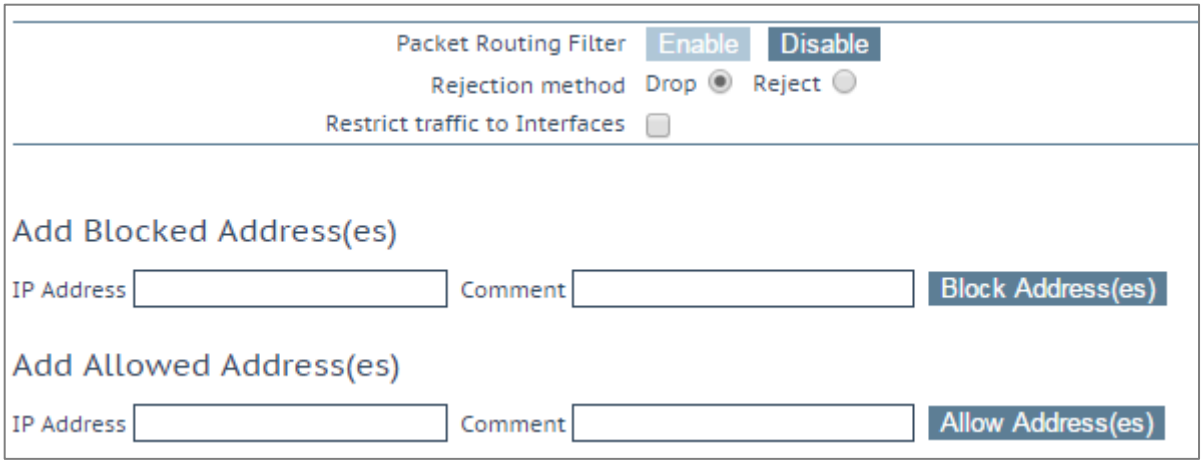

図 10-9:パケットフィルター

Packet Routing Filter（パケット・ルーティング・フィルター）

GEO を有効にすると、**"Packet Routing Filter"（パケット・ルーティング・フィルター）**はデフォルトで有効に設定され、無効に変更することはできません。GEO を無効にすると、**"Packet Routing Filter"（パケット・ルーティング・フィルター）**が設定可能になり、有効/無効を切り替えることができます。GEO 機能を持つロードマスター上で GEO を無効にするには、メインメニューにて**"Global Balancing"**を選択し、**"Disable GSLB"**を選択します。

フィルターが有効になっていない場合、ロードマスターは単純な IP フォワーダーとしても機能します。

フィルターを有効にするとロードマスターへのトラフィックが制限されますが、ロードマスターを経由したクライアントから仮想サービスへのアクセスは影響を受けません。

また、実サーバーから送信され、SNAT が設定されたロードマスターで処理されたトラフィックも影響を受けません。

"Packet Routing Filter"が無効の場合、**"Reject/Drop blocked packets"**フィールドと**"Restrict traffic to Interfaces"**フィールドは表示されません。

Reject/Drop blocked packets（ブロックされたパケットのリジェクト/ドロップ）

ホストから送信された IP パケットがアクセス制御リスト（ACL）でブロックされた場合、その要求は通常、無視（ドロップ）されます。ICMP 拒否パケットを返すようロードマスターを設定できますが、セキュリティ上の理由から、通常の場合は、ブロックされたパケットをそのままドロップすることを推奨します。

Restrict traffic to Interfaces（インターフェイスへのトラフィックを制限）

接続されているサブネット間のルーティングを制限します。

Add Blocked Address(es)（ブロックされたアドレスを追加）

ロードマスターは、「ブラックリスト」に基づくアクセス制御リスト（ACL）システムをサポートしています。アクセス制御リストに設定されたホストやネットワークは、ロードマスターが提供するサービスへのアクセスをブロックされます。

ACL が有効になるのは、パケットフィルターが有効になっている場合に限定されます。ホワイトリストは、特定の IP アドレスまたはアドレス範囲からのアクセスを許可します。ホワイトリストで指定されたアドレス（またはアドレス範囲）が、ブラックリストで指定された範囲に含まれる場合、ホワイトリストの指定が優先されます。

ブラックリストにアドレスが指定されておらず、ホワイトリストにのみアドレスが指定されている場合、ホワイトリストで指定されたアドレスからの接続のみ許可され、その他のアドレスからの接続はブロックされます。

このオプションでは、ホストまたはネットワークの IP アドレスをアクセス・コントロール・リストに追加（またはリストから削除）できます。また、システムが IPv6 アドレスファミリで構成されている場合、IPv4 に加えて IPv6 のアドレスもリストに指定できます。ネットワークを指定するには、ネットワーク識別子を使用します。

例えば、ブラックリストに **192.168.200.0/24** のアドレスを指定すると、192.168.200 のネットワーク上にあるすべてのホストがブロックされます。

アクセスリストにて特定のトラフィックをブロックするよう定義し、それと同じ IP アドレスにてワイルドカードの仮想サービスが設定されている場合、静的ポートの仮想サービスは正常に機能しません。静的ポートの仮想サービスにてそのトラフィックが拒否された後に、ワイルドカードの仮想サービスにてそのトラフィックが受け付けられます。

この場合、上記の相互作用により予期せぬ動作が引き起こされるのを防ぐため、別々の IP アドレスを使用するようにしてください。

10.1.6 VPN 管理

"VPN Management"のリンク/画面は、ロードマスターに IPsec トンネリングのライセンスが与えられている場合のみ利用できます。

IPsec トンネリングに関する詳細（セットアップ手順を含む）は、**IPsec トンネリング機能説明**を参照してください。

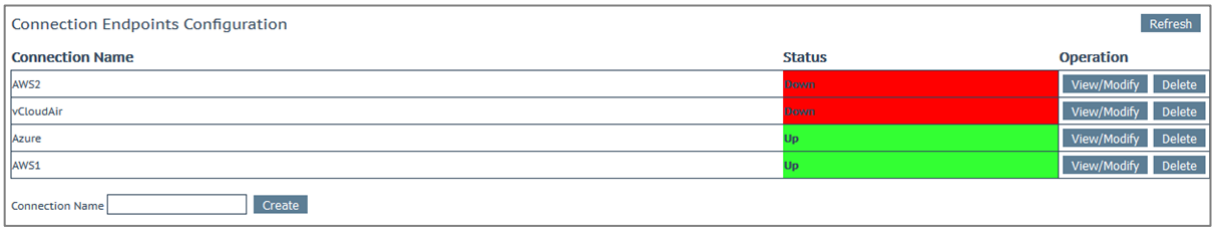

図 10-10:VPN の管理

Connection Name（接続名）

接続を識別するための一意の名前を指定します。

Create（作成）

指定した名前を使用して、一意に識別可能な接続を作成します。

View/Modify（表示/変更）

この接続の設定パラメーターを表示/変更します。

Delete（削除）

この接続を削除します。

関連する設定が完全に削除されます。接続は、それが動作中であってもいつでも削除できます。

10.1.6.1 VPN 接続の表示/変更

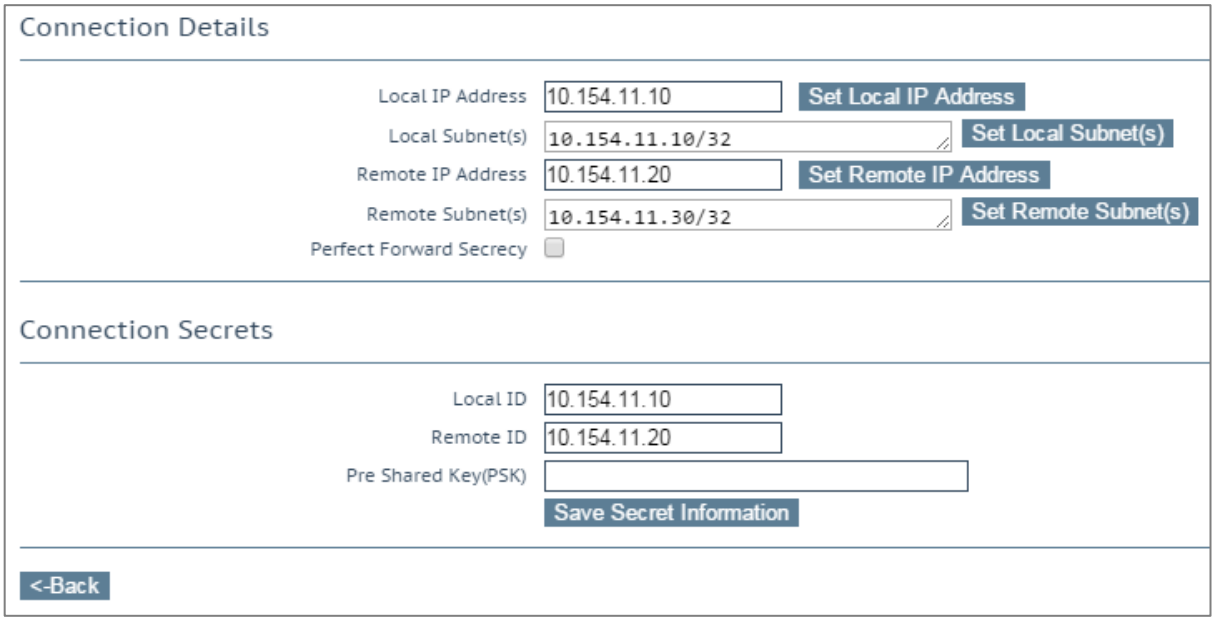

図 10-11:接続の変更

最初に接続を作成するとき、または接続を変更するときに"**View/Modify VPN Connection**"画面が表示されます。

Local IP Address（ローカル IP アドレス）

接続のローカル側の IP アドレスを設定します。

非 HA モードの場合、"**Local IP Address**"はロードマスターの IP アドレス（デフォルトゲートウェイの IP アドレス）である必要があります。

HA モードの場合、"**Local IP Address**"は共有 IP アドレスである必要があります。HA が設定済みの場合、このアドレスは自動的に設定されます。HA 構成におけるトンネリングのセットアップに関する詳細は、次のセクションを参照してください。

Local Subnet Address（ローカルサブネットアドレス）

"**Local IP Address**"が"**Local Subnet Address**"に設定されている場合、テキストボックスに値が自動的に設定されます。/32 CIDR が与えられている場合、ローカル IP が唯一のパーティシパントとなります。必要に応じて"**Local Subnet Address**"を確認してください。アド

レスを変更したかどうかにかかわらず、必ず**"Set Local Subnet Address"**をクリックして設定を適用してください。複数のローカルサブネットを指定するには、カンマ区切りのリストを使用します。最大 10 個の IP アドレスを指定できます。

Remote IP Address（リモート IP アドレス）

接続のリモート側の IP アドレスを設定します。Azure エンドポイントの場合、この IP アドレスは、仮想プライベートネットワーク（VPN）のゲートウェイ機器におけるパブリック側の IP アドレスである必要があります。

Remote Subnet Address（リモートサブネットアドレス）

接続のリモート側のサブネットを設定します。複数のリモートサブネットを指定するには、カンマ区切りのリストを使用します。最大 10 個の IP アドレスを指定できます。

Perfect Forward Secrecy（前方秘匿性）

前方秘匿性のオプションを有効/無効にします。

使用されているクラウドプラットフォームに応じて、**"Perfect Forward Secrecy"（前方秘匿性）**のどのオプションを設定すべきかが決まります。**"Perfect Forward Secrecy"（前方秘匿性）**は、それが必要なプラットフォームもあれば、それをサポートしていないプラットフォームもあります。お使いのクラウドプラットフォームで何が機能するかは、**IPsec トンネリング　機能説明**を参照してください。

Local ID（ローカル ID）

接続のローカル側の識別子です。通常、ローカル IP アドレスが使用されます。ロードマスターが HA モードでない場合、このフィールドには **Local IP Address** と同じアドレスが自動的に設定されます。

ロードマスターが HA モードにある場合、**Local ID** フィールドは自動的に**%any** に設定されます。ロードマスターが HA モードにあるとき、この値は更新できません。

Remote ID（リモート ID）

接続のリモート側の識別子です。通常、リモート IP アドレスが使用されます。

Pre Shared Key (PSK)（プレシェアードキー）

プレシェアードキーの文字列を入力します。

Save Secret Information（秘密情報を保存）

接続の識別子および秘密情報を生成/保存します。

10.2 HA とクラスタリング

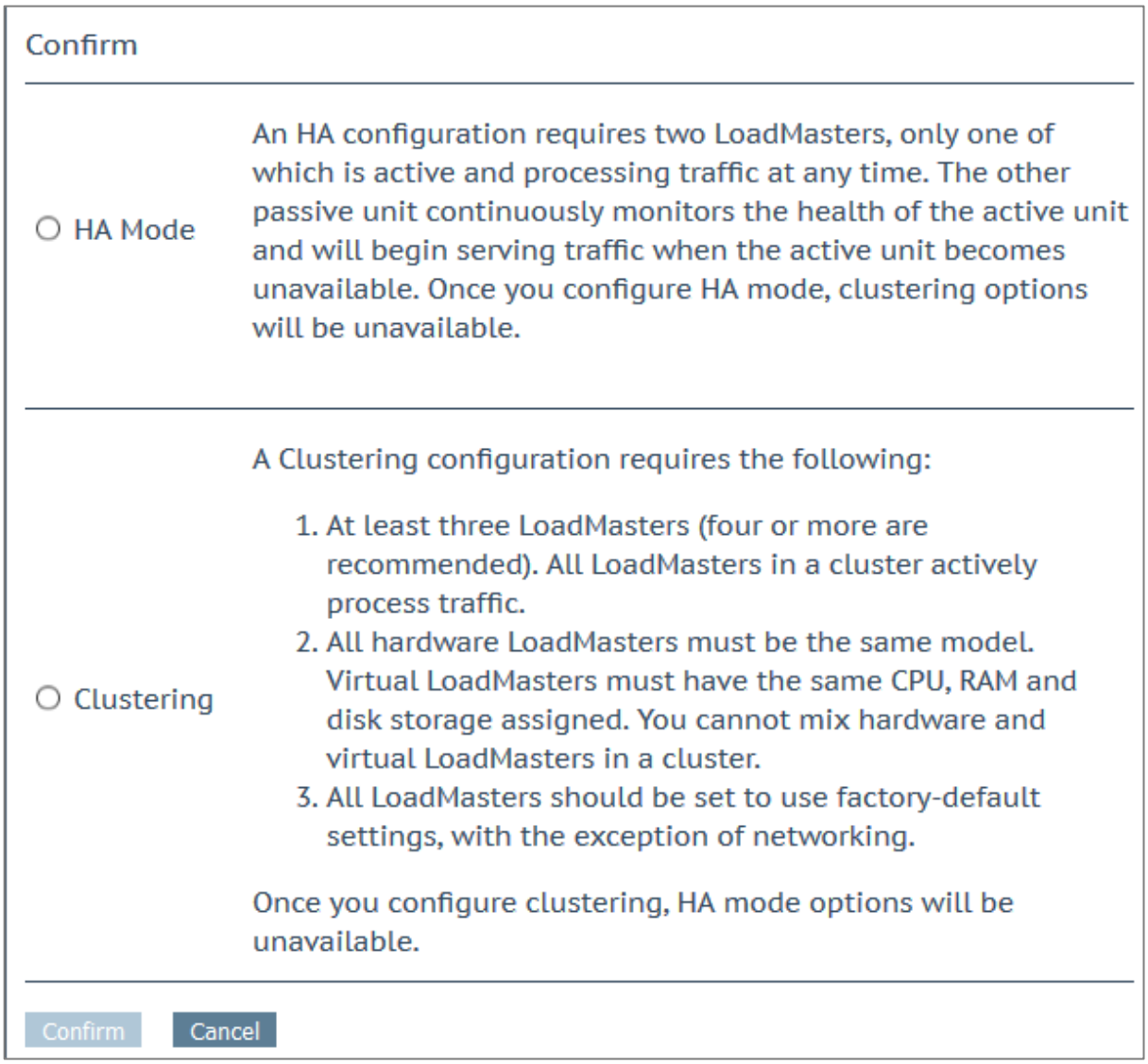

図 10-12:HA モードまたはクラスタリング

WUI のこのセクションは、ロードマスターのクラスタリングのライセンスが有効な場合のみ**"HA and Clustering "（HA とクラスタリング）**と呼ばれます。クラスタリングが設定されていない場合、このセクションは**"HA Parameters"（HA パラメーター）**と呼ばれ、上記の画面は表示されません。クラスタリングが設定されている場合、このセクションは**"Cluster Control"（クラスター制御）**と呼ばれます。

この画面は、**"HA Mode"（HA モード）**と**"Clustering"（クラスタリング）**について説明しています。目的のオプションを選択し、**"Confirm"**をクリックして次に進みます。

クラスタリングを設定した場合、HA モードのオプションは利用できません。

10.2.1 HA Mode（HA 構成モード）

ロードマスターfor Azure を使用する場合は、**セクション 10.2.1.1** を参照してください。

各ユニットのロールは、「HA モード」パラメータを設定し直すことで変更することができます。**"HA (First) Mode"**または**"HA (Second) Mode"**を**"HA Mode"**として選択した場合、共有 IP アドレスを追加するよう促すプロンプトが表示されます。"HA Mode"を変更すると再起動が必要になるので、詳細を設定したら、画面の**"Reboot"**ボタンをクリックします。ロードマスターが再起動すると、ロールが"Non HA Mode"ではない場合、**"System Configuration"**セクションで"HA"メニューオプションが使用可能になります。2 台を両方とも同じ HA モードにすると正しいペアとして構成されません。

HA ペアにログインして、完全な機能の表示および設定を行うには、共有（シェアード）IP アドレスを使用します。ユニットに与えられた IP アドレスに直接ログインした場合、WUI として表示されるメニューが異なります（下記のメニューを参照してください）。各ユニットの IP アドレスでの直接ログインは、通常そのユニットのみのメンテナンスを行うために行います。

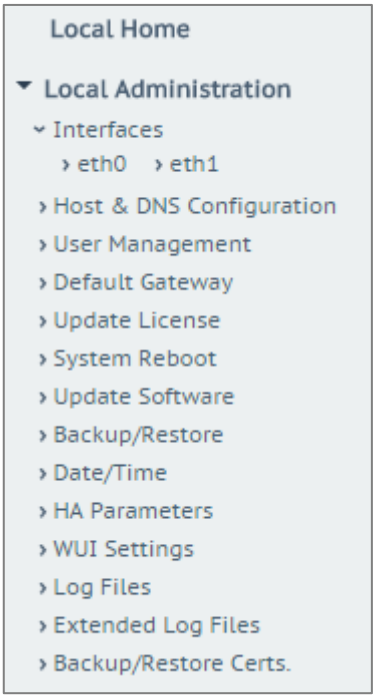

図 10-13:ダイレクト IP メニュー

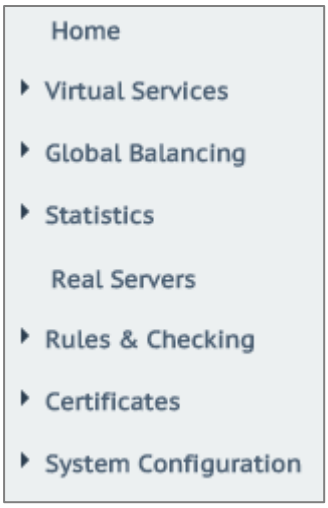

図 10-14:共有 IP メニュー

ロードマスターが HA モードになっている場合、**“HA Parameters”**メニューオプションを選択したときに以下の画面が表示されます。

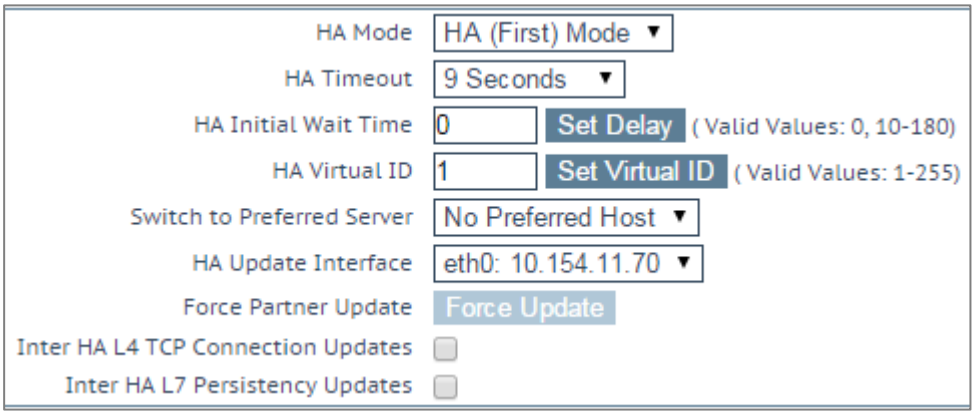

図 10-15:HA の設定

HA Status（HA 状態）

画面上部の時刻表示の隣にあるアイコンは、クラスター内のロードマスターユニットのリアルタイムステータスを示しています。左側のアイコンは、HA-1、右側は HA-2 に対

応しています。該当するステータスアイコンをクリックすると、1 番目または 2 番目の HA ユニットの WUI を開くことができます。

可能なアイコンとして、下記のパターンがあります。

緑（'A'の文字あり）		ユニットは、オンラインで正常に稼動しています。 中央に'A'の文字が表示された四角は、マスターユニットであることを表します。
緑（'A'の文字なし）		ユニットは、オンラインで正常に稼動しています。 中央に'A'の文字が表示されていない四角は、マスターユニットではないことを表します。
赤で黄色の X		ユニットはオフラインです。正しい HA 構成がなされていません。
青		両方のマシンがアクティブモードとなっています。すなわち、何らかの設定間違いが何かで両方がマスターで立ち上がっています。両ユニットのイーサネットポートの設定を確認後、一つのユニットを再リブートしてみると解決するかもしれません。
灰		3 分以内に二回以上のリブートが発生したためにパッシファイ（管理者対応を要求し、システムはホルト状態）モードです。原因究明、そしてその対処後、再リブートが必要です。***KEMP のサポートにご連絡ください。***

HA モードでは、各ユニットは、自身の直接診断目的でのみ使用する、独自の IP アドレスを持ちます。そして、単一のエンティティとして HA 構成の設定および管理を行うために使用される WUI 上の共有 IP アドレスを持ちます。

HA1 と HA2 の両方が同一のデフォルトゲートウェイと同じサブネット上に存在し、同じ物理サイト内に存在する必要があります。サイト内リンクで区分されることなく、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。

HA Mode（HA 構成モード）

スタンドアローン、HA-1（HA First）、もしくは HA-2（HA Second）の選択ができます。同じ HA モードでは、正しい HA 構成が組めません。この設定を変更するときにはシステムリブートが必要です。

> KEMP は HA 対応のライセンスを HA ユニットごとに提供し、ユニット 1 とユニット 2 として規定しています。したがって、KEMP のサポート部門と問題について話し合わずに、このオプションを変更することは推奨しません。

HA Timeout（HA タイムアウト）

スイッチオーバーが発生する前にマスターマシンを利用できなくする時間です。このオプションを使用すると、HA クラスターが障害を検出するのに要する時間を 3 秒から 15 秒まで 3 秒刻みで調整できます。デフォルト値は 9 秒です。値を低くすると、障害がより早く検出されます。一方、値を高くすると、DOS 攻撃に対する防御が強くなります。

HA Initial Wait Time（HA 起動待機時間）

ロードマスターの初回起動後、マシンをアクティブにすべきであるとマシンが判断するまでの時間です。パートナーのマシンが動作している場合、この値は無視されます。この値を変更すると、（一部のインテリジェントスイッチにより）ロードマスターが起動して接続状態になったと判断されるまでの時間を短縮できます。

HA Virtual ID（HA 仮想 ID）

このオプションは、CARP プロトコルの選択時（デフォルト）に、同じネットワーク上に 1 つ以上の HA ペアが設置されていて、間違った干渉が起こるのを防止するために必要です。そういう場合は、必ず HA ペアに異なる ID 番号を設定するようにしてください。

> ネットワーク上で HA ペアとして設定されている（または HA ペアとして設定する予定の）ロードマスターには、すべて一意の **HA 仮想 ID** 番号を割り当てる必要があります。

Switch to Preferred Server（アクティブ固定）

デフォルトでは、HA クラスターのいずれのパートナーも優先権を持っていません。そのため、スイッチオーバー後にマシンが再起動すると、そのマシンがスレーブになり、マスターになるよう強制されるまでその状態を維持します。優先ホストを指定すると、このマシンは再起動時に常にマスターになろうと試みます。そして、このマシンがマスターになると、パートナーはスレーブモードに戻ります。推奨サーバーが指定されている場合、マスターユニットで障害が発生したときスレーブユニットがマスターとなり、その後、推奨ユニットが復帰したときその推奨ユニットがマスターとなるため、フェイルオーバーイベントが二重に発生します。

HA Update Interface（HA 情報転送インターフェイス）

この設定は、HA 間の情報転送にどのインターフェイスを使用するかを指定できます。1 アーム構成では他の選択はできませんが、2 アーム、マルチアームでは他のインターフェイスへの変更ができます。

Force Partner Update（パートナーへの設定情報更新）

このパラメータは、HA が正しく同期している時のみ使用できます。“Force Update”ボタンをクリックすると、アクティブ側の設定ファイルをスタンバイ側へ強制的に上書きします。

Inter HA L4 TCP Connection Updates（L4 ステーツフル切り替え）

L4 サービス使用時、更新を有効にすると、接続テーブルが共有され、HA のスイッチオーバー時に L4 の接続が維持されます。このオプションはレイヤ 7 のサービスでは無視されます。

Inter HA L7 Persistence Updates（L7 ステーツフル切り替え）

L7 サービス使用時、このオプションを有効にすると、HA パートナー間でパーシステンス情報の共有が可能になります。HA のフェイルオーバーが発生すると、パーシステンス情報が失われます。このオプションを有効にすると、パフォーマンスが大きく影響を受けます。

HA Multicast Interface（HA マルチキャストインターフェイス）

HA 間のアップデートが有効になっている場合、マルチキャストトラフィック用のネットワークインターフェイスを用いてレイヤ 4 とレイヤ 7 のトラフィックの同期が行われます。

Use Virtual MAC Addresses（仮想 MAC アドレスを使用）

このオプションを有効にすると、スイッチオーバー時に HA ペア間で MAC アドレスが強制的に交換されます。これは、HA の IP アドレスの変更をスイッチに通知するのに使用されるグラテュイタス ARP が許可されていない場合に役に立ちます。

> このオプションは、ハードウェアのロードマスターに対してのみ利用可能です。

10.2.1.1 Azure の HA パラメータ

この画面は、ロードマスターfor Azure でのみ利用できます。

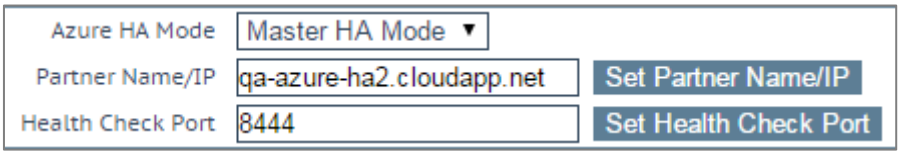

図 10-16:Azure の HA パラメータ

Azure HA Mode（Azure の HA モード）

このユニットで必要な HA モードを選択します。3 つのオプションが用意されています。

- **Master HA Mode（マスターHA モード）**
- **Slave HA Mode（スレーブ HA モード）**
- **Non HA Mode（非 HA モード）**

ロードマスターを 1 台だけ使用する場合、**"Non HA Mode"**を選択してください。

HA モードを使用する場合、1 台目のマシンを**"Master"**に設定し、2 台目のマシンを**"Slave"**に設定します。

> 2 台のユニットで同じ**"Azure HA Mode"**の値を選択した場合、HA は機能しません。
>
> 仮想サービスの設定の同期は、マスターからスレーブの方向でのみ行われます。マスターに対する変更はスレーブに複製されます。ただし、スレーブに対する変更はマスターには複製されません。

マスターユニットに障害が発生すると、接続はスレーブユニットに向けられます。障害が発生しても、マスターユニットはあくまでマスターであり、スレーブにはなりません。同様に、スレーブユニットはマスターにはなりません。マスターユニットが復旧すると、接続は自動的にマスターユニットに向けられます。

図 10-17:Master unit（マスターユニット）

ロードマスターのトップバーに表示されるモードをチェックすれば、どのユニットがマスターでどのユニットがスレーブなのかが一目で分かります。

Partner Name/IP（パートナー名/IP）

HA パートナーユニットのホスト名または IP アドレスを指定します。

Health Check Port（ヘルスチェックポート）

ヘルスチェックを実行するポートを設定します。HA を正しく機能させるには、マスターユニットとスレーブユニットで同じポートを指定する必要があります。

10.2.1.2 AWS の HA パラメーター

この画面は、ロードマスター for Amazon Web Services（AWS）でのみ利用できます。

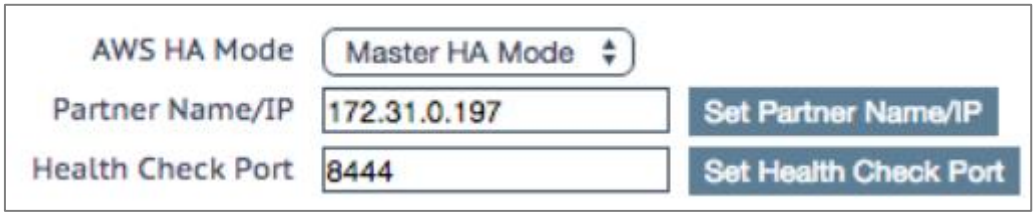

図 10-18:AWS の HA パラメーター

AWS HA Mode（AWS の HA モード）

このユニットで必要な HA モードを選択します。3 つのオプションが用意されています。

- **Master HA Mode（マスターHA モード）**
- **Slave HA Mode（スレーブ HA モード）**
- **Non HA Mode（非 HA モード）**

ロードマスターを 1 台だけ使用する場合、**"Non HA Mode"**を選択してください。

HA モードを使用する場合、1 台目のマシンを**"Master"**に設定し、2 台目のマシンを**"Slave"**に設定します。

2 台のユニットで同じ**"AWS HA Mode"**の値を選択した場合、HA は機能しません。

仮想サービスの設定の同期は、マスターからスレーブの方向でのみ行われます。マスターに対する変更はスレーブに複製されます。ただし、スレーブに対する変更はマスターには複製されません。

マスターユニットに障害が発生すると、接続はスレーブユニットに向けられます。障害が発生しても、マスターユニットはあくまでマスターであり、スレーブにはなりません。同様に、スレーブユニットはマスターにはなりません。マスターユニットが復旧すると、接続は自動的にマスターユニットに向けられます。

図 10-19:Master unit（マスターユニット）

ロードマスターのトップバーに表示されるモードをチェックすれば、どのユニットがマスターでどのユニットがスレーブなのかが一目で分かります。

Partner Name/IP（パートナー名/IP）

HA パートナーユニットのホスト名または IP アドレスを指定します。

Health Check Port（ヘルスチェックポート）

ヘルスチェックを実行するポートを設定します。HA を正しく機能させるには、マスターユニットとスレーブユニットで同じポートを指定する必要があります。

10.2.2 Cluster Control（クラスターの制御）

"Cluster Control"のオプションは、ロードマスターにクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMP の担当者にお問い合わせください。クラスタリングについての詳細は、***ロードマスターのクラスタリング　機能説明***を参照してください。

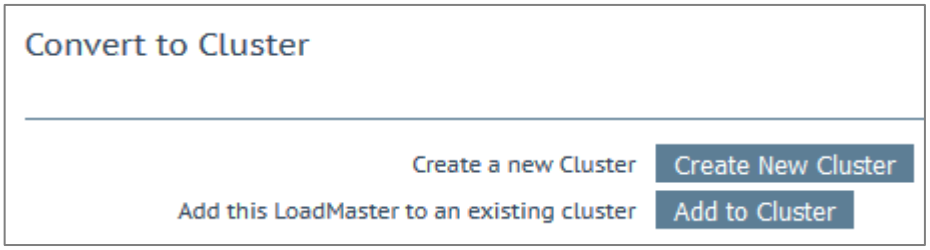

図 10-20:Cluster Control（クラスターの制御）

Create New Cluster（クラスターの新規作成）:クラスターを新たに設定するには、このボタンをクリックします。

Add to Cluster（クラスターに追加）:このロードマスターを既存のクラスターに追加します。

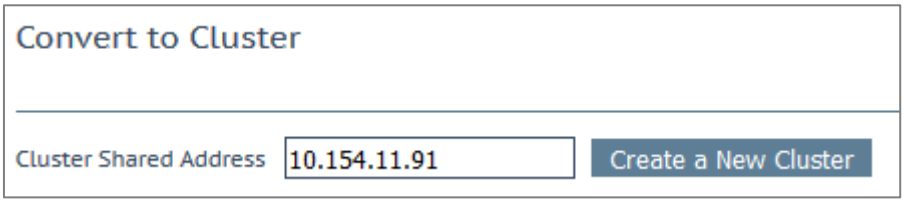

図 10-21:Creating a New Cluster（クラスターの新規作成）

"Create New Cluster"ボタンをクリックすると、上記の画面が表示され、クラスターの共有 IP アドレスを設定するよう求められます。この共有 IP アドレスは、クラスターの管理に使用されます。

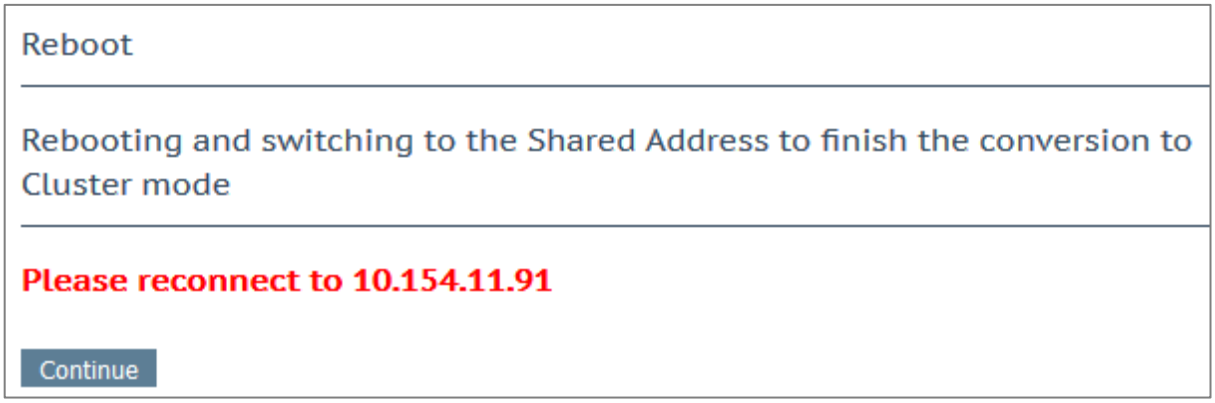

図 10-22:Rebooting（再起動）

"Create a New Cluster"ボタンをクリックすると、ロードマスターが再起動されます。先ほど設定した共有 IP アドレスに再接続するか尋ねるメッセージが表示されます。

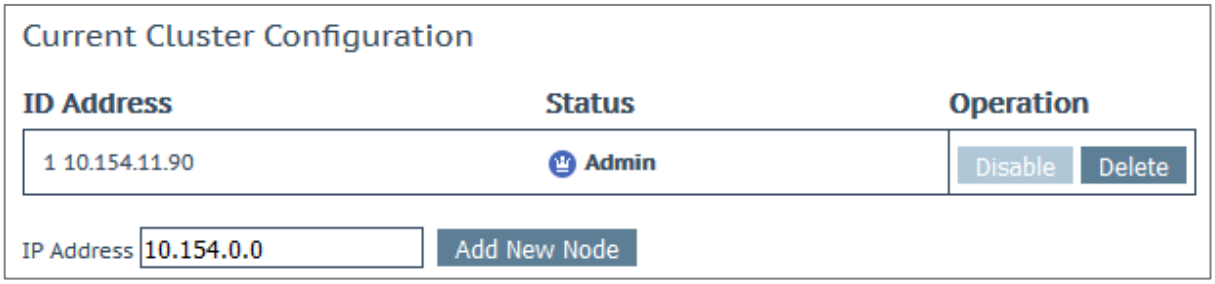

図 10-23:Cluster Control（クラスターの制御）

クラスターを作成すると、共有 IP アドレスの WUI の**"Cluster Control"**画面にて、ロードマスターのノードをクラスターに追加できるようになります。

ロードマスターの追加は、クラスターが利用可能であり、そのロードマスターがクラスターの追加を待っている場合のみ行えます。詳細な情報と手順については、**ロードマスターのクラスタリング　機能説明**を参照してください。

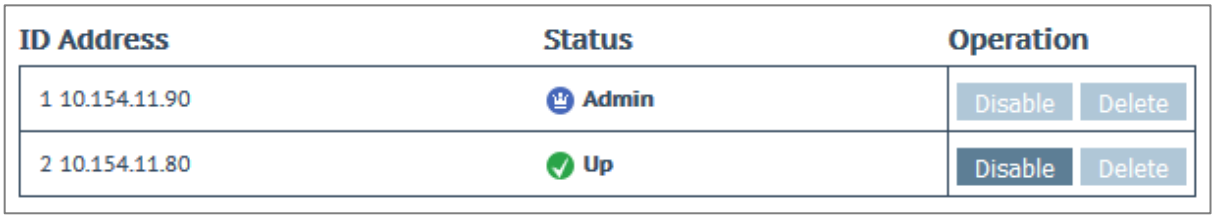

図 10-24:Cluster Control（クラスターの制御）

共有 IP アドレスの WUI の**"Cluster Control"**画面には、そのクラスターにある各ノードの詳細が表示されます。

Show Options（オプションの表示）:"Show Options"ボタンをクリックすると、**"Cluster Parameters"**セクションが表示されます。このセクションには、**Cluster Virtual ID**（クラスターの仮想 ID）と **Node Drain Time**（ノードドレイン時間）を設定するための 2 つのフィールドが用意されています。詳細については、**ロードマスターのクラスタリング　機能説明**を参照してください。

ID:クラスターの ID

Address（アドレス）:ロードマスターノードの IP アドレス。最初の IP アドレスの後ろに括弧で囲まれた 2 番目の IP アドレスが表示されている場合、2 番目の IP アドレスはインターフェイスポートの IP アドレスを表します。ステータスに応じて以下のアイコンが表示されます。

アイコン	ステータス	説明
	管理	このノードはプライマリ制御ノードです。
	無効	このノードは無効になっています。このノードには接続は送信されません。
	起動中	ノード起動中（有効化中）
	稼働中	このノードは稼働しています。
	停止中	このノードは停止しています。
	ドレイン中	このノードは無効になっており、正しい手順で接続をシャットダウンしている最中です。ドレイン停止は、デフォルトで 10 秒間継続します。この値は、**"Cluster Control"**画面の**"Node Drain Time"**の値を変更することで更新できます。詳細は、**ロードマスターのクラスタリング　機能説明**を参照してください。

図 10-25:ノードステータスアイコン

Operation（**動作**）:このノードに関して実行可能な各種動作

- **Disable**（**無効化**）:ノードを無効にします。無効化されたノードに対し、まず始めにドレイン停止が行われます。ドレイン停止時間中に、正しい手順で接続がシャットダウンされます。ドレイン終了後、このノードは無効になり、このノードにトラフィックが送信されなくなります。
- **Enable**（**有効化**）:ノードを有効にします。ノードが起動すると、そのノードは直ちにローテーションに組み込まれます。ノードは、30 秒間稼働してからオンラインになります。
- **Delete**（**削除**）:クラスターからノードを削除します。ノードを削除すると、そのノードは単体動作する通常のロードマスターインスタンスになります。その後、ロードマスターをクラスターに戻すと、共有 IP アドレスに対して行われた変更が、ノードのロードマスターに反映されます。
- **Reboot**（**再起動**）:クラスター全体のファームウェアを更新する際、ファームウェアの更新パッチをアップロードすると、**"Reboot"**ボタンが画面に表示されます。クラスター全体のファームウェアを更新するための具体的な手順については、***ロードマスターのクラスタリング　機能説明***を参照してください。

Add New Node（**ノードの新規追加**）:指定された IP を持つ新しいノードをこのクラスターに追加します。

10.2.2.1 Cluster Parameters（クラスターのパラメーター）

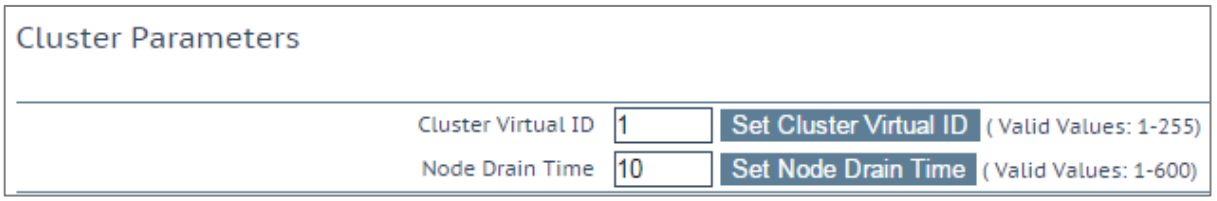

図 10-26:Cluster Parameters（クラスターのパラメーター）

"Show Options"ボタンをクリックすると、**"Cluster Parameters"**画面が表示されます。このセクションには、**"Cluster Virtual ID"**と**"Node Drain Time"**の 2 つの WUI オプションが用意されています。

Cluster Virtual ID（**クラスターの仮想 ID**）

同じネットワーク上で複数のクラスターまたはロードマスターHA システムを使用する場合、仮想 ID により各クラスターが識別されます。そのため、望ましくない干渉は発生しません。クラスターの仮想 ID はデフォルトで **1** に設定されていますが、この値は必要に応じて変更できます。仮想 ID は 1～255 の範囲で設定できます。管理用ロードマスターに対して行われた変更は、そのクラスター内のすべてのノードに反映されます。

Node Drain Time（**ノードドレイン時間**）

ノードが無効になっても、**"Node Drain Time"**テキストボックスで指定された秒数だけ、そのノードにより提供される接続を継続することができます。この間、ノードにより新たな接続は処理されません。**"Node Drain Time"**はデフォルトで **10** に設定されていますが、この値は必要に応じて変更できます。有効な値の範囲は 1～600（単位: 秒）です。

ドレン期間中は、指定されたドレン時間が経過するまで、ステータスは「ドレイン中」になります。

ドレイン時間が経過すると、ステータスが「無効」になります。

10.3 System Administration（システム管理）

各オプションは、ロードマスターの基本レベルの運用を制御します。重要なポイントとして、HA ペアで各パラメータに変更を加えるには、フローティング管理 IP アドレスを使用する必要があります。これらのオプションの多くは、システムのリブートが必要に

なります。これらのパラメータを設定／変更した場合は、ペアで唯一のアクティブなシステムだけが影響を受けます。

10.3.1 ユーザの管理

以下、ユーザー管理用の各種 WUI フィールドについて説明します。ユーザー管理と WUI 認証の詳細については、***ユーザー管理　機能説明***を参照してください。

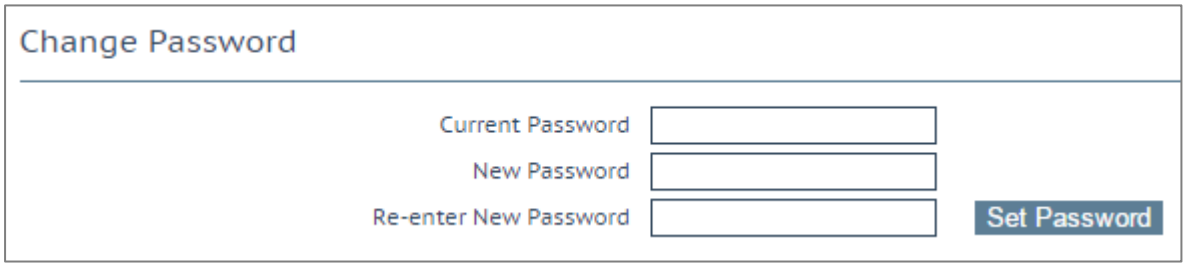

図 10-27:パスワードの変更

"Change Password"セクションでは、機器のパスワードを変更できます。これはローカルのアプライアンスにのみ適用され、HA 構成におけるパートナーのアプライアンスのパスワードには影響しません。

図 10-28:ユーザーの管理

"Local Users"セクションには、既存のローカルユーザーのリストが表示されます。既存のユーザーに関して 2 つのオプションが用意されています。

- **Modify（変更）**:既存のローカルユーザーの詳細を変更します（権限やパスワードなど）。詳細は**セクション 10.3.1.1** を参照してください。
- **Delete（削除）**:目的のユーザーを削除します。

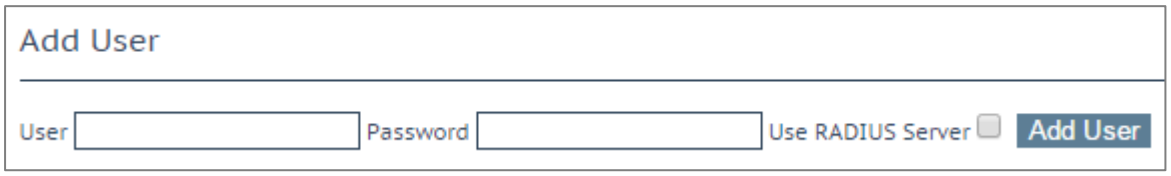

図 10-29:ユーザーの追加

"Add User"セクションでは、新規ユーザーを追加できます。

ユーザー名には最大 64 文字まで使用できます。ユーザー名は数字で始めることができます。また、以下の特殊文字に加えて英数字を含めることができます。

=~^._+#@\/-

パスワードは 8 文字以上 64 文字以下でなければなりません。**\"'`**を除いてすべての文字を使用できます。

"Use RADIUS Server"（**RADIUS サーバーを使用する**）オプションを使用すると、ユーザがロードマスターにログインするときに RADIUS サーバによる認証を行うかどうかを決定できます。このオプションを使用する前に、RADIUS サーバの詳細を設定する必要があります。

RADIUS サーバーによる認証を行う場合、ロードマスターから RADIUS サーバーにユーザーの情報が渡され、RADIUS サーバーからロードマスターにそのユーザーが認証されたかどうかが通知されます。RADIUS サーバーの設定に関する詳細は、**セクション 9.6.4** および **RADIUS の認証と権限設定　テクニカルノート**を参照してください。

セッション管理が有効になっている場合、この画面で"Use RADIUS Server"オプションは使用できません。セッション管理が有効なときに RADIUS サーバーを設定する方法については、**Section9.6.4** を参照してください。

セッション管理が有効になっている場合、**"Add User"**セクションに**"No Local Password"**チェックボックスが表示されます。ユーザがロードマスターにアクセスするときに、クライアント証明書を用いてそのユーザーを認証する場合、このオプションを有効にできます。クライアント証明書による認証を有効にするには、**"Remote Access"**画面で**"Admin Login Method"**を設定します。詳細は**セクション 9.6** または**ユーザー管理　機能説明**を参照してください。

10.3.1.1 ユーザーの編集

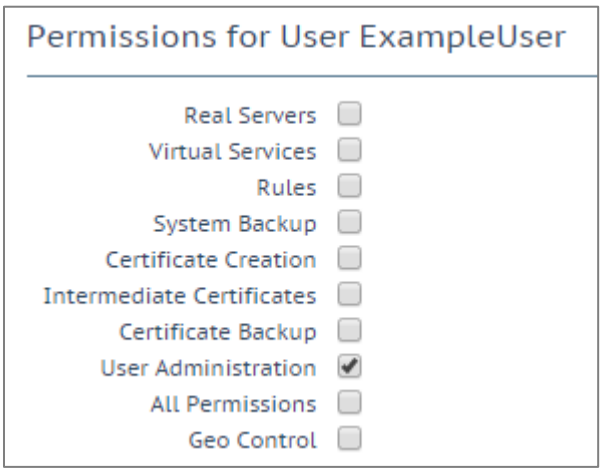

図 10-30:権限

この画面では、ユーザー権限のレベルを設定できます。この設定に基づいて、ユーザーに実行を許可する設定変更の範囲が決まります。プライマリユーザー（**bal**）は、常にすべての機能を使用する権限を持っています。セカンダリユーザーは、一部の機能が制限される場合があります。

ユーザー権限の詳細については、**KEMP ロードマスター 製品概要**を参照してください。

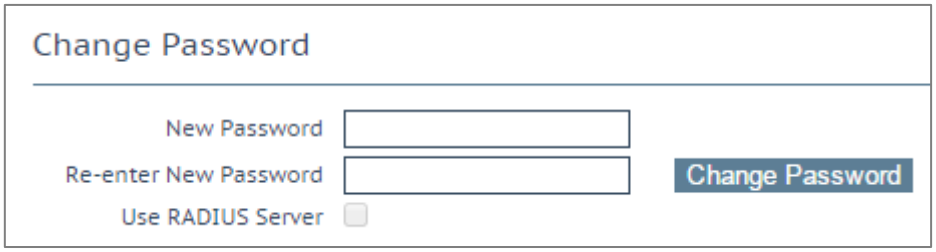

図 10-31:パスワードの変更

"Change Password"セクションでは、ユーザーのパスワードの変更が行えます。また、RADIUS サーバーによるユーザー認証を有効/無効にできます。

> セッション管理が有効になっている場合、この画面で“Use RADIUS Server”オプションは使用できません。セッション管理が有効なときに RADIUS サーバーを設定する方法については、**Section9.6.4** を参照してください。

セッション管理が有効になっている場合、**"Change Password"**セクションに**"No Local Password"**チェックボックスが表示されます。ユーザがロードマスターにアクセスするときに、クライアント証明書を用いてそのユーザーを認証する場合、このオプションを有効にできます。クライアント証明書による認証を有効にするには、**"Remote Access"**画

面で**"Admin Login Method"**を設定します。詳細は**セクション 9.6** または**ユーザー管理 機能説明**を参照してください。

名前付きユーザーは、ユーザー管理権限を持っていなくても、自分のパスワードを変更できます。名前付きユーザーが**"System Administration > User Management"**メニューオプションをクリックすると、**"Change Password"**画面が表示されます。

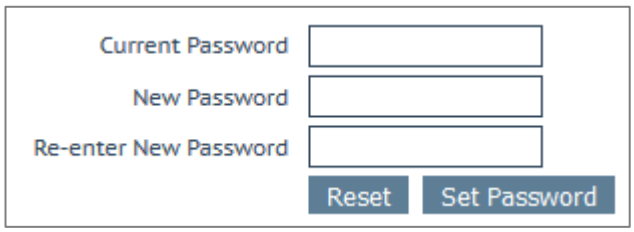

図 10-32:パスワードの変更

ユーザーは、この画面で自分のパスワードを変更できます。パスワードは 8 文字以上 64 文字以下でなければなりません。\"'を除いてすべての文字を使用できます。パスワードを変更すると、確認画面が表示されます。その後、ユーザーは、新しく設定したパスワードでロードマスターに再度ログインするよう求められます。

図 10-33:ローカル証明書

"Local Certificate"セクションでは、そのユーザーの証明書を生成できます。オプションとして、秘密鍵の暗号化で使用するパスフレーズを**"Passphrase"**に設定できます。証明書をダウンロードすると、その証明書をクライアント証明書として使うことができます。これにより、ロードマスターの API にパスワードなしでアクセスできます。"User Administration"の権限が設定されたユーザーは、自分または他のユーザーのローカル証明書を管理できます。

クライアント証明書によるロードマスターへのアクセス認証を有効にするには、**"Remote Access"**画面で**"Admin Login Method"**を設定します。詳細は**セクション 9.6** または**ユーザー管理　機能説明**を参照してください。

10.3.2　Update License（ライセンスの更新）

この画面には、現在のライセンスが有効になった日付と、現在のライセンスの有効期限が表示されます。ロードマスターのライセンスを更新する前に、KEMP の担当窓口にお

問い合わせいただくか、"Upgrade"オプションを使用する必要があります。KEMP へのお問い合わせ後または"Upgrade"オプション使用後に、オンラインとオフラインの 2 つの方法でライセンスを更新できます。各方式の画面に関する詳細は、以下のセクションを参照してください。

詳細および手順については、**ライセンス　機能説明**を参照してください。

10.3.2.1　オンライン方式

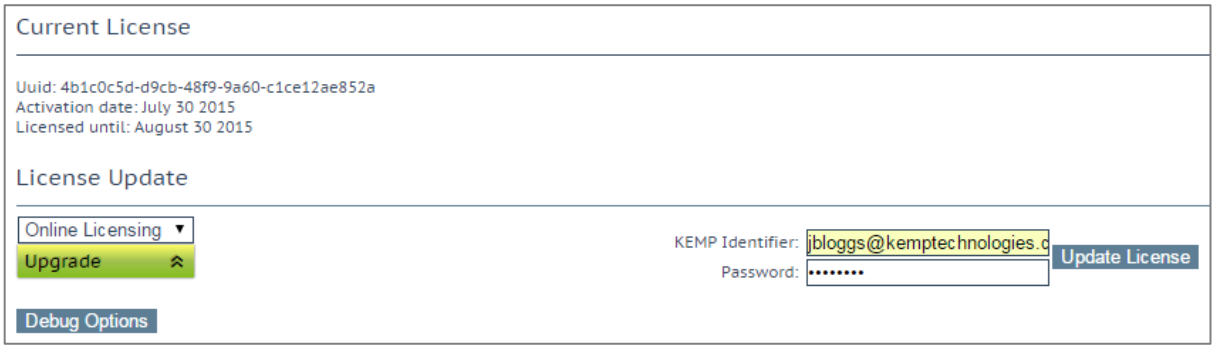

図 10-34:ライセンスの更新 - オンライン方式

オンライン方式でライセンスをアップグレードするには、ロードマスターをインターネットに接続する必要があります。オンライン方式でライセンスを設定するには、**"KEMP ID"と"Password"（パスワード）**を入力する必要があります。

10.3.2.2　オフライン方式

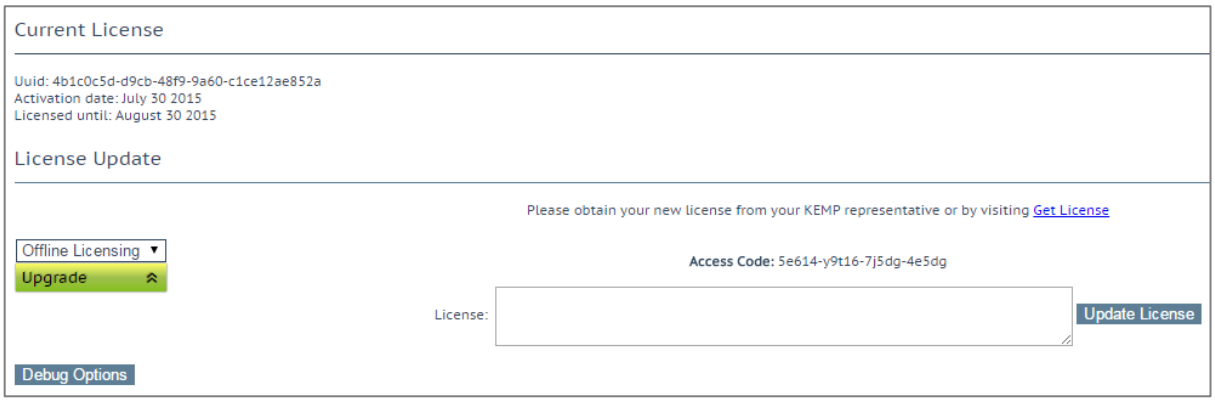

図 10-35:ライセンスの更新 - オフライン方式

オフライン方式でライセンスをアップグレードするには、ロードマスターにライセンステキストを入力する必要があります。ライセンステキストは、KEMP から入手するか、**"Get License"（ライセンスの取得）**のリンクから入手することができます。

適用するライセンスの種類によっては、再起動が必要になる場合があります。ESP ライセンスへのアップグレードの場合、更新後に再起動が必要です。

10.3.2.3 Debug Options（デバッグオプション）

"Update License"（ライセンスのアップグレード）画面には、ライセンス設定に関する問題のトラブルシューティングに役立つ、いくつかのデバッグオプションが用意されています。

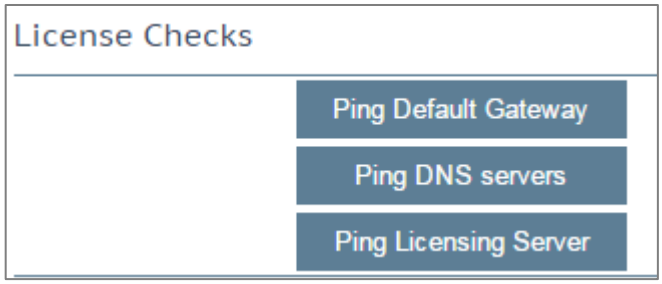

図 10-36:利用可能なデバッグオプション

"Debug Options"（デバッグオプション）ボタンをクリックすると、以下の 3 つのデバッグオプションが表示されます。

- Ping Default Gateway（デフォルトゲートウェイに ping を送信する）
- Ping DNS Servers（DNS サーバーに ping を送信する）
- Ping Licensing Server（ライセンスサーバーに ping を送信する）

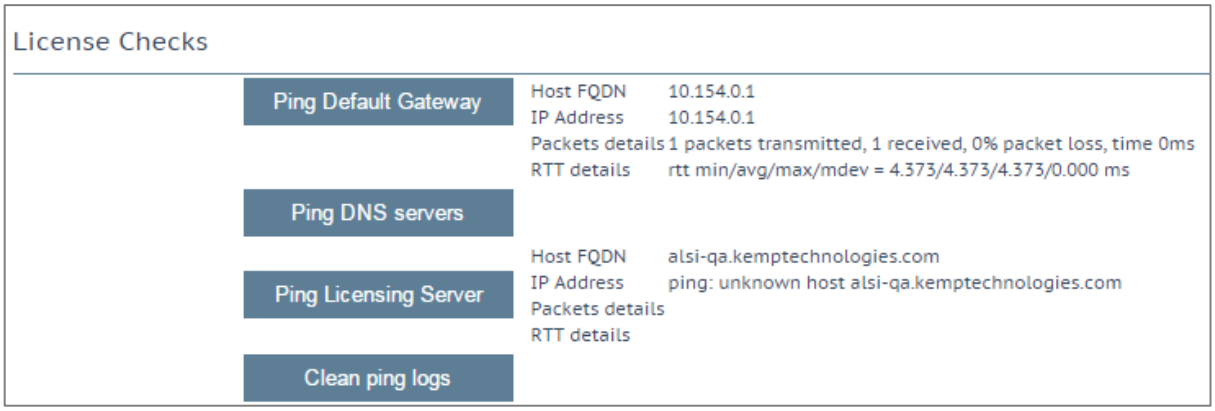

図 10-37:ping の結果

ping ボタンをクリックすると、右側の列に ping の結果が表示されます。

"Clean ping logs"（ping のログをクリアする）ボタンをクリックすると、右側の列にある情報がクリアされます。

10.3.3 System Reboot（システムリブート）

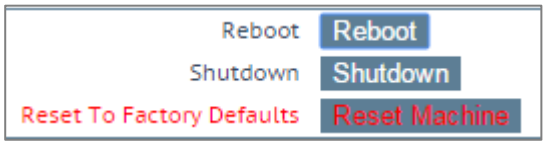

図 10-38:システムリブート

Reboot（リブート）

アプライアンスをリブートします。

Shutdown（シャットダウン）

このボタンをクリックすると、ロードマスターの電源を切る処理が行われます。何らかの理由で電源を切る処理に失敗した場合でも、CPU は停止します。

Reset Machine（マシンのリセット）

ライセンス、ユーザー名、およびパスワードの情報を除く、アプライアンスの設定をリセットします。適用の対象は、HA ペアのアクティブなアプライアンスに限定されます。

10.3.4 Update Software（ファームウェア更新）

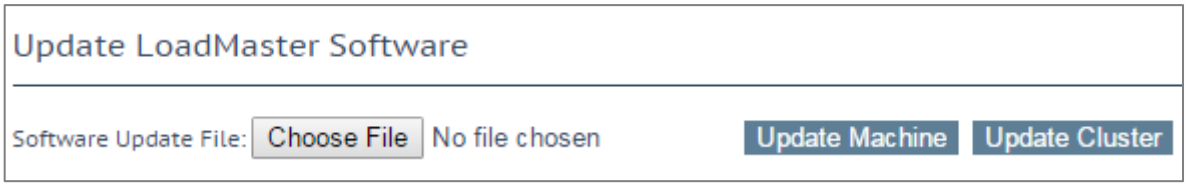

図 10-39:ソフトウェアの更新

ファームウェアの更新につきましては、弊社販売店までお問い合わせ願います。ファームウェアをダウンロードするにはインターネットにアクセスする必要があります。パッチ情報の詳細は、http://forums.kemptechnologies.com/でご覧いただけます。

Update Machine（マシンの更新）

ファームウェアの更新を行えます。パッチは、新しいファームウェアとしてリリースされますので、一旦ローカルディスクへダウンロードした後、ここにそのロケーションを指定します。このファームウェアは、ロードマスターで解凍して有効化します。パッチ

が有効になると、リリース情報を確認するよう求められます。更新を完了するには、機器を再起動する必要があります。必要に応じて、このリブートは保留できます。

Update Cluster（クラスターの更新）

> **"Update Cluster"**のオプションは、ロードマスターにクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMP の担当者にお問い合わせください。クラスタリングについての詳細は、**ロードマスターのクラスタリング　機能説明**を参照してください。

"Update Cluster"ボタンをクリックすると、クラスターにあるすべてのロードマスターのファームウェアを共有 IP アドレス経由で更新できます。クラスター全体のソフトウェアを更新するための具体的な手順については、**ロードマスターのクラスタリング　機能説明**を参照してください。

Restore Software（ファームウェア復旧）

ロードマスターのファームウェア更新が完了した場合、このオプションを使用して、以前のビルドに戻すことができます。

図 10-40:Installed Addon Packages（インストールされているアドオンパッケージ）

Installed Addon Packages（インストールされているアドオンパッケージ）

KEMP ロードマスターにはアドオンパッケージをインストールできます。アドオンパッケージでは、ロードマスターの追加機能が用意されています。今後、アドオン機能をさらに追加する予定です。

アドオンパッケージは、KEMP Technologies の Web サイト（www.kemptechnologies.com ）から入手できます。www.kemptechnologies.com

> アドオンパッケージをインストールするには、**"Choose File"**をクリックしてファイルをブラウズ/選択し、**"Install Addon Package"**をクリックします。アドオンパッケージのインストールを完了するには再起動する必要があります。同じ名前のアドオンパッケージをアップロードした場合、既存のパッケージが上書き/更新されます。

インストールしたアドオンを起動できない場合、テキストが赤で表示され、そのパッケージを起動できなかったことが吹き出し文字で示されます。

10.3.5 Backup/Restore（設定バックアップ／リストア）

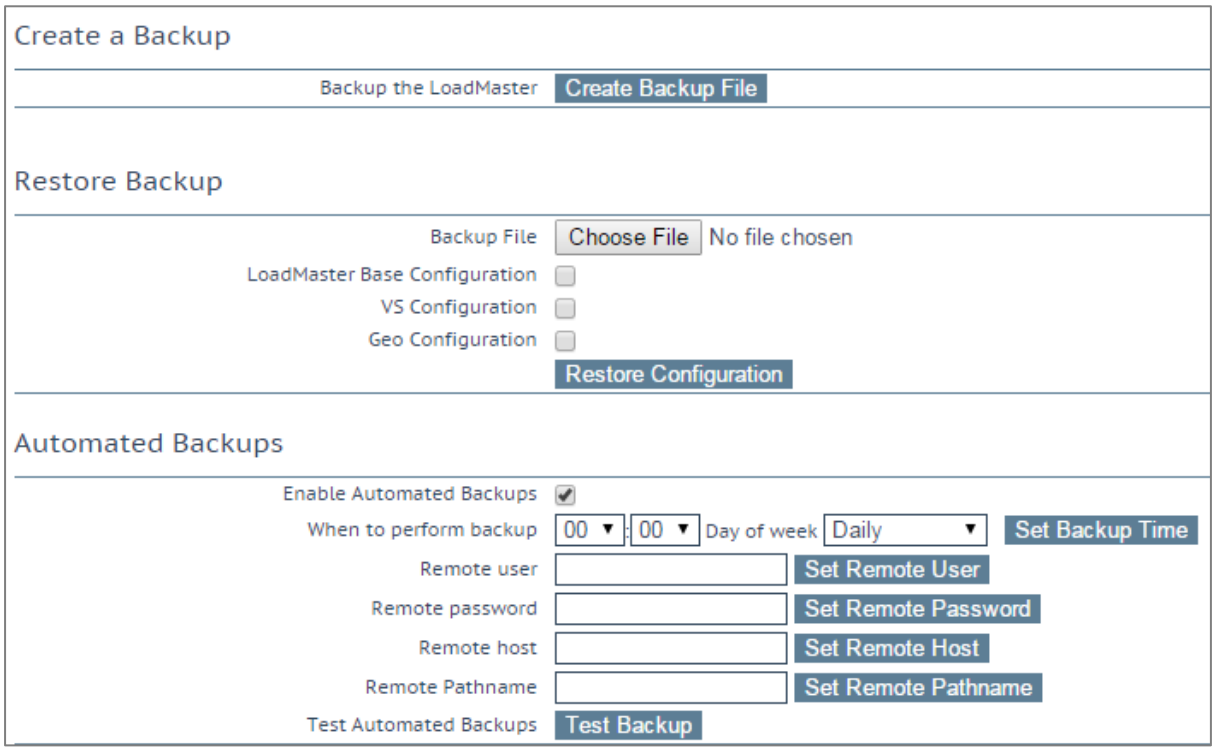

図 10-41:バックアップと復元

Create Backup File（バックアップファイルの作成）

仮想サービスの設定およびローカルアプライアンスの情報を含むバックアップを生成します。ライセンス情報と SSL 証明書情報はバックアップに含まれません。

容易に識別できるように、バックアップファイル名にはロードマスターのホスト名が含まれています。

Restore Backup（バックアップの復元）

リモートマシンから復元を実行する場合、ユーザーは復元する情報の種類（**"VS Configuration"、"LoadMaster Base Configuration"、"Geo Configuration"**、またはこの 3 つのオプションの組み合わせ）を選択できます。

> HA マシンにシングルマシンの設定をリストアすることはできません（その逆も不可）。
>
> ESP が有効になっている仮想サービスの設定を、ESP が無効になっているマシンにリストアすることはできません。

Automated Backups（自動バックアップ）

"Enable Automated Backups"チェックボックスがオンになっている場合、毎日または週単位で自動バックアップを実行するよう、システムを設定できます。

容易に識別できるように、バックアップファイル名にはロードマスターのホスト名が含まれています。

しかるべき時刻に自動バックアップが実行されない場合、NTP が正しく設定されているか確認してください。詳細は**セクション 10.3.6** を参照してください。

When to perform backup（バックアップの実行タイミング）

バックアップの時間（24 時間制）を指定します。同時に、バックアップを毎日実行するか、特定の曜日に実行するかを選択します。選択が終わったら、**"Set Backup Time"**ボタンをクリックします。

> 場合によっては、以下のような偽のエラーメッセージがシステムログに表示されることがあります。
>
> Dec 8 12:27:01 KEMP_1 /usr/sbin/cron[2065]:(system) RELOAD (/etc/crontab)
>
> Dec 8 12:27:01 KEMP_1 /usr/sbin/cron[2065]:(CRON) bad minute (/etc/crontab)
>
> これらを無視しても支障ありません。このような場合でも、通常、自動バックアップは正しく行われます。

Remote user（リモートユーザー）

リモートホストにアクセスするユーザー名

Remote password（リモートパスワード）

リモートホストにアクセスするためのパスワード。このフィールドには、英数字およびほとんどの非英数字が使用できます。以下の文字は使用できません。

- 制御文字
- ‘（アポストロフィー）
- `（グラーブ）
- 削除文字

Remote host （リモートホスト）

リモートホスト名

Remote Pathname（リモートパス名）

バックアップファイルを格納するリモートホスト上の場所

Test Automated Backups（自動バックアップのテスト）

"Test Backup"ボタンをクリックすると、自動バックアップの設定が正しく機能するかどうかチェックするテストが実行されます。テストの結果は、システムメッセージファイルで確認できます。

現在、自動バックアップの転送プロトコルは FTP のみサポートしています。

10.3.6 Date/Time（日付／時間）

時間、日付の設定が行えます。マニュアルで設定するか、NTP ホストを指定して精度の高い時刻を自動的に設定できます。

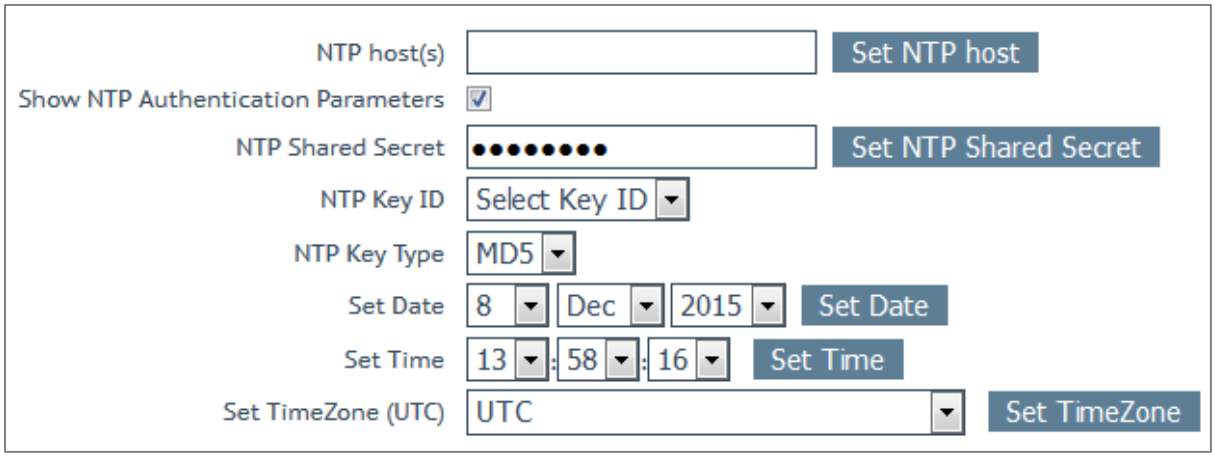

図 10-42:日付および時刻の設定

NTP host(s)（NTP ホスト）

NTP サーバーとして使用するホストを指定します。NTP は、HA 構成では強く推奨されるオプションです。単一ユニットの場合は、ユーザーが任意に設定できます。**"Set NTP host"**ボタンをクリックすると、設定された詳細に基づき時刻が更新されます。

ローカル NTP サーバーがない場合は、www.pool.ntp.org にアクセスし、使用可能な公開 NTP サーバープールの一覧を参照してください。

タイムゾーンは、常に手動で設定する必要があります。

Show NTP Authentication Parameters（NTP 認証パラメーターの表示）

ロードマスターは、暗号化された署名を用いて安全な NTP サーバーに問い合わせを行う NTPv4 をサポートします。このプロトコルは、簡単な認証方式を使用します。この方式では、共有秘密鍵を使用して、サーバーからの応答が正規のものであるかを確認します。**"Show NTP Authentication Parameters"**チェックボックスをオンにすると、NTP により認証された要求をサポートするのに必要なパラメーターが表示されます。

NTP Shared Secret（NTP 共有秘密鍵）

NTP 共有秘密鍵の文字列です。NTP の秘密鍵は、ASCII 文字で 20 文字（または 16 進数で 40 文字）まで使用できます。

NTP Key ID（NTP 鍵 ID）

NTP 鍵 ID を選択します。値の範囲は 1～99 です。サーバーごとに異なる鍵 ID を使用できます。

NTP Key Type（**NTP 鍵タイプ**）

NTP 鍵タイプを選択します。

NTPv4 を機能させるには、サーバー上に以下の形式を持つファイル（/etc/ntp.keys）を作成する必要があります。

<鍵 ID> M <秘密鍵の文字列>

…

<鍵 ID> M <秘密鍵の文字列>

鍵 ID を有効にするには、/etc/ntp.conf の trustkey の行に鍵 ID を指定する必要があります。すなわち、鍵 ID が 5 の場合、“trustedkey5”と指定する必要があります。trustedkey は複数の値を持つことができます（例: trustedkey 1 2 3 4 5 9 10）

10.4 Logging Options（ログオプション）

ロードマスターのログには、アプライアンスからのプッシュと、プルによる両方のイベントが出力されます。ロードマスターのログ情報は、アプライアンスが再起動した場合、リセットされ、維持されないことに注意してください。システム上のイベント出力記録の維持が重要な場合には、SNMP マネジャー、Syslog サーバー、SMTP サーバーなどを使用した外部デバイスへの蓄積をお勧めします。

10.4.1 System Log Files（システムのログファイル）

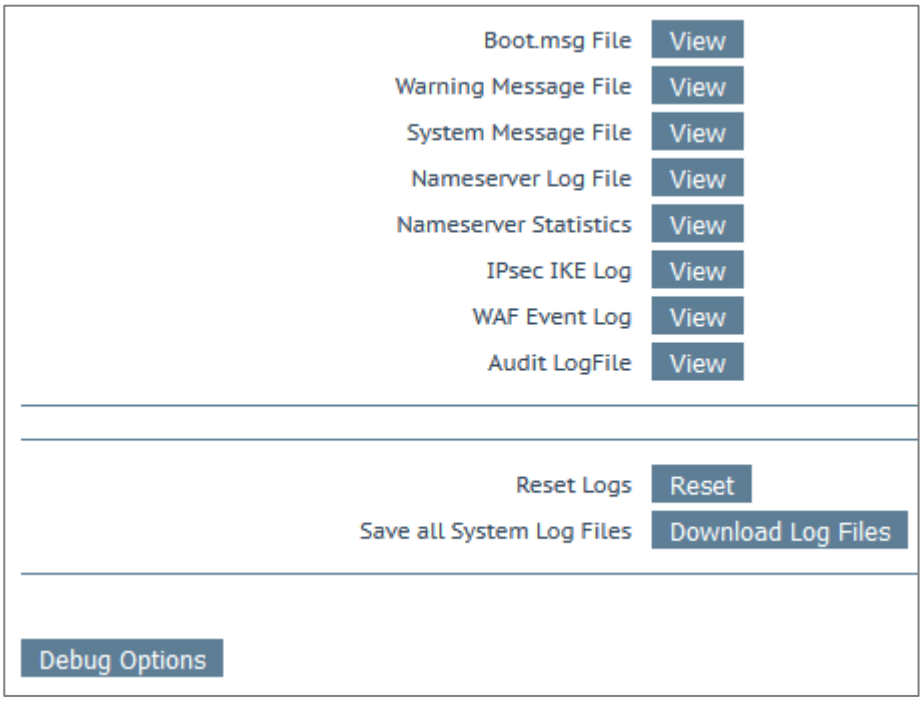

図 10-43:System Log Files（システムのログファイル）

Boot.msg File - システムがブートした時のメッセージを記録したファイルをレビューできます。

Warning Message File（警告のメッセージファイル） - ロードマスターの運用中に記録された警告を含んでいます。

System Message File（システムのメッセージファイル） - ロードマスターの運用中に記録されたシステムイベントを含んでいます。オペレーティングシステムレベルのイベントとロードマスターの内部イベントの両方が対象です。

Nameserver Log File（ネームサーバーのログファイル）- DNS ネームサーバーのログを表示します。

Nameserver Statistics（ネームサーバーの統計情報） - ネームサーバーの最新の統計情報を表示します。

IPsec IKE Log（IPsec IKE のログ）- IPsec IKE のログを表示します。

WAF Event Log - 最後にトリガーされた WAF ルールのログが格納されます。

Audit LogFile - ユーザーにより API 経由または WUI 経由で行われる各アクションのログが格納されます。これは、セッション管理が有効な場合のみ機能します。セッション管理についての詳細は、**セクション 9.7** を参照してください。

Reset Logs - すべてのメッセージを消去します。

Save all System Log Files（システムのログファイルをすべて保存） - サポート対応の一環として、KEMP のサポート部門にログを送付する必要がある場合に使用します。このボタンをクリックすることで、使用中の PC にファイルを保存した後で、販売店のサポートにそれらを転送できます。

10.4.1.1 Debug Options（デバッグオプション）

ロードマスターには、接続関連の問題を診断する際に、ユーザーや KEMP のサポート部門のスタッフを支援するため、さまざまな機能が用意されています。**[Debug Options]** ボタンをクリックすると、そのための下記画面が表示されます。

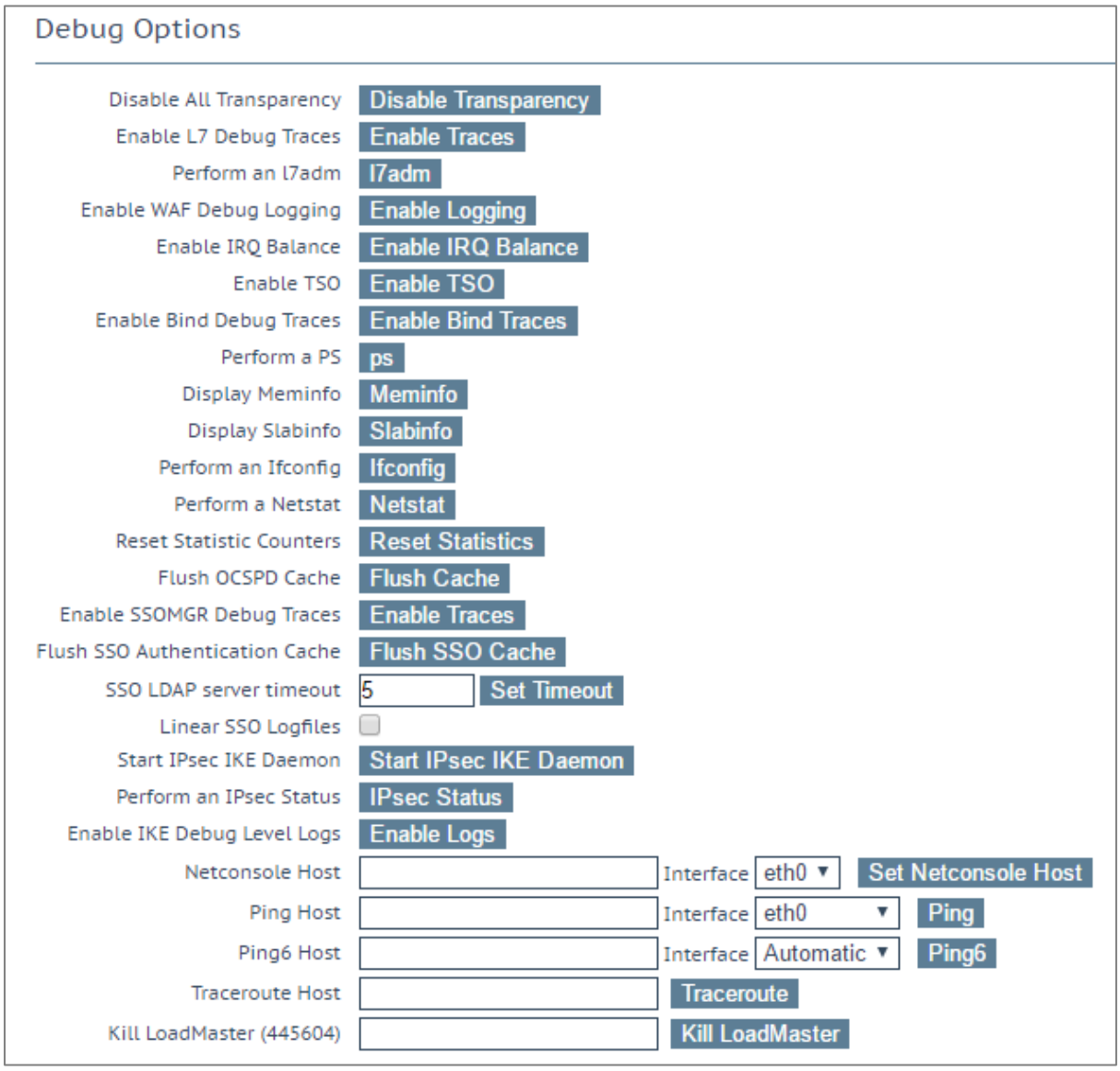

図 10-44:デバッグオプション

Disable All Transparency（**すべてのトランスペアレンシーを無効化**）

各仮想サービス上のトランスペアレンシーを無効にし、レイヤ 7 を使用するよう強制します。注意して使用してください。

Enable L7 Debug Traces（**レイヤ 7 のデバッグトレースを有効にする**）

メッセージファイルにてログトラフィックを生成します。大量のファイルが記録されるため、レイヤ 7 の処理が遅くなります。

Perform an l7adm（**l7adm の実行**）

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。

Enable WAF Debug Logging（**WAF のデバッグログを有効にする**）

WAF のデバッグトレースを有効にします。

このオプションは大量のトラフィックを生成します。また、WAF の処理速度も低下します。KEMP の技術サポートからこのオプションを使用するように要求された場合のみ、このオプションを有効にしてください。実稼働環境でこのオプションを有効にするのは推奨しません。

AFP デバッグログはクローズされません。ログが大きくなりすぎたときは、循環して使用されます。デバッグログを再度有効にするには、WAF が有効なすべての仮想サービスの設定において、WAF を無効にしてから再度有効にする必要があります。または、それらの仮想サービスに関連するルールを更新してください。

Enable IRQ Balance（**IRQ の負荷分散を有効にする**）

IRQ 負荷分散を有効にします。販売店サポート要員の指示で有効にしてください。

Enable TSO（**TSO を有効化**）

TCP セグメンテーションオフロード（TSO）を有効にします。

このオプションを変更する場合は、必ず KEMP の技術サポートにご相談ください。このオプションの変更は再起動後に有効になります。

Enable Bind Debug Traces（バインドデバッグトレースの有効化）

GEO に対するバインドデバッグトレースのログを有効にします。

Perform a PS（PS の実行）

システムのプロセス状態をレポートします。

Display Meminfo（メモリ情報の表示）

システムのメモリー使用状態を表示します。

Display Slabinfo（スラブ情報の表示）

システムの Slab 情報を表示します。

Perform an Ifconfig（Ifconfig の実行）

システムが持つすべてのイーサネットポートの情報を表示します。

Perform a Netstat（Netstat の実行）

Netstat の出力を表示します。

Reset Statistic Counters（統計カウンタのリセット）

統計カウンタをすべてゼロにします。

Flush OCSPD Cache（OCSPD のキャッシュを消去）

OCSP を使用してクライアント証明書を検証する場合、OCSP サーバーから取得した応答が OCSPD キャッシュされます。このボタンを押すと、このキャッシュを消去できます。

OCSPD のキャッシュの消去は、試験を行うときや、証明書失効リスト（CRL）が更新されたときに役に立ちます。

Enable SSOMGR Debug Traces（SSOMGR によるデバッグトレースを有効にする）

このオプションを有効にすると、ロードマスター上で設定された SSO ドメインへのログイン試行が記録されます。このオプションを有効にすると、**"Extended Log Files"**画面の **"SSOMGR Audit Logs"**にログが保存されます。ログファイルの詳細については、**セクション 10.4.2** を参照してください。

Stop IPsec IKE Daemon（IPsec IKE デーモンの停止）

ロードマスターの IPsec IKE デーモンを停止します。

このボタンをクリックすると、すべてのトンネルの接続が停止します。

Perform an IPsec Status（IPsec ステータスの表示）

生の IPsec ステータス出力を表示します。

Enable IKE Debug Level Logs（IKE のデバッグレベルのログ表示を有効化）

IPsec IKE のログレベルを制御します。

Flush SSO Authentication Cache（SSO 認証のキャッシュの消去）

“Flush SSO Cache”ボタンをクリックすると、ロードマスターに保存されているシングルサインオンのキャッシュが消去されます。また、認証サーバーのステータスがすべてリセットされ、（KCD ドメインが関係している場合は）KCD ドメインがリセットされて、設定が再度読み込まれます。これにより、シングルサインオンを使用してロードマスターに接続しているすべてのクライアントがログオフされます。

Linear SSO Logfiles（SSO ログファイルをリニアに拡張する）

デフォルトでは、新しいログファイルを保存できるように、古いログファイルは削除されます。これにより、ファイルシステムが一杯になるのを防ぐことができます。**“Linear SSO Logfiles”**チェックボックスをオンにすると、古いファイルが削除されないようにできます。

"Linear SSO Logging"を使用する場合、ログファイルを定期的に削除せずにファイルシステムが一杯になると、ログに記録されないまま仮想サービスにアクセスされるのを防ぐため、ESP が有効になっている仮想サービスへのアクセスがブロックされます。ESP が無効になっている仮想サービスへのアクセスは、"Linear SSO Logfile"機能による影響を受けません。

Netconsole Host（netconsole ホスト）

指定したホストで動作する syslog デーモンにより、重要なカーネルメッセージがすべて受信されます。syslog サーバーはローカル LAN 上に置く必要があります。また、メッセージは UDP で送信されます。

“Interface”プルダウンメニューにて、どのインターフェイスにネットコンソールホストを設定するかを選択できます。

指定したネットコンソールホストが、選択したインターフェイス上にあることを確認してください（そうでない場合はエラーが発生します）。

Ping Host（ping ホスト）

指定したホストにて ping を実行します。ping の送信元インターフェイスは、**"Interface"** ドロップダウンリストにて指定できます。**"Automatic"**オプションを選択すると、特定のネットワーク上にあるアドレスに ping を送信するための適切なインターフェイスが選択されます。

インターフェイスは、ping を行うアドレスが IPv4 と IPv6 のどちらのアドレスかを判断し、ping を実行するための正しいコマンドを選択します。数値形式のアドレスの場合は簡単ですが、数値でないアドレスは処理できないため、常に IPv4 アドレスとして処理されます。

Ping6 Host（ping6 ホスト）

特定の IPv6 ホストの ping6 を実行します。

Traceroute Host（traceroute ホスト）

特定のホストのトレースルートを実行します。

Kill LoadMaster（ロードマスターを停止する）

ロードマスターのすべての機能を恒久的に無効にします。ライセンスを再度設定すると、ロードマスターの機能を再度使用できるようになります。

ロードマスターの機能を無効にする場合は、必ず KEMP の技術サポートにご相談ください。

"Kill LoadMaster"オプションは、KEMP Condor のテナントのロードマスターでは利用できません。

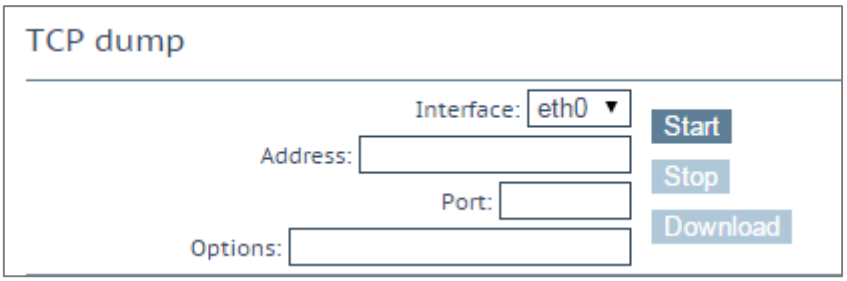

図 10-45:TCP ダンプ

TCP ダンプ

TCP ダンプは 1 つまたはすべてのイーサネットポートで取り込むことができます。アドレス、ポートパラメーター、およびオプションのパラメーターを指定できます。**"Options"**テキストボックスには最大 **255** 文字まで入力できます。

ユーザーがダンプの停止および開始を切り替えることができます。また、ダンプを特定の場所にダウンロードすることもできます。TCP ダンプの結果は、Wireshark などのパケットトレース解析ツールで解析できます。

詳細は、**VMware ツールのアドオンパッケージ　機能説明**を参照してください。

10.4.2　Extended Log Files（拡張ログファイル）

"Extended Log Files"画面では、ESP の AFP 機能に関するログのオプションが用意されています。これらのログは永続的に保存され、ロードマスターの再起動後も利用できます。オプションをすべて表示するには、⊞ アイコンをクリックします。

WAF のログはリアルタイムでは作成されません。このログは、WAF のエンジンが実際に処理を行ってから最大 2 分後に作成されます。

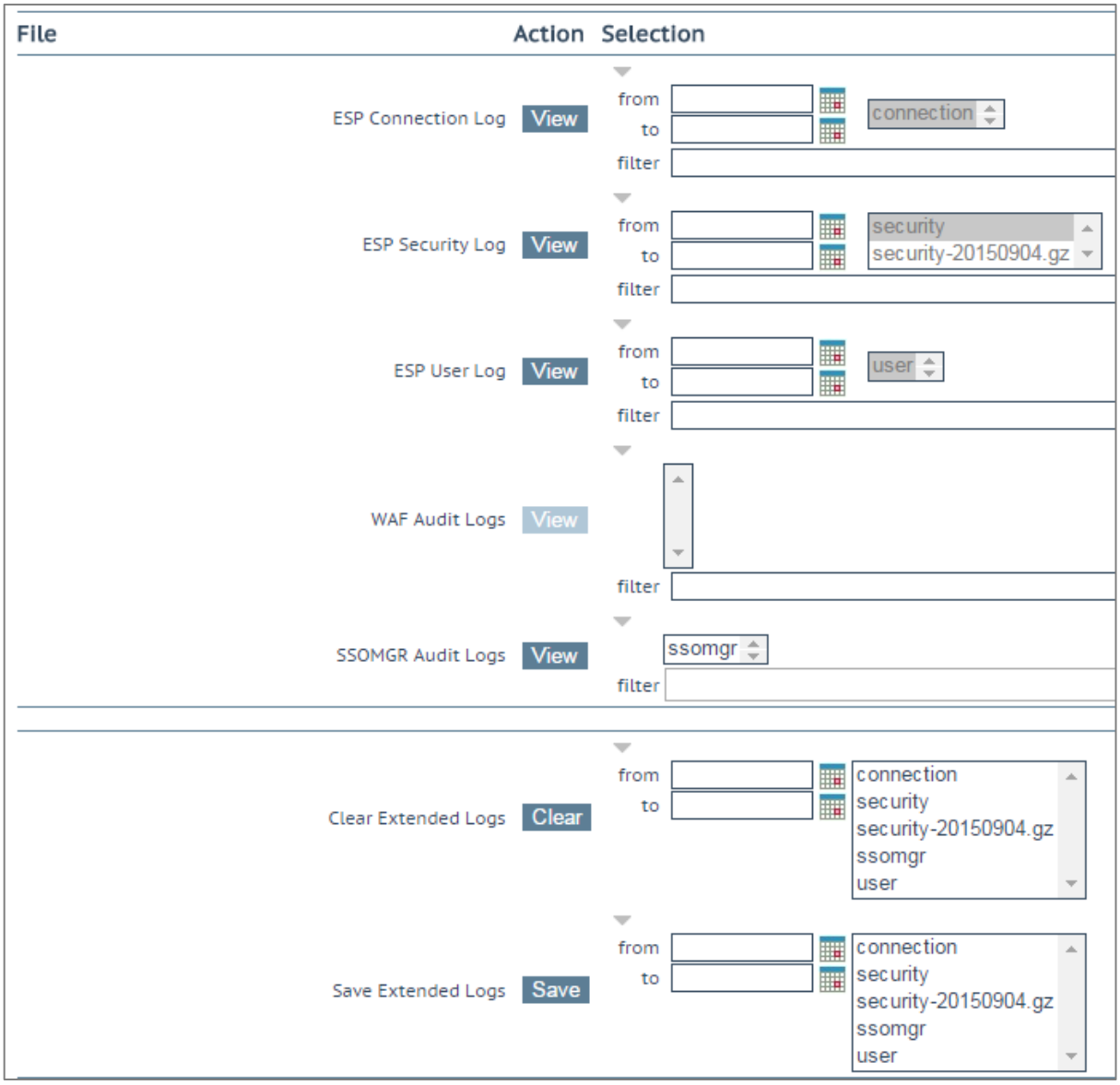

図 10-46:ESP オプション

さまざまなログファイルがロードマスターに保存されます。

- **ESP Connection Log**（**ESP 接続ログ**）:各接続を記録
- **ESP Security Log**（**ESP セキュリティログ**）:セキュリティ警告をすべて記録
- **ESP User Log**（**ESP ユーザーログ**）:全ユーザーのログイン情報を記録
- **WAF Audit Logs**（**WAF 監査ログ**）:仮想サービス設定画面の"**WAF Options**"セクションの"**Audit mode**"ドロップダウンリストで選択した内容に従って WAF のログを作成します。各ログエントリにリストされる番号は、仮想サービス ID に対応します。仮想サービス ID を取得するには、API インターフェイスが有効になって

いることを確認し（**"System Configuration" > "Miscellaneous Options" > "Remote Access" > "Enable API Interface"**）てから、Web ブラウザーのアドレスバーに **https://<LoadMasterIPAddress>/access/listvs** と入力します。Web ブラウザーのアドレスバーで、**https://*<LoadMasterIPAddress>*/access/listvs** と入力します。仮想サービスの **index（インデックス）**をチェックしてください。これが、監査ログエントリの番号に対応する番号です。

- **SSOMGR Audit Logs（SSOMGR 監査ログ）:**SSO 認証試行に関するログ。このログを有効にするには、**"Debug Options"**画面で**"SSOMGR Debug Traces"**オプションを有効にします。

ログを表示するには、目的のオプションを選択して**"View"**ボタンをクリックします。

一部のログは、さまざまな方法でフィルターできます。特定の日付範囲のログを表示するには、**"from"**フィールドと**"to"**フィールドで日付を選択し、**"View"**ボタンをクリックします。また、アーカイブされたログファイルを表示するには、ファイル名一覧から目的のファイルを選択し、**“View”**ボタンをクリックします。さらに、**“filter”**フィールドに単語や正規表現を入力し、**“View”**ボタンをクリックしても、ログファイルをフィルターできます。

SSOMGR ログファイルが空でない場合（**"Debug Options"**画面の**"SSOMGR Debug Traces"**が有効な場合）、毎日午前 0 時にこのファイルが圧縮されます。圧縮ファイル（.gz）が作成されると、そのファイルに日付スタンプで名前が付けられます。SSOMGR ファイルが圧縮されると、新しい SSOMGR ファイルが作成されます。その後、該当するログが生成されると、この新しいファイルにログが書き込まれます。ロードマスターは、圧縮された SSOMGR ファイルを最大 6 個まで同時に保持します。ファイルが圧縮されてから 7 日間経過すると、そのファイルは削除されます。

Clear Extended Logs（拡張ログのクリア）

"Clear"ボタンをクリックすると、拡張ログをすべて削除できます。

日付範囲を指定するか、ログファイル一覧から個々のログファイルを選択するか、ログファイル一覧からログの種類（たとえば、接続、セキュリティ、ユーザー）を選択し、ログファイルをフィルターしてから**“Clear”**ボタンをクリックすると、特定のログファイルを削除できます。警告メッセージが表示された場合は、**“OK”**をクリックしてください。

Save Extended Logs（拡張ログの保存）

"Save"ボタンをクリックすると、拡張ログをすべてファイルに保存できます。

日付範囲を指定するか、ログファイル一覧から個々のログファイルを選択するか、ログファイル一覧からログの種類（例えば、接続、セキュリティ、ユーザー）を選択し、ログファイルをフィルターしてから**"Save"**ボタンをクリックすると、特定のログファイルを削除できます。

10.4.3 Syslog Options（シスログ・オプション）

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ます。

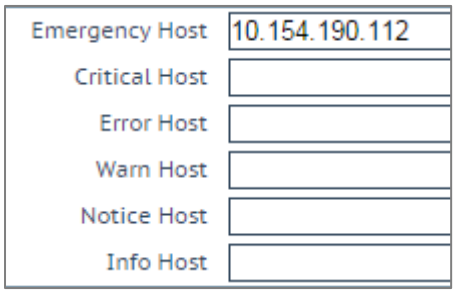

図 10-47:シスログ・オプション

該当するフィールドに該当する IP アドレスを入力し、**"Change Syslog Parameters"**をクリックすることで、このエラーメッセージをリモートの syslog サーバーに送信するようロードマスターを設定することもできます。

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。レベルは、INFO、NOTICE、WARN、ERROR、CRITICAL、EMERGENCY です。

各 Syslog フィールドでは、最大 10 個までの IP アドレスを指定できます。IP アドレスは、スペース区切りリストで区切ってください。

Syslog サーバーのセットアップ後、表示される可能性があるメッセージのタイプの例は、以下のとおりです。

- **Emergency（緊急）**:カーネル関連の重大なエラーメッセージ
- **Critical（重大）**:ユニット 1 で障害が発生し、ユニット 2 がマスターとして処理を引き継いだ状況（HA セットアップの場合）
- **Error（エラー）**:192.168.1.1 からのルートの認証エラー
- **Warn（警告）**:インターフェイスの稼働/停止
- **Notice（注意）**:時刻の同期済み
- **Info（情報）**:ローカルでアドバタイズされたイーサネットアドレス

syslog メッセージで 1 つ注意する点は、それらが上方向にカスケード接続されているということです。つまり、ホストが WARN のメッセージを受信するように設定されている場合、ログのメッセージファイルには、WARN 以下のレベルのすべてのメッセージが含まれて出力されます。

もし、WARN とその一つ下の NOTICE に同じシスログサーバーを指定した場合、NOTICE レベルのメッセージは同じホストに二回送信されます。よって、同じホストを一つ以上のレベルに設定しないことをお勧めします。

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。

10.4.4 SNMP Options（SNMP オプション）

このメニューでは、SNMP の設定を変更できます。

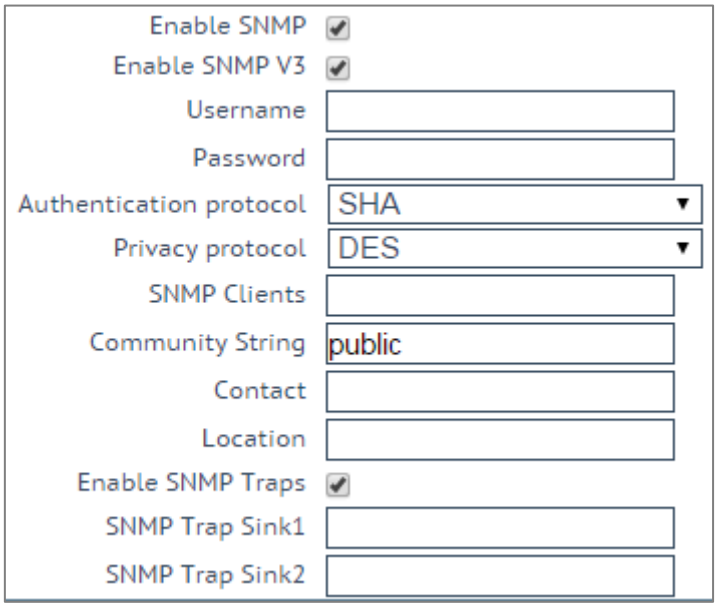

図 10-48:SNMP オプション

Enable SNMP（SNMP の有効化）

このチェックボックスは、SNMP メトリクスを有効/無効にします。たとえば、このオプションを使用すると、ロードマスターが SNMP 要求に応答するよう設定できます。

デフォルトでは、SNMP は無効になっています。

機能が有効になっている場合、次のトラップが生成されます。

- **ColdStart**　（SNMP サブシステムの開始/停止）
- **VsStateChange**（仮想サービス状態の変更）
- **RsStateChange**（実サーバー状態の変化）
- **HaStateChange（HA の状態変更）**：（HA 構成のみ:ロードマスターのフェイルオーバー）

テンプレートで作成した、ESP が有効になっている仮想サービスの監視に SNMP を使用する場合、マスターサービスに頼るのではなく、各サブ VS を直接監視するようにしてください。これは、認証プロキシのサブサービスは常に稼働中であるとしてマークされるため、その結果、そのマスターサービスも同様に稼働中であるとしてマークされることによるものです。

すべてのロードマスター固有のデータ•オブジェクトに関する情報は、3 つのエンタープライズ固有の MIB（管理情報ベース）に格納されます。

MIB ファイル	関連するデータ
IPVS-MIB.txt	仮想サーバーの統計
B-100-MIB.txt	L7 ロードマスターの設定およびステータス情報
ONE4NET-MIB.txt	エンタープライズ ID

表 10-1:MIB ファイル

SNMP を介してロードマスターの性能/コンフィギュレーションのデータを要求できるようにするには、これらの MIB ファイル（このファイルは KEMP のドキュメントページ http://kemptechnologies.com/documentation にあります）を SNMP マネジャーにインストールする必要があります。

各カウンタの説明は、ロードマスターの MIB から採取することができます。MIB 情報を読み込むためには、Linux で NADucdsnmp コマンドを使用して下記のように行います。

snmptranslate -Td -OS <oid>

ここでの < OID >は、オブジェクト識別子です。

例:<oid> = .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

snmptranslate -Td –Ov .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

.1.3.6.1.4.1.12196.12.2.1.12

RSConns	**OBJECT-TYPE**
-- FROM	**IPVS-MIB**
SYNTAX	**Counter32**
MAX-ACCESS	**read-only**
STATUS	**current**
DESCRIPTION	**"the total number of connections for this RS"**

::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12) ipvsRSTable(2) rsEntry(1) 12 }

KEMP OID は、従来化の互換性を保つため、**one4net** と呼ばれます。

ロードマスターMIB で定義されたデータオブジェクトは、WUI で表示されるカウンタのスーパーセットです。

> ロードマスター上のデータオブジェクトは、書き込み可能ではありません。よって、GET リクエスト（GET、GET-NEXT、GETBULK など）のみ使用してください。

Enable SNMP V3（SNMP V3 を有効にする）

このチェックボックスは、SNMPv3 メトリクスを有効にします。SNMPv3 は、SNMP と比べ、主にセキュリティやリモート設定機能が強化されています。

このオプションを有効にすると、2 つのフィールド、すなわち**"Username"（ユーザー名）**と**"Password"（パスワード）**のフィールドが新たに利用できるようになります。

> SNMPv3 が機能するには、**"Username"（ユーザー名）**と**"Password"（パスワード）**を設定する必要があります。
>
> パスワードは 8 文字以上でなければなりません。

Authentication protocol（認証プロトコル）

目的の**"Authentication protocol"（認証プロトコル）**（**MD5** または **SHA**）を選択します。**SHA** を推奨します。

Privacy protocol（プライバシープロトコル）

目的の**"Privacy protocol"（プライバシープロトコル）**（**AES** または **DES**）を選択します。**AES** を推奨します。

SNMP Clients（SNMP クライアント）

このオプションにより、管理者はロードマスターが特定の SNMP 管理ホストへのみ応答を返すかの指定を行います。1 つ以上のホストを指定する場合は、空白で区切って入力します。

クライアントを指定しない場合は、ロードマスターは SNMP 管理リクエストに対しての応答を不特定のホストへ返します。

SNMP Community String（SNMP コミュニティ文字列）

このオプションは、SNMP コミュニティ・ストリングの変更を許します。デフォルト値は“public”です。

"Community String"（コミュニティ文字列）では以下の文字を使用できます。**a-z, A-Z, 0-9, _.-@()?#%^+~!**.

Contact（SNMP コンタクト）

このオプションは、SNMP コンタクト名列の変更を許します。例えば、ロードマスター管理者の E-Mail アドレスなどです。

SNMP Location（SNMP ロケーション）

このオプションは、SNMP ロケーション名列を入力します。

このフィールドには、下記の文字列が使用できます。

a-z A-Z 0-9 _ .- ; , = :{ } @ ( ) ?# % ^ + ~ !

"Location"では先頭の文字にハッシュタグ記号（#）を入力しないでください。

SNMP traps（SNMP トラップ）

ロードマスターの仮想サービスや実サーバーへの重要なイベントが発生した場合、トラップが作られます。これらは、SNMP トラップシンクへ送られます。変更を行うと、ロードマスターはすべての変更が完了するまで待ち、その後、5 秒待ってからその値を読み込みます。その時点ですべての変更が安定し、SNMP トラップを送信できるようになります。この 5 秒の待ち時間中に何らかの状態変化が生じると、その状態変化が処理されて、待ち時間が再度スタートします。

Enable/Disable SNMP Traps（SNMP トラップの有効／無効化）

このトグル・オプションは、SNMP トラップの送信を有効／無効にします。

SNMP トラップは、デフォルトでは無効です。

Send SNMP traps from the shared address（SNMP トラップを共有アドレスから送信する）

このチェックボックスは、ロードマスターが HA モードにあるときのみ表示されます。

デフォルトでは、SNMP トラップは、マスターHA ユニットの IP アドレスをソースアドレスとして送信されます。このオプションを有効にすると、SNMP トラップは、マスターHA ユニットから共有 IP アドレスを使用して送信されます。

SNMP Trap Sink1（SNMP トラップシンク 1）

このオプションは、管理者がトラップの発生時に、SNMPv1 トラップをどのホストに送信するかを指定します。

SNMP Trap Sink2（SNMP トラップシンク 2）

このオプションは、管理者がトラップの発生時に、SNMPv2 トラップをどのホストに送信するかを指定します。

10.4.5 Email Options（E-Mail オプション）

この画面では、Email によるロードマスター関連イベントの警告通知を設定できます。Email 通知は、事前に定義された 6 つの情報レベルに基づいて配信できます。レベルごとに異なる受信者を設定でき、各レベルは複数の受信者を設定できます。E メール警告

は、メールサーバーによりますが、ノンセキュア、もしくはセキュア（SSL）両方の通信をサポートしています。設定と発信試験は、WUI の“System Configuration”サブメニュー下の“System Administration”オプションの“E-Mail Options”から行えます。

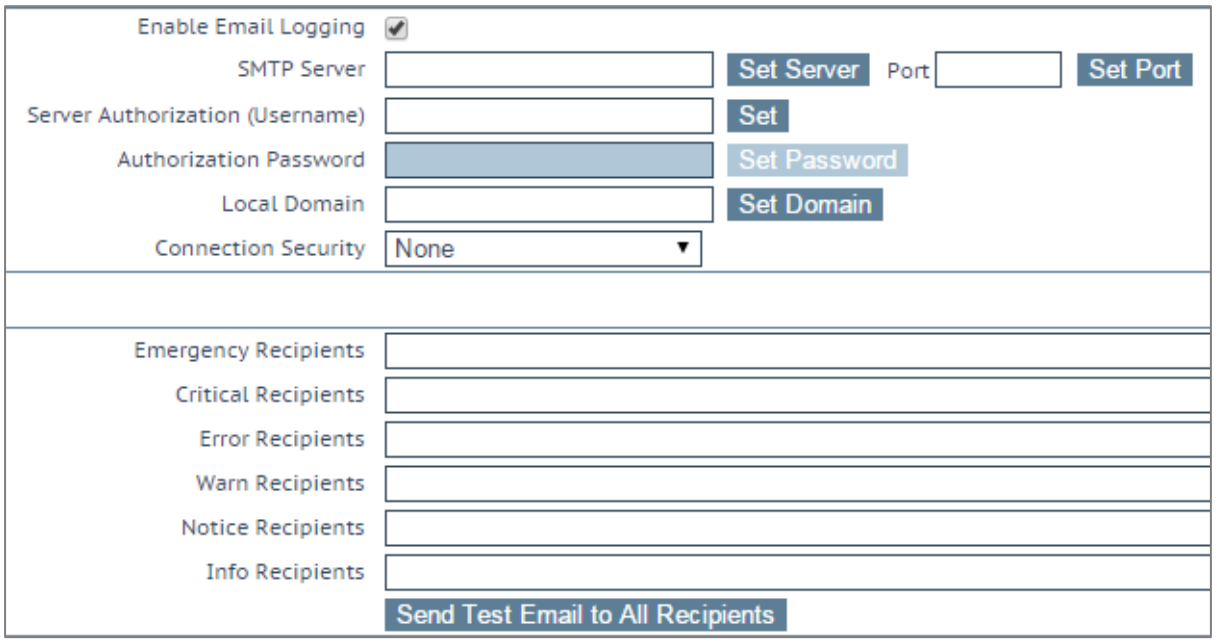

図 10-49:Email Options（E-Mail オプション）

SMTP Server（SMTP サーバー）

メールサーバーの FQDN または IP アドレスを入力します。FQDN を使用する場合は、DNS サーバーを設定してください。

Port（ポート）

E メールイベントを処理する SMTP サーバーのポートを指定します。

Server Authorization (Username)（サーバー認証（ユーザー名））

指定した SMTP サーバーが、メール配信を行うために特定権限を必要とするならば、その権限を持ったユーザー名を入力します。もし権限を必要としないならば空白のままとします。

AuthorizationPassword（認証パスワード）

上記ユーザーのためのパスワードを入力します。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み合わせて指定できます。

Local Domain（ローカルドメイン）

SMTP サーバーが、ドメインに属しているならば最上位のドメイン名を入力します。必要がなければ空白のままとします。

Connection Security（接続セキュリティ）

接続のセキュリティの種類を選択します。

- None（なし）
- STARTTLS（利用可能な場合）
- STARTTLS
- SSL/TLS

Set Email Recipient（E メール受信者の設定）

目的の通知レベルに対応する"Recipients"テキストボックスに、それぞれ担当者の Email アドレスを入力します。その重大度に加え、より高い重大度をもつものに対して通知が送信されます。そのため、複数のテキストボックスに E メールアドレスを入力する必要はありません。複数のテキストボックスに入力すると、通知が重複して送信されます。例えば、**"Critical Recipients"**テキストボックスに入力された E メールアドレスには、重大な E メールだけでなく緊急の E メールも送信されます。

以下のように、コンマ区切りリストの形式で複数の Email アドレスを入力できます。

Info Recipients（情報受信者）:info@kemptechnologies.com, sales@kemptechnologies.com

Error Recipients（エラー受信者）: support@kemptechnologies.com

リストに登録されたすべての E メール受信者にテストメールを送信するには、**“Send Test Email to All Recipients”**ボタンをクリックします。

10.4.6 SDN Log Files（SDN ログファイル）

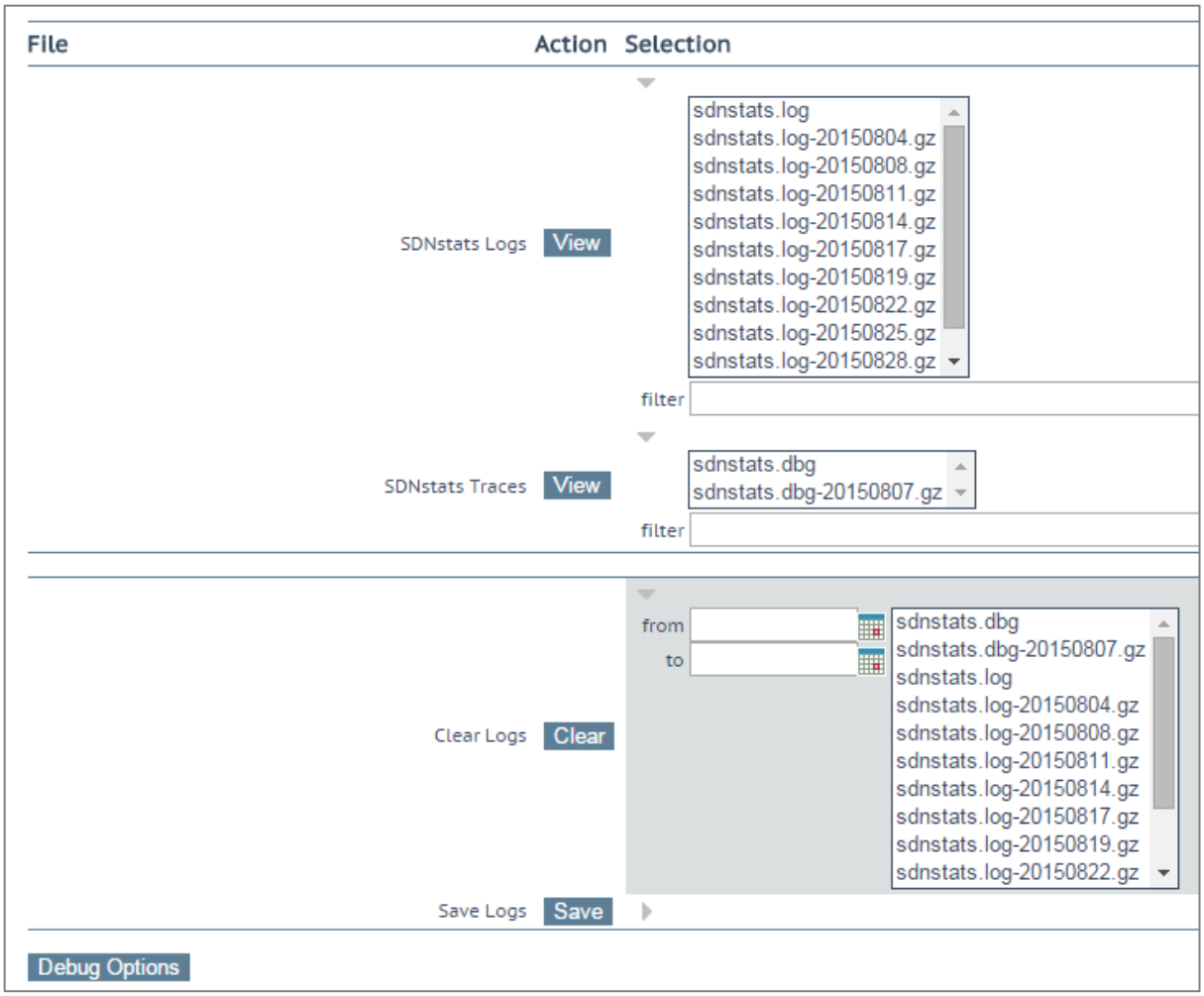

図 10-50:SDN ログファイル

"SDN Log Files"画面には、SDN 機能に関するログのオプションが用意されています。すべてのオプションを表示するには、▼アイコンをクリックします。

View SDNstats Logs（SDNstats ログの表示）

SDNstats ログを表示するには、目的のログファイルを選択して**"View"**ボタンをクリックします。

sdnstats.log がメインの循環ログファイルです。.gz ファイルは、ある特定の日におけるログのバックアップです。

また、アーカイブされたログファイルを表示するには、ファイル名一覧から目的のファイルを選択し、**“View”**ボタンをクリックします。**"filter"**フィールドに単語または正規表現を入力して"View"ボタンをクリックすると、ログファイルをフィルターできます。

View SDNstats Traces（SDNstats トレースの表示）

> このオプションは、SDNstats のデバッグログが有効のときのみ利用できます（**"System Configuration > Logging Options > SDN Log Files > Debug Options > Enable Debug Log"**）。

SDNstats ログを表示するには、目的のログファイルを選択して**"View"**ボタンをクリックします。

ファイル名一覧から目的のファイルを選択して**"View"**ボタンをクリックすることで、アーカイブされた 1 つまたは複数のログファイルを表示できます。**"filter"**フィールドに単語または正規表現を入力して"View"ボタンをクリックすると、ログファイルをフィルターできます。

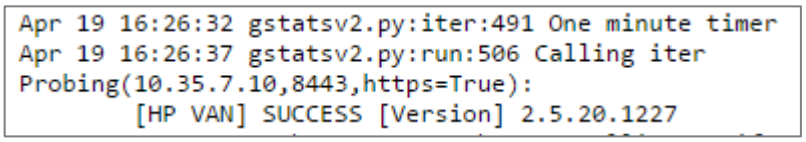

図 10-51:成功

トレースには検査結果が表示されます。この検査結果には、ロードマスターが SDN コントローラーと正しく通信できたかどうかが示されます。

Clear Logs（ログのクリア）

"Clear"ボタンをクリックすると、すべての SDN ログをクリアできます。

"from"（開始）および**"to"（終了）**フィールドで日付を指定すると、特定の範囲のログファイルを抽出できます。日付範囲を指定すると、右側のボックスにて目的のログファイルが選択されます。その場合でも、右側のボックスで個々のログファイルを選択/選択解除できます。

> **重要:sdnstats.log** を選択すると、日付範囲フィールドで選択した日付にかかわらず、そのファイルに記録されているすべてのログが消去されます。

Save Extended Logs（拡張ログの保存）

"Save"ボタンをクリックすると、すべての SDN ログをファイルに保存できます。

特定の日付範囲を指定してフィルターするか、ログファイル一覧にて 1 つまたは複数のログファイルを個々に選択して**" Save "**ボタンをクリックすると、特定のログファイルを保存できます。

10.4.6.1 Debug Options（デバッグオプション）

"SDN Debug Options"（SDN デバッグオプション）画面を開くには、**"SDN Log Files"（SDN ログファイル）**画面にて**"Debug Options"（デバッグオプション）**ボタンをクリックします。

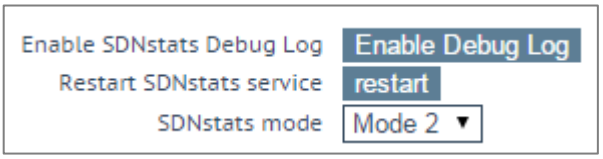

図 10-52:デバッグオプション

Enable Debug Log（デバッグログを有効にする）

SDNstats のデバッグログを有効にします。

SDN の統計値のログを表示するには、**"System Configuration > Logging Options > SDN Log Files"**を選択し、表示したいログファイルを選択して**"View"（表示）**ボタンをクリックします。

デバッグログはロードマスターのパフォーマンスに影響を与えるため、トラブルシューティング時のみ有効にしてください。

Restart SDNstats service（SDNstats サービスの再起動）

SDN の問題をトラブルシューティングする際、SDN サービス全体を再起動できます。この接続を再起動しても、トラフィックの接続には影響を与えません。このオプションは、ロードマスターと SDN コントローラーとの接続のみ再起動します。

再起動すると、**"Process ID"（プロセス ID）**が新しい ID に変わります。

"Process ID"（プロセス ID）を調べるには、**"System Configuration > Logging Options > System LogFiles"**の**"Debug"（デバッグ）**ボタンをクリックし、**"ps"**ボタンをクリックします。

このオプションは、SDN コントローラーに割り当てられているすべての接続を再起動します。

SDNstats mode（SDNstats モード）

SDN の統計情報を収集するための 2 つのモードが用意されています。

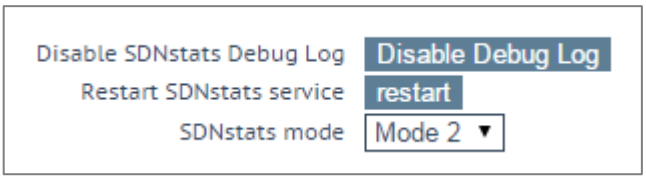

図 10-53:SDNstats mode（SDNstats モード）

モードを設定するには、**"System Configuration > Logging Options > SDN Log Files > Debug Options"**を選択し、**"SDNstats mode"（SDNstats モード）**を設定します。

各モードについて、以下で説明します。

- **Mode 1（モード 1）**:モード 1 に設定すると、サーバーに接続されているスイッチから統計情報が取り出され、その統計情報が中継されてロードマスターに返されます。
- **Mode 2（モード 1）**:モード 2 に設定すると、経路上にあるすべてのスイッチポートから統計情報が取り出されます。

10.5 Miscellaneous Options（その他のオプション）

10.5.1 WUI Settings（WUI の設定）

“bal”ユーザーまたは“All Permissions”の権限が設定されたユーザーのみ、この機能を使用できます。それ以外のユーザーの場合、画面上のボタンや入力フィールドはすべてグレー表示になります。

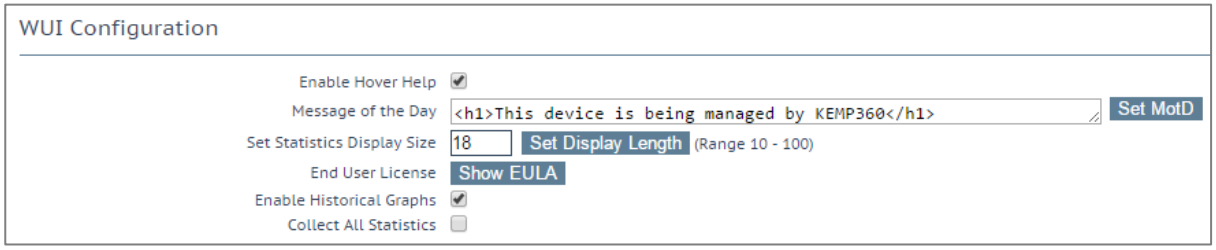

図 10-54:WUI 設定の画面

Enable Hover Help（ホバーヘルプの有効化）

フィールドの上にマウスポインターを置いたときに、青いホバーヘルプが表示されるようにします。

Message of the Day (MOTD)（本日のメッセージ（MOTD））

フィールドにテキストを入力して、**"Set MotD"**ボタンをクリックします。このメッセージは、ロードマスターのホーム画面に表示されます。

WUI のセッション管理が有効になっている場合、MOTD は HOME 画面ではなくログイン画面に表示されます。

メッセージは最大 5,000 文字まで入力できます。HTML はサポートされていますが、必須ではありません。引用符（'）と二重引用風（"）は使用できません。ただし、これらと等価の HTML 文字コードは使用できます。たとえば、&#34it&#39s allowed&#34 と入力すると、"it's allowed"という MOTD が表示されます。

Set Statistics Display Size（統計情報の表示サイズ設定）

統計情報のページに表示可能な最大行数を設定します。10～100 行の範囲でページに表示できます。

End User License（エンドユーザーライセンス）

"Show EULA"ボタンをクリックすると、ロードマスターのエンドユーザーライセンス契約が表示されます。

Enable Historical Graphs（履歴グラフを有効にする）

仮想サービスと実サーバーに関する過去の統計情報の収集を有効にします。

Collect All Statistics（全統計情報の収集）

デフォルトでは、このオプションは無効になっています。つまり、ホームページに表示するよう設定されている仮想サービスと実サーバーの統計情報だけが収集されることを意味します。このオプションを有効にすると、ロードマスターでは、すべての仮想サービスと実サーバーを対象として統計情報が収集されます。

数多くの仮想サービスや実サーバーの統計情報を収集すると、CPU の使用率が高まる可能性があります。

10.5.2 レイヤ 7 設定

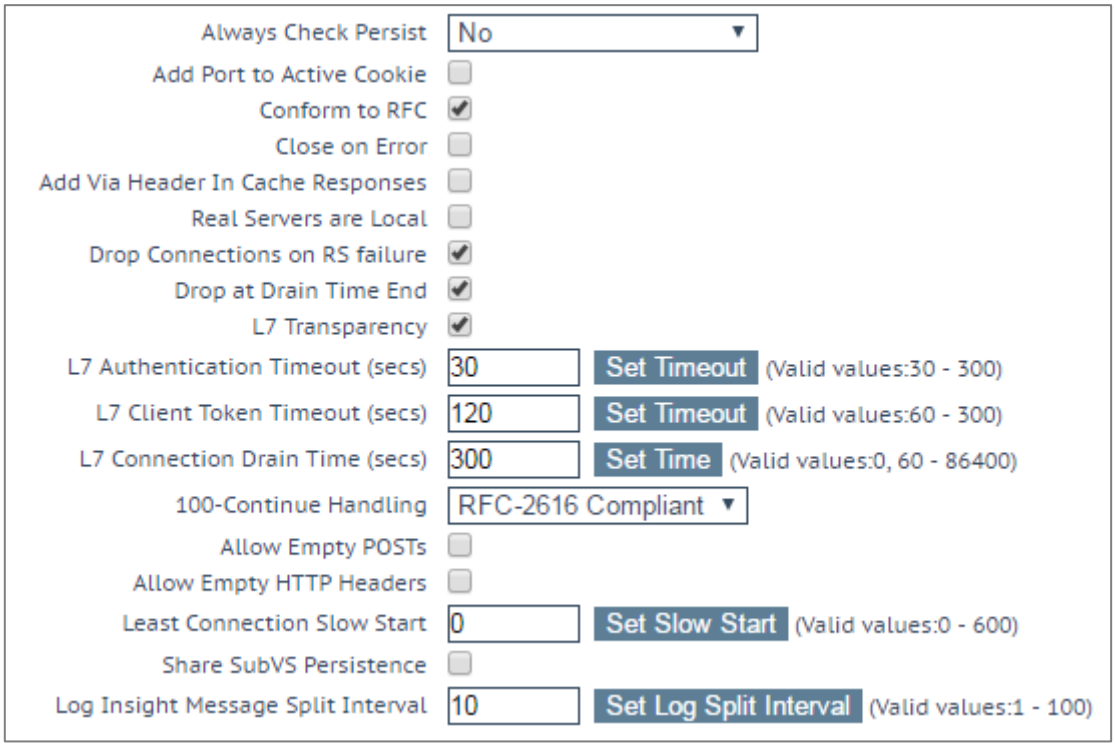

図 10-55:レイヤ 7 設定

Allow Connection Scaling over 64K Connections（64K を超える接続への拡張を許可する）

高トラフィックにおいては、VS ごとの TCP 接続数が 1 ポートの上限である 64,000 以上必要になることがあります。このオプションを使用することで、他の IP アドレスのポートを振り分けることで上限を拡張できます。他の IP アドレスの指定は、仮想サービスの属性パラメータの“Alternate Source Addresses”内に指定できます。1 つ以上の IP アドレスを指定する場合は、空白で区切って入力します。

64K を超える同時接続が必要な場合は、**“Allow Connection Scaling over 64K Connections”**オプションを有効にし、**“Alternate Source Addresses”**フィールドに代替アドレスとなる仮想サービスの IP アドレスを入力します。これにより、各仮想サービスがソースポートのプールを持てるようになります。

透過仮想サービスについては、同時接続数を 64K より大きくできません。この制限は、仮想サービスごとに適用されます。

このオプションを選択した後に代替ソースアドレスを設定した場合、**"Allow connection scaling over 64K Connections"**オプションを無効にできません。

Always Check Persist（パーシステンスを常にチェック）

デフォルトでは、L7 モジュールは HTTP/1.1 接続における最初のリクエストに対してのみパーシステンスをチェックします。このオプションで**"Yes"**を選択すると、全てのリクエストに対してパーシステンスをチェックします。**"Yes – Accept Changes"**を選択すると、接続の途中であってもパーシステンスの全ての変更が保存されます。

Add Port to Active Cookie（アクティブクッキーにポートを追加）

アクティブクッキーを使用している場合、ロードマスターは（数ある情報の中から）クライアントの IP アドレスに基づいてクッキーを作成します。ただし、プロキシサーバー経由で接続しているクライアントはすべて、同じ IP アドレスで接続していることになります。このオプションをオンにすると、クライアントのソースポートが追加されるので、クッキーのランダム性が向上します。

Conform to RFC（RFC への準拠）

このオプションは、HTTP 要求のヘッダー解析を RFC 1738 に準拠させます。

この要求は 3 つの部分で構成されています。このオプションをオンにすると、ロードマスターは HTTP リクエストの 3 つの部分から構成されている ‘GET /’ ‘パス名’ ‘HTTP / 1.1’を、パス名の最後尾としてのスペースが見つかるまでスキャンします。そして、そのスペースが見つかると、その後に続く部分が HTTP/1.x であるとみなします。パス名にスペースが含まれており、ブラウザが RFC に準拠している場合、そのパス名のスペースは"%20"にエスケープされるので、スペースのスキャンは正しく機能します。

ただし、規格に準拠していない一部のブラウザーでは、スペースがエスケープ処理されず、間違ったパス名として処理されます。そして、システムは HTTP/1.x を見つけることができないことより、ロードマスターは要求を拒否します。

この機能をオフにすると、ロードマスターは強制的にスペースはパス名の最後尾と見ます。そして、その後のパス名を HTTP/1.x の指定として処理してしまうために、リクエストは正しく処理されません。スペースを含むパス名を使用可能にするためには、RFC 1738 非準拠にしなければなりません。

Close on Error（エラー時にクローズする）

キャッシュ内のファイルの方が新しい場合など、ロードマスターがクライアントにエラーレポートを返す必要がある場合、このオプションはロードマスターによる応答の送信後に接続を強制的に終了します。このオプションを使用しないで、エラーレポートを送信した後でも、接続を継続して使用できますが、いくつかのシステムは混乱する可能性があります。このオプションは、処理を継続せずに強制的に終了します。

Add Via Header In Cache Responses（キャッシュ応答への Via ヘッダーの追加）

関連する HTTP RFC では、キャッシュから応答が帰ってきた場合には、プロキシが Via ヘッダーを追加する必要があると規定されています。残念ながら、ロードマスターの古いバージョンは、この機能に対応していませんでした。このチェックボックスは、（必要に応じて）古いバージョンとの下位互換性を有効にする目的で使用します。

Real Servers are Local（実サーバーをローカルとみなす）

ロードマスターは、透過性（選択的透過性）を目的として、ローカル/非ローカルクライアントを自動検出しています。この機能は、ほとんどのケースで問題なく動作しますが、クライアントが実サーバーである場合には適切に動作しません。このオプションをオンにすることで、実サーバーがローカルであることをロードマスター側で判定できるようになるので、選択的透過性が適切に機能します。

2 アーム環境（クライアントと実サーバーが 2 番目のインターフェイス上にある環境）にてこのオプションを有効にすると、実サーバーはクライアントから見てローカルであるかのように（非透過的に）扱われます。実サーバーが全く異なるネットワーク上にある場合、そのサーバーはローカルになることはできず、常に非ローカルとして扱われます。ローカルとは、同じネットワーク上にあることをいいます。

このオプションを有効にする際は、ネットワークトポロジーを慎重に計画してください。また、このオプションを有効にする前に、KEMP のサポートチームに必ずお問い合わせください。

Drop Connections on RS Failure（実サーバー障害時に接続をドロップする）

Microsoft Outlook ユーザーに有用なオプションであり、実サーバーの障害が検出された時点で、直ちに接続を終了します。

これは、MS Outlook ユーザーのために非常に有用なオプションです。それと同時に、**"Idle Connection Timeout"**オプションが 86400 に設定されます。詳細については、**Microsoft Exchange 2010　展開ガイド**を参照してください。

Drop at Drain Time End（ドレイン時間終了時にドロップする）

このオプションを有効にすると、無効化された実サーバーへのオープンな接続が、実サーバーのドレイン停止時間終了時にすべてドロップされます（実サーバーに継続時間が設定されていない場合は直ちにドロップされます）。

L7 Authentication Timeout (secs)（L7 認証タイムアウト（秒））

このオプションは、2 次処理（SMS や電話による確認など）を備えたサードパーティの多要素認証ソリューションとの統合をサポートします。この設定は、認証時の確認がタイムアウトするまでの、SSO フォームの待ち時間（単位: 秒）を規定します。

L7 Client Token Timeout (secs)（L7 クライアントトークンタイムアウト（秒））

認証時のクライアントトークンの待ち時間（単位: 秒）です（RSA SecurID 認証および RADIUS 認証で使用されます）。有効な値の範囲は 60～300 です。デフォルトは **120** です。

L7 Connection Drain Time (secs)（L7 接続ドレイン時間（秒））

“L7 Connection Drain Time”は、新規接続にのみ影響します。既存の接続は、その接続が終了するまで（ただし**“Drop at Drain Time End”**チェックボックスがオンになっている場合を除く）、無効化された実サーバーにアプリケーションのデータを中継し続けます。

"L7 Connection Drain Time (secs)"を **0** に設定すると、実サーバーが無効化された時点で、直ちにすべての接続がドロップされます。

サーバーがレイヤ 4 で動作している場合は、ドレインの停止は適用されません。この場合、パーシステンスレコードが破棄され、その接続は有効かつ正常に動作しているサーバーに送信されるようスケジュールされ、新たにパーシステンスレコードが作成されます。

以下の場合、新規の TCP 接続は無効化されたサーバーには送信されず、有効かつ正常に動作しているサーバーに送信されます。

- パーシステンスが無効になっている。***または***
- その接続のパーシステンスレコードの有効期限が切れていない。***または***
- 実サーバーが停止している。***または***
- ドレイン停止時間が過ぎている

上記の条件がすべて当てはまらない場合、その接続は指定したサーバーに送信され、パーシステンスレコードが更新されます。

ドレイン停止時間は、既存の接続には影響しません。

Additional L7 Header（レイヤ 7 追加ヘッダー）

HTTP/HTTPS 仮想サービスのレイヤ 7 ヘッダー挿入を有効にします。ヘッダー挿入の設定は、**"X-ClientSide"**（KEMP ロードマスター専用）、**"X-Forwarded-For"、または"None"**のいずれかを選択できます。

100-Continue Handling（100-Continue の処理）

100-Continue Handling メッセージをどのように処理するかを設定します。以下のオプションを選択できます。

- **RFC-2616 Compliant（RFC-2616 準拠）:** RFC-2616 で規定された動作に準拠します
- **Require 100-Continue（100-Continue が必要）:**100-Continue メッセージを待機するよう、ロードマスターを設定
- **RFC-7231 Compliant（RFC-7231 準拠）:** ロードマスターが 100-Continue メッセージを待たないようにします

システムにより 100 Continue メッセージがどのように処理されるかを変更するには、上記の RFC に記載されている関連技術を理解する必要があります。これらの設定を変更する前に、KEMP の技術サポートエンジニアにご相談ください。

Allow Empty POSTs（空の POST を許可）

デフォルトでは、リクエストペイロードの長さを示す Content-Length ヘッダーまたは Transfer-Encoding ヘッダーを含まない POST は、ロードマスターによってブロックされます。**"Allow Empty POSTs"**オプションを有効にすると、そうしたリクエストはペイロードデータがないものとみなされ、拒絶されなくなります。

バージョン 7.1-24 以降のリリースでは、サポートされるコンテンツ長の上限が 2GB から 2TB に増えました。

Least Connection Slow Start（**最小接続のスロースタート**）

最小接続方式または重み付け最小接続方式を使用する場合、実サーバーがオンラインになったときにそのサーバーへの接続数を制限する期間を指定し、その後、徐々に接続数を増やすように設定できます。これにより、実サーバーがオンラインになったときに接続が殺到するのを防いで、サーバーが過負荷になるのを防げます。

スロースタート期間は **0～600** 秒の範囲で設定できます。

Share SubVS Persistence（**共有サブ VS パーシステンス**）

デフォルトでは、仮想サービスの各サブ VS は個別のパーシステンステーブルを持っています。このオプションを有効にすると、サブ VS 間でその情報を共有できるようになります。この機能が動作するには、その仮想サービス内にあるすべてのサブ VS のパーシステンスモードが同じでなければなりません。このオプションを有効にするには再起動が必要です。

Persistence Mode（**パーシステンスモード**）のうち、**SSL Session ID**（**SSL セッション ID**）だけは共有できません。

共有サブ VS パーシステンス設定時、この機能を完全に動作させるにはいくつかの要件があります。

- そのサブ VS のすべての実サーバーが同じでなければならない
- すべてのサブ VS において、**"Persistence Mode"**（**パーシステンスモード**）が同じでなければならない
- タイムアウト値を同じ値に設定する必要がある

上記の要件が満たされない場合、そのサブ VS または複数のサブ VS のいずれにおいても、そのパーシステンスは正しく機能しません。

10.5.3 Network Options（ネットワーク関連オプション設定）ネットワークオプション

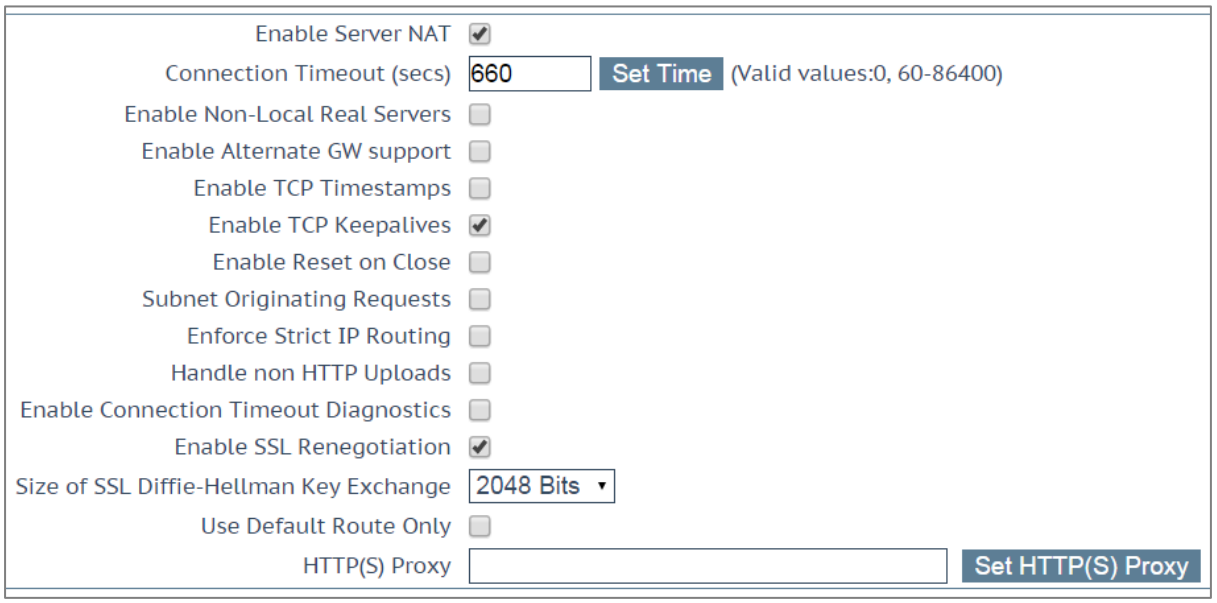

図 10-10-56:Network Options（ネットワーク関連オプション設定）ネットワークオプション

Enable Server NAT（サーバーNAT の有効化）

このオプションを選択すると、サーバーネットワークアドレス変換（SNAT）が有効になります。このオプションを無効にすると、接続時に実サーバーの IP アドレスが使用されます。

このオプションを有効にすると、デフォルトゲートウェイのプライマリアドレスと同じアドレスファミリ（IPv4/IPv6）に属するアドレスが「プライマリアドレス」に NAT 変換されます。仮想サービスにおいて**"Use Address for Server NAT"**を有効にすると、仮想サービスのアドレスが使用されます。**"Use Address for Server NAT"**オプションに関する詳細は、**セクション 3.4** を参照してください。

ソースアドレスがプライマリアドレスと同じファミリに属さない場合、そのアドレスは、そのアドレスファミリのデフォルトゲートウェイと同じネットワーク上にある最初の追加アドレスに SNAT 変換されます。

例えば、デフォルトインターフェイスのプライマリアドレスが IPv6 のアドレスであった場合、IPv6 のアドレスがそのアドレスに SNAT 変換されます。プライマリアドレスが IPv4 のアドレスであった場合、IPv6 のアドレスは、IPv6 のデフォルトゲートウェイと同じネットワーク上にある最初の追加アドレス（IPv6）に SNAT 変換されます。

同様に、デフォルトインターフェイスのプライマリアドレスが IPv4 のアドレスであった場合、IPv4 のアドレスがそのアドレスに SNAT 変換されます。プライマリアドレスが

IPv6 のアドレスであった場合、IPv4 のアドレスは、IPv4 のデフォルトゲートウェイと同じネットワーク上にある最初の追加アドレス（IPv4）に SNAT 変換されます。

Connection Timeout (secs)（接続タイムアウト（秒））

接続が閉じられる前に、接続がアイドル状態でいられる時間を秒で指定します。この値は、パーシステンスタイムアウトの値とは独立しています。

0 を設定すると、デフォルトの設定（**660** 秒）にリセットされます。

Enable Non-Local Real Servers（リモートサーバーの有効化）

非透過モード（Non ransparent）仮想サービスで、ローカルサブネット以外のサーバーを、実サーバーとして追加できます。透過モード（Transparent）の仮想サービスへは有効になりません。このパラメータを“Yes”にすると、VS 内の RS 追加時に新たなパラメータとして“Allow Remote Addresses”が表示されますので、チェックマークをいれた後でリモート RS の IP アドレスを入力します。ロードマスターがインターフェイスを 1 つしか持つことができず、実サーバーがそのインターフェイスとは異なるネットワーク上にある場合に、このオプションが必要になります。

Enable Alternate GW support（ポート 0 以外のゲートウェイの有効化）

複数のインターフェイスが有効になっている場合、このオプションは、デフォルトゲートウェイを別のインターフェイスに移行する機能を提供します。

このオプションを有効にすると、**"Interfaces"**画面に**"Use for Default Gateway"**オプションが追加されます。

"Enable Alternate GW support"オプションは、GEO のみのロードマスターの画面に別途表示されます。

Enable TCP Timestamps（L7 タイムスタンプの有効化）

ロードマスターは、デフォルトにおいて TCP 接続パケット（SYN）にタイムスタンプを含みません。L7 モードでの接続で、パフォーマンス試験などでタイムスタンプの必要がある時は、On にしてください。それ以外の一般の通常オペレーションでは、このパラメータはオフにしておくことを推奨します。

販売店のサポート要員からの要求に応じてこれを有効にしてください。

Enable TCP Keepalives（**TCP 接続のキープアライブの有効化**）

アプリケーションによっては、TCP を開いたままではタイムアウトを起こしてしまうものがあります。一般に、通常の HTTP/HTTPS サービスではキープアライブは必要ありませんが、FTP サービスなどで必要になります。

キープアライブメッセージは、ロードマスターから実サーバーとクライアントに送信されます。したがって、クライアントがモバイルネットワーク上にある場合、データトラフィックの増加が問題になる可能性があります。

Enable Reset on Close（**Reset 使用による TCP 接続クローズの有効化**）

このオプションを有効にすると、ロードマスターは通常のクローズハンドシェイクの代わりに RESET を使用して、実サーバーとの接続を終了します。このオプションによる効果が現れるのは、接続数が多く、負荷が高い場合に限定されます。

Subnet Originating Requests（**非透過モードでのソースアドレス変更**）

このオプションを有効にすると、非透過リクエストのソース IP アドレスが、該当するサブネット（すなわち、実サーバーがあるサブネット、または、静的ルートの背後にある非ローカルな実サーバーにルーティング可能なゲートウェイがあるサブネット）上のロードマスターのアドレスに設定されます。

これはグローバルなオプション/設定です。

仮想サービスごとに**"Subnet Originating Requests"**オプションを有効にすることを推奨します。

このグローバルオプションを無効にすると、各仮想サービスの**"Subnet Originating Requests"**オプションが優先されます。すなわち、仮想サービスごとに有効/無効にできます。このオプションは、仮想サービスのプロパティ画面の**"Standard Options"**セクションで設定できます（**"Transparency"**が無効の場合）。仮想サービスごとのオプションに関する詳細は、**セクション 3.4** を参照してください。

SSL の再暗号化が有効な仮想サービスに対してこのスイッチをオンにすると、その接続を処理しているプロセスを終了して再起動する必

要があるため、その仮想サービスを使用しているすべての接続が切断されます。

Enable Strict IP Routing（**厳密な IP ルーティングの有効化**）

このオプションを選択すると、アウトバウンドインターフェイスと同じインターフェイスを介してマシンに到達したパケットだけが許容されます。

これを実現するには、**"Use Default Route Only"**オプションの方が適しています。

Handle non HTML Uploads（**非 HTML のアップロード処理**）

このオプションを有効にすると、非 HTML のアップロード（FTP によるアップロードなど）が正しく機能するようになります。

Enable Connection Timeout Diagnostics（**接続タイムアウト診断を有効にする**）

デフォルトでは、接続タイムアウトログは無効になっています。これは、不要なログが大量に記録されるためです。接続タイムアウトに関するログを作成したい場合は、**"Enable Connection Timeout"**（**接続タイムアウトを有効にする**）チェックボックスをオンにします。

Enable SSL Renegotiation（**SSL の再ネゴシエーションの有効化**）

このオプションをオフにすると、クライアントにより再ネゴシエーションが要求されたときに SSL 接続が終了します。

Size of SSL Diffie-Hellman Key Exchange（**SSL のディフィー・ヘルマン鍵交換のサイズ**）

ディフィー・ヘルマン鍵交換で使用する鍵の強度を選択します。この値を変更した場合、新しい値を使用するには再起動する必要があります。デフォルトは **2048** です。

Use Default Route Only（**デフォルトルートのみ使用**）

デフォルトのルートエントリセットを持つ仮想サービスからのトラフィックを、仮想サービスのデフォルトルートが存在するインターフェイスにのみルーティングするようにします。この設定を使用すると、隣接するインターフェイスを使用してトラフィックを

直接返送することなく、ロードマスターをクライアントネットワークに直接接続できます。

このオプションを有効にすると、同じネットワーク上にあるすべての仮想サービスが影響を受けます。

HTTP(S) Proxy（HTTPS プロキシ）

このオプションを使用すると、ロードマスターがインターネットに接続する際に使用する HTTP プロキシサーバーとポートをクライアントが指定できます。

10.5.4 AFE Configuration（アプリケーション・フロント・エンド機能設定）

OCSP の設定

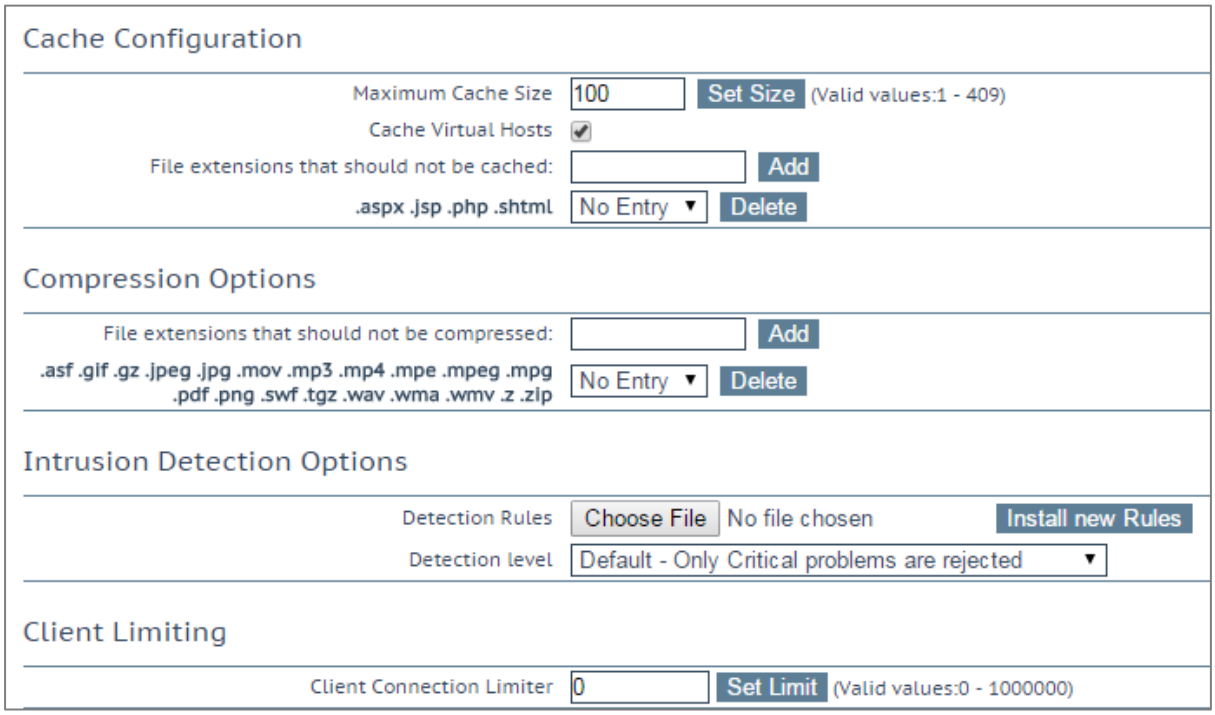

図 10-57:アプリケーション・フロント・エンド機能設定

Maximum Cache Size（最大キャッシュサイズ）

キャッシュで利用可能なメモリ容量をメガバイト単位で定義します。**"Maximum Cache Size"**は、どのくらいのメインメモリをキャッシュに割り当てるかを定義します。マシンの総メモリ容量の 50%を越えて設定することはできません。より多くのメモリをキャッシュに割り当てると、接続やパーシステンスのエントリで利用可能なメモリ量が減少し

ます。システムが正しく設定されていれば、十分なキャッシュのためのメモリ、およびシステムにより処理されると予想されるすべての接続のためのメモリが十分用意されているはずです。そうでない場合、システムのメモリが不足する可能性があります。

Cache Virtual Hosts（仮想ホストをキャッシュする）

このオプションが無効になっている場合、キャッシュ処理では、実サーバーでサポートされている仮想ホストが 1 台だけであると想定します。もし、このオプションが有効になっている場合は、実サーバーが異なるコンテンツを持つ複数の仮想ホストを持つものとしてキャッシュの処理を行います。

File Extensions Not to Cache（キャッシュしないファイル拡張子）

キャッシュされるべきではないファイルタイプのリスト。

File Extensions Not to Compress（圧縮しないファイルの拡張子）

圧縮されるべきではないファイルタイプのリスト。

Detection Rules（検出ルール）

検出ルールをインストールするには、関連する検出ルールを選択して、**"Install New Rules"**ボタンをクリックします。

SNORT ルールをインストールする場合、以下の点に注意してください。

- 宛先ポートは$HTTP_PORTS としてください
- オプションで‘msg’を設定できます。
- フローは‘to_server,established’と設定してください
- 実際のフィルターは‘content’または‘pcre’のいずれかを選択できます
- ‘http_’パラメータを追加で設定できます。
- classtype には有効な値を設定してください

最新のカスタム SNORT ルールを取得するには、SNORT のウェブサイト（https://www.snort.org/）を参照してください。
https://www.snort.org/.

Detection Level（検出レベル）

侵入防止ステムのルールのアップグレード、および検出レベルの設定変更を行えます。

- **Low** – 無拒絶、ログのみ
- **Default** – 重要な問題を含むアクセスのみ拒否
- **High** – 深刻かつ重大な問題を含むアクセスのみ拒否
- **Paranoid** – 問題が検出されたすべてのアクセスを拒否

Client Limiting（クライアントの制限）：

与えられたホストからの秒あたりの接続数の制限を設定可能です。（100K まで制限が可能）。システムに“デフォルト値の制限”を設定した後、特定のホスト/ネットワークのために異なる制限を設定できます。

ネットワークとそのネットワーク上のホストを設定する場合は、表示されるリストの順番による処理が行われるため、優先順位の高いホストより設定する必要があります。

クライアントの上限をオフにするには、**"Client Connection Limiter"**の値を **0** に設定します。

10.5.5 SDN の設定

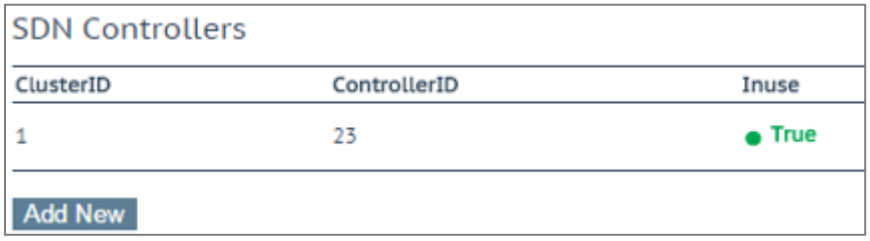

図 10-58:SDN 設定画面のセクション

新規追加

SDN コントローラー接続を新規に追加します。

Modify（変更）

既存の SDN コントローラー接続を変更します。

Delete（削除）

既存の SDN コントローラー接続を削除します。

10.5.5.1 SDN コントローラーの設定

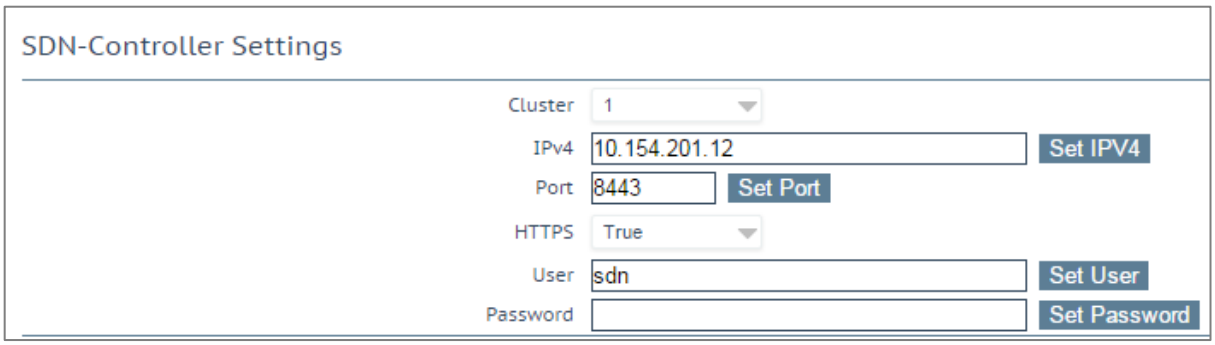

図 10-59:SDN コントローラーの設定

SDN コントローラーの接続を新たに追加する際、始めに、**Cluster（クラスター）**、**IPv4** アドレス、**Port（ポート）**を尋ねる画面が表示されます。SDN コントローラーの接続を追加後、**"SDN Statistics"**画面の**"Modify"**をクリックすることで設定を更新できます。

Cluster（クラスター）

SDN コントローラーがメンバーとなるクラスターです。

"Cluster"フィールドはデフォルトのままにしてください。

IPv4

SDN コントローラーの IPv4 アドレス。

Port（ポート）

SDN コントローラーWUI のポートです。

HP VAN コントローラーのデフォルトの**ポート**は **8443** です。

OpenDaylight SDN コントローラーのデフォルトの**ポート**は **8181** です。

HTTPS

SDN コントローラーへのアクセスに HTTP/HTTPS を使用します。

User（ユーザー）

SDN コントローラーへのアクセスで使用するユーザー名です。

Password（パスワード）

SDN コントローラーへのアクセスで使用するパスワードです。

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://kemptechnologies.com/documentation から入手できます。

仮想サービスとテンプレート機能説明

RSA の 2 要素認証　機能説明

コンテンツルール機能説明

ロードマスター5.1 から 6.0 への移行　テクニカルノート

ヘッダー変更ガイド　テクニカルノート

GEO　製品概要

GEO Sticky DNS　機能説明

パケットトレースガイド　テクニカルノート

VMware ツールのアドオンパッケージ　機能説明

カスタム認証フォーム　テクニカルノート

ポートフォローウィング　機能説明

SSL アクセラレーションサービス　機能説明

アプリケーションファイアウォールパック（AFP）カスタムルール

Kerberos Constrained Delegation　機能説明

ハードウェアセキュリティモジュール（HSM）　機能説明

IPsec トンネリング　機能説明

KEMP ロードマスター　製品概要

SDN アダプティブ負荷分散　機能説明

DoD 共通アクセスカード（CAC）認証　機能説明

RESTful API　インターフェイス説明

ライセンス　機能説明

RADIUS の認証と権限設定　テクニカルノート

ロードマスターのクラスタリング　機能説明

Microsoft Exchange 2010　展開ガイド

RADIUS の認証と権限設定　テクニカルノート

ユーザー管理　機能説明

Document History

Date	Change	Reason for Change	Ver.	Resp.
June 2015	Release updates	Updates for 7.1-28 release	1.34	LB
July 2015	Release updates	Updates for 7.1-28a release	3.0	LB
Aug 2015	Minor changes	Enhancements made	4.0	LB
Sep 2015	Release updates	Updates for 7.1-30 release	5.0	LB
Dec 2015	Minor changes	Enhancements made	6.0	LB
Jan 2016	Minor changes	Updated Copyright Notices	7.0	LB
Mar 2016	Minor changes	Enhancements made	8.0	LB
May 2016	Minor changes	Enhancements made	9.0	LB
July 2016	Release updates	Updates for 7.1.35 release	10.0	LB