Web ユーザ インターフェイス（WUI）
設定ガイド

2018 年 6 月

目次

1　はじめに

KEMP Technologies 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 サービスとアプリケーションインフラストラクチャを最適化にできます。KEMP Technologies 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 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 LoadMaster の Web ユーザインターフェイス（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 LoadMaster の各種機能の設定方法について詳しく説明します。

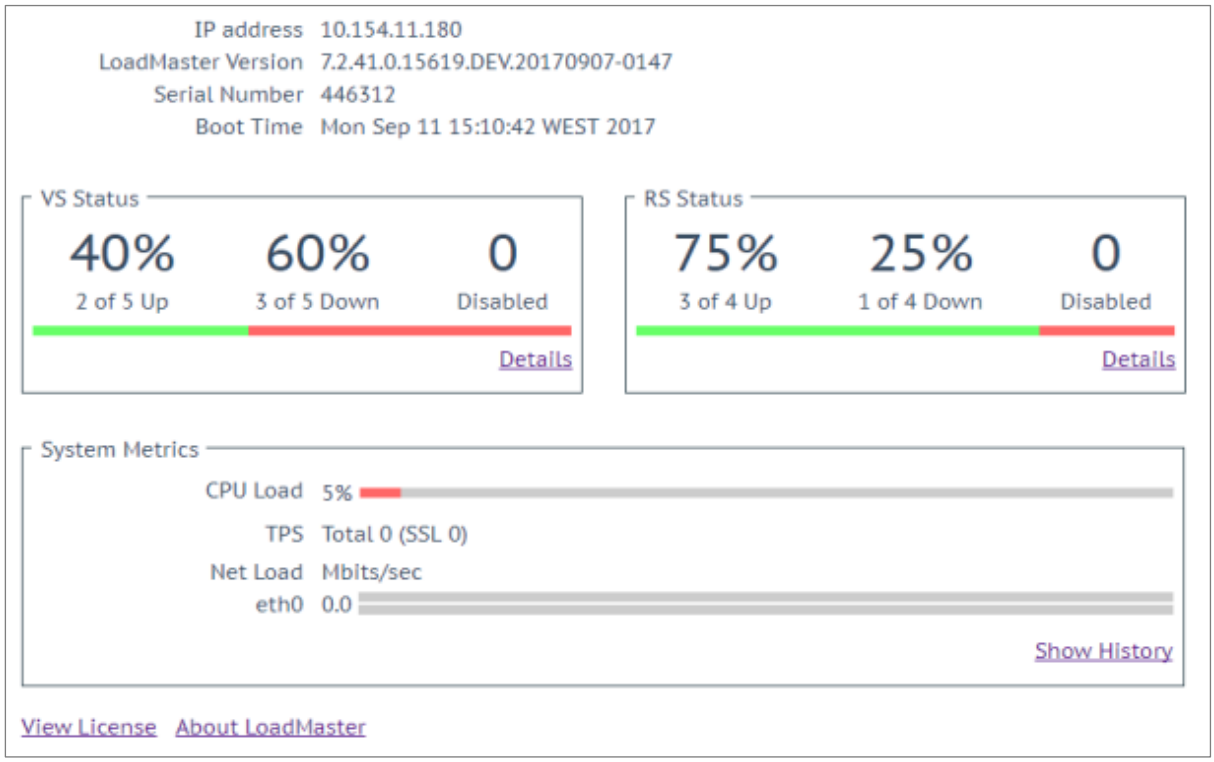
LoadMaster で使用可能なメニューオプションは、本ドキュメントで説明しているものと異なる場合があります。LoadMaster で使用可能な機能は、有効になっているライセンスの種類によって異なります。ライセンスをアップグレードされる場合は、FXC 株式会社の担当窓口までご連絡ください。

1.2 対象読者

本ドキュメントは、WUI を使って KEMP LoadMaster を設定するユーザを対象としています。

2　ホーム画面

メニューの[Home] をクリックするとホーム画面を表示します。このページでは LoadMaster に関する基本情報を表示します。



いずれかのパネルに情報が表示されない場合は、ブラウザの設定をデフォルトにリセットしてみてください。

2.1 ログイン情報

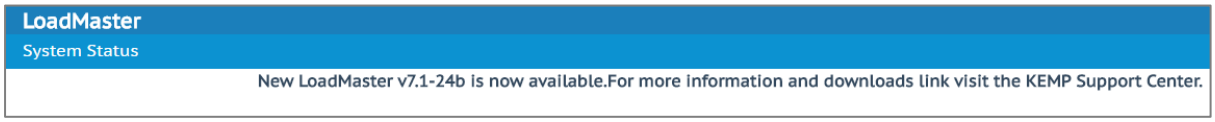
イニシャル後に LoadMaster にログインすると、[Session Management] を有効にしていると、いくつかのログイン情報を表示します：

- カレントユーザの最後のログイン時間と IP アドレス
- カレントユーザの直近 30 日のログインした回数
- カレントユーザの最後のログイン後、任意のユーザ（未知のユーザ）が企てたログインの失敗総数

より詳細な Session Management 情報は、「OCSP の設定」のセクションを参照してください。

2.2 一般情報

IP Address : LoadMaster の IP アドレス
LoadMaster virsion : LoadMaster のファームウェアバージョン



[Allow Update Checks] 機能が有効場合、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を表示します。自動チェック機能を有効にするには、>Certificates & Security >Remote Access で選択ができます。詳細は「アドミニストレータのアクセス」セクションを参照してください。

Serial Number : LoadMaster のシリアル番号
Boot Time : サーバを最後にリブートした時刻

2.3 バーチャルサービスとリアルサーバの状態

VS Status（バーチャル ステータス）

このセクションでは、バーチャルサービスの監視情報を表示します（稼働中のバーチャルサービスの割合や、無効になっているバーチャルサービス数など）。[Details] のリンクをクリックすると、View/Modify Services 画面を表示します。

1 時間ごとに、バーチャルサービス、SubVS、リアルサーバ数（稼働/停止中の数など）に関する syslog メッセージを生成します。syslog メッセージは状態が変化したときにも生成します。

RS Status（リアルサーバ ステータス）

このセクションではリアルサーバの監視情報を表示します（稼働中のリアルサーバの割合や、無効になっているリアルサーバ数など）。[Details] のリンクをクリックすると、リアルサーバ画面を表示します。

2.4 WAF ステータス

Web アプリケーション ファイアウォール（WAF）のステータスセクションでは、1 つ以上のバーチャルサービスで WAF が有効かどうかを表示します。ここでは以下の値を表示します。

- WAF が処理したリクエストの総数（すべてのリクエストでブロックされたかどうかを表示します）。それぞれの接続では、インバウンド リクエストとアウトバウンド レスポンスをセットで記録します。
- WAF によって処理した（ブロックした）イベントの総数
- 現在時刻まで（xx：00：00 以降）に発生したイベントの数
- 深夜以降（日付が変わってから）に発生したイベントの数
- 一日の中で、イベントカウンタが設定している閾値を超えた回数。たとえば、閾値が 10 でイベントが 20 回発生すると、カウンタは 2 になります。閾値はバーチャルサービスごとに、>Virtual Service >View/Modify Services >WAF Option 画面の[Hourly Alert Notification Threshold] フィールドで設定します。詳細は「Web アプリケーションファイアウォール（WAF）」セクションを参照してください。

2.5 システム メトリックス

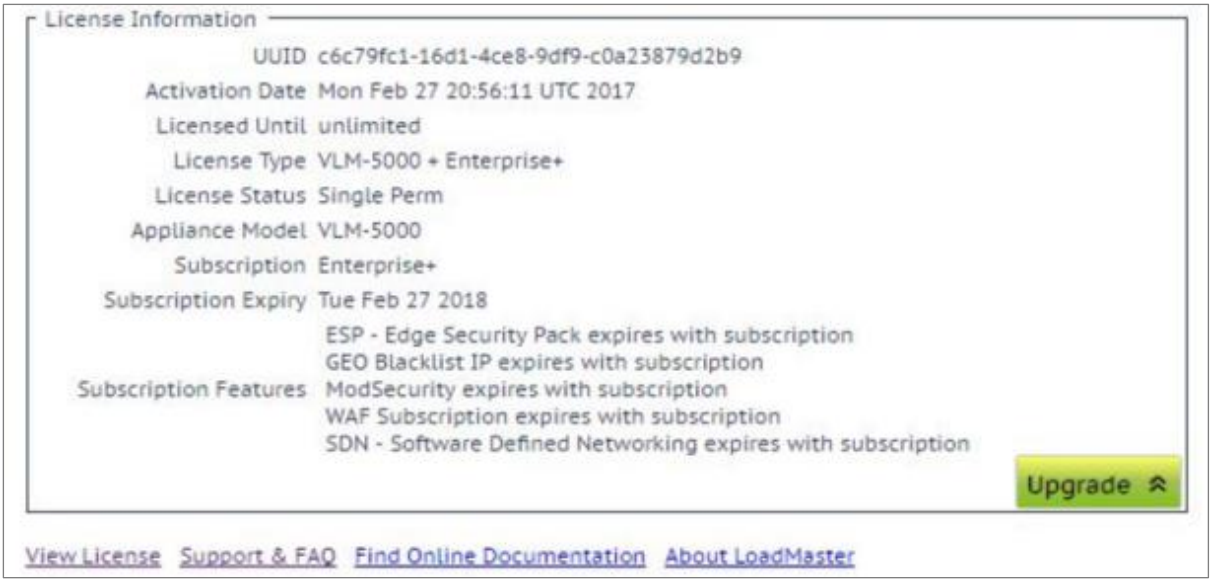
CPU Load : LoadMaster アプライアンスの CPU 負荷率
TPS [conn/s] : 1 秒当たりの総トランザクション数と 1 秒当たりの SSL トランザクション数
Net Load : インターフェイスごとのネットワーク負荷（Mbit/秒）。設定したインターフェイスのみ表示します。
CPU Temp : CPU の温度（ハードウェアがサポートしている場合のみ）

CPU 負荷とネットワークト負荷は 5 秒ごとにデータを更新します。Dell の LoadMasters では、SNMP を使用した以下のハードウェア統計情報が取得できます。

- 温度
- ファンの回転速度
- 電源状況
- 電圧と電流

これらの値は、SNMP を使用してのみ有効です。詳細な情報は「SNMP オプション」セクションを参照してください。

2.6 ライセンス情報



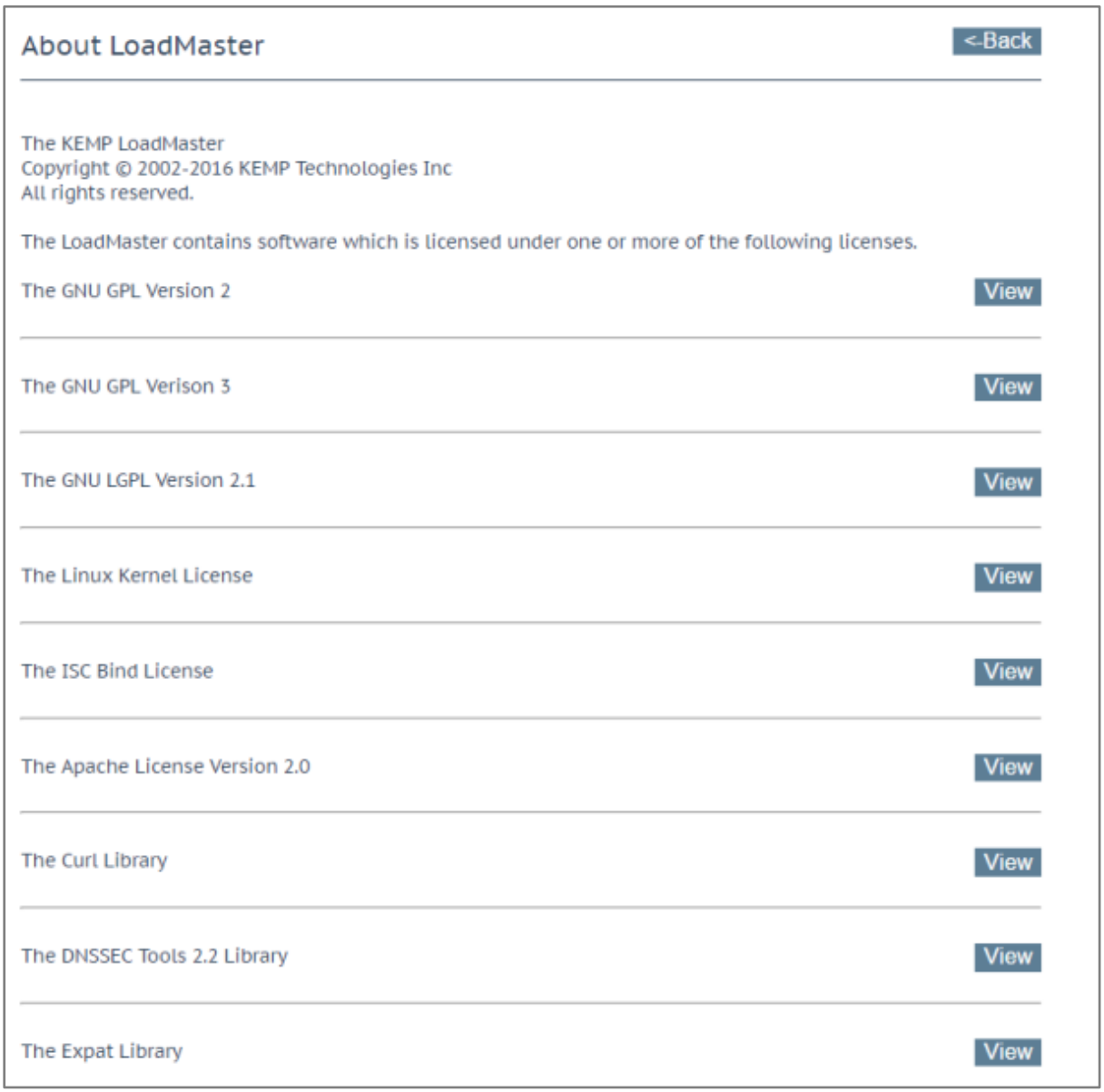
[View License] クリックすると、LoadMaster ライセンスのアクティベーション日や終了日などを含む、モデル名、サブスクリプションの有効期限、サブスクリプションの機能詳細を表示します。

サブスクリプションの有効期限が切れると、[License Information] セクションにメッセージを表示します。
サブスクリプションを更新される場合は、FXC 株式会社までお問合せください。

Upgrade : LoadMaster をアップグレードする場合は、FXC 株式会社にお問合せください。

2.7 LoadMaster について

[About LoadMaste] ページでは、LoadMaster が使用するサードパーティ ソフトウェアのライセンスを表示します。

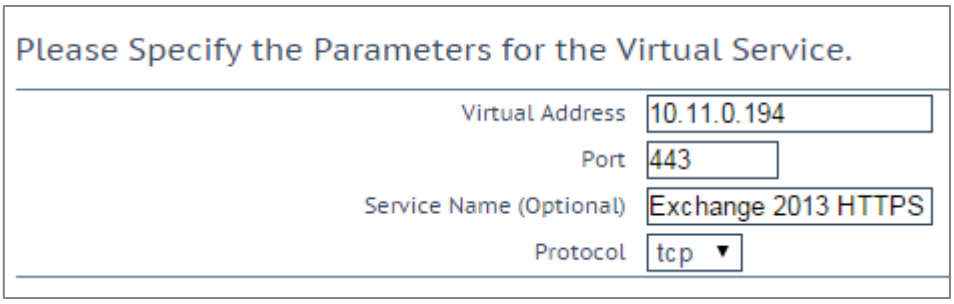


ライセンスを表示するには、該当する項目の [View] ボタンをクリックしてください。

3 バーチャル サービス

これ以降、本ドキュメントでは LoadMaster の WUI 左側に表示される
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



ここでは、仮想 IP（VIP）アドレス、ポート番号、プロトコル、名前を定義し、新しいバーチャルサービスを作成します。これらの値はテキストボックスにマニュアル入力し、プロトコルタイプはプルダウンリストから選択します。

お使いの LoadMaster 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。このリストは、作成するバーチャル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、サービスに対応するテンプレートが選択できます。

テンプレートの詳細な情報は、KEMP ドキュメントページの「Virtual Services and Templates Feature Description」を参照してください。

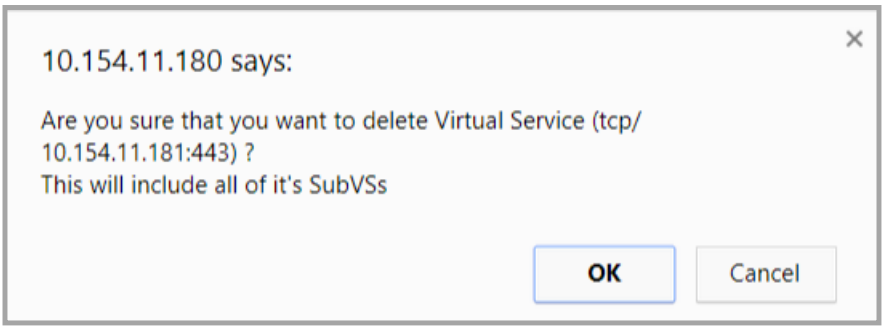
LoadMaster による Exchange の構成は、概ね 13 のバーチャルサービスが上限です。

3.2 表示と変更（設定済みの HTTP サービス）

この画面は、LoadMaster に設定したバーチャルサービスをリスト表示します。各バーチャルサービスの主要な設定内容を表示し、サービスの変更削除と新規作成に対応するオプションを用意しています。

注 意

削除すると元に戻せませんので、[Delete] は注意して扱ってください。



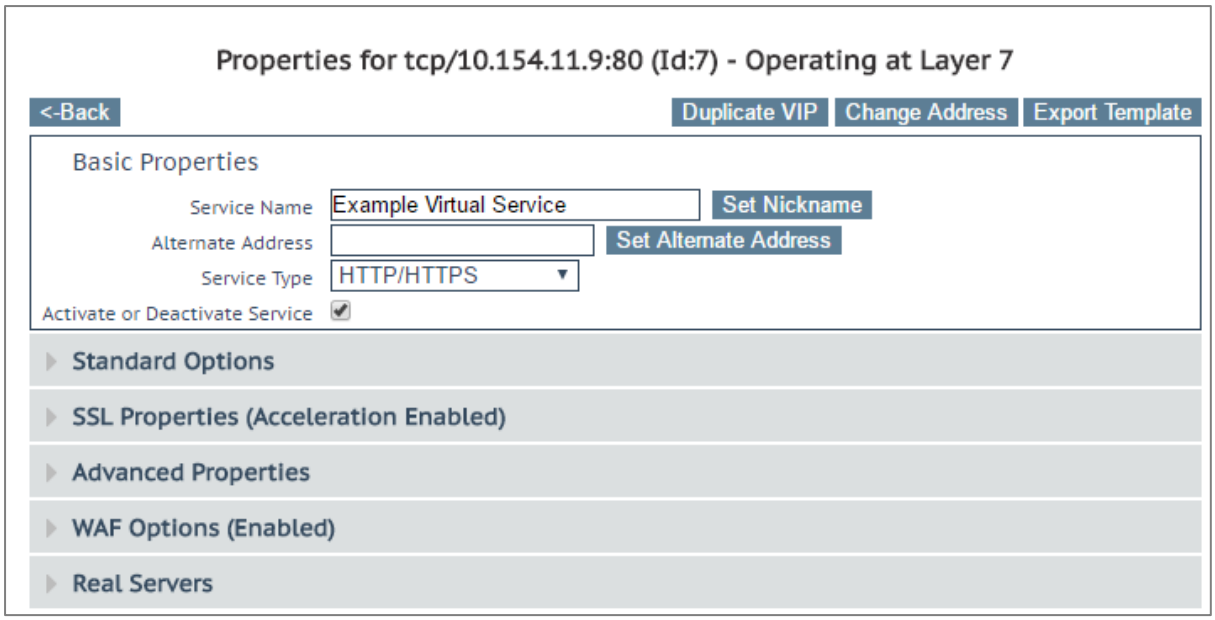
SubVS を含むバーチャルサービスを削除しようとすると、確認の警告を表示します。[OK] をクリックして削除を確認します。

バーチャルサービスの状態も表示されます。バーチャルサービス作成時、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、「リアルサーバ」を参照してください。

バーチャルサービスのステータスは、次のいずれかになります。

- **Up :** 1 つ以上のリアルサーバが稼働している状態です
- **Down :** 1 つのリアルサーバも稼働していません
- **Sorry :** すべてのリアルサーバがダウンしたため、ヘルスチェックなしで別に設定した Sorry サーバにトラフィックを転送します
- **Disabled :** バーチャル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、バーチャルサービスが無効になっています
- **Redirect :** 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、リダイレクトバーチャルサービスを作成できます。詳細は「アドバンス プロパティ」セクションを参照してください
- **Fail Message :** 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「アドバンス プロパティ」セクションを参照してください。
- **Unchecked :** リアルサーバのヘルスチェックが無効になっています。すべてのリアルサーバが稼働状態であるという前提でアクセスされます。
- **Security Down :** LoadMaster が認証サーバにアクセスできません。エッジ・セキュリティ・パック（ESP）が適用されているバーチャルサービスへのアクセスは、LoadMaster により拒否されます。
- **WAF Misconfigured :** 特定のバーチャルサービスの 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、ステータスは赤字で[WAF Misconfigured] を表示します。バーチャル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、必要に応じてそのバーチャルサービスの 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、バーチャルサービスのプロパティ画面です。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。



- **Basic Properties :** バーチャルサービスの基本情報を設定します
- **Standard Options :** バーチャルサービスの中で最も広く使われる機能をせっていします
- **SSL Properties :** SSL アクセラレーションを使用している場合、[Acceleration Enabled] と表示します。この画面で SSL 機能を設定します。
- **Advanced Properties :** バーチャルサービスの追加機能を設定します
- **WAF Options :** Web アプリケーション ファイアウォール（WAF）オプションを設定します
- **ESP Options :** エッジセキュリティ（ESP）に関するオプションを設定します
- **Real Servers :** バーチャルサービスの実サービスであるリアルサーバと SubVS の割り当てを行います

各フィールドとオプションは、サービスタイプ、と機能の有効/無効に応じて表示が切り替わります。
このスクリーンショットは、必ずしもお使いの LoadMaster の画面と一致するものではありません。

3.3 ベーシック プロパティ

[Basic Properties] の設定欄の右上に以下の 3 つのボタンがあります。

Duplicate VIP（VIP の複製）

関連する SubVS を含め、バーチャルサービスをコピーします。バーチャルサービスのすべての設定は、新しいバーチャルサービスに複製されます。このボタンをクリックすると、コピーしたバーチャルサービスの IP アドレスとポートを指定する画面を表示します。

Change Address（アドレスの変更）

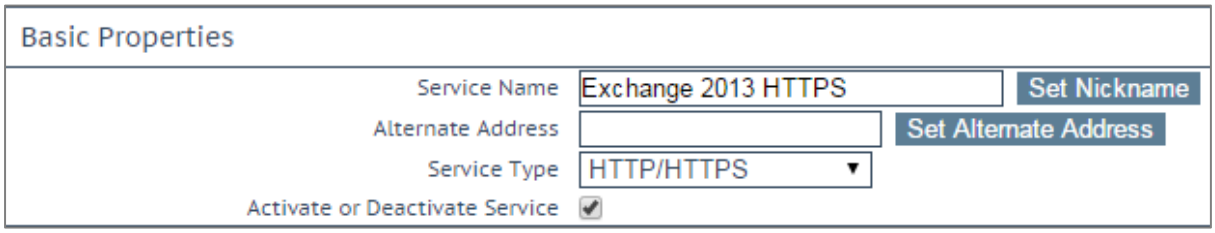
このボタンをクリックすると、バーチャルサービスの仮想 IP アドレスとポートを変更する画面を表示します。

Export Template（テンプレートのエクスポート）

バーチャル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、バーチャルサービスを素早く簡単に作成できます。

> カスタム **Cipher セット**を使用するバーチャルサービスでテンプレートをエクスポートした場合、そのテンプレートをインポートする LoadMaster には同じカスタム **Cipher セット**を用意しなければなりません

テンプレートから作成されたバーチャルサービスは、テンプレートに基づいてすべての設定を保持しています。必要なバーチャルサービスの設定は、適宜変更が必要になります。テンプレートの詳細な情報は、KEMP ドキュメントページの「Virtual Services and Templates Feature Description」を参照してください。



Service Name（サービス名）

このテキストボックスは、作成するバーチャルサービスにニックネームの割り当てができます。また、設定したのニックネームを変更することもできます。

> 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（代替アドレス）

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、バーチャル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。

[Service Type] を設定すると、バーチャルサービスのオプションが変化します。負荷分散するアプリケーションのタイプに応じて設定する[Service Type] 明らかにすることが重要です。

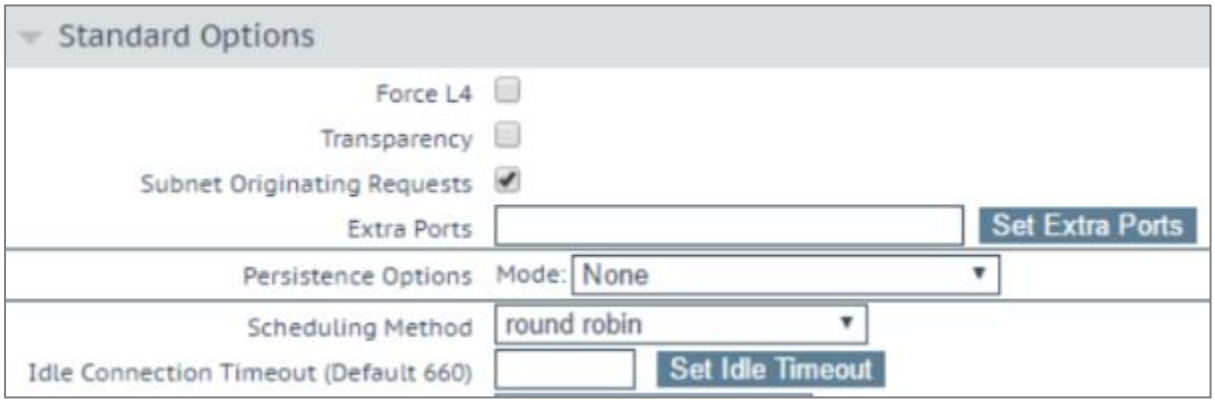
> WebSocket Virtual Services must be get to the Generic Service Type.

HTTP/2 パススルー サービスタイプは HTTP/2 トラフィックを許可します。ただし、現在のアドレス変換（[transparency] 、[subnet originating] [alternate source] ）以外のレイヤ 7 オプションは提供していません。

Activate or Deactivate Service（サービスのアクティブと非アクティブ）

このチェックボックスでは、バーチャルサービスの有効/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。

3.4 スタンダード オプション



Force L4（フォース L4）

このチェックボックスをオンにすると、バーチャルサービスはレイヤ 4 の実行になります。レイヤ 7 ではありません。この設定は特定の状況でのみ必要ですので、不確かな場合は選択しないでください。

L7 Transparency（L7 透過モード）

L7 では接続を透過します。これは、リアルサーバに届く接続がクライアントから直接送られるように見えるます。また、接続を透過しない場合、リアルサーバの接続は LoadMaster からの接続でとして見えます。KEMP は、一般的な設定で L7 の透過を無効にすることを推奨しています。

透過性を有効にすると、バーチャルサービスは透過的になります（NAT（ネットワークアドレス トランスファー）を行いません）。ただし、クライアントの IP、バーチャルサービスの IP、リアルサーバの IP が同じサブネット上にある場合、バーチャルサービスは自動的に送信元 IP を NAT します（非透過を有効にします）。

[Real Servers are local] オプションを有効にすると、[L7 Transparency] が有効でも、リアルサーバへは NAT 処理（非透過モード）になります。これは、リアルサーバがクライアントのリクエストを答えるだけでなく、バーチャルサービスへリクエストを発信する場合に限って発生します。リアルサーバの詳細情報は、L7 コンフィグレーションを参照してください。

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。

[Subnet Originating Requests] が有効な場合、リアルサーバへ送信するソースアドレスは、LoadMaster のインターフェイスアドレスになります。このオプションを無効にすると、ソースアドレスはバーチャルサービスの IP アドレスになります。[L7 Transparency] が有効になっている場合、ソースアドレスはクライアントの IP アドレスになり、[Subnet Originating Requests] オプションは無視されます。

リアルサーバがサブネット上にあり、[Subnet Originating Requests] オプションが有効な場合、LoadMaster のサブネットアドレスがソース IP アドレスになります。

[Subnet Originating Requests] は、ローカルに配備したリアルサーバ向けの設定です。リアルサーバがローカルではなく、デフォルトゲートウェイのインターフェイスでない場合は、再暗号化についての問題はありません。[Alternate Source Addresses] フィールドにローカルアドレスを強制指定すると、通常の接続とバーチャルサービスの再暗号化で問題なく動作します。

[subnet originating requests] オプションは、バーチャルサービスごとに設定できます。もし、すべてのバーチャルサービスを一括設定する場合は、>System Configuration >Miscellaneous Options >Network Options の[Subnet originating Requests] を有効にします。

バーチャルサービスごとに[Subnet Originating Requests] オプションを有効にすることを推奨します。

一括設定オプションについては「ネットワーク オプション」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、バーチャルサービスごとに制御できます。

SSL の再暗号化が有効なバーチャルサービスに対してこのスイッチをオンにすると、そのバーチャル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（エクストラ 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。

ポート番号は、バーチャルサービスで設定しているポートの他に、連続しない番号やシーケンシャルな番号をを指定できます。フィールドに入力するポート番号はスペースかカンマで区切り、最大 510 ポートまでの範囲を指定できます。

エクストラ ポートは、ポート範囲で入力する、空白かカンマで区切った単一ポートで入力することができます。例えば、[8000-8080,9002,80,8050,9000] のよう入力すると、ポート 80、8000～8080、9000、9002 を追加します。

Server Initiating Protocols（サーバ起動のためのプロトコル）

デフォルトでは、LoadMaster はクライアントからデータを受け取るまでリアルサーバとの接続を開始しません。これはデータの送信の前に、リアルサーバとの通信に必要な確定したプロトコルが動作しないようにするためです。

バーチャルサービスがこれらのプロトコルのいずれかを使用する場合は、ドロップダウンリストからそのプロトコルを選択して正しく機能するようにします。

選択できるプロトコルは次のとおりです。

- SMTP
- SSH
- IMAP4
- MySQL
- POP3
- その他のサーバ起動のためのプロトコル

バーチャルサービスのポート番号を 80、8080、443 で設定している場合は[Server Initiating Protocol] オプションを表示しません。

Persistence Options（パーシステンス オプション）

パーシステンスはバーチャルサービスごとに設定します。このセクションでは、サービスの設定でパーシステンスを有効に設定しているとき、パーシステンス タイプとパーシステンス タイムアウトの値を設定できます。

パーシステンスが有効な場合、LoadMaster はクライアントを最初に接続したリアルサーバのセッションを保持します。つまり、同じクライアントは引き続き同じリアルサーバに接続します。タイムアウト値は、この接続の継続時間を決定します。

パーシステンスのタイプは、以下のドロップダウンリストに表示するオプションから選択できます。

- **Source IP Address（ソース IP アドレス）**
  リクエストを送信するクライアントのソース IP アドレスをパーシステンスの識別に使用します。
- **Super HTTP（スーパーHTTP）**
  LoadMaster で、HTTP と HTTPS サービス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が一意作成したフィンガープリントを使用して適切なリアルサーバへの接続を維持します。フィンガープリントは、以下の組み合わせの値に基づいています。
  フィンガープリントは、[User-Agent] フィールドと[Authorization] ヘッダ（存在する場合）を組合せた値に基づいています。同じヘッダの組み合わせを持つ接続は、同じリアルサーバに接続します。
- **Server Cookie（サーバクッキー）**
  LoadMaster は、HTTP ヘッダ内の特別に設定されたクッキーの値をチェックします。同じクッキーを使用するリクエストは、同じリアルサーバに配信します。
- **Server Cookie or Source IP（サーバクッキーとソース IP）**
  サーバクッキーのパーシステンスが失われた場合は、ソース IP をベースのパーシステンスに切り替ります。

- **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、サーバではなく LoadMaster 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リクエストが LoadMaster のバーチャルサービスに到達すると、LoadMaster は特定の Cookie を探します。目的のクッキーがない場合、LoadMaster は[Set-Cookie] 命令で HTTP ストリームにアクティブクッキーを挿入します。既存のクッキーには影響しません。
  サーバクッキー パーシステンス メソッドにより、LoadMaster が生成するクッキーの値は各クライアントでユニークになり、クライアントを明確に識別できます。この手法では、サーバがクッキーの生成と管理を行う必要がなく、サーバ負荷を軽減できるメリットがあります。クライアント別に接続を分散させるには、L7 構成でアクティブクッキー機能に AddPort を有効にすることです。このオプションの詳細については、「L7 コンフィグレーション」を参照してください。
  アクティブクッキーのパーシステンスを使うと、セッションとセッションの有効期限が切れるまでクッキーが有効になります。たとえば、パーシステンス タイムアウトが 10 分でアクティブクッキー パーシステンスを使用すると、クライアントが午後 2 時に接続し、2.05pm で切断、再接続すると、パーシステンスのタイムアウト値をリセットします。パーシスタンス タイムアウトが経過した後にクライアントがバーチャルサービスに接続しようとすると、古いクッキーが提示されます。LoadMaster はパーシステンス テーブルをチェックし、有効なエントリがないことを確認します。LoadMaster はクライアント用の新しいクッキーを生成し、そのパーシスタ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とソース IP）**
  アクティブなクッキーのパーシステンスが失われた場合は、ソース IP がベースのパーシステンスに切り替ります。

- **Hash All Cookies（ハッシュ オールクッキー）**
  ハッシュ オールクッキー方式は、HTTP ストリーム内のすべてのクッキーの値でハッシュを作成します。同じ値を持つクッキーは、要求ごとに同じサーバに配信します。値が変わると、これまでの接続は新しい接続として扱い、クライアントを負荷分散アルゴリズムに従ってサーバに割り当てます。

- **Hash All Cookies or Source IP（ハッシュ オールクッキーとソース IP）**
  ハッシュ オールクッキーまたはソース IP はハッシュ オールクッキーと同じです。ただし、HTTP 文字列にクッキーが存在しない場合にソース IP パーシステンスに切り替ります。

- **Super HTTP and Source IP Address（スーパーHTTP とソース IP）**
  スーパーHTTP と同じですが、ソース IP アドレスを文字列に追加することでハッシュの結果による分配性を改善します。

- **URL Hash（URL ハッシュ）**
  URL ハッシュ パーシステンスを使用すると、LoadMaster は同じ URL を持つリクエストを同じサーバに配信します。

- **HTTP Host Header（HTTP ホストヘッダ）**
  HTTP ホストヘッダ パーシステンスを使用すると、LoadMaster は HTTP ホストヘッダ内の同じ値を含むすべてのリクエストを同じサーバに配信します。
- **Hash of HTTP Query Item（HTTP クエリ ハッシュ）**
  この方式は、サーバ パーシステンスとまったく同じ振舞いをしますが、URL のクエリ文字列が名前付きの項目として検査の対象になります。同じクエリ アイテム値を持つすべてのクエリを同じサーバに配信します。
- **Selected Header（指定ヘッダ）**
  指定ヘッダ パーシステンスを使うと、LoadMaster は定義したヘッダと同じ値を含むすべてのリクエストを同じサーバに配信します。
- **SSL Session ID（SSL セッション ID）**
  SSL セッションには、セッション保持を可能にするセッション ID があります。

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、バーチャルサービスの[Service Type] を[Generic] に設定し、SSL アクセラレーションを無効にする必要があります。

バーチャルサービスが SSL サービスであり、オフロードをしない場合、LoadMaster はレイヤ 7 ストリーム内のデータを操作できません。その理由は、データが暗号化されており、LoadMaster は復号化でないからです。
上記のシナリオで、ソース IP を基にしないパーシステンス モードの要求がある場合、この設定が唯一の解決手段です。SSL セッションを開始するとセッション ID が生成されます。このセッション ID を使用すると、クライアントを適切な正しいサーバに接続保持することができます。
ただし、この方法にはいくつかの弱点があります。最新のブラウザの多くは、セッション ID を短い間隔で再生成するので、基本的にはセッション ID が上書きとなります。結果としてパーシステンス タイムアウト間隔を長く設定しても効果が出ません。

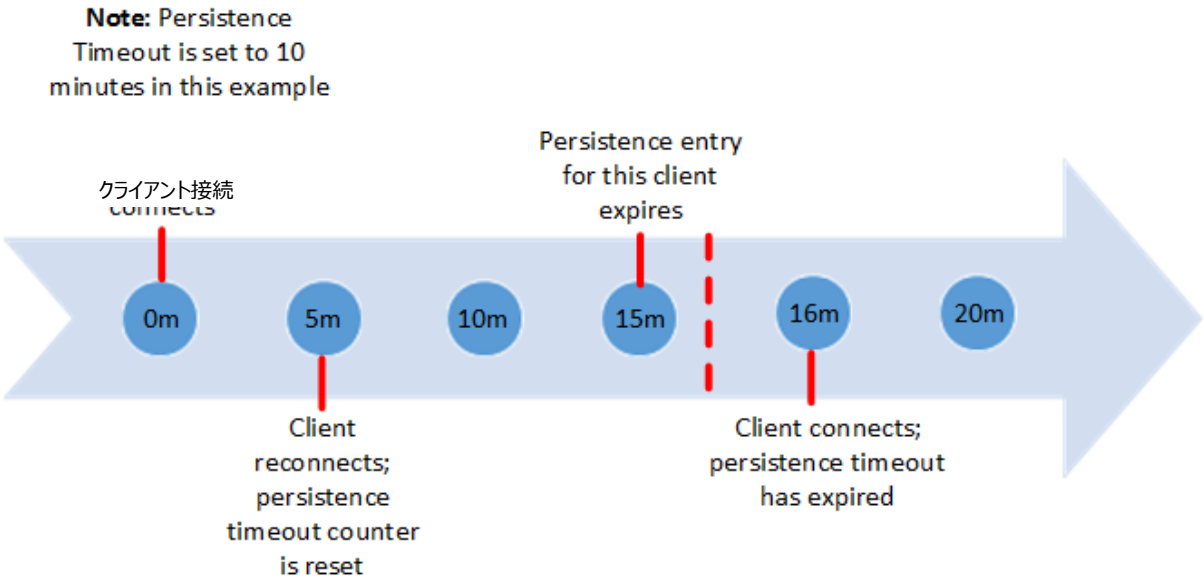
- **UDP Session Initiation Protocol (SIP)（セッション イニシエーション プロトコル（SIP））**
  このパーシステンス方式は、UDP ベースのバーチャルサービスで[Force L4] が有効になっている場合にのみ使用できます。SIP は HTTP のように、リクエストとレスポンスのトランザクションを使用します。最初にいくつかのヘッダフィールドを含む INVITE リクエストを送信します。このヘッダフィールドはパーシステンスで使用ができます。

Timeout（タイムアウト）

各パーシステンス方式には、設定可能なタイムアウト値があり、ユーザごとにパーシステンスをどのくらいの長さにするかを決め、1 分から 7 日間の間で時間を選択します。

このタイムアウト タイマは、初期の接続で起動します。タイムアウト時間内にクライアントが再接続すると、パーシステント タイムアウト値が更新されます。たとえば、1 時間に設定したパーシステンス タイムアウト環境で、クライアントが 14 時に接続し 15 時より前に切断した場合、このクライアントが再接続すると同じリアルサーバでパーシ

ステンスを維持します。このとき、このクライアントのパーシステンス タイマは設定値である 1 時間にリセットされます。



タイムアウト時間内にクライアントがバーチャルサービスに繰り返し接続すると、クライアントのリクエストは同じリアルサーバに継続して配信します。例えば、以下のシナリオが考えられます。

- パーシステンス タイムアウトが 10 分に設定されている
- クライアントは、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

このとき、要求は、利用可能な（ヘルスチェックに応答している）リアルサーバに配信します。

クライアントが 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リアルサーバに配信します。接続が 10 分以上オープンな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ることになり、LoadMaster はそのクライアントに新しいパーシステンスエントリを作成し、新規のリアルサーバにリクエストを配信します。これは接続の確定でパーシステンスのカウントダウンを開始するのであって、接続の終了時ではないためにこ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ときは、十分なタイムアウト時間を設定していないことが原因になるケースがあります。パーシステンスのタイムアウト値が十分な長さでない場合は、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。一般には、リアルサーバのタイムアウト値に合わせてこの値を設定することが推奨されます。

Header field name（ヘッダフィールド名）

LoadMaster において、パーシステンスモードで[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を表示します。パーシステンス情報の基となるヘッダフィールド名をここで入力してください。

Scheduling Methods（スケジューリング方式）

このセクションは LoadMaster が、特定のサービスに対してリアルサーバを決定するためのスケジューリング方式について説明します。スケジューリング方式は次のとおりです：

- **Round Robin（ラウンドロビン）**
  ラウンドロビンでは、セッションを順番にリアルサーバへ割り当てます。たとえば、最初のセッションはリアルサーバ 1 に接続し、二番目のセッションはリアルサーバ 2 に接続します。
- **Weighted Round Robin（重み付けラウンドロビン）**
  この方式は、リアルサーバの重み付け値を使用して、どのリアルサーバを優先するかを決定します。高い重み付けのリアルサーバほど、配信するコネクションの割合が高くなります。
- **Least Connection（最小接続）**
  この方法では、セッションを接続数が最も少ないリアルサーバに割り当てます。
- **Weighted Least Connection（重み付け最小接続）**
  最小接続と同様ですが、重み付けによる配信の偏りがあります。
- **Resource Based (Adaptive)（リソースベース アダプティブ）**
  アダプティブ スケジューリング方式は、リアルサーバの負荷を定期的にモニターし、すべてのリアルサーバの負荷が等しくなるようにコネクションを配信します。詳細は、「スケジューリング方法」セクションを参照してください。
- **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（SDN を使用するかどうかにかかわらず）を使用しているバーチャルサービスは、制御システムと見なすことができます。これは、リアルサーバ間で負荷を均等に配分し、コントローラがそれを基に誤差計算するからです（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（リアルサーバの重み）も計算します。
- **Fixed Weighting（固定重み付け）**
  すべてのトラフィックは、利用可能な最も重み付けの高いリアルサーバに配信します。リアルサーバは、設定時に重み付けを行います。2 つのリアルサーバの重み付けを同じにすると正しい動作になりませんので、必ず異なる値を設定してください。

固定重み付けの場合、重みの高いリアルサーバは緑の星印で表示します。

- **Weighted Response Time（重み付け応答時間）**
  LoadMaster は、15 秒ごとにヘルスチェックプの応答にかかる時間を測定し、この時間に応じてリアルサーバの重みを調整します。重み付けが増えると、そのリアルサーバに配信するトラフィックが増加します。リアルサーバの応答時間が早いほど重み付けが大きくなり、リアルサーバに転送す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 アドレスから生成したハッシュ値を使用して、リクエストを同じリアルサーバへ配信します。これは、リアルサーバは常に同じホストからの接続であることを意味します。この方式を設定すると、他のソース IP パーシステンス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 アドレスだけに依存し、現在のサーバ負荷を無視します。このため、特定のリアルサーバが高負荷になったり、リアルサーバ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 （アイドルコネクション タイムアウト デフォルト 660）

アイドル状態の接続を切断するまでの秒数を指定します。このフィールドに設定できる特殊な値がいくつか用意されています。

- 0 を設定すると、[L7 connection timeout] のデフォルト時間を使用します。デフォルトのタイムアウト値は >System Configuration >Miscellaneous Options >Network Options で変更できます。
- 1 を設定するとパケットを最初に配信した後に接続を破棄します。このとき、レスポンスを期待せず、レスポンス処理も行いません。
- 2 を設定すると DNS 方式の動作になります。応答メッセージ後のコネクションを切断します。

[Idle Connection Timeout] に特別な値である 1、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、バーチャルサービスが返信するパケットの IP ヘッダの DSCP（Differentiated Services Code Point）を設定します。この設定により、次のデバイスやサービスにトラフィック処理と優先順位の設定を指示します。LoadMaster は、優先順位の高いパケットを低いパケットより先に送信します。

各オプションについて、以下に説明します。

- **Normal-Service :** 特別な優先順位をトラフィックに割り当てない
- **Minimize-Cost :** 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 :** 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 :** 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] 機能が有効なのは L7 トラフィックだけです。L4 トラフィックでは、機能しません。

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

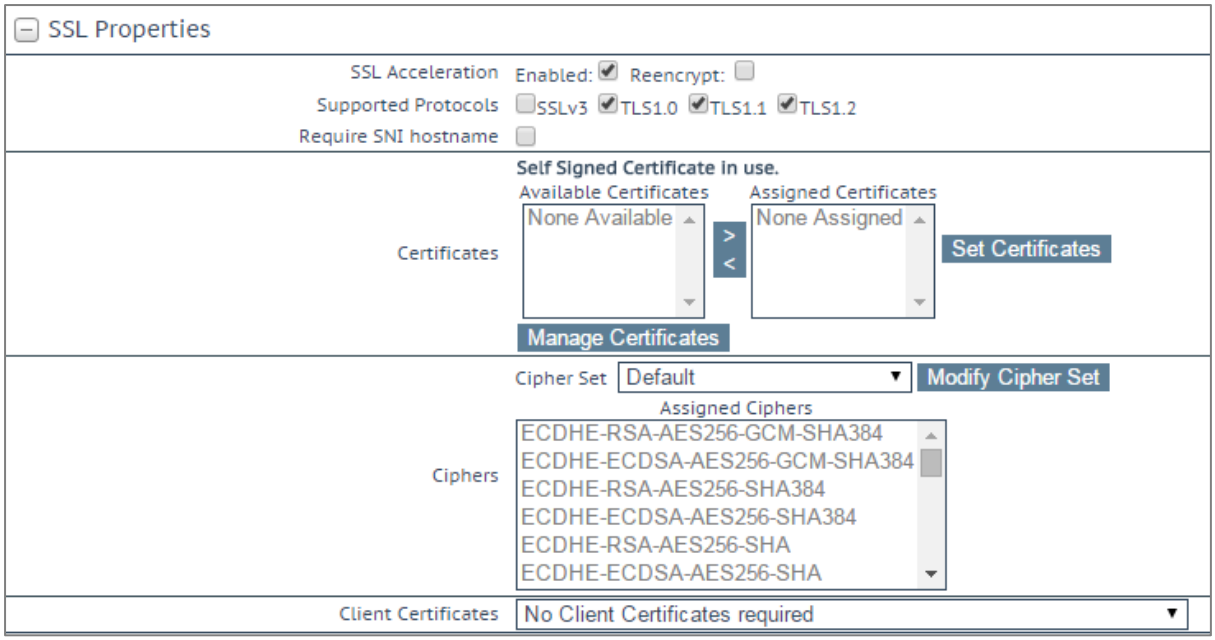
LoadMaster が SNAT でリアルサーバを接続する場合、デフォルトでは LoadMaster のソース IP アドレスがインターネットで使用されます。[Use Address for Server NAT] オプションを選択すると、バーチャルサービスを構成するリアルサーバは、バーチャルサービスのアドレスをソース IP アドレスとして使用できます。

このオプションは、SNMP などのサービスでもっとも有効です。これは、LoadMaster がパブリックドメイン内にあり、LoadMaster 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 DNS の逆引きチェックを必要とするときです。

リアルサーバがこのオプションが設定する複数のバーチャルサービスがある場合、サーバが要求するデスティネーション ポートと一致するバーチャルサービスの IP アドレスをソース IP アドレスとして使用します。一致するポートがない場合は、LoadMaster の IP アドレスをソース IP アドレスとして使用します。

[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バーチャル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しません。

3.5 SSL プロパティ



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、バーチャル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リアルサーバに送信される前に再度暗号化します。

Reversed（逆方向）：このチェックボックスをオンにすると、LoadMaster からリアルサーバ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バーチャルサービスとの接続で、このバーチャル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、クライアントからリアルサーバへのデータパスは送信中、常に暗号化されます。

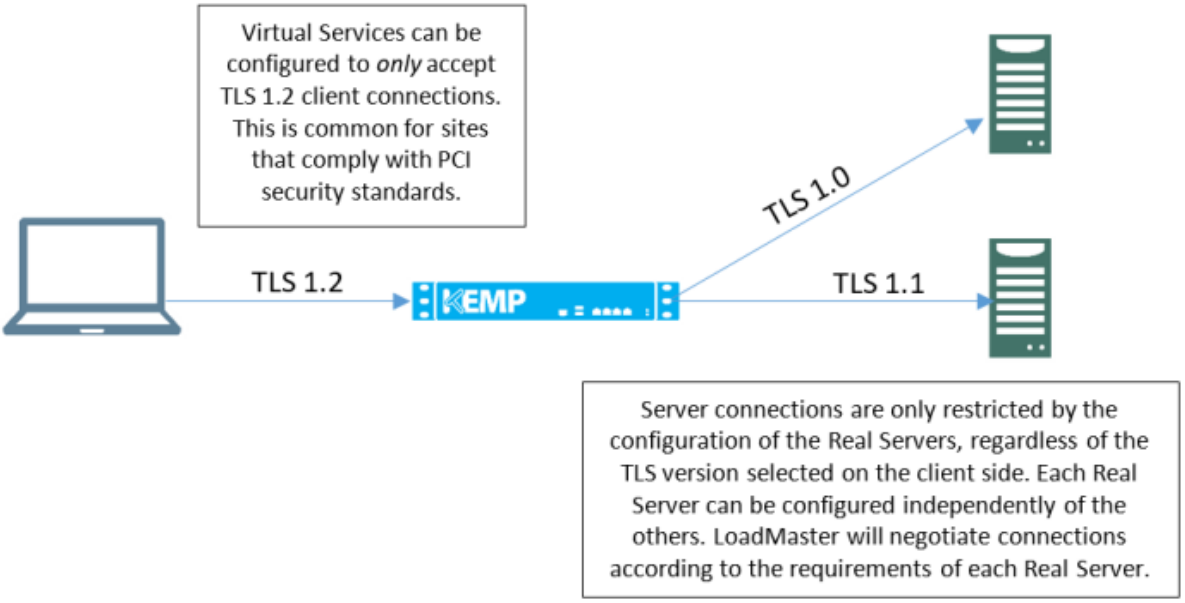
Supported Protocols（サポートするプロトコル）

[Supported Protocols] セクションのチェックボックスでバーチャルサービスがサポートするプロトコルを指定できます。デフォルトでは、TLS1.1 と TLS1.2 は有効で、SSLv3 と TLS1.0 は無効になっています。

バージョン 7.2.37 以降、再暗号化が有効になっていると、LoadMaster と背後のリアルサーバ間でネゴシエートできる TLS バージョンは、クライアント側で設定した TLS バージョンによって制限されなくなりました。

LoadMaster がサポートするすべての TLS バージョンと Cipher は、リアルサーバの制限によらずにネゴシエートできます。このことは、例えば、アプリケーションアクセスに対する厳重なセキュリティを持つクライアントの安全性を

確保した上で、安全性の低い TLS バージョンと Cipher のみをサポートするレガシーサーバへ接続ができることを意味します。この例は以下のイラストで説明します。



Require SNI hostname（SNI ホスト名の要求）

[Require SNI hostname] を選択すると、ホスト名を必ず TLS クライアントの Hello メッセージに含まれす必要があります。

[Require SNI hostname] を無効にすると、一致するホストヘッダが見つからなかった場合に最初の証明書を使用します。

[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です。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。

SAN（Subject Alternative Name）証明書では、代替ソース名はホストヘッダと一致しません。

ワイルドカード証明書はサポートしますが、ルートドメイン名が RFC 2459 に準拠しないことに注意してください。ドットの左側だけが一致します。ルートドメイン名と一致するように証明書を追加する必要があります。たとえば、www.kemptechnologies.com はワイルドカードを使った *.kemptechnologies.com に一致しますが、Kemptechnologies.com は一致しません。

HTTPS ヘルスチェックで SNI ホスト情報を送信するには、関連するバーチャルサービスの[Real Servers] セクションで[Use HTTP / 1.1] を有効にし、ホストヘッダを指定してください。これの設定がない場合は、リアルサーバの IP アドレスが使用されます。

Certificates（証明書）

左側の[Available Certificates] リストに、利用可能な証明書を表示します。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矢印ボタンをクリックし[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、「SSL 証明書」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、LoadMaster はクライアントからもサーバからも証明書を取得します。LoadMaster はクライアント証明書をヘッダに転記し、そのデータをサーバに送信します。このとき、サーバ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 LoadMaster 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）

リアルサーバに接続するときに使用する 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 セット

Cipher Set とは、暗号化/復号化を行うアルゴリズムのことです。

SSL アクセラレーションが有効になっているバーチャルサービスには、Chipher Set が割り当てられます。Cipher Set には、システム定義の Cipher Set とカスタム Cipher Set のいずれかを使用できます。システム定義の Cipher Set を使用すると、目的の Cipher を素早く簡単に選択でき、強度の高い暗号を簡単に適用できます。カスタム Cipher Set の作成と編集を行うには、[Modify Cipher Set] をクリックします。

Cipher

[Ciphers] リストは読み取り専用で、LoadMaster に登録済みの Cipher 一覧を表示します。[Modify Cipher Set] ボタンをクリックすると、[Cipher Set Management] 画面を表示します。この画面では、カスタム Cipher Set の新規作成と既存のカスタム Cipher Set を編集できます。

Client Certificates（クライアント証明書）

- **No Client Certificates required :** 有効にすることで、全クライアントからの HTTPS リクエストを受け入れます。推奨する設定です。
  デフォルトでは、LoadMaster 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 LoadMaster 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:** 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 :** 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。また、LoadMaster は ヘッダの追加とクライアント証明書情報をアプリケーションに転送します。
- 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
  - Client Certificates and pass DER through as X-CLIENT-CERT
  - Client Certificates and pass PEM through as SSL-CLIENT-CERT
  - Client Certificates and pass PEM through as X-CLIENT-CERT

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

OCSP（オンライン証明書ステータスプロトコル）を使用してクライアントの証明書の正当性を検証します。

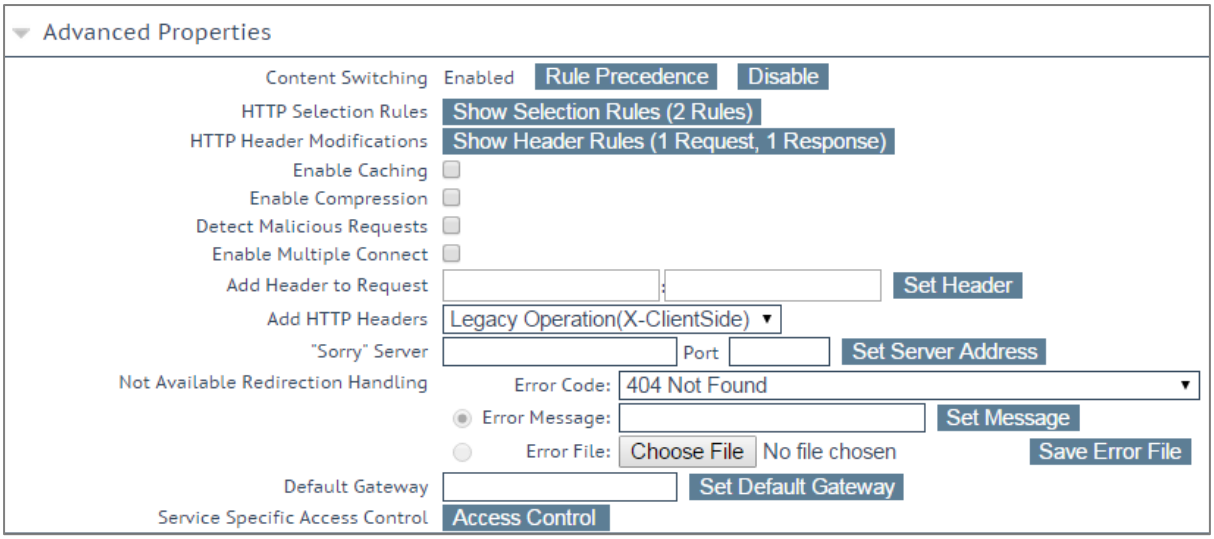
このオプションは ESP が有効な場合のみ表示されます。

Strict Transport Security Header（正確なトランスポート セキュリティヘッダー）

このオプションを有効にすると、LoadMaster が生成するすべてのメッセージ（ESP およびエラーメッセージ）に正確なとトランスポート セキュリティヘッダーを追加できます。ドロップダウンで以下のオプションが選択できます。

- Don't add the Strict Transport Security Header （ヘッダーを追加しない）
- Add the Strict Transport Security Header - no subdomains（サブドメイン無しでヘッダーを追加する）
- Add the Strict Transport Security Header - include subdomains（サブドメインを含めたヘッダーを追加する）

3.6 アドバンスド プロパティ

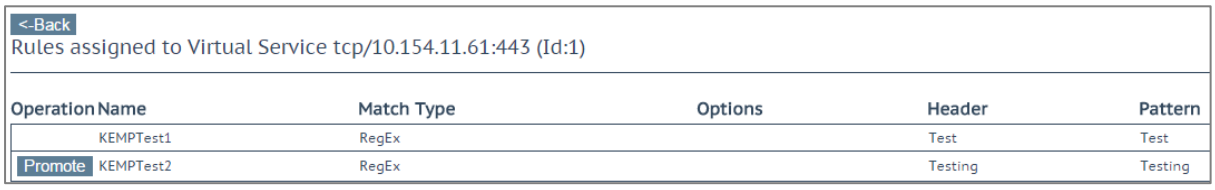


Content Switching（コンテンツスイッチ）

[Enable] ボタンをクリックすると、設定中のバーチャル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。有効にすると、該当するリアルサーバにルールを割り当てる必要があります。リアルサーバにルールを割り当てるには、リアルサーバ設定の[None] ボタンをクリックします。ルールがリアルサーバに割り当てられると、[None] には割り当てたルールの数を表示します。

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、リアルサーバにルールが割り当てられている場合のみ表示します。



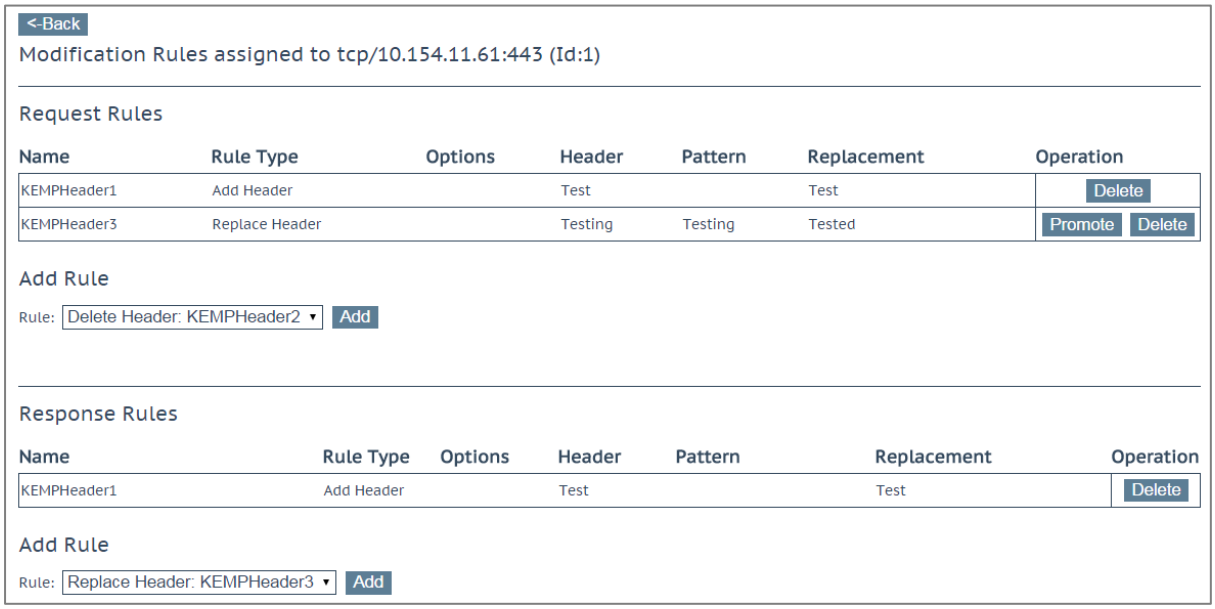
この画面は、バーチャルサービス内のリアルサーバに割り当たコンテンツスイッチ用ルールをルールの適用順に表示します。ルールの優先順位を上げるには、ルールは[Promote] ボタンで優先順位を変更できます。

HTTP Selection Rules（HTTP 選択ルール）

バーチャルサービスに割り当てられた選択ルールを表示します。

HTTP Header Modifications （HTTP ヘッダの変更）

[Show Header Rules] をクリックすると、ヘッダ変更ルールを実装順に表示します。ルール数（リクエストタイプとレスポンスタイプのルール数）は実際のボタンに表示します。

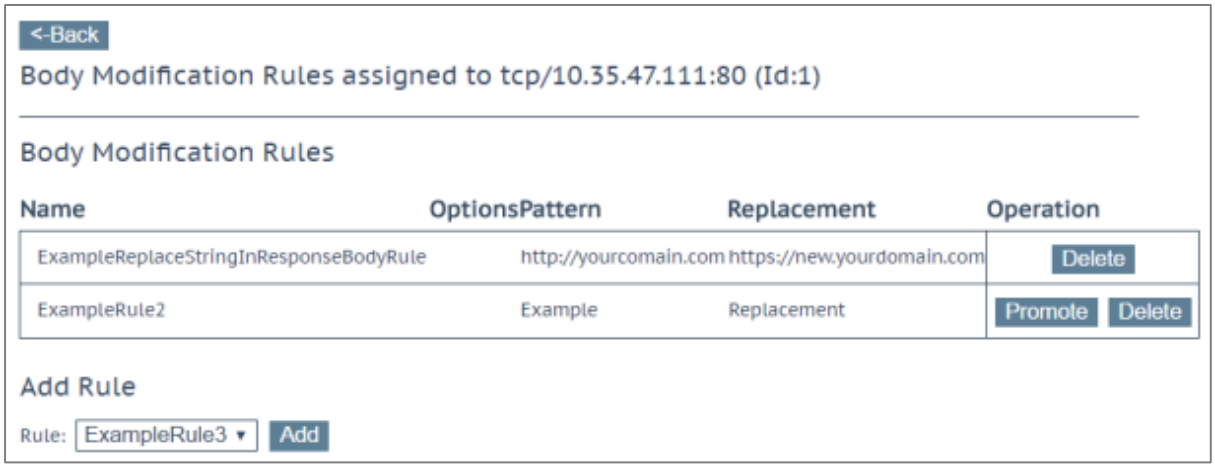


この画面でヘッダ変更ルールの追加/削除ができます。ルールの適用順序を変更するには、[Promote] ボタンをクリックします。

Response body rules are not compatible with Kerberos Constrained Delegation (KCD). If KCD is enabled on a Virtual Service, it is not possible to assign a body rule to it.

Response Body Modification（レスポンスボディ変更）

[Show Body Modification] ボタンをクリックすると、バーチャルサービスに割り当てられたレスポンスボディ変更ルールを表示します。ボタンのラベルに割り当てられたルール数を表示します。



この画面から、レスポンスボディ変更ルールをバーチャルサービスに追加／削除できます。[Promote] ボタンをクリックすると、ルールの適用順を変更できます。

Enable HTTP/2 Stack（HTTP/2 スタックの有効化）

LoadMaster は HTTP/2 のクライアント要求を直接処理します。HTTP/2 のリクエストはセキュアな接続で行われます。このオプションを有効にするには、SSL プロパティが設定され、最適な Cipher Set を選択していることを確認してください。エンドユーザエクスペリエンスを最適化するには、[Enable Caching] チェックボックスを選択してください。

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、リアルサーバの処理に伴う負荷と帯域幅を節約できます。

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（最大キャッシュ使用量）

このオプションはバーチャル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。たとえば、それぞれが 50%の制限で稼働する 2 つのサービスサービスでは、キャッシュストアの 100%を使用します。デフォルトは[No Limit] です。キャッシュストアを均一に使用するために、キャッシュサイズを制限することをお薦めします。それぞれのバーチャルサービスで設定できるキャッシュの使用率により、最大キャッシュ使用量の確認と調整ができます。キャッシュが有効なバーチャルサービスに割り当てられるキャッシュ スペースが残っていない場合、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）

LoadMaster が送るファイルは Gzip で圧縮します。

キャッシュなしで圧縮を有効にすると、LoadMaster のパフォーマンスが低下する可能性があります。
バーチャルサービスで圧縮とキャッシングが共に有効な場合、キャッシュされたコンテンツのみ圧縮を適用します（コンテンツがキャッシュされる場合）。最初の要求は圧縮しません。キャッシュにのみ使用します。システムはキャッシュと圧縮のいずれかのみを実行します。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、LoadMaster の WUI の >Systems Configuration >Miscellaneous 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 LoadMaster により多くの RAM を追加する必要があります。

Detect Malicious Requests（悪意のあるリクエストを検出 IDS 機能）

IPS（イントリュージョン プレベンション システム）サービスは、リアルタイムに攻撃を緩和とリアルサーバの分離を行うことで、リアルサーバのインライン保護を提供します。侵入防止は、業界標準の SNORT データベースに基づいており、侵入の警告をリアルタイムで提供します。

> ルールの更新やカスタマイズを行うには、SNORT の Web サイトを参照してください。
>
> 検出コードは HTTP クラスのルールのみを処理します。

[Detect Malicious Requests] チェックボックスをオンにすると、HTTP と HTTPS（オフロード）のバーチャルサービスごとに IPS が有効になります。SNORT ルールに一致したリクエストの処理には、2 つのオプションがあります。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。[Drop Connection] はルールが一致するとレスポンスを行いません。[Send Reject] はルール一致でクライアントへ HTTP の「400 Invalid Request」で応答します。どちらのオプションを選択してもリクエストをリアルサーバに配信しません。

Enable Multiple Connect（複数接続を有効）

このオプションを有効にすると、LoadMaster とリアルサーバとの間の接続処理を LoadMaster 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（ポートフォローイング）

ポートフォローイングは、HTTP から HTTPS（SSL）へ接続へスイッチする時に、同じリアルサーバにセッション維持を提供します。ポートフォローイングは、UDP と TCP 間の接続でも可能です。

ポートフォローイ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。

- ポートフォローイングを有効にするバーチャルサービスは、HTTPS サービスです
- HTTP サービスが存在しなければなりません
- バーチャルサービスは、いずれも L7 の[Super HTTP] か[Source IP Address] パーシステンスモードが選択しなければなりません

> SubVS 上ではポートフォローウィングは利用できません。

詳細情報は KEMP ドキュメントページの「Port Following」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を追加）

リアルサーバに送信されるすべてのリクエストに挿入するヘッダフィールド名とのキーの値を入力します。この機能の設定は[Set Header] ボタンをクリックします。

Copy Header in Request（リクエストにヘッダをコピー）

リアルサーバにリクエストを送信する前に、ソースヘッダ フィールド名を新しいヘッダフィールドにコピーいます。コピーするソースヘッダのフィールド名を[To Header] テキストボックスに入力します。

Add HTTP Headers（HTTP ヘッダの追加）

このオプションを使用すると、HTTP ストリームに追加するヘッダを選択できます。以下のオプションの利用が可能です。

- Legacy Operation(X)
- None（なし）
- X-Forwarded-For（+ Via）または X-Forwarded-For（No Via）
- X-ClientSide（+ Via）または X-ClientSide（No Via）
- Via Only（Via のみ）

レガシーオプションでは、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が追加されます。それ以外では何も行いません。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、指定した動作を実行します。

Sorry Server（Sorry サーバ）

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。LoadMaster は、利用可能なリアルサーバがない場合、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 サーバの IP アドレスは、LoadMaster 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 バーチャルサービスの場合、Sorry サーバはリアルサーバ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 バーチャルサービスを使用する場合、Sorry サーバ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 で設定できます。

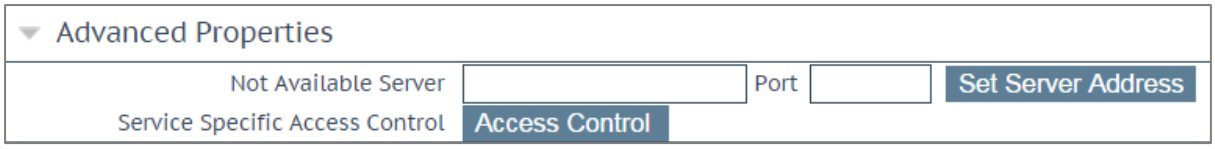
SSL 再暗号化を使用している場合、Sorry サーバ機能は正しく動作しません。

Not Available Redirection Handling（利用不可でのリダイレクション）

リクエストに対応するリアルサーバ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 :** リアルサーバが利用できない場合、LoadMaster は定義したエラーコードを伴ってリクエストを終結します。エラーコードは選択した値を設定します。
- **Redirect URL :** リアルサーバが利用できず、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。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 URI（ユニフォームリソースアイデンティファイヤ）を表す「%s」などのワイルドカードも使用できます。
- **Error Message :** リアルサーバが利用できないときのエラーレスポンスを返すとき、指定したエラーメッセージをレスポンスに追加します。セキュリティ上の理由から、「Document has moved」の文字だけを含む HTML ページを返送し、リクエストに含まれる情報は返送しません。
- **Error File :** リアルサーバが利用できないときの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 ページを返送できます。エラーページの最大サイズは 16KB です。

Not Available Server/Port（利用不可でのサーバとポート）



UDP のバーチャルサービスでは、利用不可時のサーバとポートを指定できます。このオプションは、リクエストを応答ができるリアルサーバ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 VS の追加）

ポート 80 バーチャル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 にクライアントをリダイレクトします。

このリダイレクタを使用するには、[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 バーチャルサービスを作成し、関連するバーチャルサービスから WUI オプションを表示しなくなります。

Default Gateway（デフォルトゲートウェイ）

レスポンスをクライアントに返すために使用されるバーチャルサービス固有のゲートウェイを指定します。設定がない場合、グローバル デフォルトゲートウェイを使用します。

[Set Default Gateway] ボタンをクリックすると、デフォルトゲートウェイを実装します。バーチャルサービスのデフォルト ゲートウェイは、設定したバーチャルサービスのみが使用します。

>System Configuration >Miscellaneous Options >Network Options でグローバルの[Use Default Route Only] （デフォルトルートのみ使用）オプションを設定している場合、[Default Gateway]を設定しているバーチャルサービスのトラフィックは、デフォルトルートを設定しているインターフェイスに転送します。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、LoadMaster 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）

アドレスリストの指定がない場合、LoadMaster はバーチャルサービスの 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、LoadMaster 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。

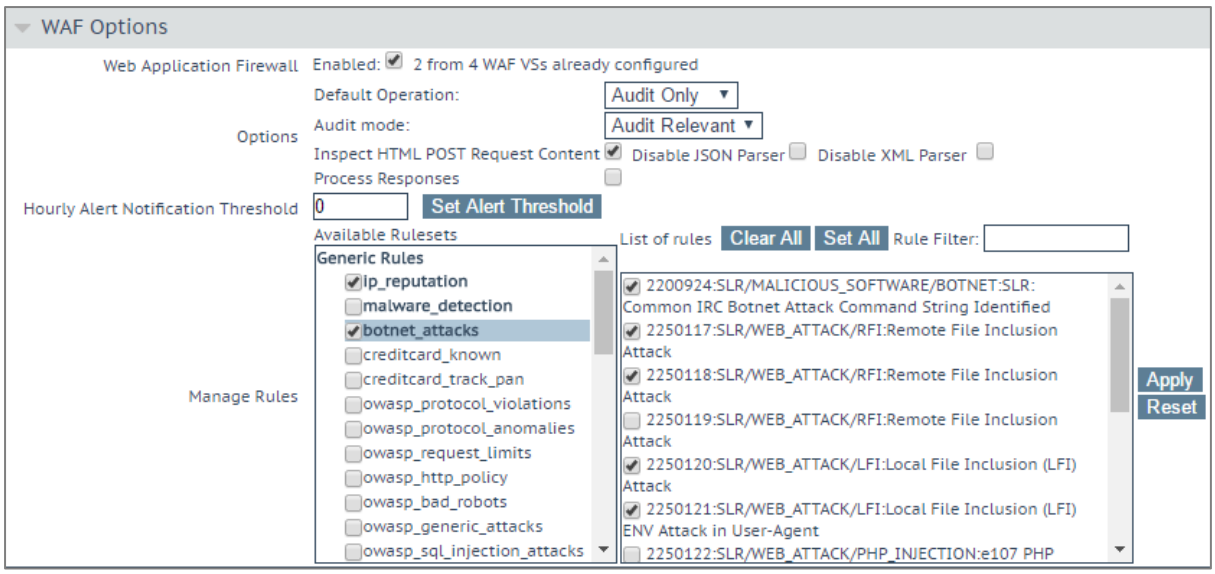
このオプションは、「L7 コンフィグレーション」画面の[Allow connection scaling over 64K Connections]オプションが有効になっている場合のみ利用可能です。

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

バーチャルサービス固有の ACL（アクセス コントロール リスト）を変更できます。

[Access Control Lists] オプションが有効な場合、[Extra Ports] オプションは正しく機能しません。

3.7 Web アプリケーション ファイアウォール（WAF）



こ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。

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 が有効なバーチャルサービスがいくつ存在するかと、WAF が有効なバーチャル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 が有効なバーチャル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、LoadMaster 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 LoadMaster 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 LoadMaster の OS では、仮想およびベアメタル型の LoadMaster 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 オペレーション）

WAF のデフォルトオペレーションを選択します。

- **Audit Only :** 監査専用モードです。ログを作成しますが、リクエストや応答をブロックしません。

- **Block Mode :** リクエストや応答をブロックします。

Audit mode（オーディット モード）

どのログを記録するかを選択します。

- **No Audit :** データを記録しません
- **Audit Relevant :** 警告レベル以上のデータを記録します。この設定はデフォルトオプションです。
- **Audit All :** バーチャルサービスを通過する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。通常運用で[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 リクエストの検査）

このオプションを有効にすると、POST リスエストの内容も検査します。

3 つの追加オプション（[Enable JSON Parser] 、[Enable XML Parser] 、[Enable Other Content Types] ）は、[Inspect HTML Post Request Content] が有効な場合のみ利用できます。

Enable JSON Parser（JSON パーサの有効）

JASON（Java スクリプトオブジェクト表記法）リクエストの検査を有効にします。

Enable XML Parser（XML パーサの有効）

XML リクエストの検査を有効にします。

Enable Other Content Types（その他のコンテンツタイプの有効）

XML と JSON 以外の POST コンテンツタイプの検証を有効にします。

その他のコンテンツタイプの検査を有効にすると、システムリソース（CPU とメモリ）の使用率が増加する可能性があります。特定のコンテンツタイプ リストは考慮する必要があります。

このオプションを有効にすると、WAF 解析のための POST コンテンツタイプをカンマ区切りで入力できるテキストボックスが用意されます。デフォルトでは、XML/JSON を除くすべてのタイプが有効です。

Process Responses（レスポンスの検査）

このオプションを有効にすると、リアルサーバからの応答を検証します。

このオプションは CPU とメモリを著しく消費します。
リアルサーバが 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 時間周期のアラート閾値）

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閾値です。0 を設定するとアラートが無効になります。この閾値は、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、閾値を 10 に設定し、20 個のイベントが発生した場合、このカウンタは 2 になります。

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、バーチャルサービスに割り当てる（またはバーチャル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バーチャル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。バーチャル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を維持します。

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。LoadMaster 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。

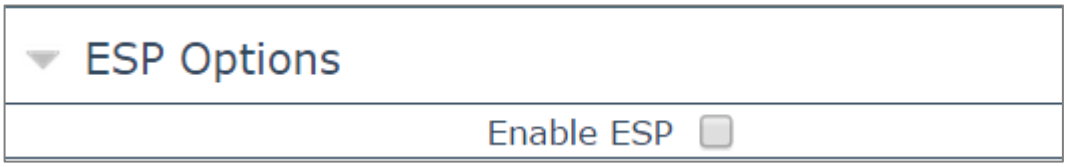
[Set All] ボタンをクリックすると、選択したすべてのルールが有効になります。

[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。

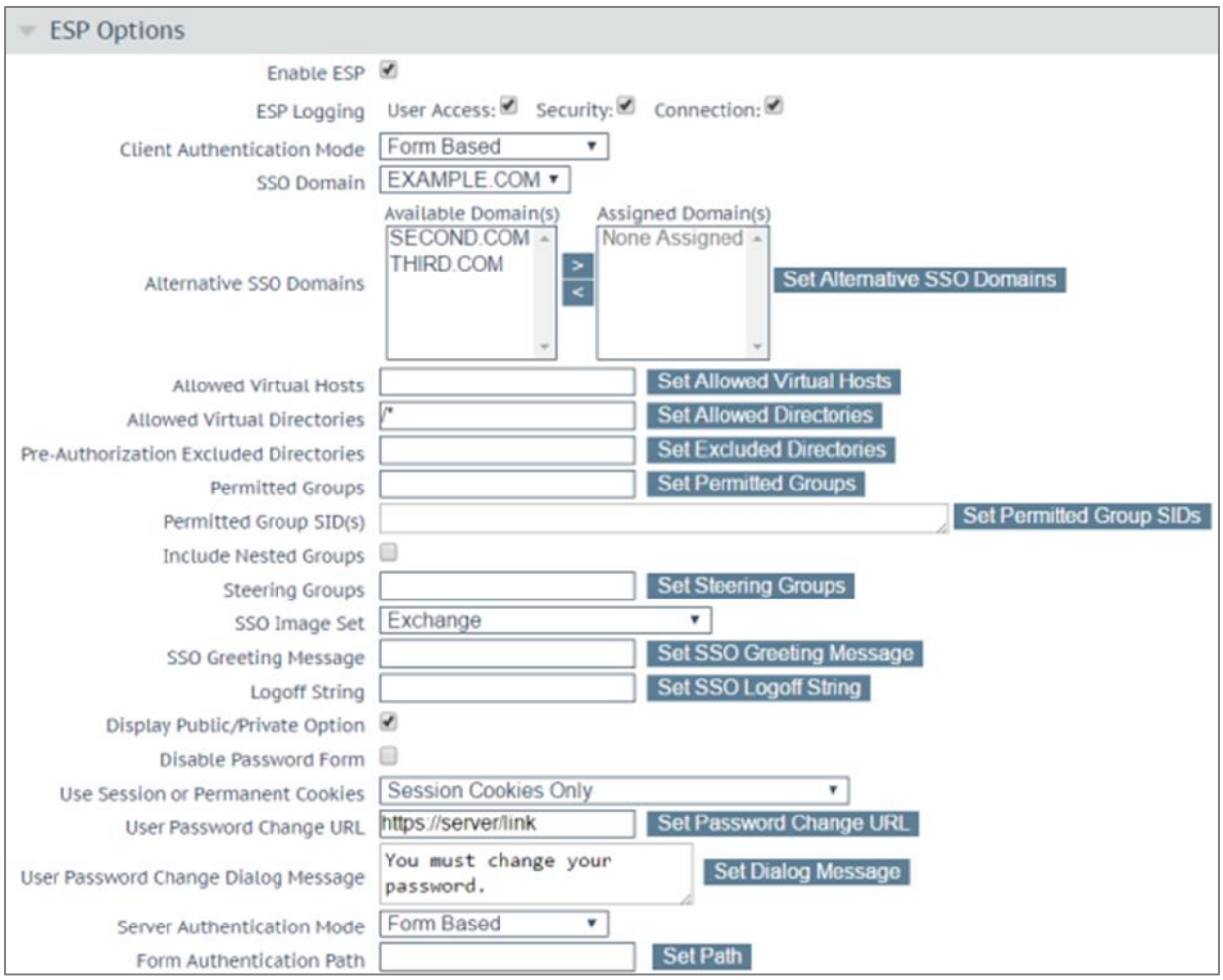
3.8 エッジセキュリティパック（ESP）のオプション

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。



この後[ESP Options] 画面で ESP のすべてのオプションを表示します。

ESP 機能は、バーチャルサービスが HTTP、HTTPS、SMTP でのみ有効にできます。



Enable ESP（ESP の有効）

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）

ESP 機能では 3 種類のログを記録します。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。以下のログを記録します。

- **User Access :** 全ユーザのログイン情報を記録
- **Security :** すべてのセキュリティ警告を記録
- **Connection :** それぞれの接続状態を記録

ログは永久保存が可能で、LoadMaster 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、「拡張ログファイル」セクションを参照してください。

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

LoadMaster に接続を試みるクライアントの認証方法を指定します。以下に示す方法が利用可能です。

- **Delegate to Server :** 認証をサーバに委任する
- **Basic Authentication :** 標準の基本認証を使用する
- **フォームベース :** LoadMaster が認証するためのユーザ情報を入力フォームを使用する
- **Client Certificates :** 発行機関で証明されたクライアント証明書で認証する
- **NTLM :** ドメイン名とユーザ名を含む NTLM 証明書で対話形式のログオン処理を行う
- **SAML :** LoadMaster は SAML サービスプロバイダのロールをサポートします。サービスプロバイダは、安全なゲートアクセスを提供します。

[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）

バーチャル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の詳細情報は「SSO ドメイン管理」セクション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。

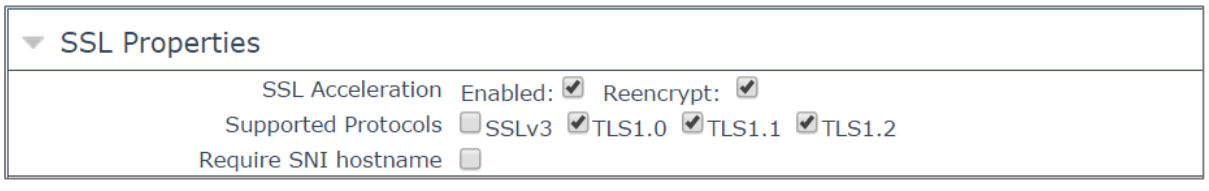
[Configuration type] で[Inbound Configuration] が設定された SSO ドメインのみ、この[SSO Domain] フィールドにオプションとして表示します。

Alternative SSO Domains（代替 SSO ドメイン）

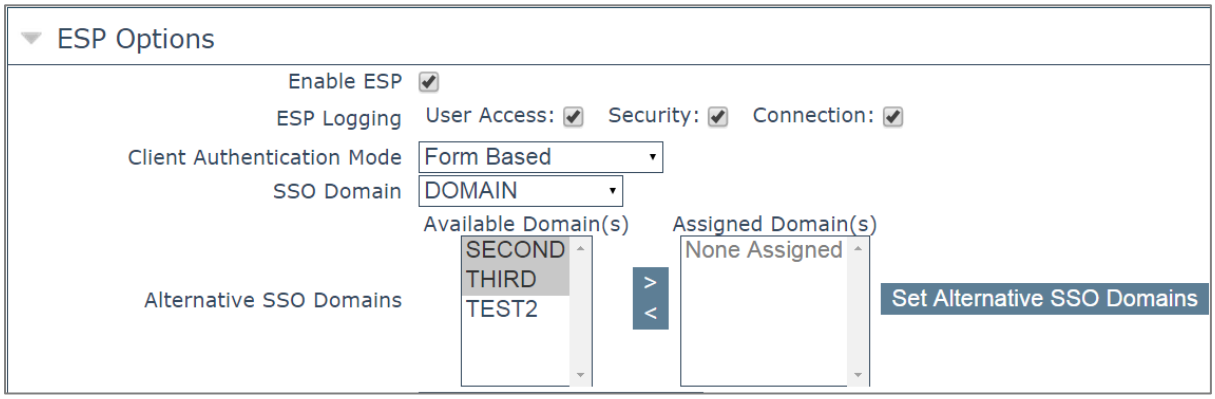
多くの組織では、顧客やパートナーと情報を共有するため、エクストラネットを使用しています。エクストラネットのポータルは、複数のアクティブディレクトリドメインからのユーザを持つ可能性があります。個々のドメインからのユーザを同時に認証するのではなく、[Alternative SSO Domains] （代替 SSO ドメイン）を割り当てることで、1 つのバーチャルサービスを使用して複数のドメイン ユーザを同時に認証できます。

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] に設定している場合のみ表示します。

SSO ドメインの設定方法についての詳細は「SSO ドメイン管理」セクションを参照してください。

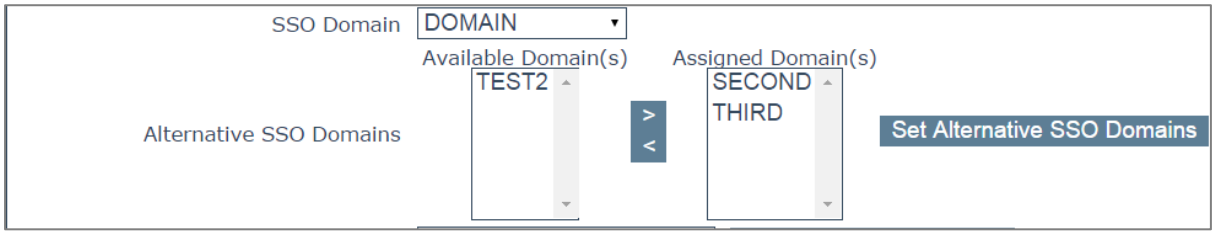


[Alternative SSO Domains] （代替 SSO ドメイン）を使用するため、「SSL プロパティ」セクションの[SSL Acceleration] の[Enabled] と[Reencrypt] のチェックボックスがオンになっていることを確認してください。



[SSO Domain] のドロップダウンにあ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するドメインです。

以前に設定したドメインは[Available Domain(s)] にリスト表示します。



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、特定のバーチャル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、すべてバーチャルサービスに割り当てることができます。

2. [Set Alternative SSO Domains] 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] のドロップダウンから[Basic Authentication] 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。ユーザ名の欄にドメイン名を入力しない場合、通常、[Default SSO Domain] のドロップダウンで選択したドメインにログオンします。

バーチャルサービスの状態を見るには、メインメニューから >Virtual Services >View/Modify Services を表示します。

[Virtual Services] リストは、各サービスの現在の状態を表示します。

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を[Status] カラムに表示します。

Allowed Virtual Hosts（許可されたバーチャルホスト）

バーチャルサービスは、指定したバーチャルホストのみアクセスできます。指定のないバーチャルホストはブロックします。

アクセスを許可するバーチャルホストの指定は、[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。

このフィールドを空欄にすると、バーチャルサービスをブロックします。

ESP オプションで[Permitted Groups field] を使用する場合は、[Permitted groups] のディレクトリが SSO Domain に設定していることを確認してください。例えば、SSO Domain に webmail.example を設定し、webmail が example.com の Permitted groups ディレクトリにない場合、ドメインは機能しません。この場合、SSO Domain は example.com にする必要があります。

Allowed Virtual Directories（許可されたバーチャルディレクトリ）

バーチャルサービスは、アクセスを許可したバーチャルホスト内で指定したバーチャル ディレクトリのみアクセスできます。指定のないバーチャルディレクトリはブロックされます。

アクセスを許可するバーチャルディレクトリの指定は、[Allowed Virtual Directories] フィールドにバーチャル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（事前認証の対象外ディレクトリ）

このフィールドで指定したバーチャルディレクトリは、このバーチャルサービスで事前認証されず、関連するリアルサーバに直接渡されます。

Permitted Groups（許可グループ）

このバーチャル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、このバーチャルサービスにより発行されたユーザがログインするには、そのユーザ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 つのバーチャルサービスにつき 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、バーチャル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。LoadMaster 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、LoadMaster 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: IT Users）、スペースで区切られたリストは正しく機能しません。

- [Domain Users] グループは新しいユーザのデフォルトのプライマリグループですので使用しないでください。
- 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。
- グループは完全な名称ではなく、定義した名称を指定してください。

Permitted Group SID(s)（許可グループの SID）

このフィールドは[Permitted Groups] フィールドと同じです。許可グループを指定する場合は、[Permitted Groups] フィールドか[Permitted Group SID(s)] フィールドのいずれかを入力します。

[Permitted Group SID(s)] フィールドには、このバーチャルサービスにアクセスできるグループの SID を指定できます。各グループ名はセミコロンで区切ります。入力後に[Set Permitted Group SID(s)] をクリックしてください。

Include Nested Groups（ネスト 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のみアクセスを許可します。このオプションを有効にすると、最上位レベルと最初の下位レベルのグループに属するユーザのアクセスを許可します。

Steering Groups（ステアリング グループ）

ステアリング グループは、AD（アクティブ ディレクトリ）のグループメンバーシップ上のユーザが始動するクライアント トラフィックを、バーチャルサービスに設定した個々のリアルサーバへ誘導するために使用します。例えば、4 つのリアルサーバを定義するバーチャルサービスを想定した場合、2 つのリアルサーバは、AD グループ 1 にプライマリとして関連付けし、別の 2 つのリアルサーバは AD グループ 2 にプライマリとして関連付けを設定します。ユーザがバーチャルサービスへアクセスしたとき、定義したグループメンバーシップを検証し、その情報で適切なリアルサーバ

にリクエストを誘導します。グループメンバシップに基づいて選択されたリアルサーバが利用できない場合、デフォルト動作はバーチャルサービスで設定しているスケジューリング方法で代替します。

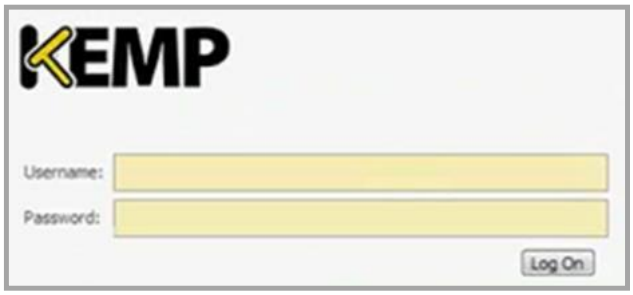
詳細な情報は、KEMP ドキュメント ページの ESP Steering Groups Technical Note を参照してください。

Steering groups are not available if using Basic Authentication or SAML authentication.

SSO Image Set（SSO の画像設定）

このオプションは、[Client Authentication Mode] のプルダウンで[Form Based] を選択し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。ここには、[Exchange] 、[Blank] 、[Dual Factor Authentication] の 3 つのオプションを用意しています。英語以外の表示オプションもあります。

- Exchange（エクスチェンジ フォーム）

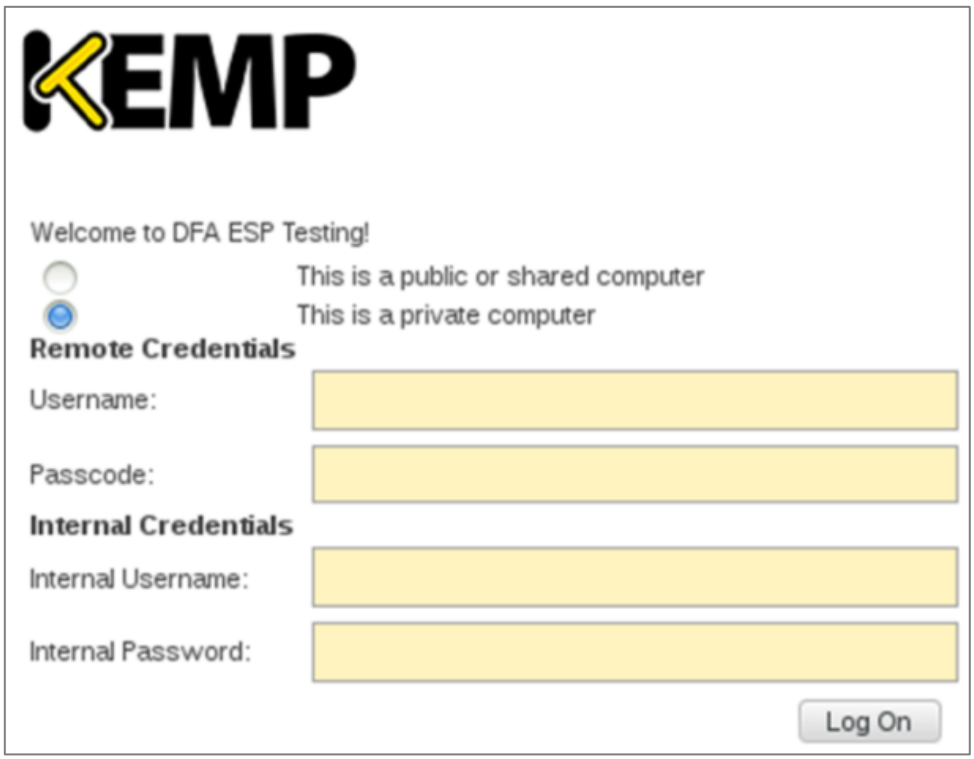


エクスチェンジフォームは KEMP のロゴを表示します。

- Blank（ブランク フォーム）

ブランク フォームは KEMP のロゴを表示しません。

- Dual Factor Authentication（2 要素認証）



2 要素認証フォームには、4 つのフィールドがあります。このうち 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で認証する前に、RADIUS などのリモート認証サーバ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で認証するための証明書です。

関連する[SSO Domain] の[Authentication Protocol]（認証プロトコル）が[RADIUS and LDAP] に設定いている場合、[SSO Image Set] を[Dual Factor Authentication] に設定する必要があります。

SSO Greeting Message（SSO グリーティングメッセージ）

このオプションは、[Client Authentication Mode] で[Form Based] を選択している場合に利用できます。ログインフォームにテキストを追加してカスタマイズができます。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。

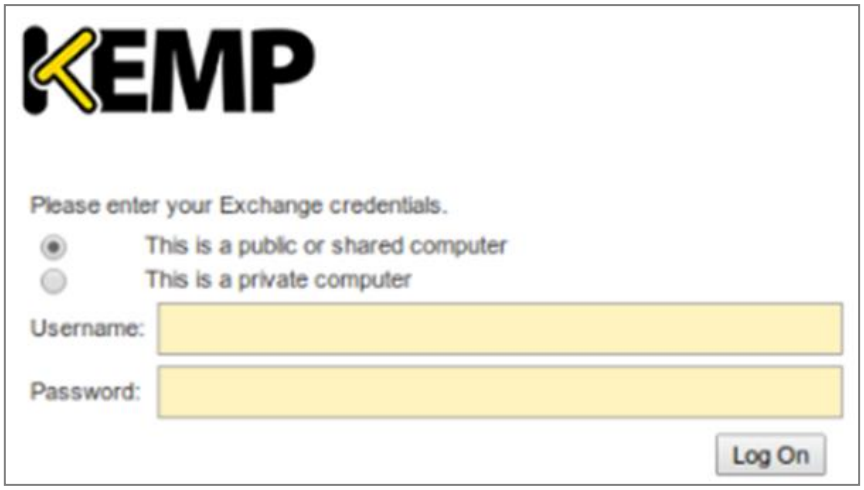
サポートしない文字があります。「`」（アクセント文字）と「'」（シングルクォート）はサポートしません。アクセント文字が SSO グリーティングメッセージに使用された場合、その文字は表示されません。たとえば、a`b`c は abc になります。シングルクォートを使うとユーザはログインできなくなります。

Logoff String（ログオフ ストリング）

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 バーチャルサービスの場合は、[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、スペースの区切りを使用します。

照合する 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 LoadMaster はユーザ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）



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を表示します。[Session timeout] の値は、ログインフォームでユーザが選択したオプションに基づいて、「SSO ドメインの管理」画面で指定する[public] /[private] で設定します。ユーザが[Private] を選択すると、そのセッションにユーザ名が保存されます。これらのフィールドの詳細については、「SSO ドメインの管理」セクション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、ログインページのパスワードフィールドを表示しません。このオプションは、RSA SecurID 認証を使用する場合など、パスワード検証が不要な場合に有効にします。デフォルトでは無効になっています。

Use Session or Permanent Cookies（セッション/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 :** 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 :** パブリックコンピュータにセッションクッキーを送信します。
- **Permanent Cookies Always :** 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。

パーマネントクッキーは IE（インターネット エクスプローラ）でのみ動作します。IE にはサードパーティークッキーの受入れと、信頼できるサイトの登録が必要です。

ログイン時にユーザのブラウザ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。

User Password Change URL（ユーザ パスワード変更 URL）

これは、フォームベースでの LDAP 認証の使用に関係します。ユーザがパスワードを変更するための URL を指定します。たとえば、

https://mail.kempqakcd.net/owa/auth/expiredpassword.aspx?url=/owa/auth.owa

ユーザのパスワードが期限切れになるか、パスワードをリセットする必要がある場合は、この URL とパスワード変更ダイアログメッセージをログインフォームに表示します。

この URL は必要に応じて、認証のために除外リストに入れなければなりません。

Exchange 2010 環境でこの期限切れのパスワード機能を使用する場合：

- 事前許可除外ディレクトリは、/owa/auth.owa / owa / auth * /owa/14.3.123.3**に設定する必要があります。14.3.123.3 は、除外されたディレクトリに追加する必要がある Exchange サーバのサブパスです。
- パスワードを変更する場合、Exchange 2010 SP1 RU3 以降がクライアントに展開されていない限り、ユーザは[パスワードの変更] ウィンドウの[ドメイン¥ユーザ名] フィールドにユーザプリンシパル名（UPN）（例：joebloggs@example.com）を使用できませんアクセスサーバ。

詳細については、次の Microsoft TechNet の記事を参照してください。

https://technet.microsoft.com/en-us/library/bb684904(v=exchg.141).aspx

User Password Change Dialog Message（ユーザパスワード変更ダイアログ メッセージ）

このテキストボックスは[User Password Change URL] テキストボックスに何かが設定されている場合にのみ表示されます。ユーザがパスワードをリセットする必要がある場合に、ログインフォームに表示されるテキストを指定します。特殊文字の入力はできません。

Server Authentication Mode（サーバ認証モード）

リアルサーバにより LoadMaster 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
- **Form Based :** [Client Authentication Mode] を[Form Based] に設定している場合、[Server Authentication Mode] は[Form Based] に設定できます。もし、[Form Based] を[Server Authentication Mode] に選択している場合、[Form Authentication Path] と呼ば

れる別のフィールドを表示します。[Form Authentication Path] フィールドに入力すると、[Form POST Format] フィールドを表示します。クライアント側のユーザ名/パスワードは、フォームベースの認証で POST フォーマットのフォームを POST ボディに注入します。
この機能は、主に Microsoft Exchange の展開で使用し、Exchange 2013 と 2016 でテストされています。このため、Exchange 2013 と 2016 では以下の文字列を明示的に構成する必要はありません。これらは実装時のデフォルトです。

- **Form Authentication Path :** /owa/auth.owa
- **Form POST Format :**
  destination=%s#authRedirect=true&flags=4&forcedownlevel=0&username=%s&password=%s&passwordText=&isUtf8=1

[Form POST Format] フィールドは[Form Authentication Path] をセットした時だけ表示します。

もし、Exchange でない場合、リアルサーバとの対話に基づく評価でその後適切な設定を行うことを推奨します。

[Client Authentication Mode] に [Delegate to Server] を選択した場合、[Server Authentication mode] は[None] を自動選択します。同様に、[Client Authentication Mode] に [Basic Authentication] を選択した場合、[Server Authentication mode] は [Basic Authentication] を自動選択します。

特定のクライアント認証プロトコルを選択する場合、サーバ認証プロトコルとの互換性を確認することが重要です。

Client Authentication Mode	Default Compatible Server Authentication Mode
Delegate to Server	None
Basic Authentication	Basic Authentication
Form Based	Basic Authentication
	KCD
	Form Based
	None
NTLM	KCD
	None
Client Certificate	KCD
SAML	KCD
	None

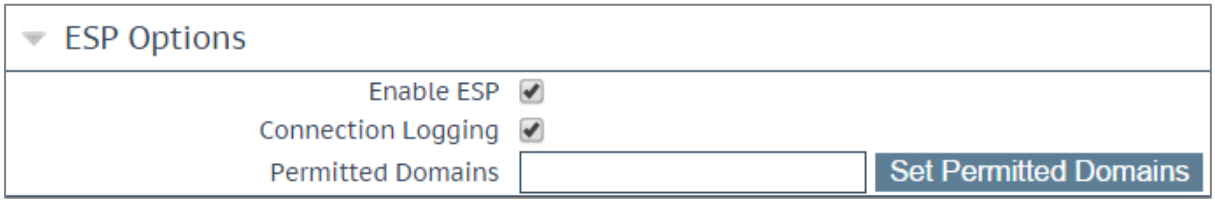
Server Side configuration（サーバ側設定）

このオプションは[Server Authentication mode] の値が[KCD] に設定しているときのみ表示します。

サーバ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 のバーチャルサービスと ESP

SMTP バーチャルサービス（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）。



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。

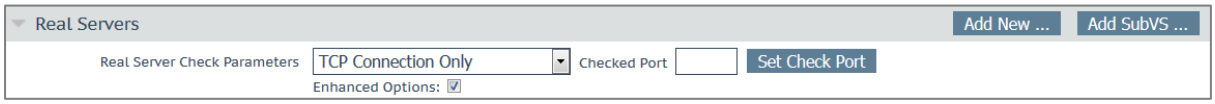
Permitted Domains（許可ドメイン）

このバーチャル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、バーチャルサービスにて 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。

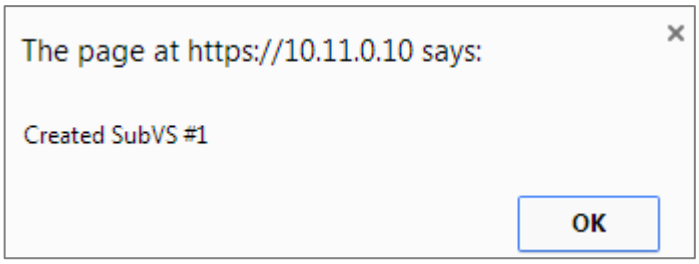
3.9 SubVS サービス

バーチャルサービス内には SubVS を作成できます。SubVS は設定済みのバーチャルサービスからリンクするバーチャルサービスで、上位のバーチャルサービスの IP アドレスを使用します。SubVS には、上位のバーチャルサービスや別の SubVS 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）ができます。これにより、関連性のあるバーチャルサービスを、同じ IP アドレスでグループ化することが可能になります。これは、Exchange や Lync のように、多くのバーチャルサービスで構成するサービスに有効です。

バーチャルサービスの権限を持つユーザは、SubVS を追加できます。
リアルサーバの権限を持つユーザは、SubVS を追加できません。

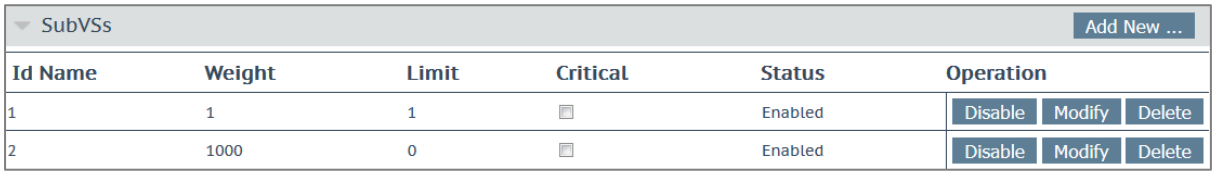


SubVS を作成するには、>Virtual Services >View/Modifiy Services >[Real Servers] セクションを展開し、[Add SubVS] ボタンをクリックします。



この後に、SubVS が作成されたことを示すメッセージが表れます。

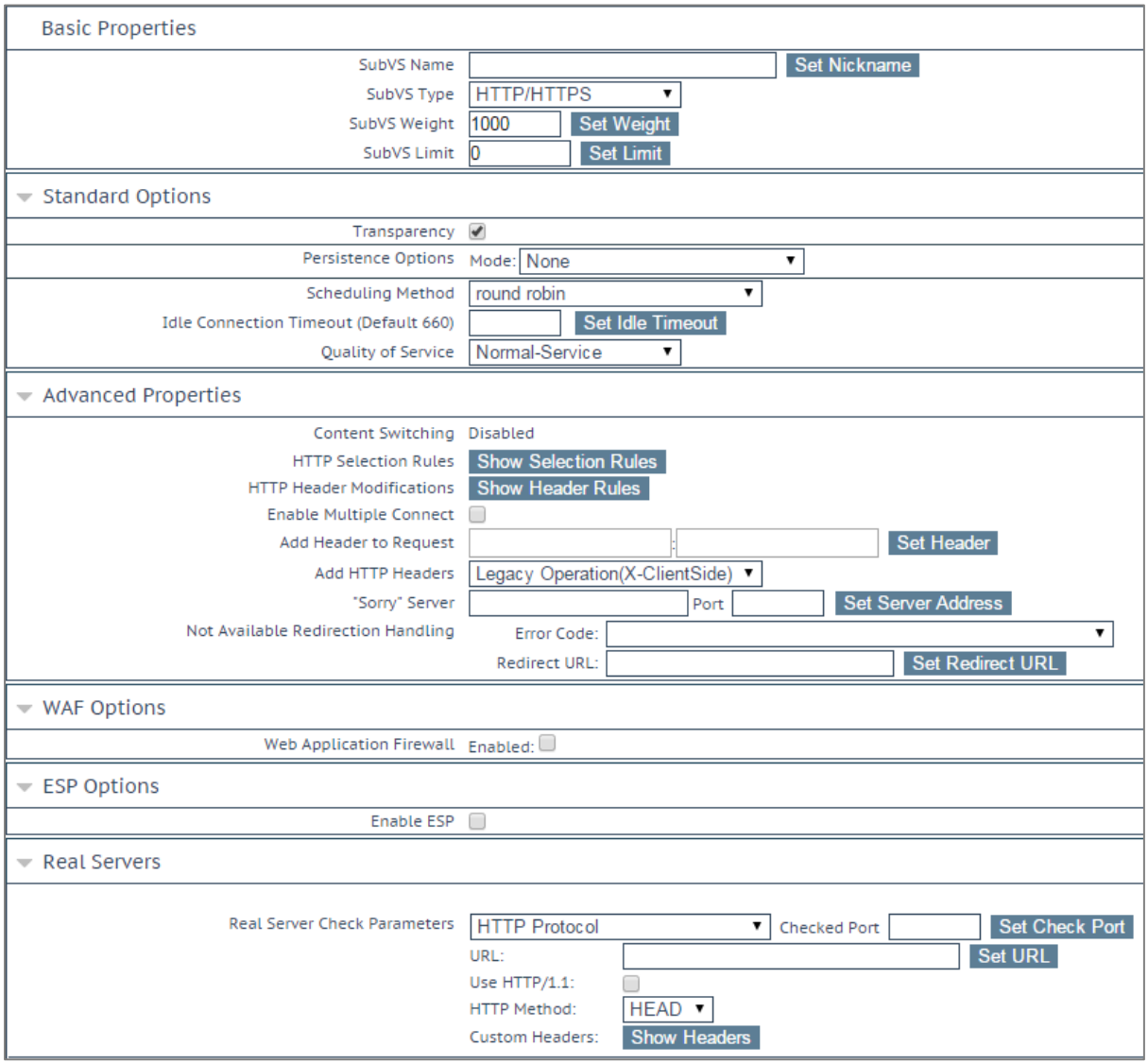
リアルサーバと SubVS を同じバーチャルサービスに関連付けることはできません。ただし、リアルサーバを SubVS に関連付けることは可能です。



SubVS を作成すると、バーチャル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。

ここにはバーチャルサービスの下のすべての SubVS を表示します。[Critical] チェックボックスをオンにすると、バーチャルサービスを利用可能にするために SubVS が必要なことを示します。重要でない SubVS が停止しても、バーチャルサービスが稼働中と判断しワーニング メッセージだけログします。[Critical] をチェックした SubVS が停止した場合、クリティカル メッセージをログし、バーチャルサービスは停止状態になります。[Email Options] を設定している場合、関係する受信者にメールを送信します。[Email Options] の詳細については、「メールオプション」セクションを参照してください。バーチャルサービスが停止中と認識すると、そのバーチャルサービスに Sorry サーバかエラーメッセージが設定されている場合、その応答を行います。

SubVS の設定を変更するには、該当する SubVS の[Modify] ボタンをクリックすると、SubVS の設定画面を表示します。この画面には、通常のバーチャルサービスで利用可能な設定オプションの一部を表示します。



また SubVS は通常のバーチャルサービス表示で、該当する SubVS の[Modify] ボタンをクリックしても変更できます。SubVS を持つバーチャルサービスは、仮想 IP アドレスセクションで異なる色で表示され、その SubVS がリアルサーバセクションにリスト表示されます。SubVS の詳細情報を見るには、上位のバーチャルサービスを展開すると SubVS 情報が表れます。

SubVS を含むバーチャル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 SubVS を削除する必要があります。

SubVS の ESP オプションは、上位のバーチャルサービスとは異なる設定にできますが、上位のバーチャルサービスと SubVS 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 リモートターミナル サービスの表示と変更

このセクションは、LoadMaster の Exchange とは関係ありません。

[Generic Type] といったバーチャル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、LoadMaster はセッション ディレクトリから提供された「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。LoadMaster のパーシステンス 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、LoadMaster 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 LoadMaster 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、LoadMaster は名前を照会し、最初の接続時と同じサーバに再接続します。LoadMaster が情報の保持時間を制限するために、パーシステンスタイムアウトを使用します。

[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スで使用します。

バーチャルサービスのサービスチェック

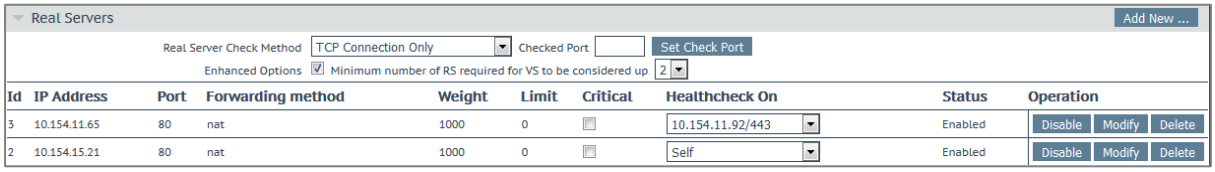
[ICMP] 、[TCP] 、[RDP] の 3 つのオプションのみ利用できます。リモート端末プロトコル（RDP）は、リアルサーバのサービスポート（ポート 3389）に対して TCP 接続を開きます。LoadMaster は、サーバにコード 1110（接続要求）を送信します。サーバからコード 1110（接続確認）が送信されると、LoadMaster は、接続を閉じてそのサーバがアクティブであるとしてマーキングします。設定された回数だけ接続を要求しても、設定された応答時間内にサーバから応答が返されなかった場合、または、他のステータスコードが返された場合、そのサーバは動作していないとみなします。

3.11 リアルサーバ

このセクションは、バーチャルサービスにアサインされているリアルサーバ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リアルサーバ属性の要約を表示し、リアルサーバの追加、削除、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、各リアルサーバへのルールの追加、削除もこのセクションで行えます。

Real Server Check Method（リアルサーバチェック方法）

このパラメータで、リアルサーバ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、リアルサーバ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。



以下の表では、リアルサーバ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。リアルサーバ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、リアルサーバ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]、[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	ICMP Ping をリアルサーバへ送信します
HTTP	HTTP GET／HEAD リクエストを送信します
HTTPS	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	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
DNS	ネームサービスプロトコルを使用します
Binary Data	送信文字列と応答内容を 16 進数で指定します
LDAP	ヘルスチェックに使用する LDAP エンドポイントを選択します。ヘルスチェックプロトコルとして LDAP を選択している場合は、リアルサーバの IP アドレスとポートの代わりに、サーバの IP アドレス（1 つまたは複数のアドレス）と LDAP エンドポイント設定のポートが使用されます。LDAP エンドポイントの詳細については、「LDAP 設定」セクションを参照してください。
None	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:	ICMP Ping をリアルサーバへ送信します
TCP	TCP 接続を試みます
RDP	リアルサーバに 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	ヘルスチェックを行いません

UDP バーチャルサービスの場合、ICMP Ping と DNS（ネームサービス プロトコル）が利用できます。

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）、いずれかのリアルサーバが利用可能であれば、そのバーチャル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、バーチャル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リアルサーバ数を指定することができます。

Minimum number of RS required for VS to be considered up（VS が稼働状態を認識する最低 RS 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、複数のリアルサーバが存在する場合に表示されます。

バーチャル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リアルサーバ数を選択してください。

利用可能なリアルサーバ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。一部のリアルサーバ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。メールオプションが設定されている場合、関係する受信者にメールを送信します。メールオプションの詳細については、「メールオプション」セクション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リアルサーバが利用可能な場合であっても、"Critical"とマークされたリアルサーバが利用不可能になると、そのバーチャル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、バーチャルサービスが停止中であり、そのバーチャルサービスが Sorry サーバを設定しているかエラーメッセージを設定している場合に応答します。

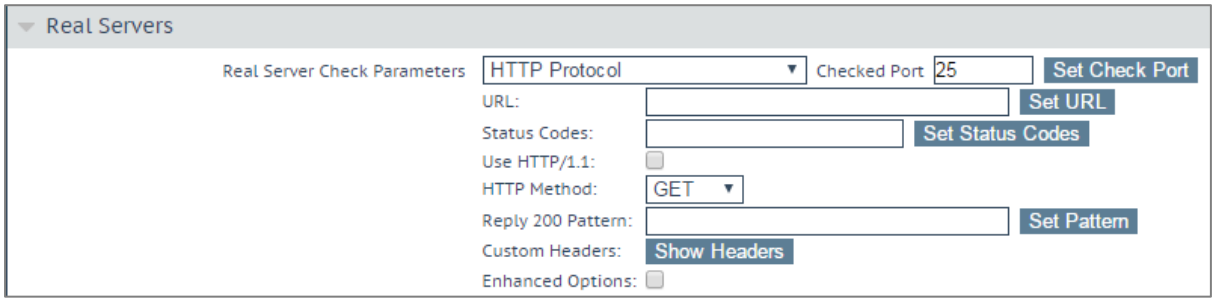
最小数としてトータルのリアルサーバ数を設定しているとき、リアルサーバを 1 つ削除すると、この最小数は自動的に 1 つ減ります。

SubVS でコンテキストルールを使用する場合、必要なリアルサーバの最小数が持つ意味が異なります。ルールが割り当てられている利用可能なリアルサーバ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。利用可能なリアルサーバ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 SubVS は停止中とマークされ、その旨をログに記録します。

SubVS 上のリアルサーバが重要であるとマークした場合、そのリアルサーバが停止すると、その SubVS は停止状態になります。ただし、SubVS が重要であるとマークしていない限り、上位のバーチャルサービスは停止状態になりません。

3.11.1 HTTP または HTTPS 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。



[HTTP Method] で[POST] を選択すると、[post data] オプションを表示します。
[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します。

- 200-299
- 301
- 302
- 401

また、2xx 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を行い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します。

カスタムのヘルスチェックコードを設定している場合、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で設定します。

- チェックコードは、最大 127 文字（32 個の有効なコード）で構成します。
- 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します。
- 設定されたコードにより、デフォルトの設定が上書きします。

  – 2xx 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、LoadMaster 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、リアルサーバ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バーチャルサービスの 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、該当するバーチャルサービスの[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を指定してください。この設定を行わない場合、リアルサーバの 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。

LoadMaster は、サーバ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、LoadMaster 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 PCRE（Perl Compatible Regular Expression）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、KEMP ドキュメントページの「Content Rules, Feature Description」ドキュメントを参照してください。

Custom Headers（カスタムヘッダ）

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/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/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] 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。リアルサーバ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. ユーザ名とパスワードは、「ユーザ名: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（例：「Basic 」）を追加します。

例えば、ユーザエージェントが、ユーザ名に「Aladdin」を使用し、パスワードに「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。

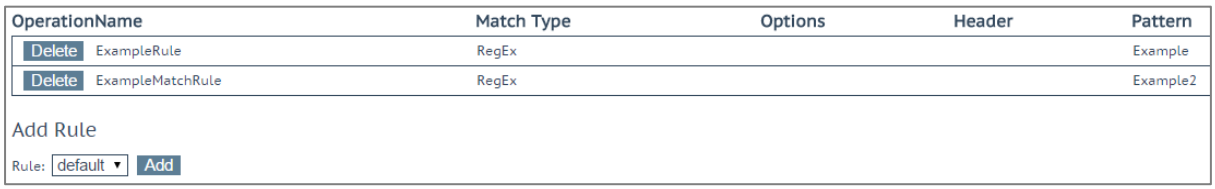
Authorization:Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

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

Rules（ルール）

リアルサーバ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、リアルサーバセクションに[Rules] 列が表示されます。[Rules] 列には、リアルサーバ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。

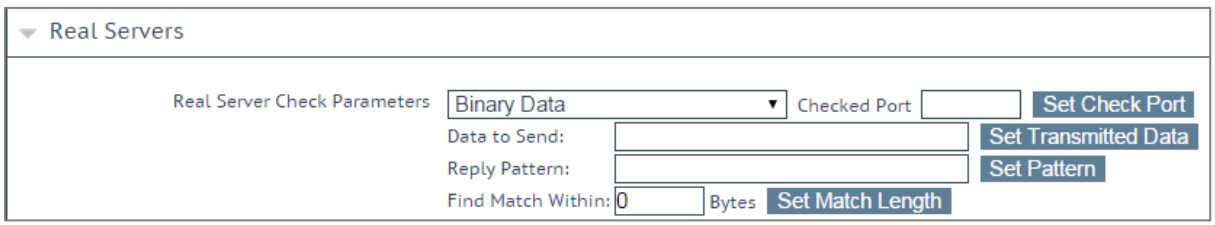
[Rules] 列のボタンをクリックすると、[Rules Management] 画面が表示されます。



この画面では、リアルサーバ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。



Data to Send（送信データ）

リアルサーバに送信する 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）

リアルサーバ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、LoadMaster はそのリアルサーバ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、リアルサーバ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）

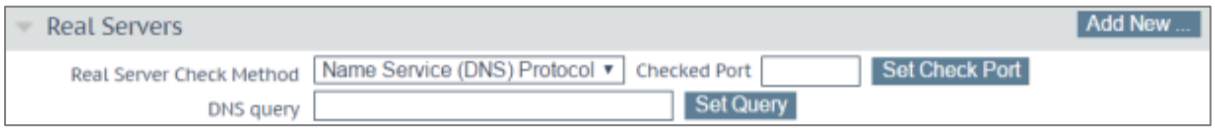
応答が返されると、LoadMaster は、[Reply Pattern] で指定された文字列をその応答内で検索します。LoadMaster は、このフィールドで指定されたバイト数まで検索します。

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リアルサーバからデータを読み込みます。リアルサーバから最大 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 ネームサーバ（DNS）プロトコルのヘルスチェック

ネームサーバ（DNS）プロトコルのヘルスチェックは、UDP バーチャルサービスを使用している場合にのみ使用できます。



Checked Port（チェックするポート）

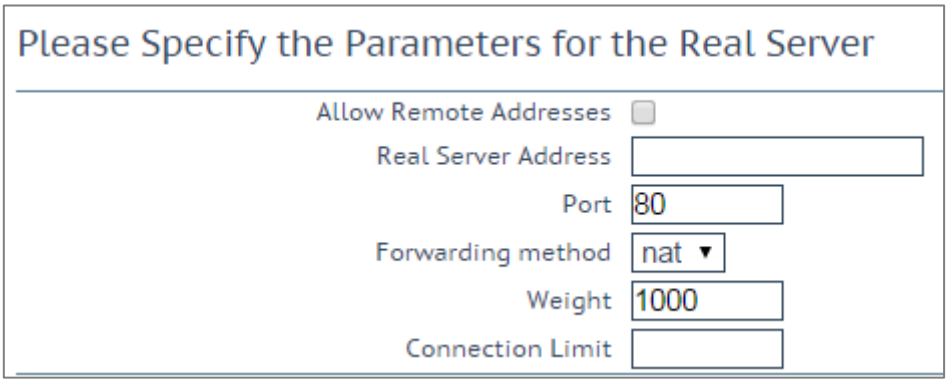
ポートの指定がない場合は、リアルサーバのポートを使用します。

DNS query（DNS クエリ）

ネームサーバから要求されるクエリ文字列を指定します。このフィールドの最大長は 126 文字です。

3.11.4 リアルサーバの追加

[Add New] ボタンをクリックすると、リアルサーバのプロパティを設定する次の画面を表示します。



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リアルサーバのみバーチャル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リアルサーバをバーチャル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、System Configuration >Miscellaneous Options >Network Options[Enable Non-Local Real Servers] を選択する必要があります。

代替ゲートウェイ/非ローカルのリアルサーバ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（リアルサーバ アドレス）

リアルサーバのアドレスには、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。リアルサーバの変更中に、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 the Host & DNS Configuration section を参照してください。リアルサーバ追加時に FQDN を使用する場合、FQDN 名はサーバ追加時に解決されます。名前の解決に失敗した場合、リアルサーバは作成されず、エラーが発生します。

Port（ポート）

リアルサーバ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）

NAT（Network Address Translation）とルート フォワーディングの両方で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）

リアルサーバの重み。これは重み付け負荷分散方式の[Weighted Round Robin）、[Weighted Least Connection]、[Adaptive] で使用します。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、リアルサーバ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 2 が、サーバ 1 と比較して 4 倍の CPU 性能とすると、サーバ 2 を 4000 とし、サーバ 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、リアルサーバ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バーチャル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。

リアルサーバは、最大 1024 台まで使用できます。これは全体の上限で、リアルサーバは既存のバーチャルサービスに分配されます。例えば、あるバーチャルサービスが 1000 台のリアルサーバを使用している場合、残りのバーチャルサービスは 24 台のリアルサーバしか使用できません。

LoadMaster Exchange では、設定できるリアルサーバに最大 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、そのリアルサーバ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、「リアルサーバ」セクションを参照してください。

バーチャルサービス編集画面のリアルサーバのセクションには、各リアルサーバの[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、バーチャルサービスが利用可能であると認識されるためにはこのリアルサーバが必要であることを意味します。このリアルサーバが機能しなくなる（または無効になる）と、この仮想サーバは停止中であるとマークされます。

SubVS 上のリアルサーバが重要であるとマークされている場合、そのリアルサーバが停止すると、その SubVS は停止中であるとマークされます。ただし、SubVS が重要であるとマークされていない限り、その親のバーチャル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 台のリアルサーバしか停止していなくても、そのリアルサーバが重要なサーバに設定されている場合、そのバーチャル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、バーチャルサービスが停止中であると認識され、そのバーチャルサービスが Sorry サーバを設定しているかエラーメッセージを設定している場合に応答します。

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「リアルサーバ」セクションを参照してください。

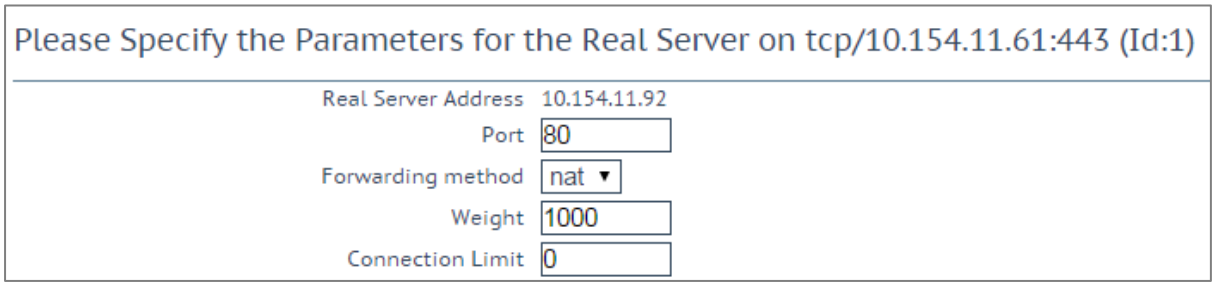
バーチャルサービス編集画面のリアルサーバのセクションには、各リアルサーバの[Healthcheck On] ドロップダウンリストが用意されています。このドロップダウンリストでは、どのリアルサーバに基づいてヘルスチェックを行うかを指定できます。このオプションを[Self] に設定してこのリアルサーバの状態に基づきヘルスチェックを行わせることも、他のリアルサーバを選択することもできます。例えば、リアルサーバ 1 が停止している場合、リアルサーバ 1 に基づきヘルスチェックを行っているリアルサーバは、それらのリアルサーバの状態にかかわらず、すべて停止中であるとマークされます。

以下に、いくつかの注意点を示します。

- リアルサーバはリアルサーバのみフォローできます。SubVS はフォローできません。
- リアルサーバは、第三のリアルサーバをフォローしているリアルサーバをフォローできます。最初の 2 つのリアルサーバの状態は、第三のリアルサーバの状態を反映します。
- リアルサーバ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。
- リアルサーバ（単体のリアルサーバまたはバーチャルサービスに含まれるリアルサーバ）が削除された場合、そのリアルサーバをフォローしているすべてのリアルサーバが通常動作にリセットされます（バーチャルサービスのヘルスチェックオプションが使用されます）。
- バーチャルサービスに含まれるすべてのリアルサーバが他のバーチャルサービスに含まれるリアルサーバをフォローしている場合、そのバーチャルサービスのヘルスチェックパラメータは WUI に表示しません（この設定はどのリアルサーバ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、そのバーチャルサービスをフォローしているすべてのリアルサーバのヘルスチェックが無効になります。

3.11.5 リアルサーバの設定変更

リアルサーバの[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。



Real Server Address（リアルサーバのアドレス）

このフィールドには、リアルサーバ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、リアルサーバ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、リアルサーバ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・リターンはレイヤ 4 でのみ使用できます。

Weight（重み）

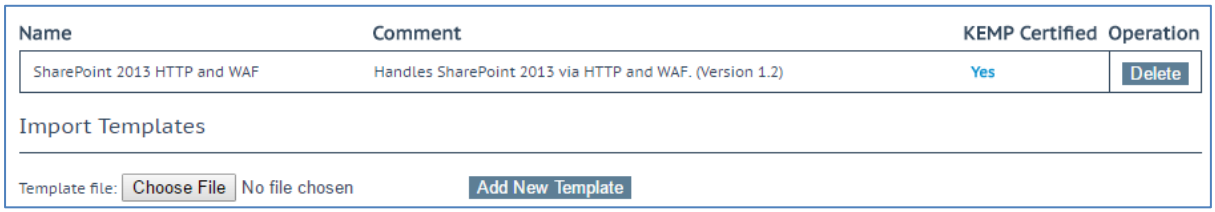
重み付けラウンドロビン方式を使用する場合、サーバに送信するトラフィックの相対比率は、リアルサーバの重みに基づき決定されます。高い値が設定されたサーバは、より多くのトラフィックを受信します。

Connection Limit（接続上限）

ローテーションから除外されるまでに、リアルサーバ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 テンプレートの管理

テンプレートを使用すると、バーチャルサービスのパラメータが自動的に作成/設定されるため、バーチャル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バーチャルサービスを設定するには、LoadMaster 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。



[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] をクリックします。

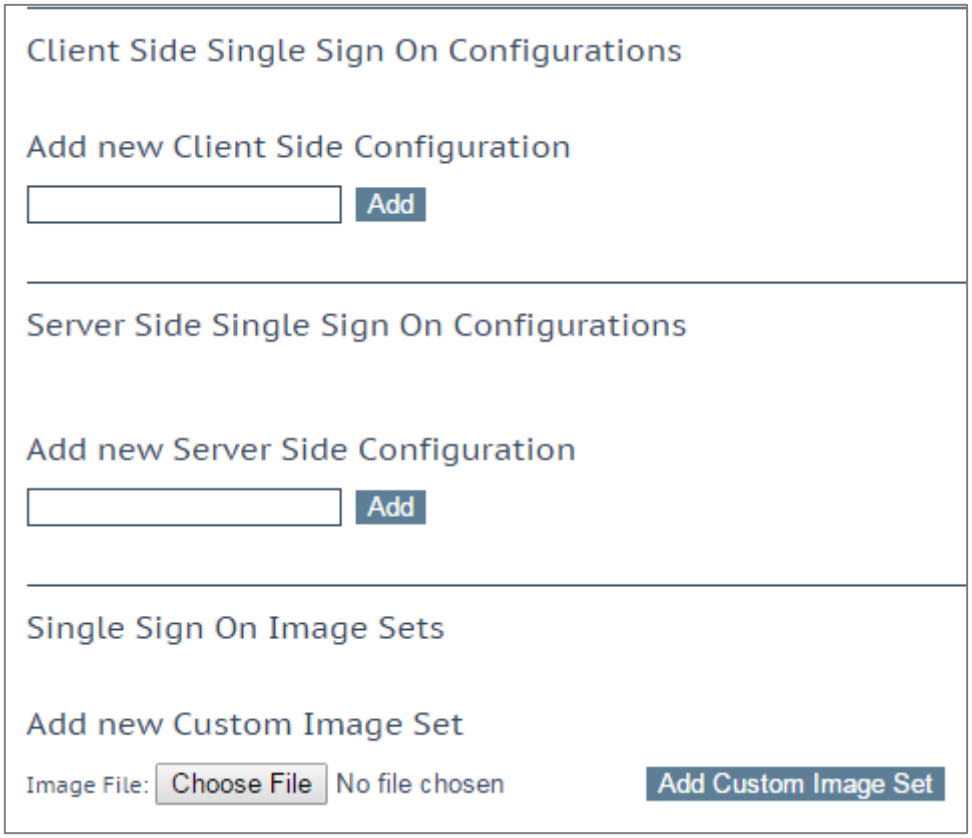
"KEMP Certified"列には、そのテンプレートが KEMP から提供されたかどうかが表示されます。テンプレートが認証されている場合、そのテンプレートは KEMP から提供されたものです。テンプレートが認証されていない場合、そのテンプレートはユーザにより作成された（バーチャルサービスからエクスポートされた）可能性があります。

テンプレートを使用してバーチャルサービスを作成、構成する方法、KEMP テンプレートを入手する場所など、テンプレートの詳細については、KEMP ドキュメントページの「Virtual Services and Templates Feature Description」を参照してください。

3.13 SSO ドメインの管理

ESP（エッジセキュリティ パック）を使用する前に、ユーザは最初に SSO（シングルサインオン）ドメインを LoadMaster 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 サーバによって認証されたバーチャル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。



[Manage SSO] メニューオプションをクリックすると、[Manage Single Sign On Options] 画面を表示します。

3.13.1 SSO ドメイン

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

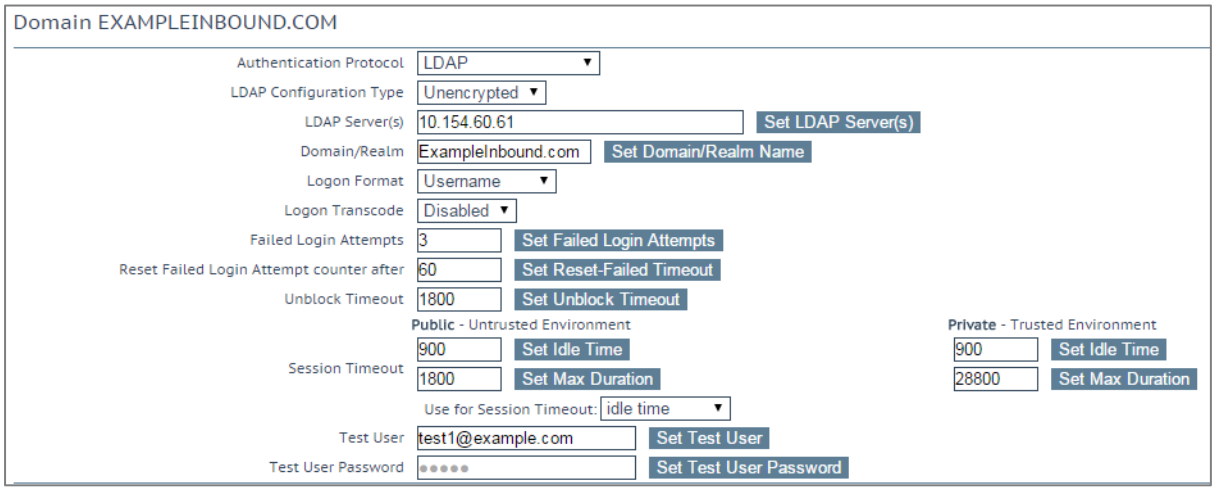
[Client Side]（クライアントサイド）の構成では、[Authentication Protocol] を[LDAP]、[RADIUS]、[RSA-SecurID]、[Certificates]、[RADIUS and LDAP]、[RSA-SecurID and LDAP] に設定できます。

[Server Side] 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。[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



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）
- SAML

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

LDAP Endpoint（LDAP エンドポイント）

使用する LDAP エンドポイントを選択します。LDAP エンドポイントの詳細については、「LDAP 設定」セクションを参照してください。

LDAP エンドポイントを選択して、[Manage LDAP Configuration] ボタンをクリックすると[LDAP Endpoints] 設定画面に移ります。LDAP エンドポイントの詳細は LDAP 設定を参照してください。

このオプションは、認証プロトコルが[LDAP] 、[RADIUS and LDAP] 、[RSA-SecurID and LDAP] に設定されている場合にのみ使用できます。

RADIUS/RSA-SecurID Server(s)（Radius、RSA-SecureID サーバ）

ドメイン認証に使用するサーバの IP アドレスをサーバ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 シェアード シークレット）

このシェアード シークレットは、RADIUS サーバと LoadMaster の間で使用する共通鍵です。

このフィールドは認証プロトコルが[RADIUS] または[RADIUS and LDAP] に設定されている場合に使用できます

Check Certificate to User Mapping（証明書とユーザ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 Feature Description」を参照してください。

Allow fallback to check Common Name（フォールバックでのコモンネーム チェックを許可）

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します。

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名を作成するのにも使用されます。例:

- **Principalname :** <ユーザ名>@<ドメイン>
- **username :** <ドメイン>¥<ユーザ名>

[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 認証マネージャの設定ファイル）

このオプションは認証プロトコルを RSA セキュア ID にセットした時に有効です。

このフィールドは、RSA 認証マネージャ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 Two Factor Authentication Feature Description を参照してください。

RSA Node Secret File（RSA ノード秘密ファイル）

このオプションは認証プロトコルを RSA セキュア ID にセットした時に有効です。

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

RSA 認証マネジャ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」の選択内容によります。

Not Specified（指定しない）

ユーザ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] 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名（domain¥name@domain.com など）を入力する必要があります。

Username Only（ユーザ名のみ）

このオプションを[Logon Format] 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名のみ使用されます(ドメインは削除されます)。

[Username Only] オプションは、[RADIUS] と[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 リアルサーバ））

リアルサーバ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)] フィールドは、[Authentication Protocol] に以下のオプションを設定したときに表示します。

- 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)] フィールドは、[Authentication Protocol] に以下のオプションを設定したときに表示します。

- RADIUS and LDAP
- RSA-SecurID and LDAP

Logon Transcode（ログオン 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、ユーザはロックされません。

ユーザがロックされると、そのユーザ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] 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] 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] と[idle time] のどちらを使用するかを指定できます。

Idle time : 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 : 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を使用）

セッションタイムアウトの動作で[max duration] か[idle time] を選択します。

ユーザ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。

Use LDAP Endpoint for Healthcheck（LDAP エンドポイント ヘルスチェックを使用）

ヘルスチェックに LDAP エンドポイント管理者のユーザ名とパスワードを使用するには、このチェックボックスを選択します。これを有効にすると、[Test User] と[Test User Password] のテキストボックスは使用できなくなります。

LDAP エンドポイントの詳細については、「LDAP 設定」セクションを参照してください。

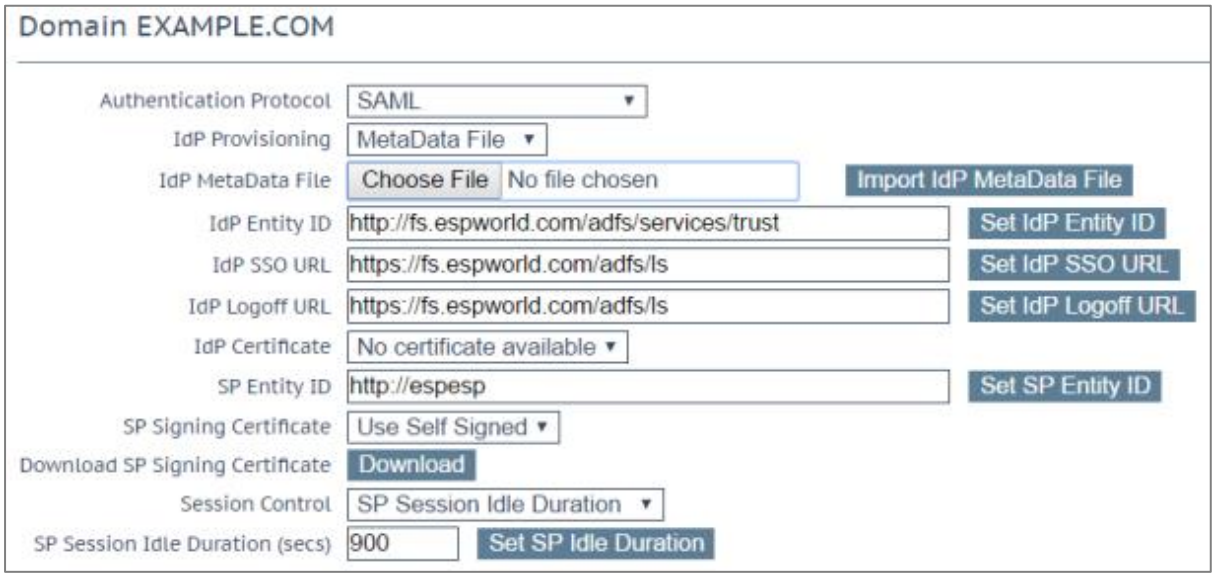
このオプションは、次のプロトコルでのみ使用できます。
[LDAP]、[Certificates]、[RADIUS and LDAP]、[RSA-SecurID and LDAP]

Test User and Test User Password（テストユーザ と テストユーザ 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アカウントの資格情報を入力します。LoadMaster は、この情報に基づいて、認証サーバ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。

3.13.1.1.1 クライアントサイド（インバウンド）SAML SSO ドメイン

[Authentication Protocol] を[SAML] に設定している場合フィールドは異なります。SAML 固有のフィールドは以下で説明します。



IdP Provisioning（Idp プロビジョニング）

[Manual] オプションで、IdP フィールドの詳細データをマニュアル入力できるようになります。

[MetaData File] オプションで、IdP メタデータファイルをアップロードできるようになります。この結果、[IdP Entity ID]、[IdP SSO URL]、[IdP Logoff URL] などの IdP アトリビュートの構成が簡単になります IdP からメタデータファイルをダウンロードできます。

IdP Metadata File（Idp メタデータファイル）

このフィールドは、[IdP Provisioning] フィールドを[Metadata File] に設定している場合に表示します。ファイルをアップロードするには、[Browse] をクリックして関連するファイルに移動して選択し、[Import IdP MetaData File] をクリックします。

IdP Entity ID（Idp エンティティ ID）

IdP エンティティ識別子を指定します。

IdP SSO URL

IdP SSO URL を指定します。

IdP Logoff URL（Idp ログオフ URL）

IdP ログオフ URL を指定します。

IdP Certificate（Idp 証明書）

IdP 証明書は、IdP から受け取った SAML レスポンスの内容を含んだアサーションの検証の条件に重要な要素になります。証明書がなければ、検証は続行できません。

SP Entity ID（SP エンティティ ID）

これは、リクエストメッセージが LoadMaster から送信されたときに、IdP がエンティティの理解、受け入れ、知識を可能にするために共有する識別子です。これは、ADFS サーバ上の信頼関係のあるパーティを識別子するために関連付けが必要です。

SP Signing Certificate（SP 証明書の署名）

ログオンのコンテキストで送信するリクエストに署名することはオプションです。現在、LoadMaster はこれらの要求に署名しません。

ログオフ リクエストのコンテキストでは必須であり、これらの要求に署名する必要があります。これは、なりすましを避け、ログオフ機能に関して特別なセキュリティを提供するためです。これにより、ユーザはハッキングされることも、不必要なログオフが発生することもありません。

[SP Signing Certificate] ドロップダウンリストでは、自己署名証明書または第三者証明書を使用して署名を実行することができます。

Download SP Signing Certificate（SP 署名の証明書をダウンロード）

自己署名入りの証明書を使用する場合は、[Download] をクリックして証明書をダウンロードします。この証明書は、依拠当事者の署名に追加するために IdP サーバ（たとえば ADFS）にインストールする必要があります。

ADFS サーバは、公開鍵を使って LoadMaster が生成した署名を検証するために、証明書が要求します。

Session Control（セッションコントロール）

関連するセッションコントロール オプションを選択します。 使用可能なオプションは次のとおりです。

- SP Session Idle Duration
- SP Session Max Duration
- IdP Session Max Duration

IdP の最大デュレーションの値は LoadMaster では設定できません。値は IdP プロトコルから取得されます。IdP 認証応答に値が設定されていない場合、デフォルト値の 30 分が IdP 最大デュレーションとして割り当てられます。

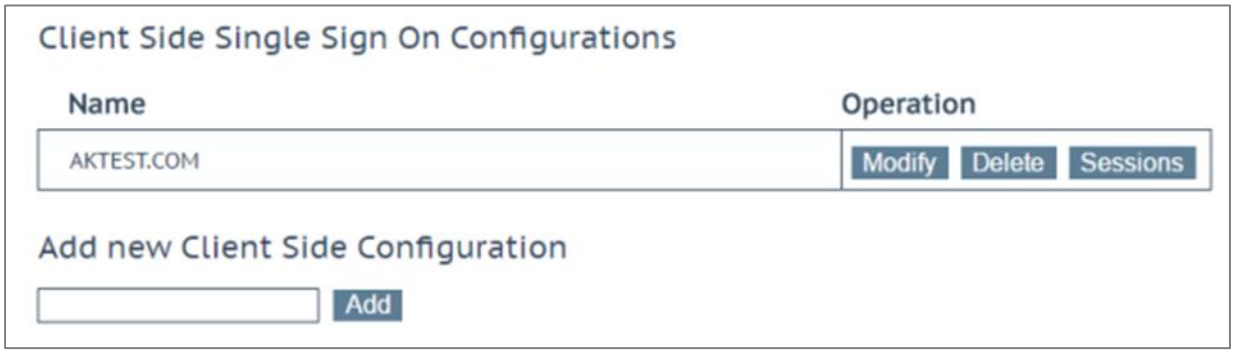
SP Session Idle Duration（SP セッション アイドル期間）

セッションアイドル期間を秒単位で指定します。 このフィールドは、[SP Session Idle Duration] が [Session Control] オプションとして設定されている場合にのみ表示します。

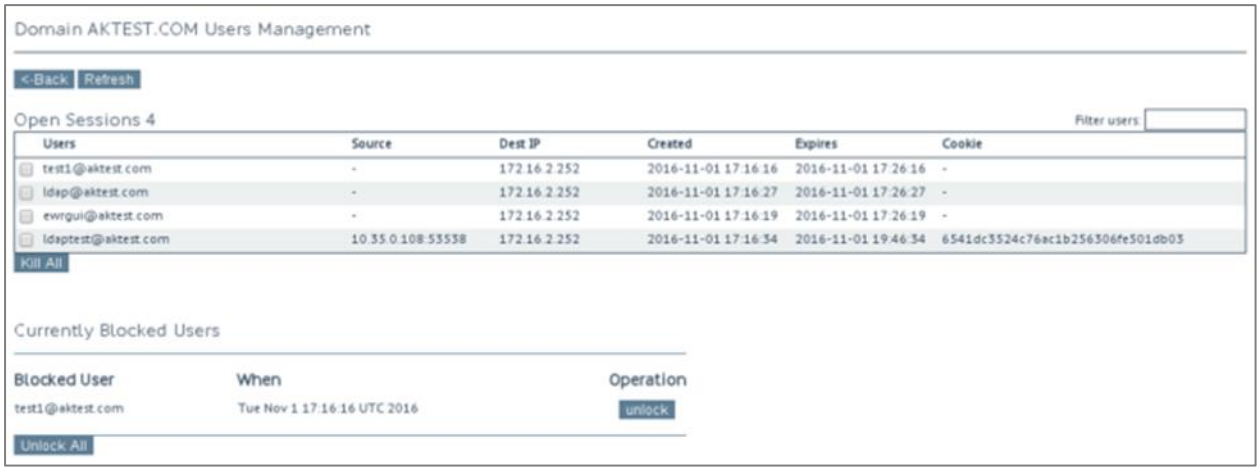
SP Session Max Duration（SP セッション最大期間）

セッション最大期間を秒単位で指定します。このフィールドは、[SP Session Max Duration] が[Session Control] オプションとして設定されている場合にのみ表示します。

3.13.1.1.2 セッション



クライアント側の SSO ドメイン名の[Sessions] ボタンをクリックすると、そのドメイン上の現在開いているセッションを一覧表示する画面を表示します。

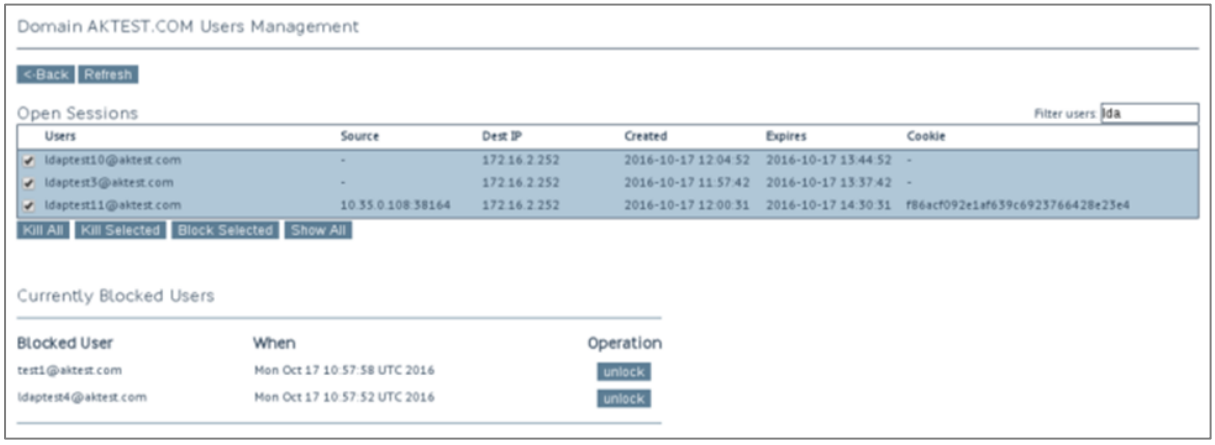


[Filter users] テキストボックスに検索語を入力し、リストをフィルタリングできます。
各セッションについて以下の情報が提供されています。

Users : クライアントのユーザ名/ドメイン
Source : クライアント（ホスト）の IP アドレスと送信元ポート
Dest IP : コネクションの宛先 IP アドレス
Created : コネクションが作成された日時

Expires : コネクションを切断する日時
Cookie : コネクションで使用している Cookie

[Kill All] ボタンをクリックすると、開いているすべてのセッションを強制終了します。（SSO キャッシュをフラッシュします）。



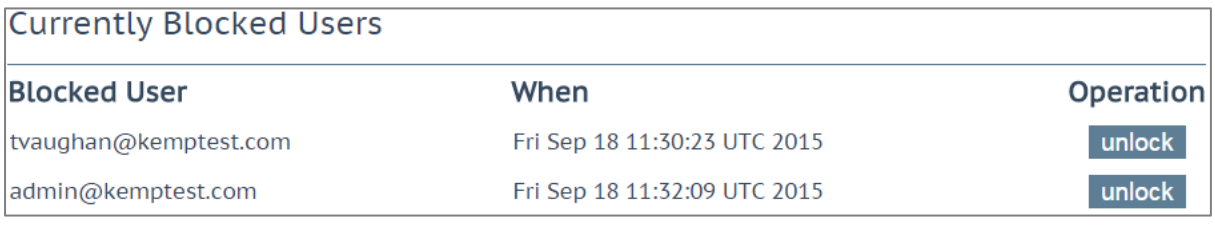
いづれかのセッション（複数選択も可）を選択すると、いくつかのオプションを提供します。

- Kill Selected
- Block Selected
- Show All

セッション終了の操作で、ログメッセージを監査ログに追加します。以下は例です：

- **cookie なしセッションの終了ログ：**
  mmm dd hh:mm:ss LM ssomgr: Deleted a session tester@aktest.com:- for domain AKTEST.COM
- **cookie セッションの終了ログ：**
  mmm dd hh:mm:ss LM ssomgr: Deleted a session ldaptest@aktest.com: 420cf78373643b3c0171d95c757e7bf3 for domain AKTEST.COM
- **すべてのドメインのセッションログ：**
  mmm dd hh:mm:ss LM ssomgr: Deleted all domain AKTEST.COM user sessions

Currently Blocked Users（ブロックされたユーザ）



このセクションには、現在ブロックされているユーザとそのユーザをブロックした日時をリスト表示します。[Operation] ドロップダウンリストで[unlock] ボタンをクリックすると、ブロックを解除できます。

1 つのユーザを異なる形式で表した場合、それらはすべて同じユーザ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 つのユーザ名として扱われます。

3.13.1.2 サーバサイド（アウトバウンド）SSO ドメイン

Authentication Protocol（認証プロトコル）

このプルダウンリストで認証サーバとの通信プロトコルを選択できます。アウトバウンド（サーバサイド）構成では[Kerberos Constrained Delegation] （KDC）オプションのみ利用できます。

KDC に関する詳細は、KEMP ドキュメントページの Kerberos Constrained Delegation を参照してください。

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やコンピュータ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名）

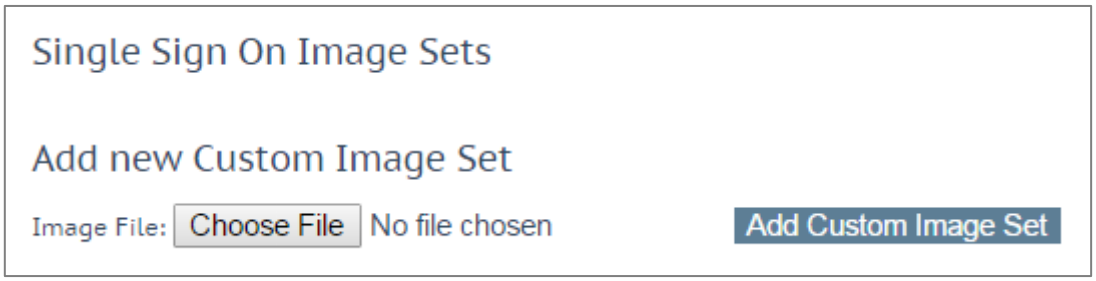
LoadMaster を設定する前に、Windows のドメイン（アクティブディレクトリ）にてユーザを作成して信頼を受ける必要があります。また、このユーザが委任を使用するよう設定する必要があります。この信頼された管理者ユーザアカウントは、パスワードが提供されていない場合に、ユーザやサービスの代わりにチケットを取得するのに使用されます。この信頼されたユーザのユーザ名を、このフィールドに入力する必要があります。

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パスワード）

Kerberos で信頼されたユーザのパスワードです。

3.13.2 SSO の画像設定

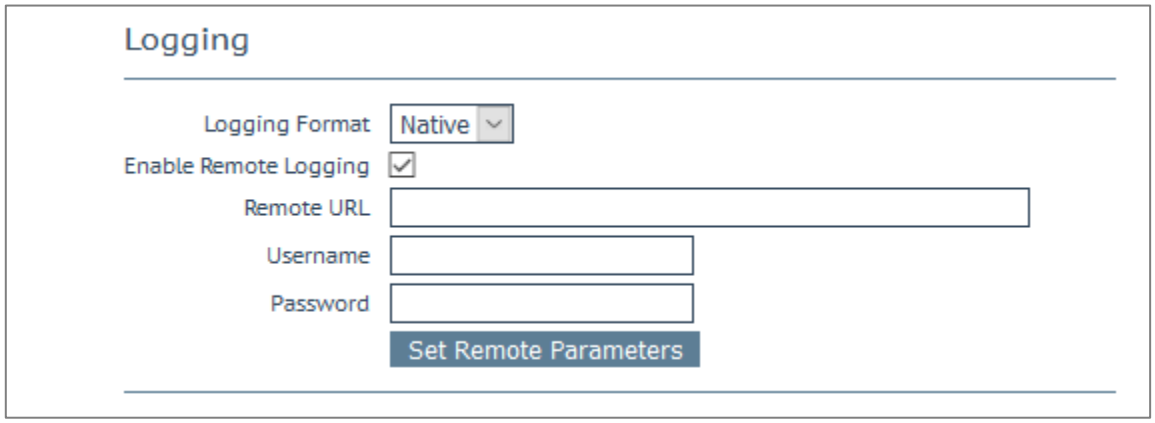


新規画像を設定するには、[Choose File] をクリックし、ファイルをブラウズ/選択して[Add Custom Image Set] をクリックします。ファイルを追加すると、追加した画像がこのページにリスト表示されます。また、バーチャルサービス編集画面の[ESP Options] セクションにある[SSO Image Set] ドロップダウンリストでも選択可能です。

.tar ファイルの作成方法等、SSO の画面設定に関する詳細は、「Custom Authentication Form, Technical Note」を参照してください。

3.14 WAF の設定

この画面を開くには、LoadMasterWUI のメインメニューで Virtual Services > WAF Settings を選択します。



Logging Format（ログ フォーマット）

監査ログの表示形式に応じて、ネイティブまたは JSON のいずれかを選択します。

Enable Remote Logging（リモートログを有効にする）

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）

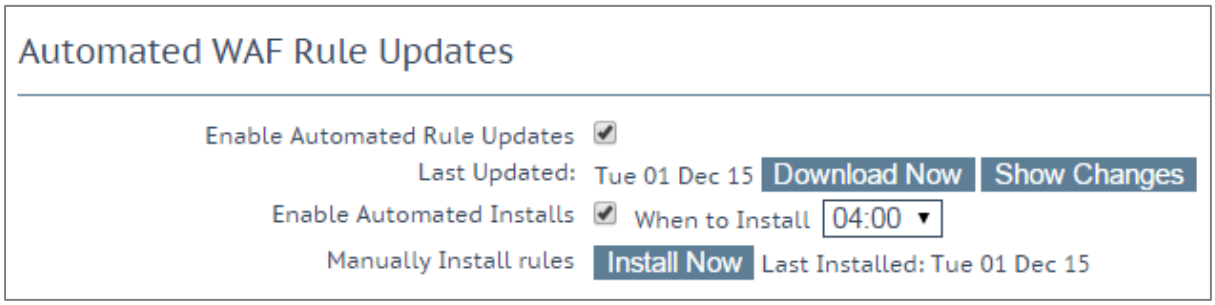
リモートログサーバのユニフォームリソースアイデンティファイアー（URI）を指定します。

Username（ユーザ名）

リモートログサーバのユーザ名を指定します。

Password（パスワード）

リモートログサーバのパスワードを指定します。



WAF サブスクリプションが期限切れになると、自動および手動のダウンロードオプションの表示がグレーになります。

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、最新ルールをダウンロードした日を表示します。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を用意しています。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 Technologies 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）

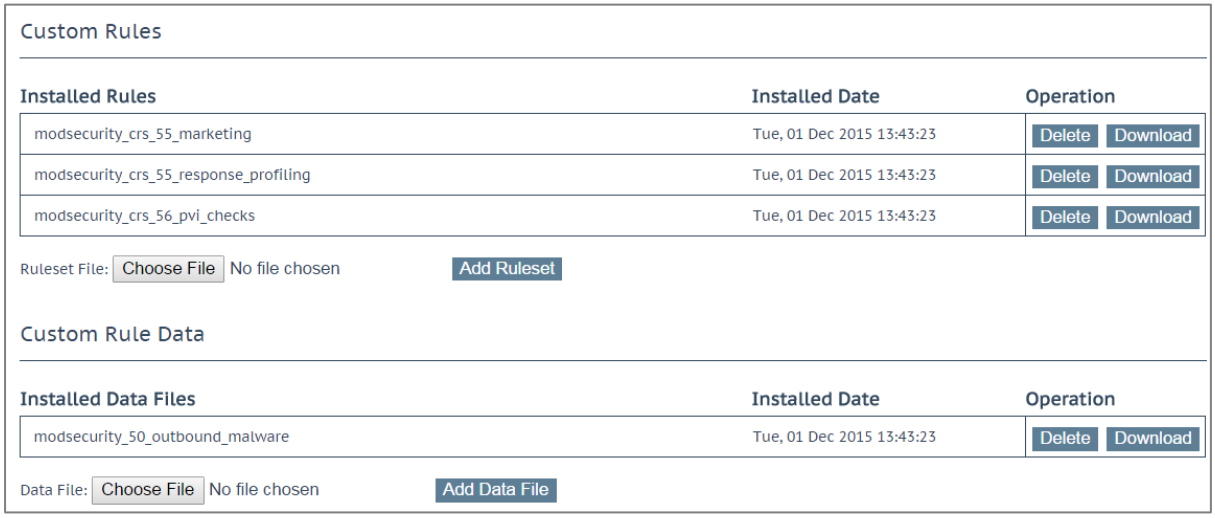
このチェックボックスをオンにすると、指定した時刻に最新のルールが毎日自動的にインストールされます。

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。



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

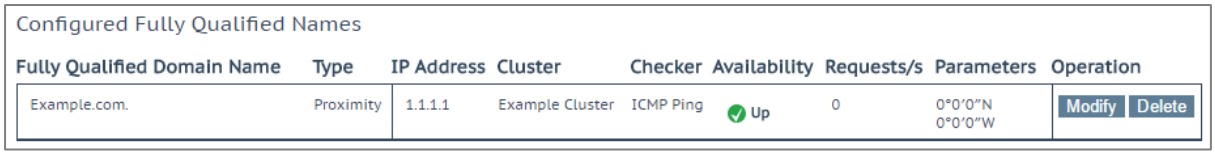
構成によっては、このメニューオプションを使用できない可能性があります。この機能は GSLB 機能パックに含まれており、LoadMaster に適用されているライセンスに基づいて有効になります。このオプションを利用するには、ライセンスをアップグレードする必要があるので、KEMP にご連絡ください。

4.1 GSLB の有効/無効

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] は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 >Network Setup >Packet Routing Filter で[Packet Routing Filter] を有効/無効にできます。

4.2 FQDN の管理

FQDN（Fully Qualified Domain Name）は、絶対ドメイン名とも呼ばれ、DNS（ドメインネームシステム）のツリー階層で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。FQDN の特徴は曖昧さがないこと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 の末尾はドットになります。



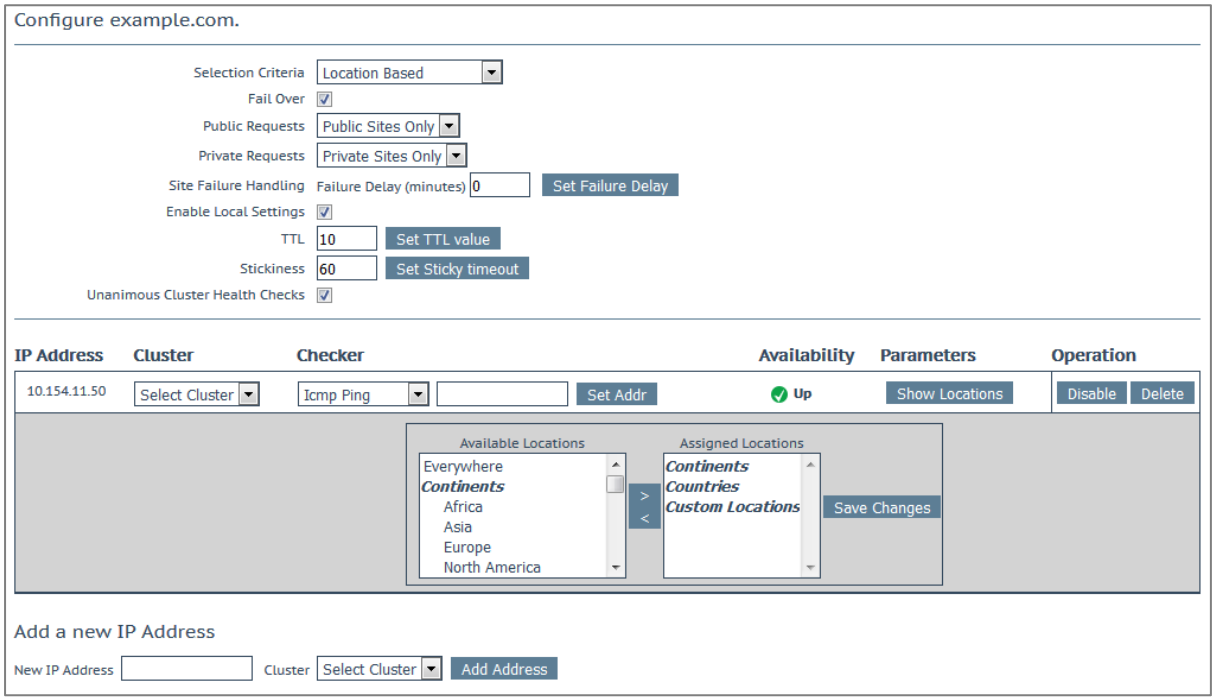
この画面から、FQDN の[Add] または[Modify] を選択できます。

4.2.1　FQDN の追加

FQDN

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 FQDN の追加と変更



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 :** サーバーファーム（クラスタ）の利用可能なサーバにトラフィックを順次配信します。
- **Weighted Round Robin :** 受信したリクエストは、サーバ単位に割り当てた静的な重み付けを基にして、クラスタ全体に順次配信します。
- **Fixed Weighting :** 他のリアルサーバに小さい重みの値が与えられている場合に限定して、最も重みが大きいリアルサーバが使用されます。
- **Real Server Load :** LoadMaster 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、サーバの状態を一定の間隔でチェックします。
- **Proximity :** 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] 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 :** 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] と[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。例えば、アイルランドのサイトが利用できない場合、アイルランドからのリクエストは、ヨーロッパの他のサイトに送信します。もし、ヨーロッパのサイトも利用できない場合は、[Everywhere] に設定したサイトに送信します。このサイトの利用できない場合は、同じ大陸にある有効なサイトをラウンドロビン方式でサイトを選択します。

[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
Public Requests	Public Only	Public	Public
	Prefer Public	Public	Public、Public がない場合は Private
	Prefer Private	Public	Private、Private がない場合は Public
	All Sites	Public	Private および Public
Private Requests	Public Only	Private	Private
	Prefer Public	Private	Private、Private がない場合は Public
	Prefer Private	Private	Public、Public ない場合は Private
	All Sites	Private	Private および Public

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 サーバやクライアントデバイスで GEO LoadMaster 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] の詳細については、「GEO Sticky DNS, Feature Description」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 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にアドレスを追加し、そのクラスタ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）

必要に応じて、IP アドレスを含むクラスタを選択できます。

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 LoadMaster からのバーチャルサービスの 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バーチャルサービスの 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。
    ポートをもたないバーチャル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バーチャルサービスがヘルスチェックによりチェックされます。バーチャル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。
    ポートをもつバーチャル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バーチャル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, Product Overview.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（リアルサーバの負荷）：**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、測定対象のバーチャルサービスは[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）

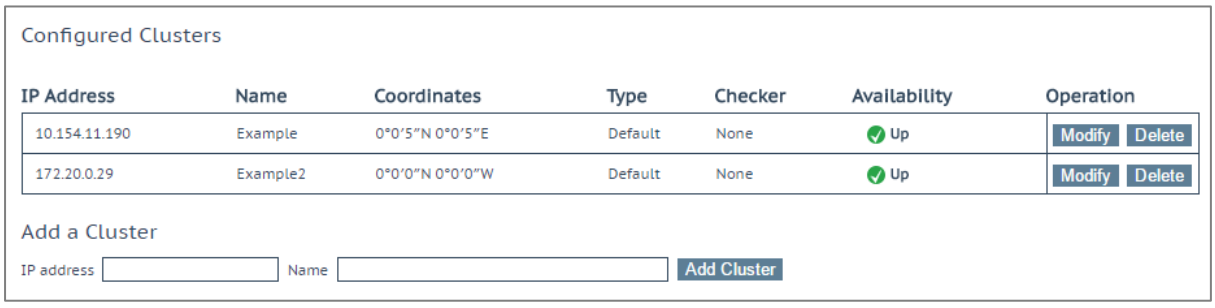
IP アドレスを削除するには、該当する IP アドレスの[Operation] 列で[Delete] ボタンをクリックします。

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。

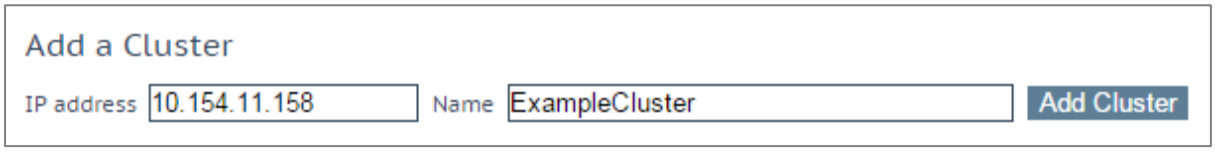
4.3 クラスタの管理

GEO クラスタは、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を用いてヘルスチェックが行われます。



「Manage Clusters」画面には、クラスタの[Add] 、[Modify] 、[Delete] オプションが用意されています。

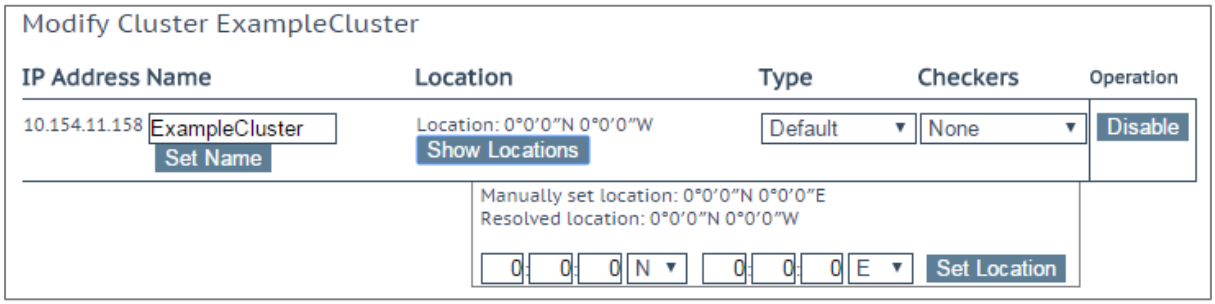
4.3.1 Add a Cluster（クラスタの追加）



クラスタを追加する場合は、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 : クラスタの IP アドレス
Name : クラスタの名前。この名前は、他の画面でクラスタを識別する目的で使用できます

4.3.2 Modify a Cluster（クラスタの変更）



Name（名前）
クラスタの名前。

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）
クラスタのタイプとして、[Default] 、[Remote LM] 、[Local LM] を選択できます。

Default : 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、クラスタに対するヘルスチェックが行われます。

- None：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 :** 指定したポートにてクラスタの 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：[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：このタイプのクラスタ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、クラスタを無効にできます。

4.3.3 Delete a Cluster（クラスタの削除）

クラスタを削除するには、該当するクラスタの[Operation] 列で[Delete] ボタンをクリックします。

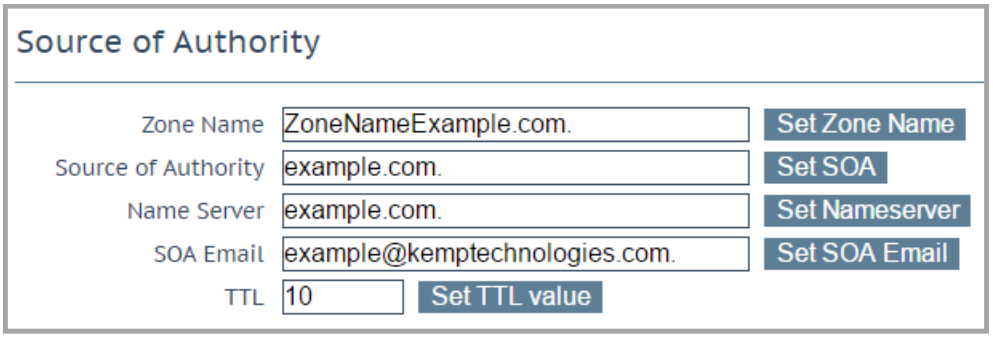
[Delete] 機能の使用時は、十分に注意してください。この削除処理を元に戻す方法はありません。

4.3.4 GEO クラスタのアップグレード

GEO クラスタ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。



Zone Name（ゾーン名）

使用するゾーン名を入力します。DNSSEC 設定にはゾーン名が必要です。ゾーン内のすべての FQDN は、指定のキーで署名されています。ゾーン外のすべての FQDN は引き続き機能しますが、応答に署名はありません。

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）

[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）。

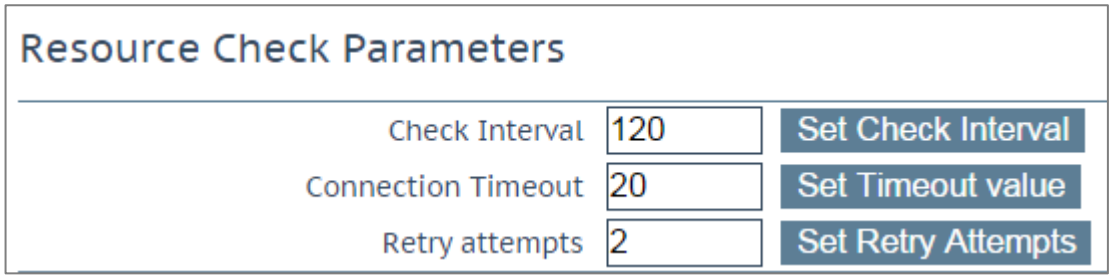
SOA Email（SOA Email アドレス）

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 サーバやクライアントデバイスで GEO LoadMaster 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。

4.4.1 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。

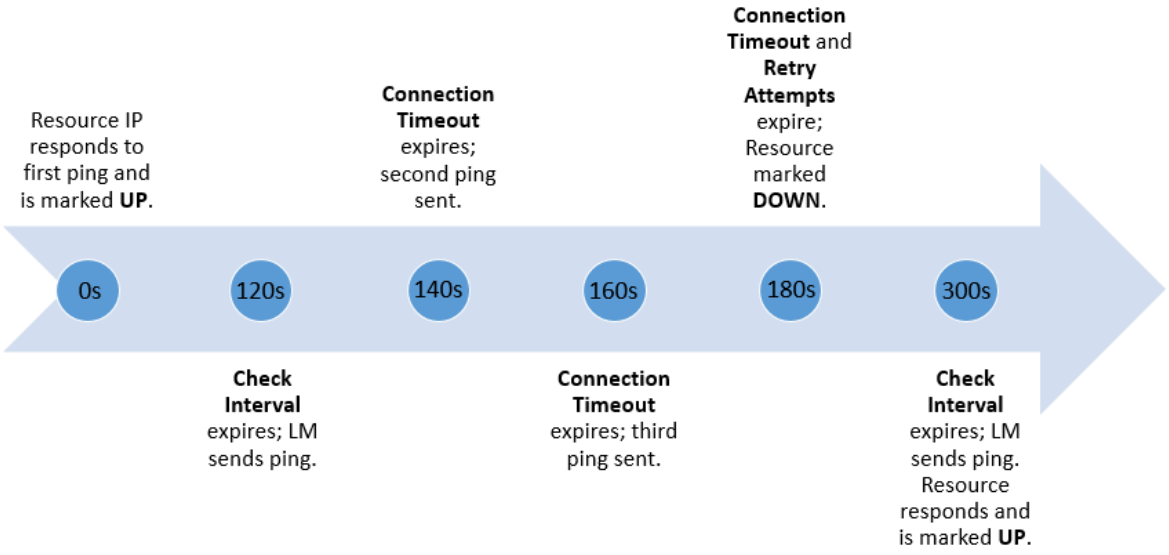
Retry Attempts（再試行回数）

ダウン状態として記録され、正常に動作しているリアルサーバ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、LoadMaster 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、LoadMaster 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］タイマがリセットされます。
3. 120 秒経過後、LoadMaster 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、LoadMaster はこのリソースを稼働中とマークし、［Check Interval］タイマをリセットします。



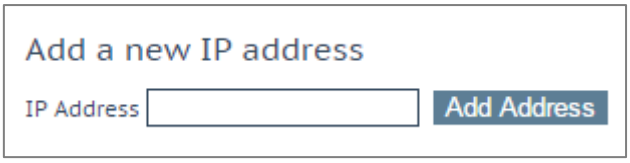
4.4.2 スティッキネス（持続性）

[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、KEMP ドキュメントページの「EO Sticky DNS, Feature Description」を参照してください。

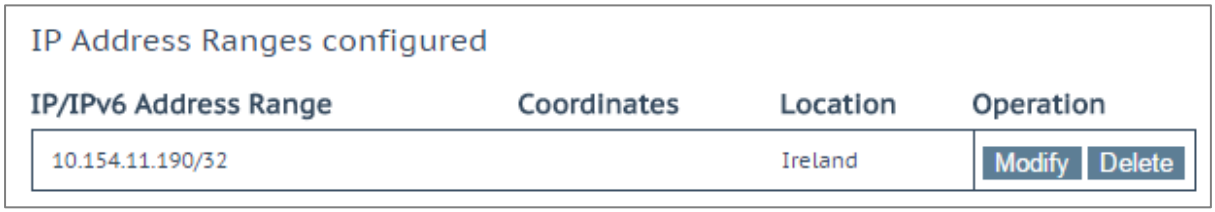
4.4.3 位置データの更新

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、FXC 株式会社の KEMP サポートにお問い合わせください。

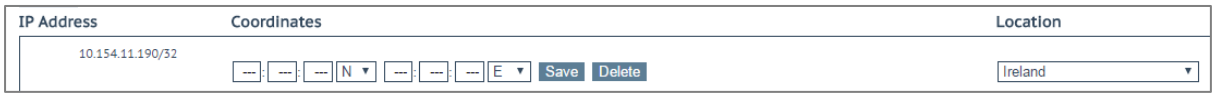
4.5 IP 範囲の選択条件



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。



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。



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 CIDR（Classless Inter-Domain Routing）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）

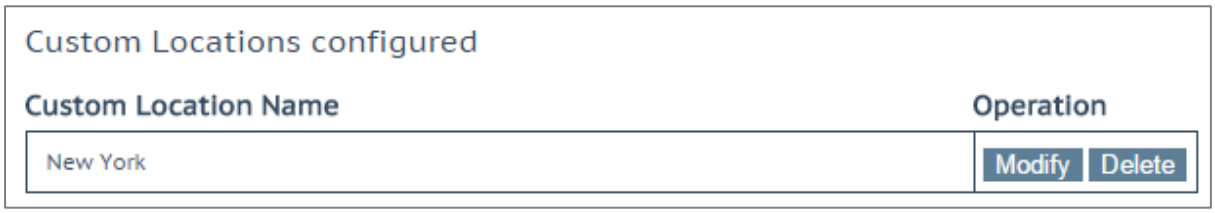
位置を示す緯度と経度を入力します。

Location（位置）

アドレスに割り当てる位置を指定します。

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。

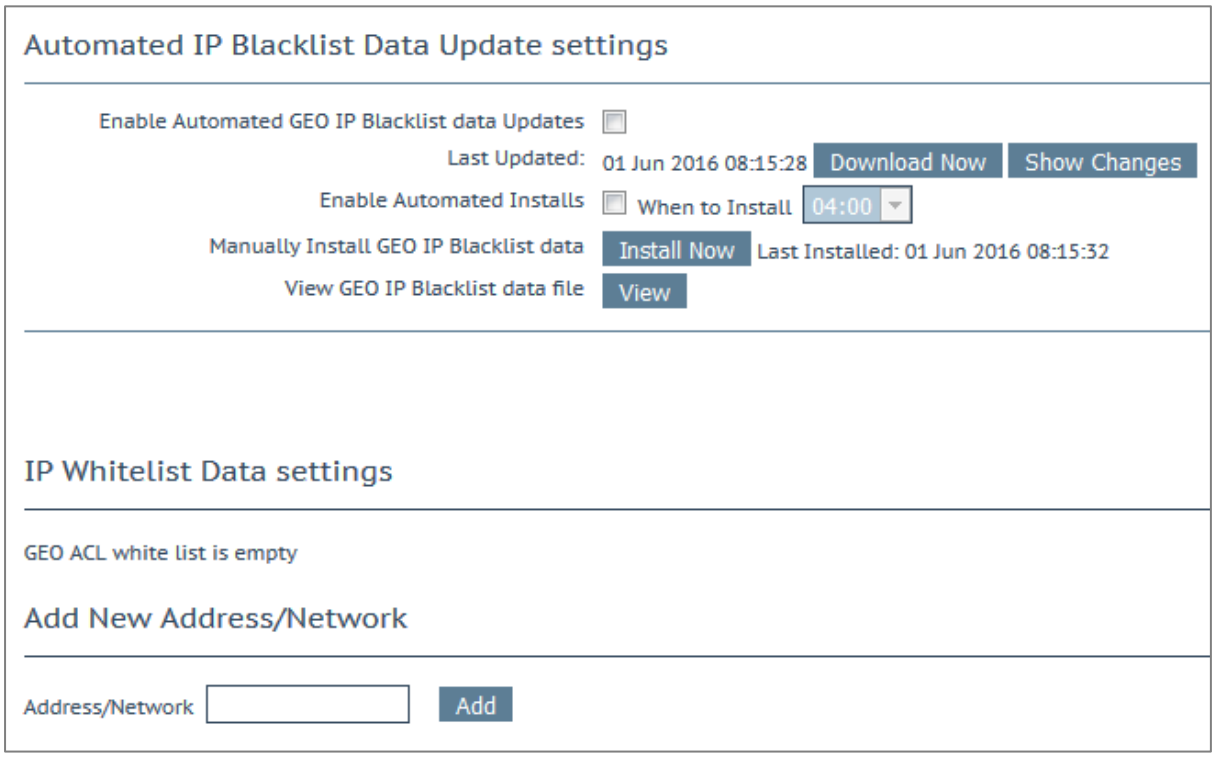


このセクションでは、カスタムロケーションの編集と削除も行えます。

4.6 IP 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。

This is a licensable feature. If you cannot see these options, or if any fields are grayed out, please contact KEMP to upgrade your license.
これはライセンスに関連する機能です。これらのオプションが表示されない場合、またはフィールドがグレーアウトしている場合は、FXC 株式会社の担当窓口に連絡してライセンスをアップグレードしてください。



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、通知メッセージを表示します。

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を表示します。

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 アドレスを表示します。

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。

4.7 DNSSEC の設定

DNSSEC を設定する前にゾーンを定義する必要があります。ゾーンを定義するには、>Global Balancing > Miscellaneous Params に移動し[Zone Name] を指定します。

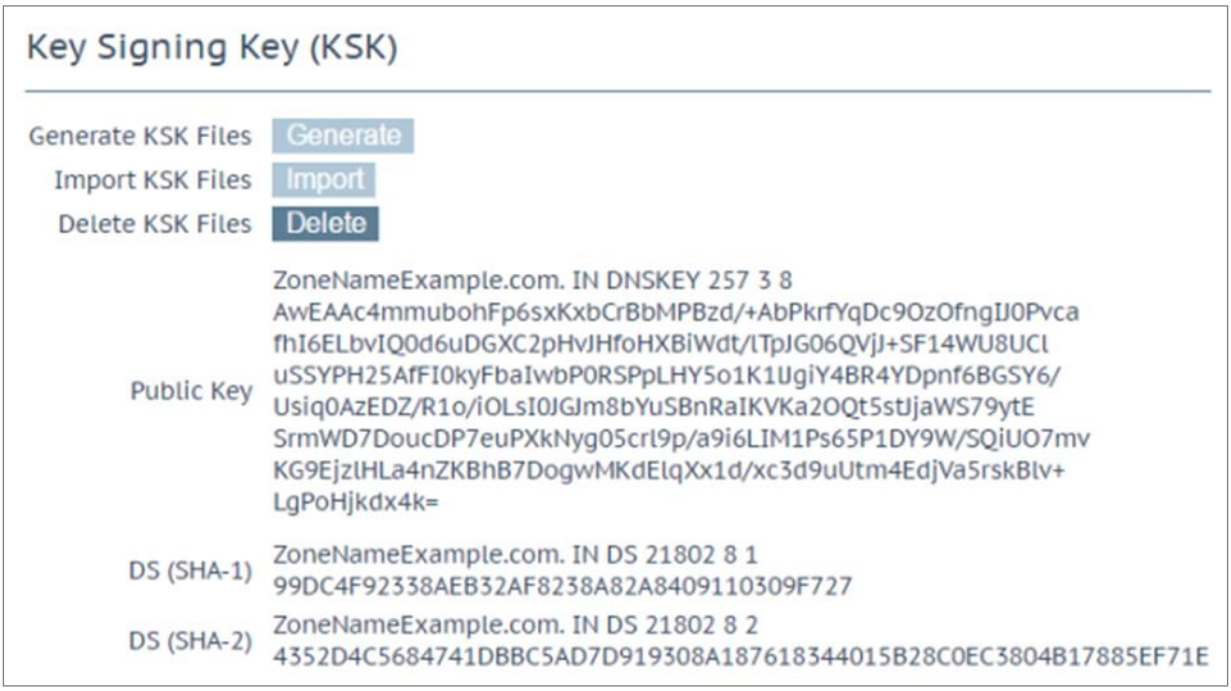
ゾーン名を定義したら、KSK（Key Signing Keys）を設定する必要があります。 設定には次の 2 つの選択肢があります：

- [Import] をクリックし、ファイルの場所を参照して KSK ファイルをインポートします。
- [Generate] をクリックして KSK ファイルを生成する

「Generate Key Signing Key Files」画面で、暗号化アルゴリズムと鍵サイズを選択します。
以下のアルゴリズムがサポートされています。

- NSEC3RSASHA1
- RSASHA256
- RSASHA512

デフォルトは RSASHA256 です。.
サポートする鍵サイズは 1024、2048、4096 ビットです。デフォルトは 2048 です。



KSK ファイルの生成/インポートが完了すると、DNSSEC 画面に KSK の詳細を表示し、KSK ファイルを削除するオプションを表示します。

最後のステップでチェックボックスをオンにして DNSSEC を有効にします。

5 統計情報

5.1 リアルサーバの統計情報

[Global] （システム）、[Real Servers]、[Virtual Services]、WAF について LoadMaster の動作状態を表示します。

5.1.1 システム統計

Total CPU Activity（合計 CPU アクティビティ）

このグラフは、LoadMaster の以下の CPU 使用率を表示します。

統計	説明
User	ユーザ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	アイドル状態の CPU のパーセンテージ
I/O Waiting	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

4 つのパーセンテージの合計は 100%になります。

Core Temperatures : LoadMaster ハードウェア機器の各 CPU コアの温度を表示します。仮想アプライアンス型 LoadMaster の統計画面では CPU 温度を表示しません。

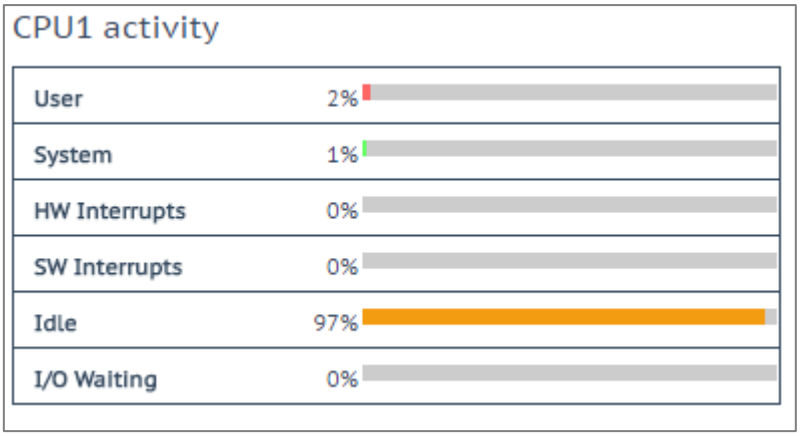
Dell 製ハードウェアを使う LoadMasters は、SNMP を使用して以下の統計情報を取得できます。

- Temperature（温度）
- Fan speed（ファンスピード）
- Power supply（電源供給）
- Voltage current（電圧/電流）

これらの値は、SNMP でのみ使用できます。 SNMP オプションの詳細については、「SNMP オプション」セクションを参照してください。

CPU Details

各 CPU の統計情報を取得するには、[CPU Details] で目的の番号ボタンをクリックします。



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 つの統計情報を追加で表示します。

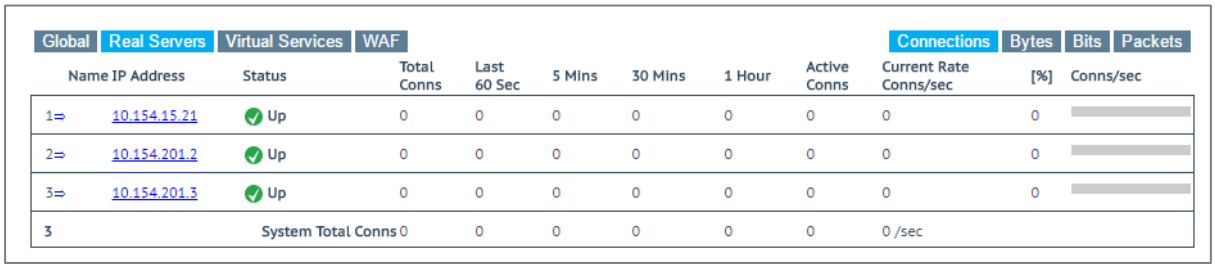
Memory usage

メモリの使用容量と空き容量を棒グラフで表示します。

Network activity

各インターフェイスのネットワーク・スループットを棒グラフで示します。

5.1.2 リアルサーバ



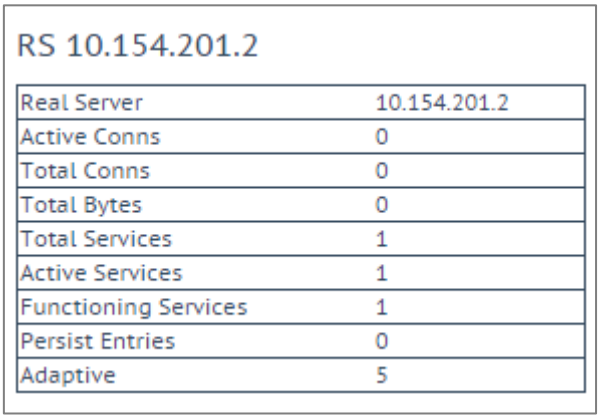
5 統計情報

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、またはパケット数を表示します。ページの右上にあるボタンをクリックすると、表示単位が切り替わります。各リアルサーバの値は、リアルサーバにアクセスしているすべてのバーチャルサービスの値を表しています。

リアルサーバに複数のバーチャルサービスを割り当てている場合、番号の右側にある矢印（⇒）をクリックすると、各リアルサーバの統計情報をバーチャルサービスごとに参照できます。矢印のクリックでビューを展開し、リアルサーバが割り当てられた各バーチャルサービスの統計情報を表示します。

SSL を実装するサービスでは、暗号化されたバーチャルサービスのパケットは統計情報で参照できません。

Name : [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、リアルサーバの IP アドレス、およびバーチャルサービス（列を展開すると表示される）を表示します。リアルサーバの IP 列のリンクをクリックすると、新たな画面が開き、そのリアルサーバに関する各種統計情報が表示されます。


RS 10.154.201.2

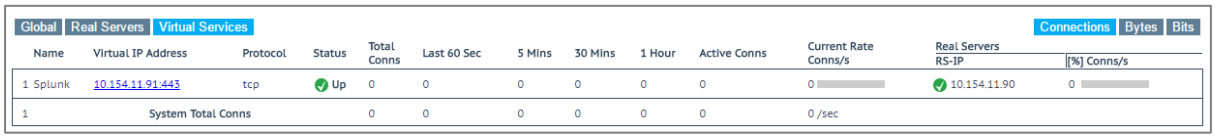
Real Server	10.154.201.2
Active Conns	0
Total Conns	0
Total Bytes	0
Total Services	1
Active Services	1
Functioning Services	1
Persist Entries	0
Adaptive	5

Status : リアルサーバの状態が表示されます。
Adaptive : このオプションは、バーチャル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 : このオプションは、バーチャルサービスのスケジューリング方式が[resource based (SDN adaptive)] に設定されている場合のみ表示されます。コントローラから収集された情報により、[Adaptive] 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、リアルサーバ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。リアルサーバの重みにより、トラフィックをどこに送信するかが決定されます。複数のバーチャルサービスにてリアルサーバ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、リアルサーバが設定されているすべてのバーチャル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、リアルサーバが設定されているバーチャルサービスの数を表します。例えば、[Weight] が 972/2 の場合、2 つのバーチャルサービスで設定しているリアルサーバの重みの平均値が 972 であることを意味します。
Total Conns : トータルの接続数です。

レイヤ 4 UDP 接続では[connection count] は常に「0」です。

Last 60 Sec : 過去 60 秒間におけるトータルの接続数
5 Mins : 過去 5 分間におけるトータルの接続数
30 Mins : 過去 30 分間におけるトータルの接続数
1 Hour : 過去 1 時間におけるトータルの接続数
Active Conns : 現在アクティブな接続のトータルの数
Current Rate Conns/sec : 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 : 1 秒当たりの接続数をグラフ表示したもの
System Total Conns : この行には、各列の合計が表示されます。

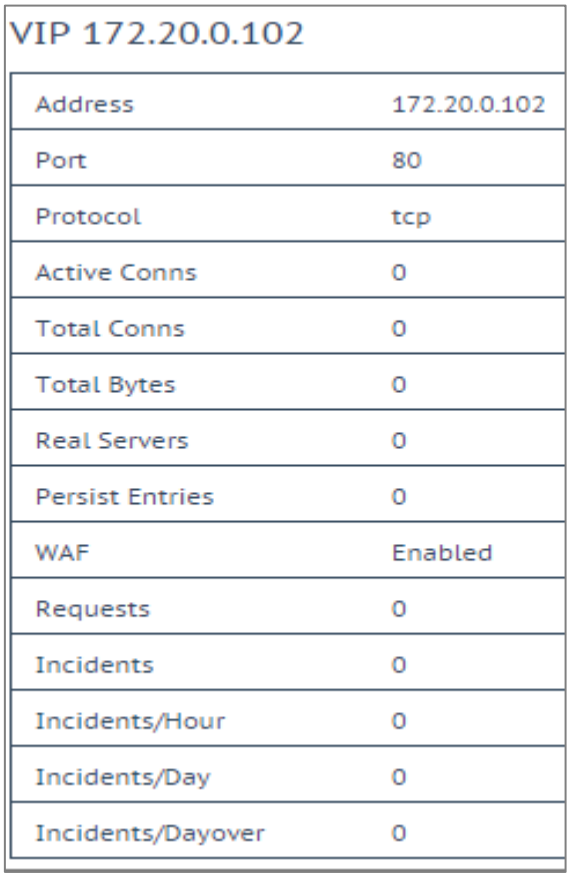
5.1.3 バーチャルサービス



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。バーチャルサービスのリアルサーバに対する分配のパーセンテージが表示されます。

Name : バーチャルサービスの名前
Virtual IP Address : バーチャルサービスの IP アドレスとポート

5 統計情報



VIP 172.20.0.102

Address	172.20.0.102
Port	80
Protocol	tcp
Active Conns	0
Total Conns	0
Total Bytes	0
Real Servers	0
Persist Entries	0
WAF	Enabled
Requests	0
Incidents	0
Incidents/Hour	0
Incidents/Day	0
Incidents/Dayover	0

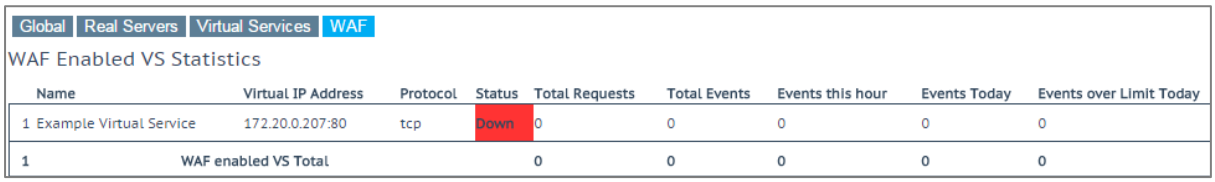
[Virtual IP Address] カラムのリンクをクリックすると、新たな画面が開き、そのバーチャルサービスに関する各種統計情報を表示します。

Address : バーチャルサービスの IP アドレス
Protocol : バーチャルサービスのプロトコル tcp または udp を選択できます。
Active Conns : 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
Total Bytes : 送信されたトータルのバイト数
Real Servers : このバーチャルサービスにおけるトータルのリアルサーバの数
Persist Entries : 入力されたパーシステンスエントリのトータルの数
WAF : バーチャルサービスで 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 : 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 : 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 : 現在の時間内（xx.00.00 以降）：に発生したイベントの数
Incidents/Day : 真夜中（ローカル時刻）以降に発生したイベントの数
Incidents/Dayover : 1 日のうちに、設定された警報閾値をイベントカウンタが越えた回数例えば、閾値が 10 に設定されており、20 個のイベントが発生した場合、このカウンタは 2 に設定されます。警報閾値

は、バーチャル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、バーチャルサービスごとに設定できます。詳細は「Web アプリケーション ファイアウォール（WAF）」セクションを参照してください。

System Total Conns : この行には、各列の合計が表示されます。

5.1.4 WAF



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 : 一番左の列には、WAF が有効なバーチャルサービスのトータルの数が表示されます。

Name : WAF が有効なバーチャルサービスの名前

Virtual IP Address : バーチャルサービスの IP アドレスとポート

Protocol : バーチャルサービスのプロトコル（TCP または UDP）

Status : バーチャルサービスの状態取り得るステータスに関する詳細は「表示と変更（設定済みの HTTP サービス）」参照してください。

Total Requests : 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 : 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（xx.00.00 以降）に発生したイベントの数

Events Today : 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、このカウンタは 2 に設定されます。警報しきい値は、バーチャル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、バーチャルサービスごとに設定できます。「Web アプリケーション ファイアウォール（WAF）」セクションを参照してください。

5.2 履歴グラフ

「Historical Graphs」画面には、LoadMaster の統計情報をグラフ表示します。設定可能なこのグラフには、LoadMaster で処理されているトラフィックの情報を視覚的に表示します。

LoadMaster のファームウェア バージョン 7.1.35 から新しいファームウェアにアップグレードした後、[Historical Graphs] を表示しないことがあります。この問題の解決は、統計カウンタをリセットすることです。>System Configuration >Extended Log Files >System Log Files >Debug Options >Reset Statistics

5 統計情報

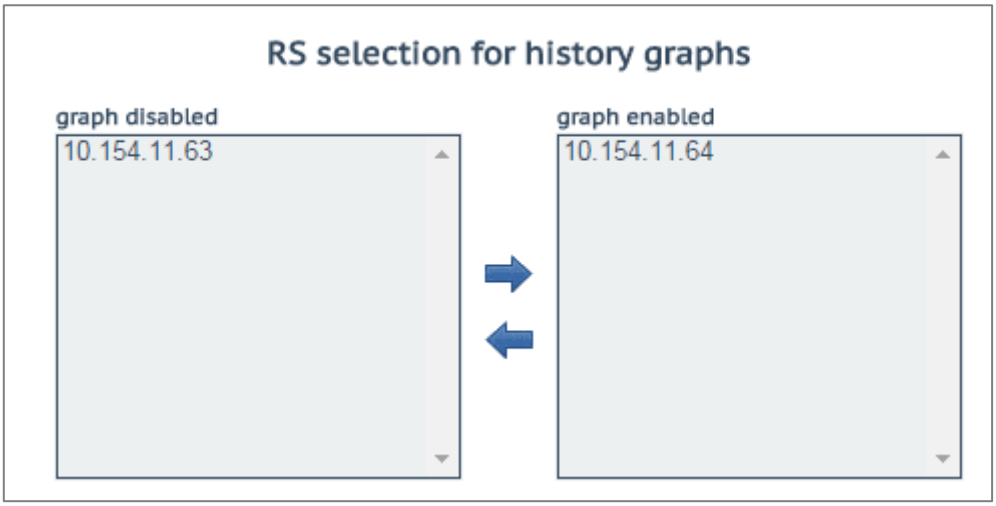
各インターフェイスのネットワークアクティビティに関するグラフが用意されています。バーチャルサービスの全体情報および個別情報に関するグラフや、リアルサーバの全体情報および個別情報に関するグラフを表示するオプションも用意されています。

時間表示の密度はドロップダウンから[hour]、[day]、[month]、[quarter]、[year] オプションの選択で指定できます。

ネットワークインターフェイスのトラフィックはドロップダウンから[Packet]、[Bits]、[Bytes] オプションの選択で測定単位を選択できます。

バーチャルサービスおよびリアルサーバのグラフはドロップダウンから[Connections]、[Bits]、[Bytes] オプションの選択で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、バーチャル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、バーチャルサービスの設定ウィンドウが表示されます。



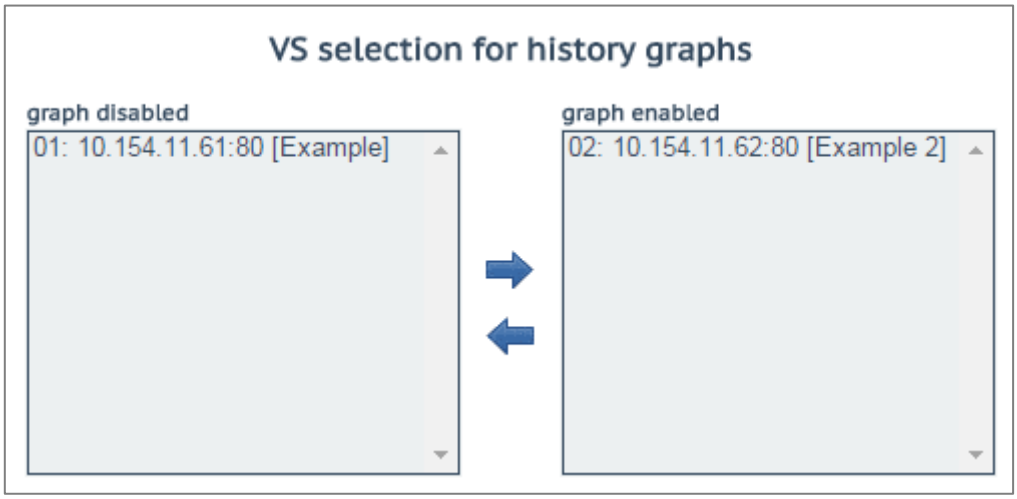
このダイアログで、バーチャルサービスの統計情報表示を追加/削除できます。

「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 個のバーチャル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。

5 統計情報



[Real Servers] パネルの設定アイコンを クリックすると、どのリアルサーバ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、リアルサーバ設定ダイアログが別ウィンドウで表示されます。

このダイアログで、リアルサーバの統計情報表示を追加/削除できます。

最大 5 個のリアルサーバ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バーチャルサービスとリアルサーバの統計情報だけを収集、保存します。バーチャルサービスとリアルサーバ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。

数多くのバーチャルサービスやリアルサーバ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。

LoadMasterWUI 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)

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:

5 統計情報

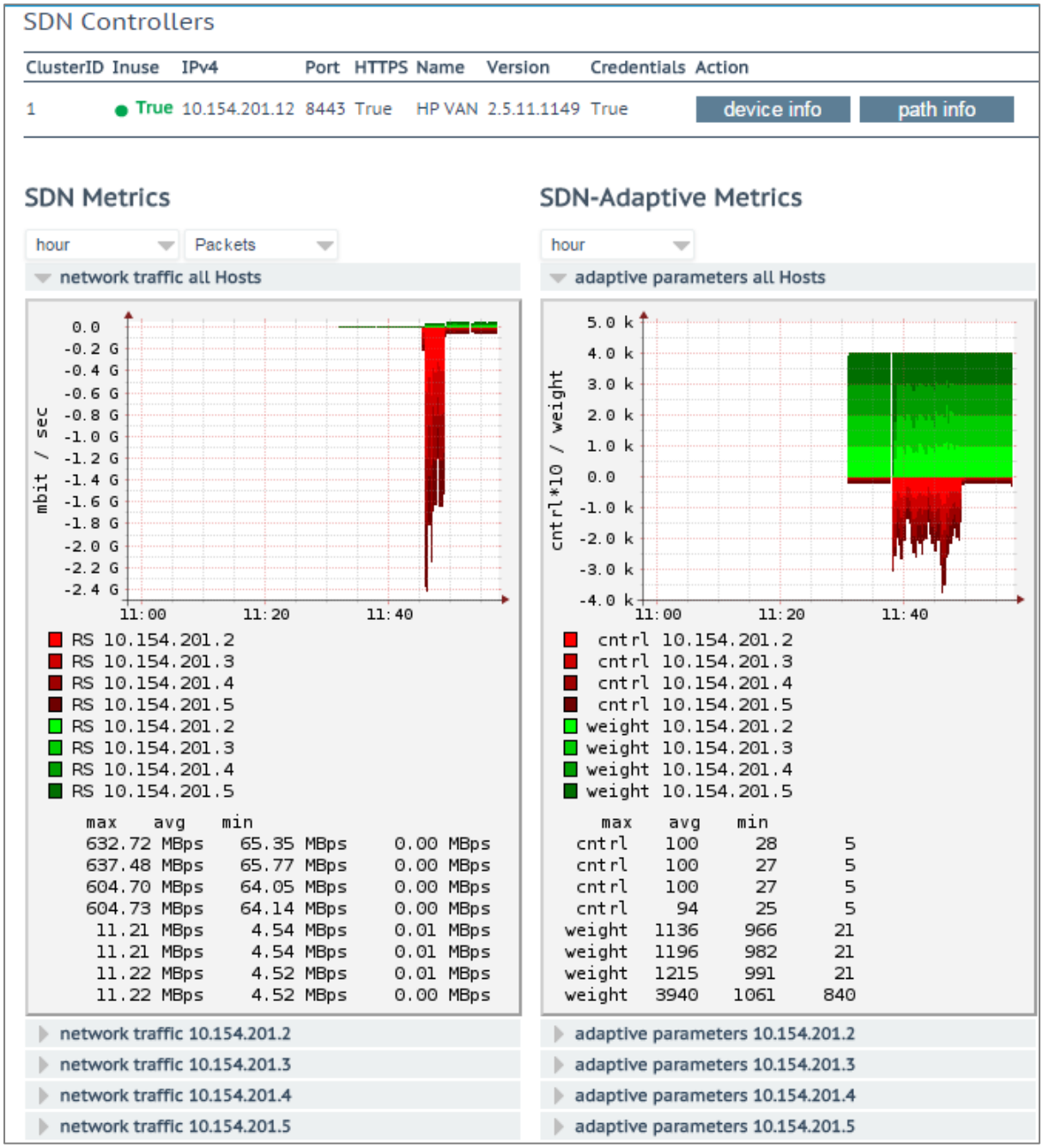
1 秒あたりの接続数のグラフに、倍率「m」とともに 200 という値が表示されています。前記の表に示すように、「m」は「ミリ」を表します。そのため、その時点における 1 秒あたりの接続数の絶対的な値を調べるには、200 という値に倍率 10^(-3)を掛ける必要があります:

- 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、LoadMasterWUI メインメニューの >Statistics >SDN Statistics を展開します。



LoadMaster が SDN コントローラに接続されると、[Name] 、[Version] 、[Credentials] を表示します。

Statistics section（統計情報の選択）

LoadMaster が SDN コントローラと通信するまで統計情報は表示しません。
[Name] 、[Version] 、[Credentials] の表示がない場合、LoadMaster は SDN コントローラに接続していないことを示します。この場合、設定の誤りか、SDN コントローラ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 :** 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リアルサーバ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 :** 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、リアルサーバの重みが低下します。

6.1 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

[device info] （デバイス情報）ボタンをクリックすると、コントローラとスイッチ間で OpenFlow が有効にスイッチの情報を表示しあす。

6 SDN 統計情報

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

Interface Info

ID	Name	State	Mac
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

Node Info

ID	VID	Port	Mac
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

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。

6.1.1 パス情報

Path Info

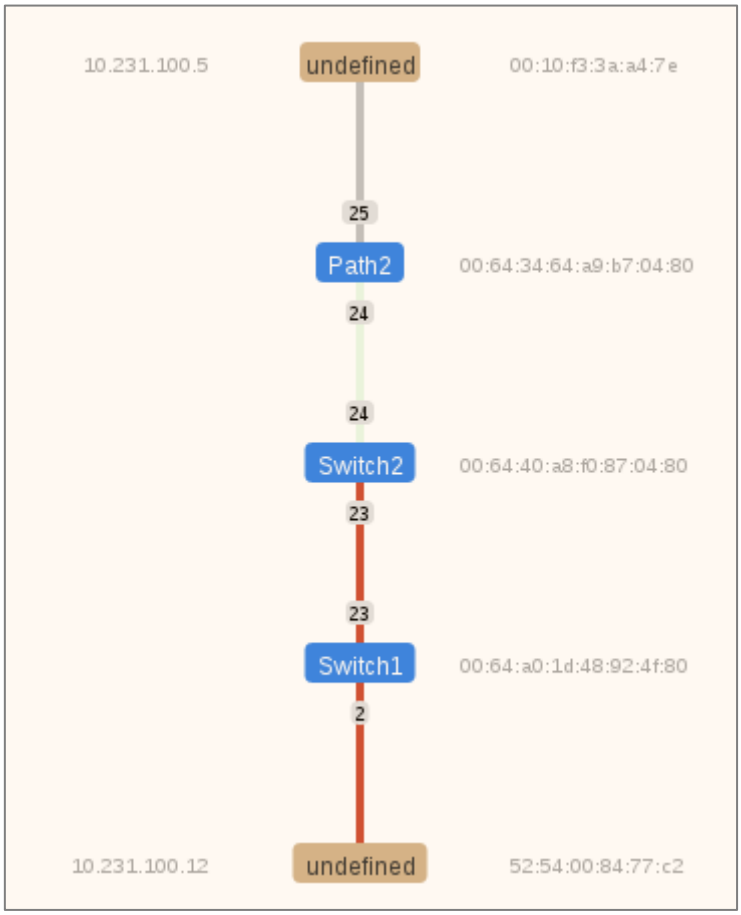
Dir	Source	Dest	Switch		
			Idx	Name	Dpid
=>	10.231.100.5	10.231.100.12	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80
<=	10.231.100.12	10.231.100.5	0	Path2	00:64:34:64:a9:b7:04:80
			1	Switch2	00:64:40:a8:f0:87:04:80
			2	Switch1	00:64:a0:1d:48:92:4f:80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

[path info] ボタンをクリックすると、パス情報を表示します。

パス情報を表示するには、LoadMaster と SDN コントローラ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] 列にある[=>] または[<=] のアイコンをクリックします。

6 SDN 統計情報



この画面には、LoadMaster、リアルサーバ、およびその間にあるスイッチが表示されます。LoadMasterとリアルサーバは茶色で表示されます。LoadMaster は上に表示され、リアルサーバ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 DPID（データパス ID）を表示します。DPIP は、コントローラ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、LoadMaster とリアルサーバの MAC（メディアアクセス制御）アドレスを表示します。また、LoadMaster とリアルサーバの IP アドレスを左側に表示します。

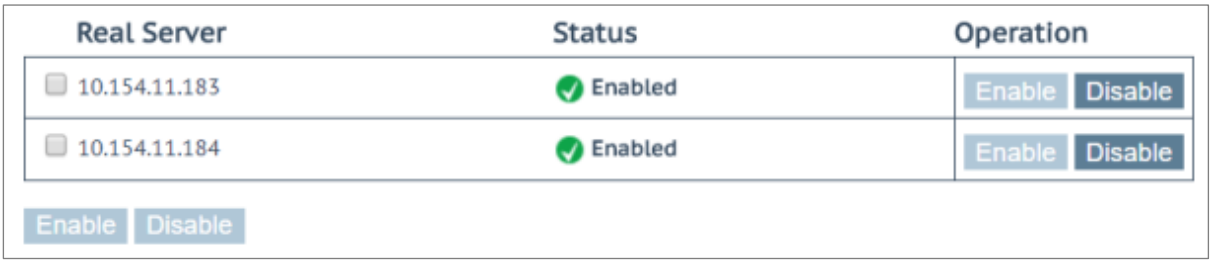
パスの色の意味は以下のとおりです。

- **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：**LoadMaster 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] の間のパスは正常ですが、[Switch2] 、[Switch] とリアルサーバ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　リアルサーバ



この画面には、リアルサーバの現在のステータスが表示されます。また、各リアルサーバを[Disable] または[Enable] に設定するオプションが用意されています。リアルサーバ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）。操作する対象のリアルサーバ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、複数のリアルサーバを同時に[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 つのバーチャルサービスでリアルサーバが有効になっていることを表します）。

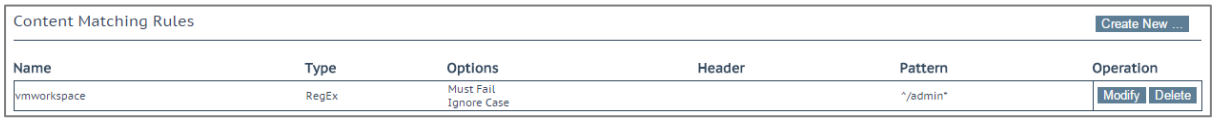
注意
リアルサーバを無効にすると、それを使用するように設定されたすべてのバーチャルサービスで無効になります。もし一つだけリアルサーバが利用可能でも、バーチャルサービスは事実上停止しトラフィックは通過しません。

DNS 名が割り当てられたリアルサーバは、DNS 名のないリアルサーバの上または下に表示されます。リアルサーバのリストをソートするには、[Real Server] か[Status] カラムの見出し文字をクリックします。

8 ルールとチェック

8.1 コンテンツ ルール

8.1.1 コンテンツマッチ 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。

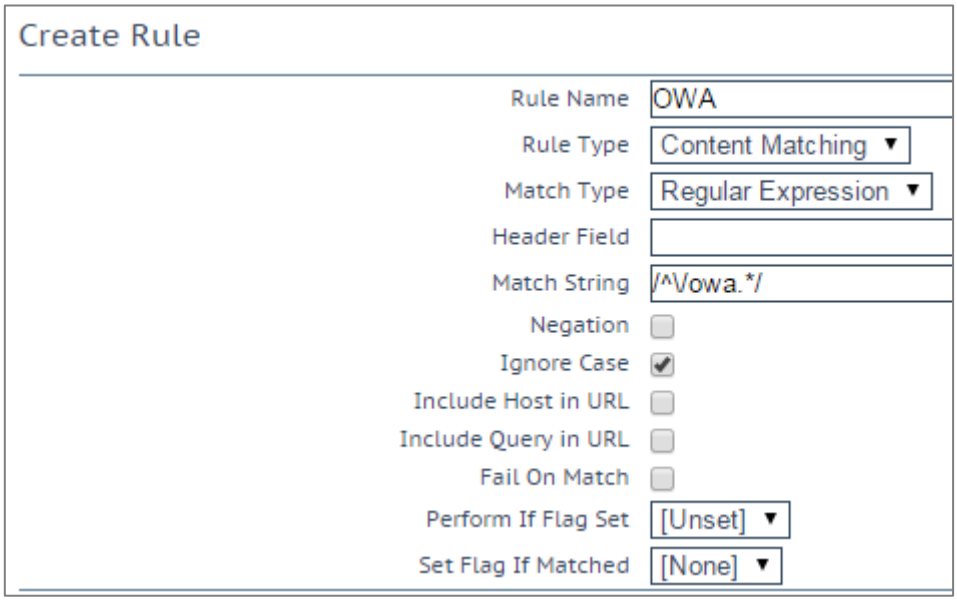
ルールの種類:

- **Content Matching :** ヘッダとボディ内のコンテンツ照合と一致の確認
- **Add Header :** ルールに従ったヘッダの追加
- **Delete Header :** ルールに従ったヘッダの削除
- **Replace Header :** ルールに従ったヘッダの置き換え
- **Modify URL :** ルールに従って URL の変更
- **Replace String in Response Body :** ルールに従ったボディ内テキストの置き換え

ルール設定の詳細については、「Content Rules, Feature Description」ドキュメントを参照してください。

8.1.2 コンテンツ マッチ

[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。



Rule Name（ルール名）

ルール一覧でリストするルール名称です。

Match Type（マッチタイプ）

- **Regular Expression :** ヘッダをルールの文字列と比較
- **Prefix :** ルールに従って、ヘッダのプレフィックスと比較
- **Postfix :** ルールに従って、ヘッダのポストフィックスと比較

Header Field（ヘッダフィールド）

ヘッダフィールド名のマッチを行います。ヘッダ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 GET、POST、HEAD など HTTP メソッドに基づいて、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します。

リクエストボディについては、[Header Field] テキストボックスに「body」と入力することで照合できます。

Match String（マッチ文字列）

マッチ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、KEMP ドキュメントページの「Content Rules, Feature Description」を参照してください。

egation（反転）

マッチパターン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（マッチしない時に処理）

ルールにマッチした場合、常に接続しません。

Perform If Flag Set（フラグセット時に実行）

指定フラグがセットされている場合のみこのルールを実行します。

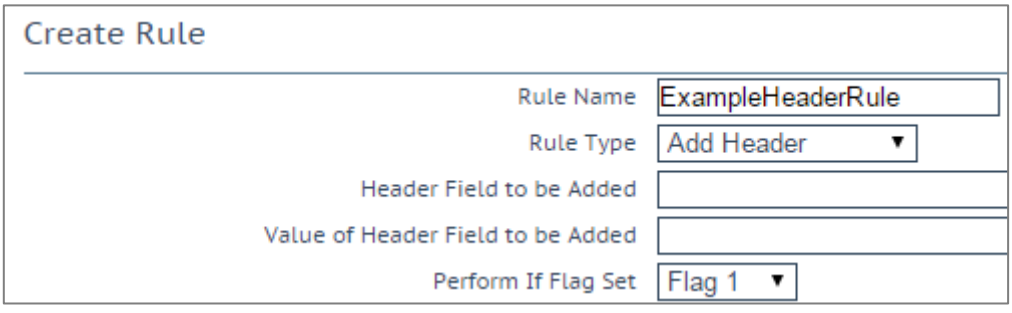
Set Flag If Matched（マッチ時にフラグをセット）

このルールにマッチすると、指定したフラグをセットします。

[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、KEMP ドキュメントページの「Content Rules, Feature Description」を参照してください。

8.1.3 ヘッダの追加

[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。



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（追加するヘッダフィールド）

追加するヘッダ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（追加するヘッダフィールドの値）

ヘッダ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。255 文字まで入力できます。

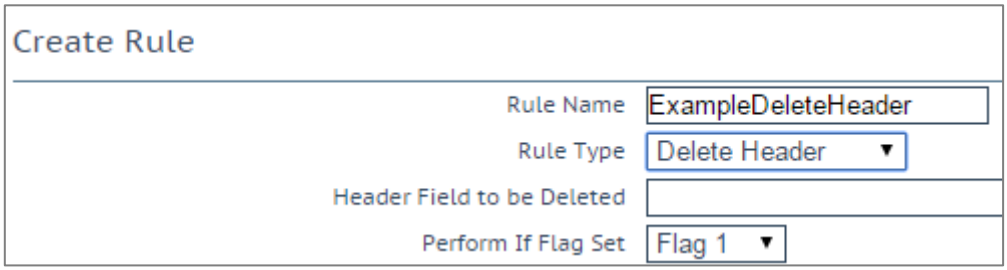
Perform If Flag Set（フラグセット時に実行）

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を実行します。

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コンテンツ マッチセクションを参照してください。

8.1.4 ヘッダの削除

[Rule Type] で[Delete Heade] を選択したときのオプションを以下に示します。



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（削除するヘッダフィールド）

削除するヘッダ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。

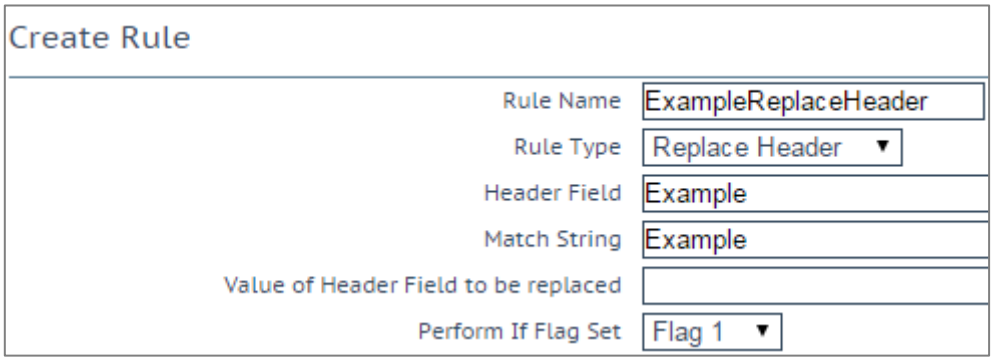
Perform If Flag Set（フラグセット時に実行）

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を実行します。

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コンテンツ マッチセクションを参照してください。

8.1.5 ヘッダの置換

[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。



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（ヘッダフィールド）

置換するヘッダ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（置換するヘッダフィールドの値）

置換するヘッダ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。

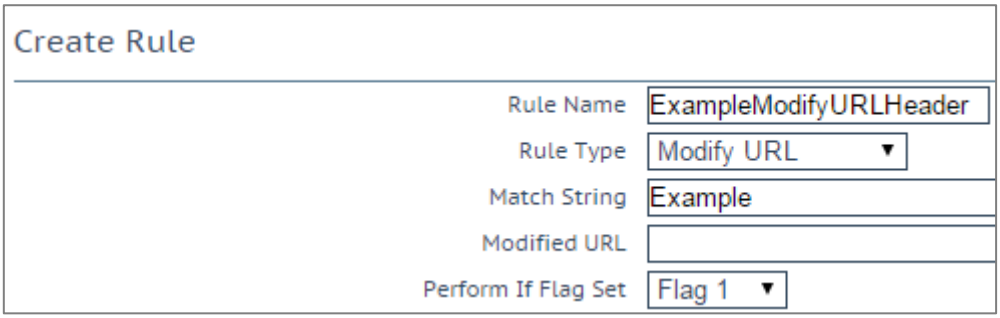
Perform If Flag Set（フラグセット時に実行）

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を実行します。

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コンテンツ マッチセクションを参照してください。

8.1.6 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。



Rule Name（ルール名）

ルールの名前を入力する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。

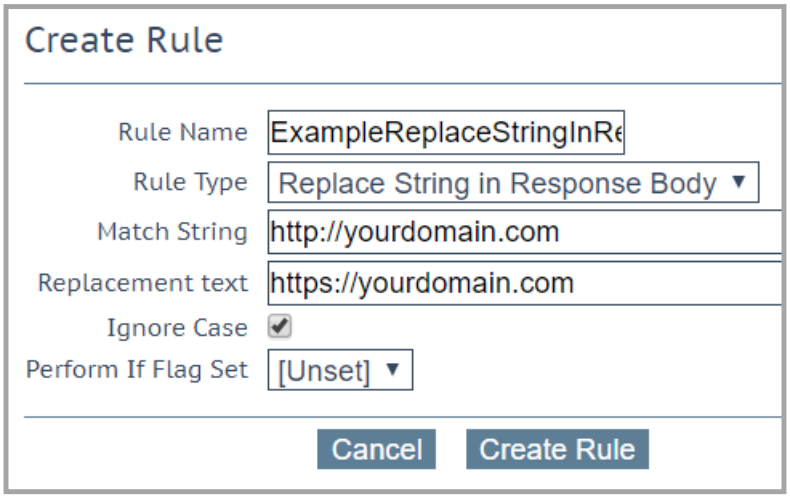
Perform If Flag Set（フラグセット時に実行）

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を実行します。

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コンテンツ マッチセクションを参照してください。

8.1.7 レスポンス ボディ文字列の変更

[Rule Type] で[Replace String in Response Body] はレスポンス ボディの文字列の変更ができ、次のオプションを使用できます。



Rule Name（ルール名）

ルール名を入力するテキストボックスです。ユニークな名称が必要です。

Match String（マッチ文字列）

マッチする文字れるです。

Replacement text（置き換え文字列）

変更する文字列です。

Ignore Case（大文字小文字の無視）

このチェックボックスを有効にすると比較文字列の大文字/小文字を無視します。

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を実行します。

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コンテンツ マッチセクションを参照してください。

8.1.8 ヘッダの変更

ヘッダの変更の詳細については、KEMP ドキュメントページの「Header Modification Guide, Technical Note」を参照してください。

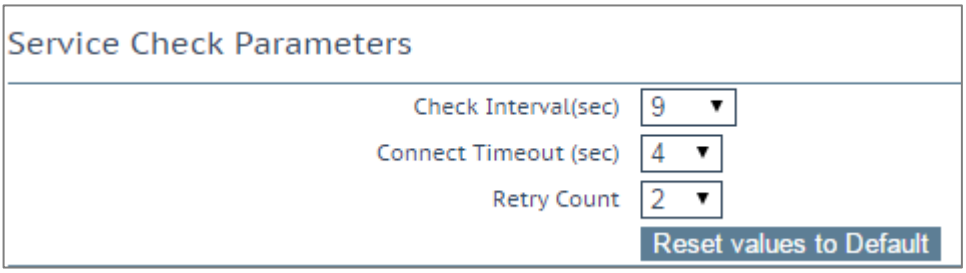
8.2 チェック用パラメータ

「Check Parameters」画面にアクセスするには、LoadMaster WUI のメインメニューから >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、バーチャルサービスで選択した[Scheduling Method（スケジュール方式）] に応じて[Adaptive Parameters] か[SDN Adaptive Parameter] のいずれかのセクションを表示します。[Scheduling Method] が[resource based (adaptive)] に設定している場合、[Adaptive Parameters] の入力セクションを表示します。[Scheduling Method] が[resource based (SDN adaptive)] に設定している場合、[SDN Adaptive Parameters] 入力セクションを表示します。

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 ヘルスチェック パラメータ

LoadMaster は、リアルサーバとバーチャルサービスの可用性を監視するために、レイヤ 3、レイヤ 4、レイヤ 7 のヘルスチェックを行います。



Check Interval(sec)（チェック インターバル（秒））

このフィールドは、連続したチェックのインターバル時間を秒数で指定します。

推奨値は 9 秒で、LoadMaster のデフォルト値です。値の範囲は、9 秒（最小値）から 901 秒（最大値）までです。

ここで求められる最小値は、リトライ回数（2 回）× 接続タイムアウト（4 秒）＋ 1 で、デフォルトの 9 秒になります。最大値は、リトライ回数（15 回）× 接続タイムアウト（60 秒）＋ 1 で、901 秒になります。

WUI では、チェック インターバルに 120 を超える値を設定する場合、他の 2 つのオプションを先に設定します。それ以外の場合、インターバルを設定できる最大値は 120 です。

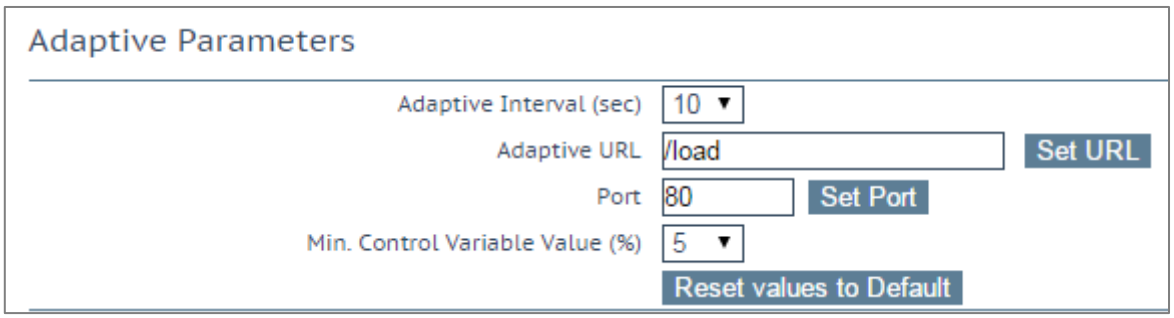
Connect Timeout (sec)（接続タイムアウト（秒））

HTTP リクエストには 2 つのフェーズがあります。1.サーバへの接続と 2.ファイルを取得です。 タイムアウトは各フェーズごとに指定できます。デフォルト値は 4 秒で、有効な値の範囲は 4～60 です。

Retry Count（リトライ回数）

サーバが機能していないと判断するために、チェックを試行する回数を指定します。デフォルト値は 2 回で、有効な値の範囲は 2～15 です。

8.2.2 アダプティブ パラメータ



Adaptive Interval (sec)（インターバル（秒））

これは、LoadMaster がリアルサーバの負荷をチェックする間隔（秒）です。この値が低いほど、LoadMaster は負荷に対して敏感になりますが、LoadMaster 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から取得します。この URL は、サーバ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、サーバの負荷が高くなると）、LoadMaster はそのサーバに渡すトラフィックを減らします。これにより、サーバの負荷が「適応制御」されます。

サーバの負荷が 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。

アダプティブ方式でチェックするすべてのサーバは、URL を同じにする必要があります。

この機能は、HTTP ベースのバーチャル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、リアルサーバ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。

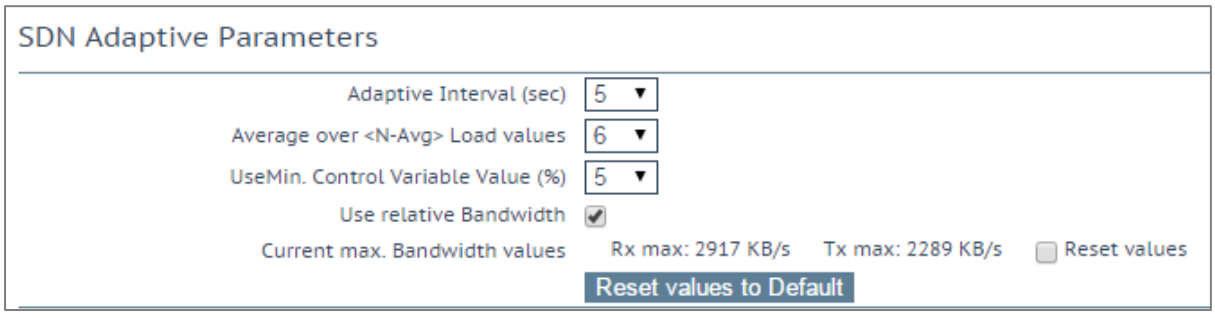
Port（ポート）

LoadMaster が、リアルサーバの負荷値を 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 (%)（最小の負荷制御バリュー（%））

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ための閾値です。負荷がこの閾値未満になると、ロードバランサーは重み付けを用いたスケジューリング方式（通常は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 アダプティブ パラメータ



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、リアルサーバ負荷の値を得るために SDN コントローラをポーリングします。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（アダプティブ値はリアルサーバの「Statistics」画面に表示します）。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します。

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

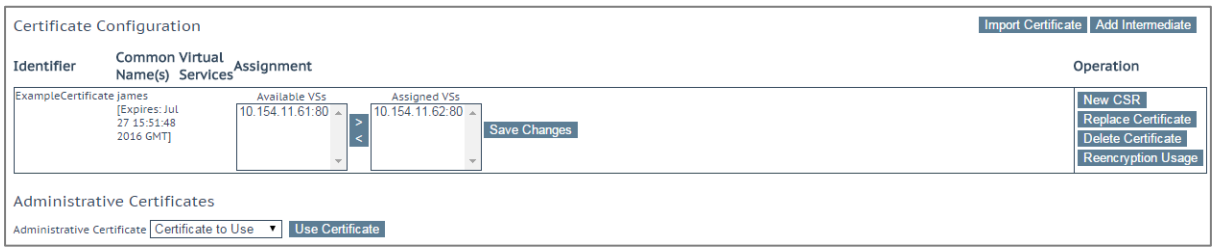
このセクションでは、LoadMaster WUI の「Certificates & Security」画面について説明します。

9.1 SSL 証明書

SSL 証明書の画面は、HSM（ハードウェアセキュリティモジュール）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、KEMP ドキュメントページの「Hardware Security Module (HSM), Feature Description」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 がイネーブルでない



上図は、SSL 証明書の管理画面を示しています。

Import Certificate —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「中間証明書」セクション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) — サイトの完全修飾ドメイン名（FQDN）。
Virtual Services — 証明書が関連付けられるバーチャルサービス。
Assignment — 割り当てられた利用可能なバーチャルサービスのリスト
Operations（操作） —

- **New 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、「CSR 生成」セクションを参照してください。

- **Replace Certificate :** 導入済み証明書のアップデイト、入替えが行えます。
- **Delete Certificate :** 対象となる証明書を削除します。
- **Reencryption Usage :** 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バーチャル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 がイネーブル

秘密鍵識別子（Private Key Identifier）

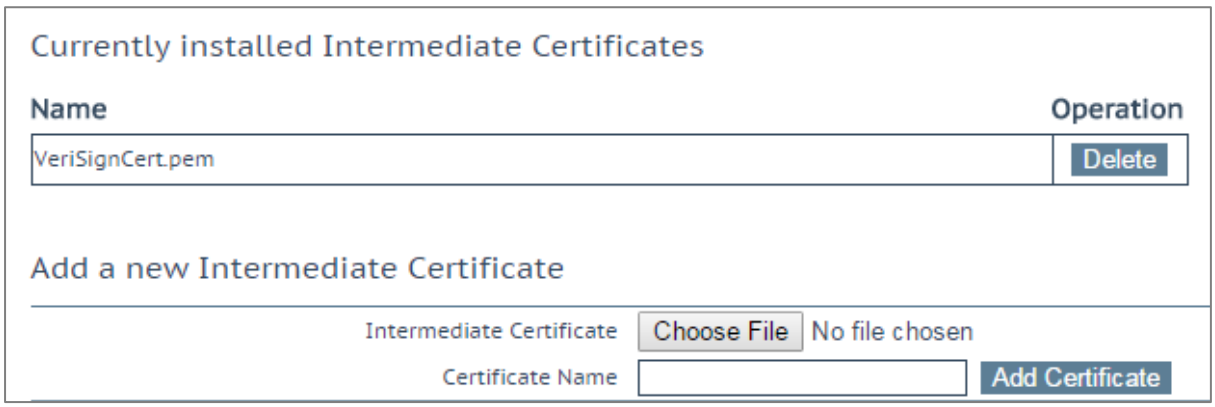
HSM が有効のとき、[Generate CSR] オプションは、LoadMaster のメインメニューから「Manage Certificates」画面に移動します。

識別可能な LoadMaster の秘密鍵名を入力し、[Generate CSR] をクリックします。「CSR 生成」画面のフィールドは、[Use 2048 bit key] がないことを除き、「CSR 生成」セクションで説明した内容と同じです。

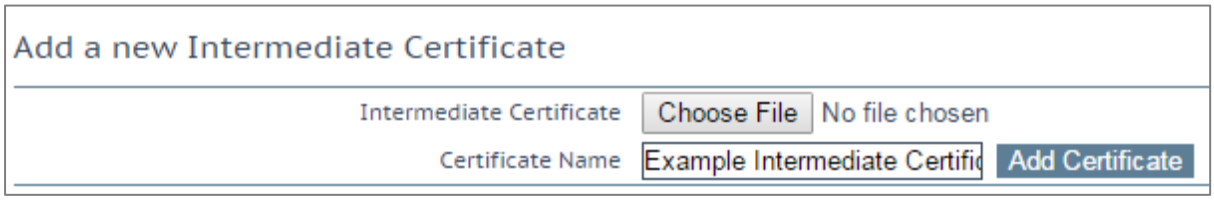
Add Intermediate — 詳細は「中間証明書」セクションを参照してください。
Private Key — この列には秘密鍵名が表示されます。
Common Name(s) — サイトの FQDN（完全修飾ドメイン名）。
Virtual Services — 証明書が関連付けられるバーチャルサービス。
Assignment — 割り当てられた利用可能なバーチャルサービスのリスト
Operations（操作） —

- **Import Certificate :** 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 :** 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を表示します。

9.2 中間証明書



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。

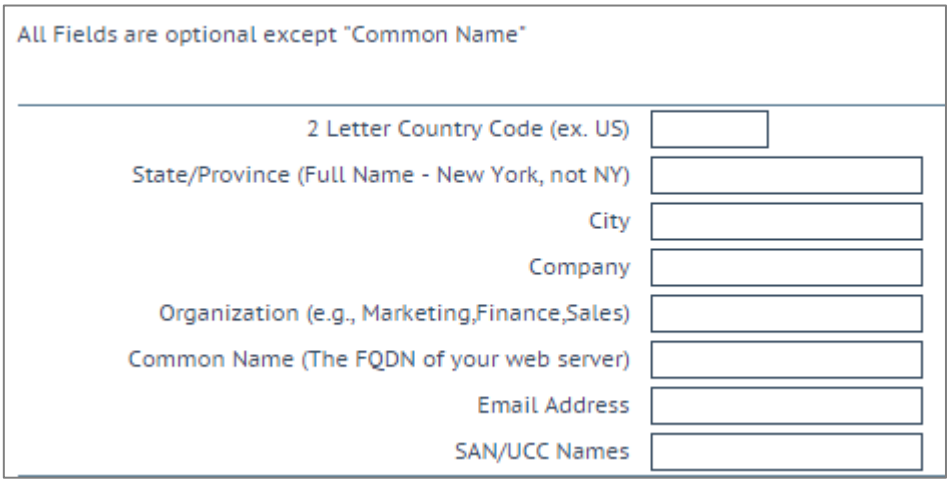


すでに証明書を持っている場合、または CSR からすでに証明書を受け取っている場合、[Choose File] をクリックして証明書をインストールできます。証明書を選択して、[Certificate Name] に目的の名前を入力します。この名前には、アルファベット文字しか使用できません。また、最大 32 文字という制限があります。

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中間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。

9.3 CSR の生成

証明書が存在しない場合は、「Certificate Signing Request（CSR）」画面から必要な情報を入力して、[Create CSR] ボタンをクリックします。LoadMaster によって生成される CSR は SHA256 を使用します。



2 Letter Country Code (ex. US)（2 文字国名コード）

証明書に含める 2 文字国コードです。日本であれば「JP」と入力します。

State/Province (Entire Name – New York, not NY)（州/行政地域名）

証明書に含める州名です。日本では県名の入力が一般的です。略さずに入力します。

City（都市名）

証明書に含める都市名です。

Company（企業名）

証明書に含める企業名です。

Organization (e.g., Marketing,Finance,Sales)（組織名）

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）

サービス提供のためのドメイン名（FQDN）です。

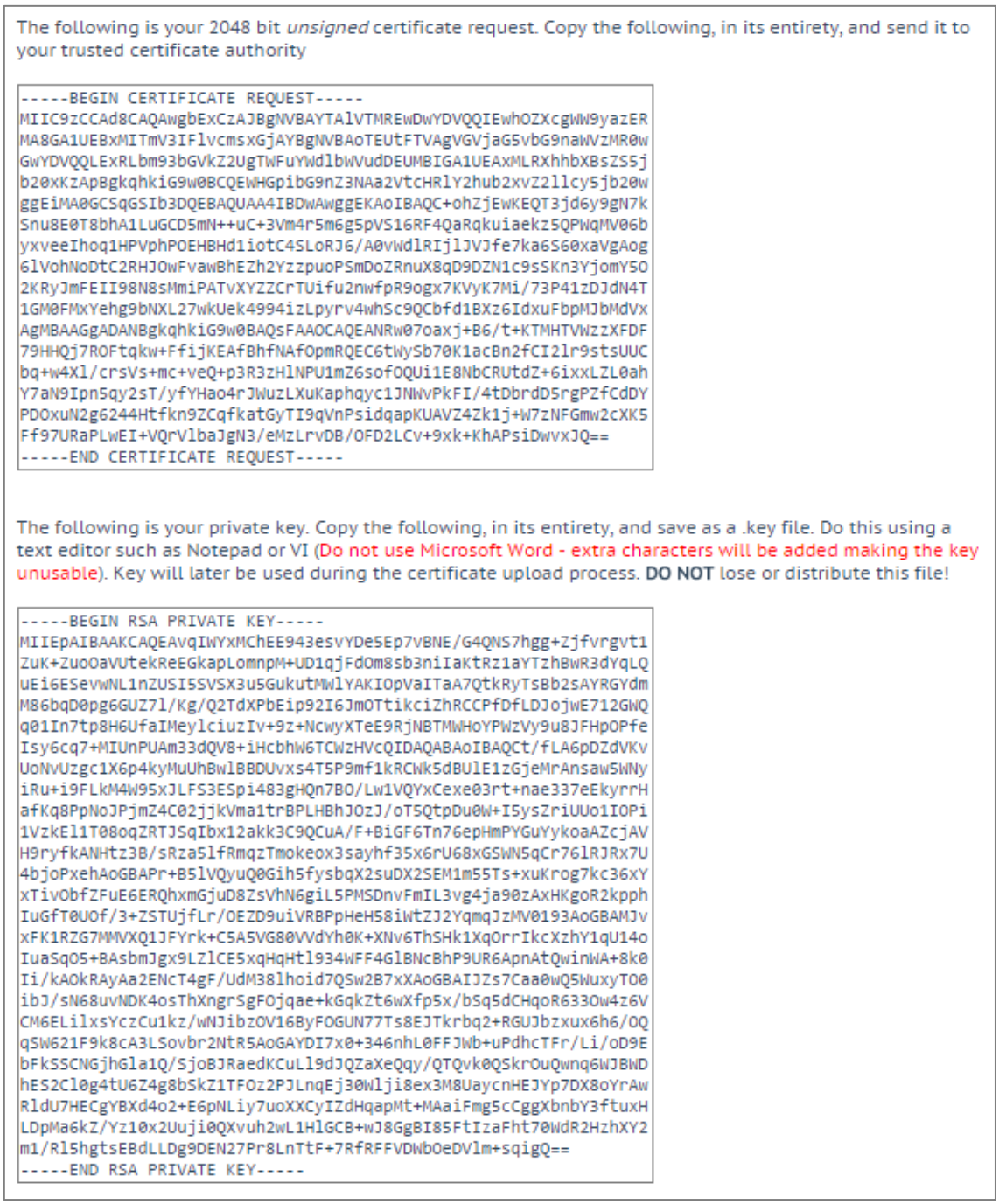
Email Address（E メールアドレス）

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、次の画面を表示します。



The following is your 2048 bit *unsigned* certificate request. Copy the following, in its entirety, and send it to your trusted certificate authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9zCCAd8CAQAwgbExCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazER
MA8GA1UEBxMITmV3IFlvcmsxGjAYBgNVBAoTEUtFTVAgVGVjaG5vbG9naWVzMR0w
GwYDVQQLExRLbm93bGVkZ2UgTWFuYWdlbWVudDEUMBIGA1UEAxMLRXhhbXBsZS5j
b20xKzApBgkqhkiG9w0BCQEWHGpibG9nZ3NAa2VtcHRlY2hub2xvZ2llcy5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+ohZjEwKEQT3jd6y9gN7k
Snu8E0T8bhA1LuGCD5mN++uC+3Vm4r5m6g5pVS16RF4QaRqkuiaekz5QPWqMV06b
yxveeIhoq1HPVphPOEHBHd1iotC4SLoRJ6/A0vWdlRIjlJVJfe7ka6S60xaVgAog
6lVohNoDtC2RHJOwFvawBhEZh2YzzpuoPSmDoZRnuX8qD9DZN1c9sSKn3YjomY5O
2KRyJmFEII98N8sMmiPATvXYZZCrTUifu2nwfpR9ogx7KVyK7Mi/73P41zDJdN4T
1GM0FMxYehg9bNXL27wkUek4994izLpyrv4whSc9QCbfd1BXz6IdxuFbpMJbMdVx
AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEANRw07oaxj+B6/t+KTMHTVWzzXFDF
79HHQj7ROFtqkw+FfijKEAfBhfNAfOpmRQEC6tWySb70K1acBn2fCI2lr9stsUUC
bq+w4Xl/crsVs+mc+veQ+p3R3zHlNPU1mZ6sofOQUi1E8NbCRUtdZ+6ixxLZL0ah
Y7aN9Ipn5qy2sT/yfYHao4rJWuzLXuKaphqyc1JNWvPkFI/4tDbrdD5rgPZfCdDY
PDOxuN2g6244Htfkn9ZCqfkatGyTI9qVnPsidqapKUAVZ4Zk1j+W7zNFGmw2cXK5
Ff97URaPLwEI+VQrVlbaJgN3/eMzLrvDB/OFD2LCv+9xk+KhAPsiDwvxJQ==
-----END CERTIFICATE REQUEST-----
```

The following is your private key. Copy the following, in its entirety, and save as a .key file. Do this using a text editor such as Notepad or VI (Do not use Microsoft Word - extra characters will be added making the key unusable). Key will later be used during the certificate upload process. **DO NOT** lose or distribute this file!

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvqIWYxMChEE943esvYDe5Ep7vBNE/G4QNS7hgg+Zjfvrgvt1
ZuK+ZuoOaVUtekReEGkapLomnpM+UD1qjFdOm8sb3niIaKtRz1aYTzhBwR3dYqLQ
uEi6ESevwNL1nZUSI5SVSX3u5GukutMWlYAKIOpVaITaA7QtkRyTsBb2sAYRGYdm
M86bqD0pg6GUZ7l/Kg/Q2TdXPbEip92I6JmOTtikciZhRCCPfDfLDJojwE712GWQ
q01In7tp8H6UfaIMeylciuzIv+9z+NcwyXTeE9RjNBTMWHoYPWzVy9u8JFHpOPfe
Isy6cq7+MIUnPUAm33dQV8+iHcbhW6TCWzHVcQIDAQABAoIBAQCt/fLA6pDZdVKv
UoNvUzgc1X6p4kyMuUhBwlBBDUvxs4T5P9mf1kRCWk5dBUlE1zGjeMrAnsaw5WNy
iRu+i9FLkM4W95xJLFS3ESpi483gHQn7BO/Lw1VQYxCexe03rt+nae337eEkyrrH
afKq8PpNoJPjmZ4C02jjkVma1trBPLHBhJOzJ/oT5QtpDu0W+I5ysZriUUo1IOPi
1VzkEl1T08oqZRTJSqIbx12akk3C9QCuA/F+BiGF6Tn76epHmPYGuYykoaAZcjAV
H9ryfkANHtz3B/sRza5lfRmqzTmokeox3sayhf35x6rU68xGSWN5qCr76lRJRx7U
4bjoPxehAoGBAPr+B5lVQyuQ0Gih5fysbqX2suDX2SEM1m55Ts+xuKrog7kc36xY
xTivObfZFuE6ERQhxmGjuD8ZsVhN6giL5PMSDnvFmIL3vg4ja90zAxHKgoR2kpph
IuGfT0UOf/3+ZSTUjfLr/OEZD9uiVRBPpHeH58iWtZJ2YqmqJzMV0193AoGBAMJv
xFK1RZG7MMVXQ1JFYrk+C5A5VG80VVdYh0K+XNv6ThSHk1XqOrrIkcXzhY1qU14o
IuaSqO5+BAsbmJgx9LZlCE5xqHqHtl934WFF4GlBNcBhP9UR6ApnAtQwinWA+8k0
Ii/kAOkRAyAa2ENcT4gF/UdM38lhoid7QSw2B7xXAoGBAIJZs7Caa0wQ5WuxyTO0
ibJ/sN68uvNDK4osThXngrSgFOjqae+kGqkZt6wXfp5x/bSq5dCHqoR633Ow4z6V
CM6ELilxsYczCu1kz/wNJibzOV16ByFOGUN77Ts8EJTkrbq2+RGUJbzxux6h6/OQ
qSW621F9k8cA3LSovbr2NtR5AoGAYDI7x0+346nhL0FFJWb+uPdhcTFr/Li/oD9E
bFkSSCNGjhGla1Q/SjoBJRaedKCuLl9dJQZaXeQqy/QTQvk0QSkrOuQwnq6WJBWD
hES2Cl0g4tU6Z4g8bSkZ1TFOz2PJLnqEj30Wlji8ex3M8UaycnHEJYp7DX8oYrAw
RldU7HECgYBXd4o2+E6pNLiy7uoXXCyIZdHqapMt+MAaiFmg5cCggXbnbY3ftuxH
LDpMa6kZ/Yz10x2Uuji0QXvuh2wL1HlGCB+wJ8GgBI85FtIzaFht70WdR2HzhXY2
m1/Rl5hgtsEBdLLDg9DEN27Pr8LnTtF+7RfRFFVDWbOeDVlm+sqigQ==
-----END RSA PRIVATE KEY-----
```

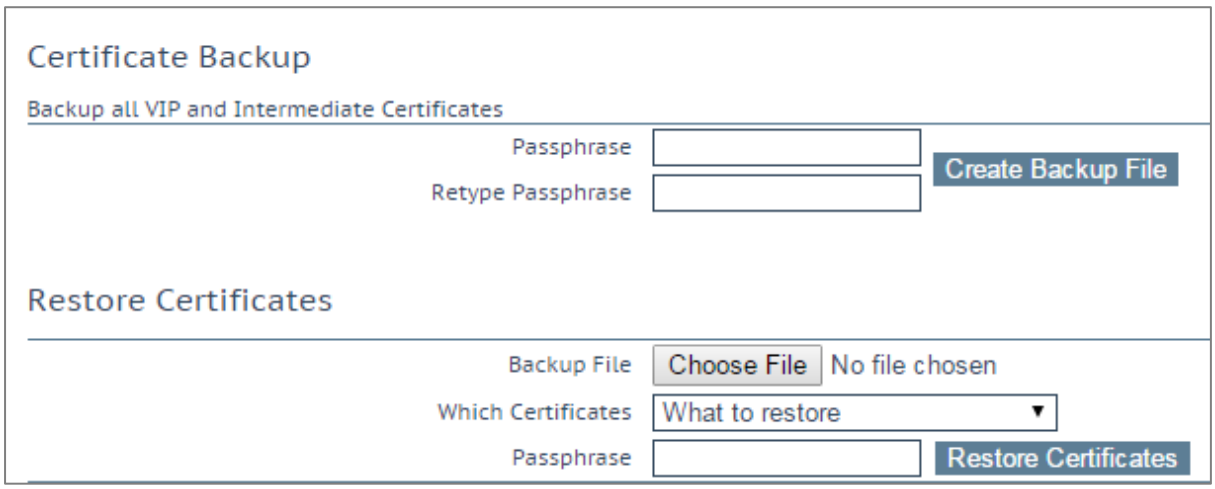
上部のボックスの文字列は、プレーンテキストファイルに貼り付けて、CA（認証局）に送信します。認証局は情報を検証して署名した証明書を返します。

下部のボックスは秘密鍵ですので、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しますが、他に公開してはいけません。秘密鍵は、プレーンテキストファイルにコピーし安全な場所で保管してください。Microsoft Word などのアプリケーションは使わないでください。

9.4 証明書のバックアップとリストア

この画面は、HSM が有効かどうかにより異なります。LoadMaster 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 がイネーブルでない



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 : 証明書のバックアップファイルを選択します
Which Certificates : リストアする証明書を選択します
Passphrase : 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ワードを入力します

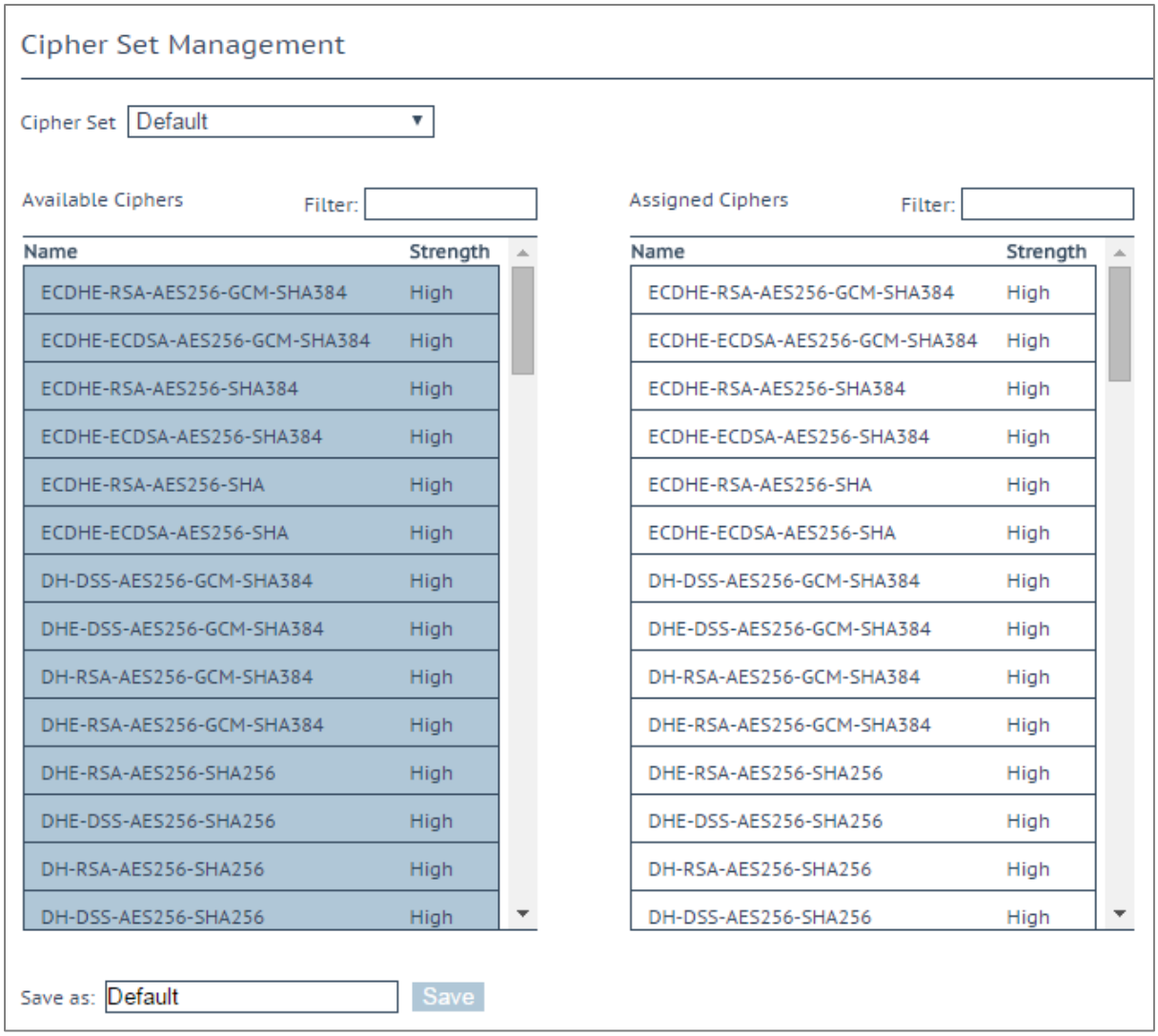
9.4.2 HSM が有効な場合

Backup Intermediate Certificates : 証明書をバックアップするときに、必須のパスフレーズを 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を選択します
Passphrase : 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ワードを入力します

9.5 Cipher の選択



Cipher セットの管理

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：**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。「管理用 WUI へのアクセス」セクション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 :** OpenSSL が更新される前の古い LoadMaster 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。

LoadMaster 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、KEMP ドキュメントページの「SL Accelerated Services, Feature Description」を参照してください。

KEMP Technologies では、最新の可用情報を元に、必要に応じて暗号セットを変更します。

[Available Ciphers] （利用可能な暗号）と[Assigned Ciphers] （割り当てられた暗号）の 2 つのリストを表示します。画面にある[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] と[Assigned] リストに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。

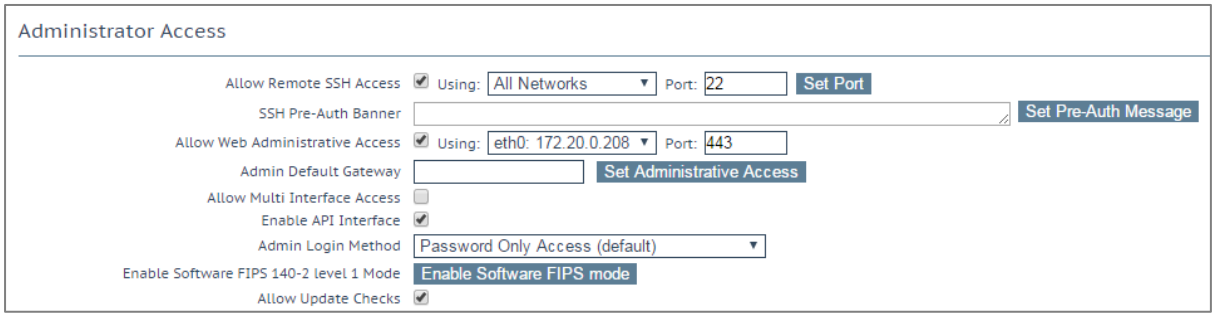
設定済みの暗号セットに対する変更は行えません。ただし、設定済みの暗号セットをベースにして必要な変更を行い、その暗号セットを新しいカスタム名で保存することができます。[Save as] テキストボックスに新しい名前を入力し、[Save] ボタンをクリックします。カスタム暗号セットは、複数のバーチャルサービスで使用することができます。また、WUI の暗号セットとして割り当てることができます。

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。

9.6 リモートアクセス

このセクションでは、LoadMaster WUI の「Remote Access」画面の各種エリアについて説明します。

9.6.1 アドミニストレータのアクセス



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 LoadMaster 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」ユーザのパスワードを設定していない場合は、SSH 接続を介したログインはできません。

Using（使用）

管理用 SSH のリモートアクセスを許可するアドレスを指定します。

Port（ポート）

管理用 SSH のリモートアクセスを許可するポートを指定します。

SSH Pre-Auth Banner（SSH 事前認証バナー）

SSH 事前認証の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 管理用アクセスの許可）

このチェックボックスをオンにすると、LoadMaster 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] 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。

Using（使用）

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] 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] をクリックします。

Admin Default Gateway（アドミン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] 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）

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を表示します。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した[Additional addresses] の IP 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] 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。証明書の詳細は、KEMP ドキュメントページの SSL Accelerated Services 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 個のアドレスをリスンします。

RADIUS Server（RADIUS サーバ）

ここでは、LoadMaster へのユーザアクセスの認証に使用する RADIUS サーバのアドレスを入力できます。RADIUS サーバを使用するには[Shared Secret] （シェアード シークレット）を指定します。

シェアード シークレットは、LoadMaster と RADIUS サーバの間で共通鍵として使用する文字列のことです。

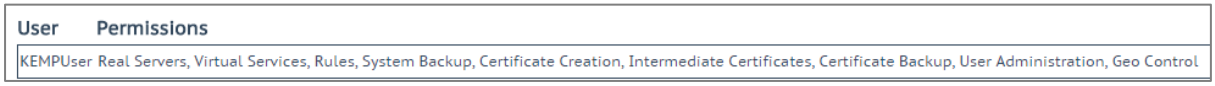
[Revalidation Interval] で、RADIUS サーバがユーザを再認証する頻度を指定します。

RADIUS Server Configuration（RADIUS サーバの設定）

LoadMaster とともに RADIUS が正しく機能するよう設定するには、RADIUS サーバに認証情報を設定し、RADIUS の応答メッセージを LoadMaster 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、LoadMaster の権限と**エラー! 参照元が見つかりません。**のように対応しています。

応答メッセージ	LoadMaster の権限
real	リアルサーバ
vs	Virtual Services（バーチャルサービス）
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（中間証明書）
certbackup	証明書のバックアップ
users	ユーザの管理
geo	OCSP の設定

応答メッセージの値は、[All Permissions] を除き、図のように WUI のユーザ権限のページと対応させる必要があります。



Linux 版の FreeRADIUS サーバを設定する場合、「/etc/freeradius/users」で指定したセクションに、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」に LoadMaster の IP アドレスを含める設定をします。このファイルには、RADIUS に接続可能な IP アドレスの一覧が含まれます。

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 サーバを設定する方法については、KEMP ドキュメントページの「the WUI Authentication and Authorization section」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 API（アプリケーションプログラム インターフェイス）を有効にします。

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、「管理用 WUI へのアクセス」セクションまたは、KEMP ドキュメントページの「User Management, Feature Description」を参照してください。

LoadMasterWUI 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) :** このオプションを選択すると、ユーザ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 :** ユーザは、ユーザ名/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、LoadMaster はその証明書が一致するかチェックします。LoadMaster 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 SAN（サブジェクト代替名）もしくは CN（コモンネーム）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、ユーザはその LoadMaster へのアクセスを許可されます。この動作は、API とユーザ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、LoadMaster は、ユーザ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に要求します。
- **Client certificate required :** 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 ユーザのみ SSH 経由でログイン可能）。
- **Client certificate required :** [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 サーバを設定する必要があります。OCSP サーバの設定に関する詳細は、KEMP ドキュメントページの「the Cipher Sets section」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 LoadMaster にログインすることはできません。ただし、bal 以外のユーザを作成し、そのユーザに[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ません（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 認証に関する詳細は、KEMP ドキュメントページの「User Management, Feature Description」を参照してください。

Enable Software FIPS 140-2 level 1 Mode（FIPS 140-2 レベル 1 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、「管理用 WUI のアクセス」セクションを参照してください。

この LoadMaster 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 LoadMaster 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。LoadMaster で FIPS を有効にすると、FIPS を無効にできません。LoadMaster 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。

LoadMaster が FIPS レベル 1 モードになっている場合、LoadMasterWUI の右上に「FIPS-1」と表示します。

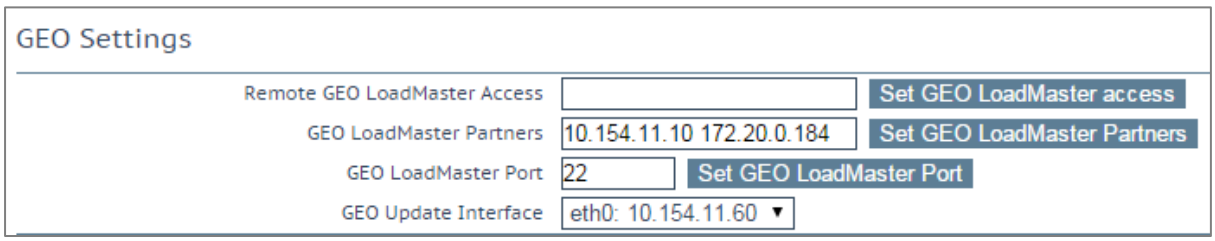
FIPS レベル 1 では、非 FIPS LoadMaster とは異なる暗号セットを持っています。[Default] の暗号セットが用意されていますが、これ以外のシステム定義の暗号セットを選択することはできません。

FIPS を有効にすると、RADIUS での認証ができなくなります。

Allow Update Checks（アップデイ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 LoadMaster 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



Remote GEO LoadMaster Access（GEO LoadMaster 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 LoadMaster パートナー）

GSLB パックを含む GEO 機能は、LoadMaster 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 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ります。
FXC 株式会社の担当窓口にお問い合わせください。

パートナーGEO LoadMaster 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 LoadMaster は、DNS 設定と同期します。

GEO LoadMaster の連携を設定する前に、正しい設定、または推奨の設定を行った GEO LoadMaster をバックアップする必要があります。そして、このバックアップは、この LoadMaster のパートナーとなる別の LoadMaster に保存する必要があります。詳細と手順は、KEMP ドキュメントページの「GEO, Feature Description」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。

GEO LoadMaster Port（GEO LoadMaster のポート）

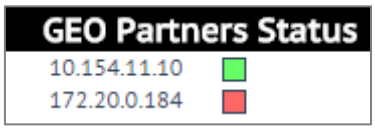
GEO LoadMaster がこの LoadMaster ユニットと通信するために使用するポートです。

GEO update interface（GEO 更新インターフェイス）

SSH 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。 これは GEO パートナーが通信するためのインターフェイスです。

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。



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。

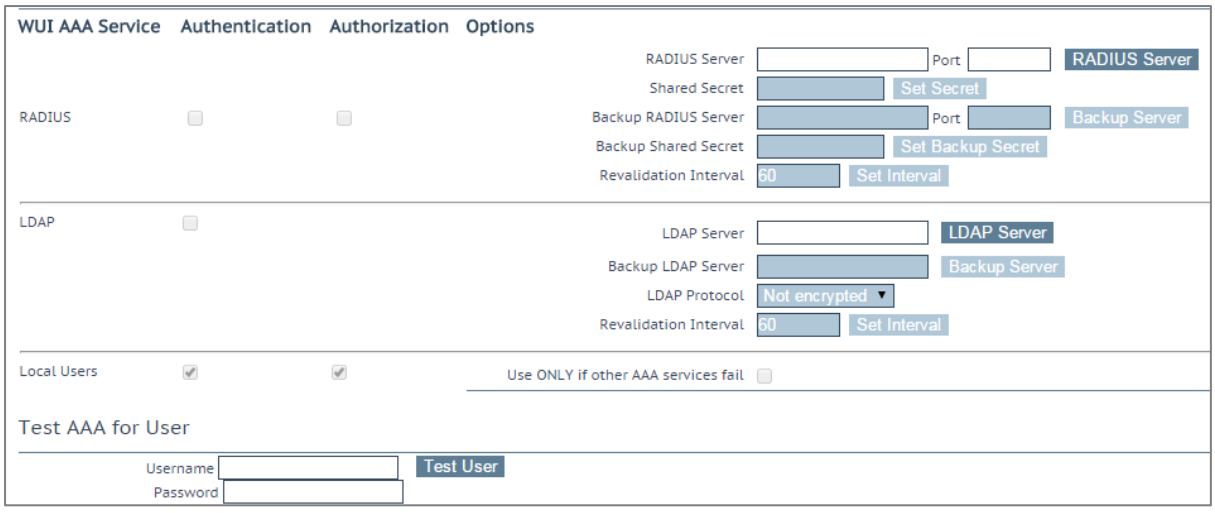
GEO パートナーの赤のステータスは、LoadMaster が通信できないことを示しています。原因のひとつとして、いずれかのパートナーの電源がオフになっていることが考えられます。この場合、停電が発生しているか、ケーブルが接続されていない可能性があります。

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をログに出力します。このメッセージには、そのパートナーの IP アドレスが含まれます。

9.6.4 WUI の認証と権限設定

WUI Authorization Options（WUI の権限設定オプション）

「Remote Access」画面の[WUI Authorization Options]ボタンをクリックすると、「WUI Authentication and Authorization」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。



「WUI Authentication and Authorization」画面では、ログイン認証と権限の許可設定に関するオプションを管理できます。

Authentication（認証）

ユーザは、LoadMaster にログインする前に認証を受ける必要があります。LoadMaster では、ローカルユーザの認証方式の他に、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、LoadMaster は以下の順序でユーザ認証を試みます。

1. RADIUS
2. LDAP
3. ローカルユーザ

例えば、RADIUS サーバを利用できない場合、LDAP サーバが使用されます。LDAP サーバも利用できない場合は、ローカルユーザ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の認証方式が選択されます。

Authorization（権限設定）

LoadMaster では、RADIUS またはローカルユーザ認証でユーザ権限を設定できます。ユーザ権限の設定では、ユーザが LoadMaster 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、LoadMaster 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、LoadMaster は、ローカルユーザ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 ユーザは常に、ローカルユーザ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 サーバの設定）

- **RADIUS Server（RADIUS サーバ）**
  WUI から LoadMaster へアクセスするユーザの認証に使う RADIUS サーバのアドレスとポート番号を入力します。
- **Shared Secret（シェアード シークレット）**
  RADIUS サーバの共有秘密鍵を入力します。
  シェアード シークレットとは、LoadMaster と RADIUS サーバ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）**
  WUI から LoadMaster へアクセスするユーザの認証に使うバックアップ用 RADIUS サーバのアドレスとポート番号を入力します。このサーバは、メインの RADIUS サーバが故障したときに使用します。
- **Backup Shared Secret（バックアップ用シェアード シークレット）**
  このテキストボックスには、バックアップ RADUS サーバのシェアード シークレットを入力します。
- **Revalidation Interval（再認証インターバル）**
  RADIUS サーバがユーザを再認証する頻度を指定します。

LDAP Endpoint（LDAP エンドポイント）

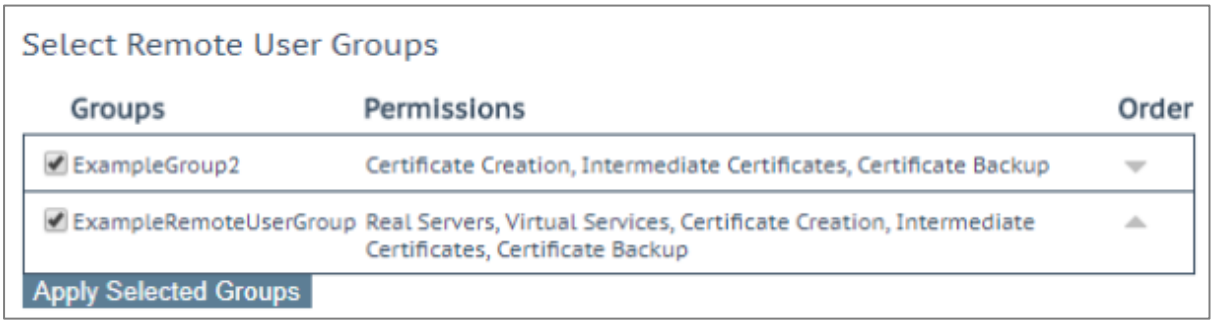
関連する LDAP エンドポイントを選択します。[Manage LDAP Configuration] ボタンをクリックすると「LDAP Configuration」画面に移ります。LDAP エンドポイントに関する詳細は、LDAP 設定を参照してください。

クライアントユーザがクライアント証明書で認証されている場合、CN（コモンネーム）は小文字になります。このためアクセス権許可に関連して、パスワードを持たないローカルユーザ エントリも小文字でなければなりません。

Remote User Groups（リモートユーザ グループ）

選択しているリモートユーザ グループを表示します。選択、クリア、グループのオーダは[Select Groups] をクリックします。

グループの選択とその適応が重要です。グループを選択していない場合は、グループチェックが実施できずリモートユーザはグループチェックなしにログインができてしまいます。



この画面で表示するグループは、>System Configuration >System Administration >User Management で設定したリモートユーザ グループの内容です。

詳細情報はユーザの管理を参照してください。

ユーザログインの際、以下の条件が一致した場合に、アクティブ ディレクトリ上のユーザグループのチェックを実施します。

- WUI の LDAP 認証が有効な場合
- グループリストを定義している場合
- ログインユーザがローカルで定義していないか[Local Users] オプションが無効の場合

この画面でグループの順序を変更できます。チェックは最初のグループから行います。最初のグループで一致するとアクセスが有効になり、それ以上のチェックは行いません。ユーザアクセスは一致するグループがない場合は、ユーザアクセスは行われず、対応したメッセージを Syslog に記録します。グループチェックでログインしたユーザには、一致したグループの権限が与えられます。

Nested Groups（グループのネスト）

ユーザネストグループのイネーブル/ディセーブルは、「WUI Authentication and Authorization」画面の[Nested groups] チェックボックスで行います。

Domain（ドメイン）

グループでの WUI 認証を使用するとき、ユーザ名にドメインを設定していない場合にドメインを定義することができます。「prefix¥username」形式で Wiondows にログインする場合、常にこのドメインでグループ検索を行います。

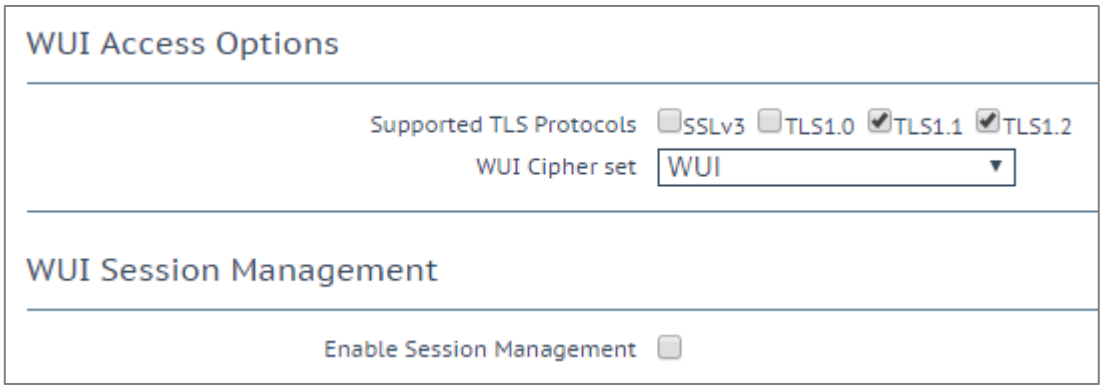
ドメインフィールドはグループを設定しているときだけ表示します。

Local Users Configuration（ローカルユーザの設定）

- **Use ONLY if other AAA services fail（AAA サービス失敗時の使用）**
  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に、ローカルユーザの認証/権限設定方式を使用します。

- **Test AAA for User（ユーザの AAA をテスト）**
  ユーザの資格情報をテストするには、「Username」と「Password」フィールドに、テストするユーザのユーザ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、ユーザの認証情報をチェックできます。

9.7 管理用 WUI のアクセス



Supported TLS Protocols（サポートする TLS プロトコル）

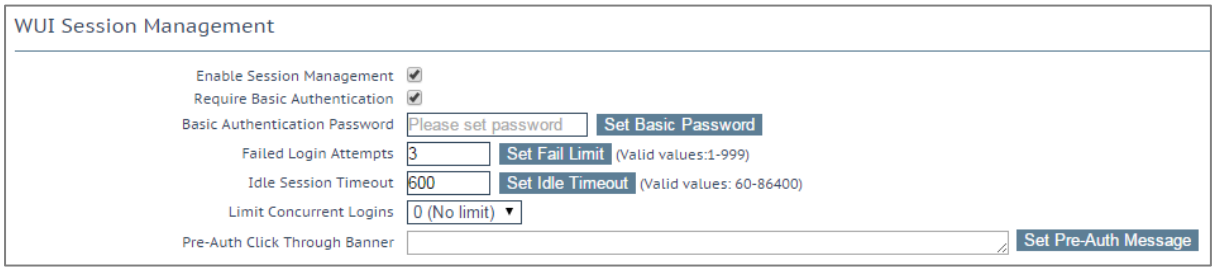
ここでは、SSLv3、TLS1.0、TLS1.1、TLS1.2 のプロトコルを用いて LoadMaster に接続できるかどうかを指定するためのチェックボックスが用意されています。TLS1.1 と TLS1.2 はデフォルトで有効になっています。SSLv3 は一部の古いブラウザでしかサポートされていないため、SSLv3 だけを選択することは推奨されません。Web ブラウザから WUI に接続する場合、ブラウザと WUI の両方で相互にサポートされている最もセキュリティの高いプロトコルが使用されます。

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、「Cipher 選択」セクションを参照してください。

WUI Session Management（WUI セッション管理）



ファームウェアバージョン 7.1.35 以降の LoadMaster は、初期状態では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。

コントロール	bal ユーザ	全権限を持つユーザ	管理権限を持つユーザ	その他のユーザ
Session Management	変更化	表示のみ	表示のみ	なし
Require Basic Authentication	変更化	表示のみ	表示のみ	なし
Basic Authentication Password	変更化	表示のみ	表示のみ	なし
Failed Login Attempts	変更化	変更化	表示のみ	なし
Idle Session Timeout	変更化	変更化	表示のみ	なし
Limit Concurrent Logins	変更化	変更化	表示のみ	—
Pre-Auth Click Through Banner	変更化	変更化	表示のみ	なし
Currently Active Users	変更化	変更化	表示のみ	なし
Currently Blocked Users	変更化	変更化	表示のみ	なし

WUI セッション管理を使用する場合、2 段階認証を使用できます。

[Enable Session Management] チェックボックスがオンになっており、[Require Basic Authentication] が無効になっている場合、ユーザはローカルのユーザ名とパスワードでログインできます。「bal」や「user」を使用してのログインは求められません。

[Enable Session Management] と[Require Basic Authentication] のチェックボックスが両方ともオンになっている場合、LoadMaster 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名です）。

「user」（ユーザ権限）は、管理者権限である「bal」の証明書ではなく「user」の証明書を提供できるようにするためです。「user」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 アカウントのみ設定できます。

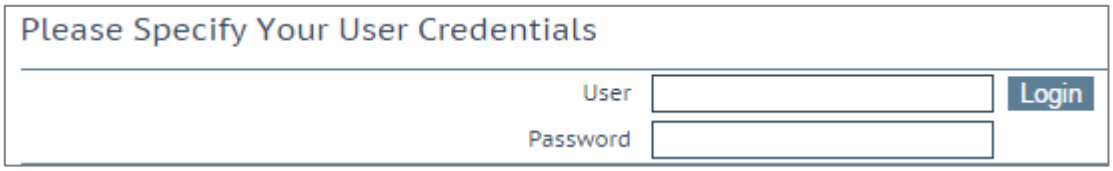
基本認証でログインしたら、ローカルのユーザ名とパスワードでログインしてセッションを開始します。

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、ユーザは、引き続き LoadMaster 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 のユーザ名として、test ではなく test@kemp.com と入力する必要があります。



ログインしたユーザは、画面の右上隅にある[Logout] ボタンを クリックするとログアウトできます。WUI のセッション管理機能が有効にすると、WUI のセッション管理のためのオプション項目をすべて表示します。

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、LoadMaster 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（これらはシステムが定義するデフォルトのユーザ名です）。

基本認証でログインしたら、ローカルのユーザ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」アカウントのログイン用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。LoadMaster が、弱いパスワードと判断した場合、新たにパスワードを入力するよう求めるメッセージを表示します。

「bal」アカウントのみ、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ます。この回数を上回ってログインに失敗したユーザ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。

ユーザがブロックされた場合、「bal」または[All Permissions] の権限のあるアカウントのみ、ブロックされたアカウントを解除できます。

「bal」がブロックされた場合、「bal」アカウント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）

ユーザセッションをログアウトする前に、ユーザがアイドル状態（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）

LoadMaster の管理者は、このオプションを使用して、1 人のユーザが LoadMasterWUI 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。

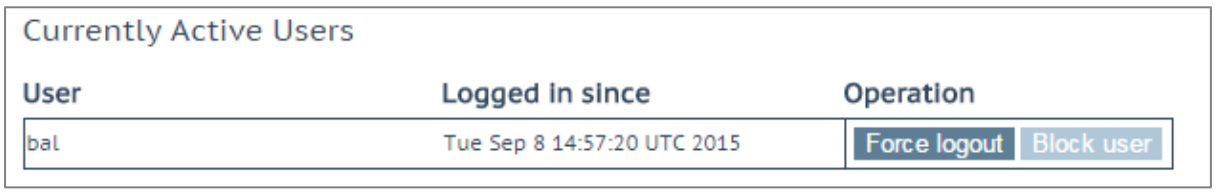
入力した値はトータルのログイン数を表します。この値には「bal」のログインが含まれます。

Pre-Auth Click Through Banner（事前認証バナー）

LoadMaster の WUI ログインページの前に表示される事前認証バナーを設定します。このフィールドにはプレーン テキスト、または HTML コードを入力できます。Java スクリプトの入力はできません。最大 5,000 文字まで入力できます。

Active and Blocked Users（アクティブユーザとブロックユーザ）

「bal」または[All Permissions] の権限が設定されたユーザのみこの機能を使用できます。[User Administration] 権限を設定したユーザでは、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。その他のユーザでは、この部分を画面に表示しません。



Currently Active Users（現在のアクティブ ユーザ）

このセクションには、LoadMaster にログインしている全ユーザのユーザ名とログイン時刻をリスト表示します。

すぐにユーザをログアウトして強制的にシステムに戻すには、[Force logout] ボタンをクリックします。

ユーザがシステムにログインできないようにするには[Block user] ボタンをクリックします。 ブロックを解除するか LoadMaster が再起動するまで、ユーザはシステムにログインできません。[Block user] ボタンをクリックしても強制的なログオフはできません。これを行うには、[Force logout] ボタンをクリックします。

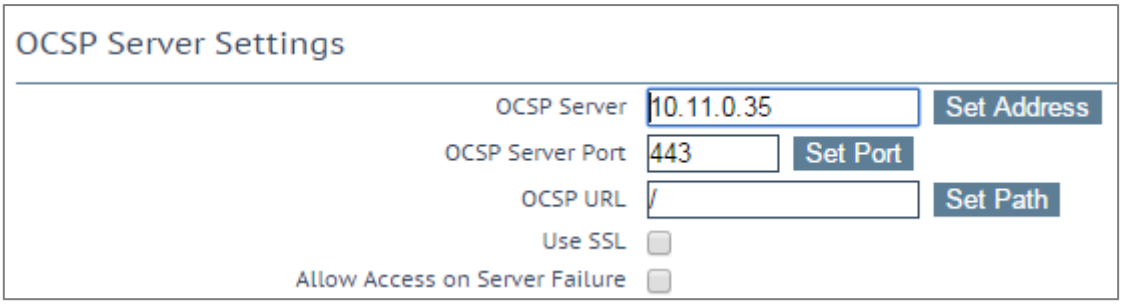
ユーザがログオフせずにブラウザを終了した場合、そのセッションは、タイムアウトになるまでアクティブなユーザのリストでオープンな状態を継続します。その後、タイムアウトになる前にそのユーザが再度ログインすると、そのユーザは別セッションでのログインになります。

Currently Blocked Users（現在のブロックされたユーザ）

このセクションでは、ブロックされた時点でのユーザ名とログイン時刻をリスト表示します。

ブロックされたユーザ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。

9.8 OCSP の設定



OCSP Server（OCSP サーバ）

OCSP サーバのアドレスです。

OCSP Server Port（OCSP サーバポート）

OCSP サーバのポートです。

OCSP URL

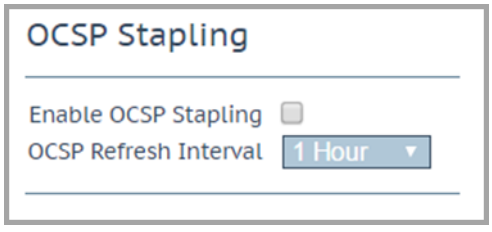
OCSP サーバにアクセスするための URL です。

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（サーバ障害発生時のアクセスを許可する）

OCSP サーバ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 サーバ接続障害またはタイムアウトを処理します。



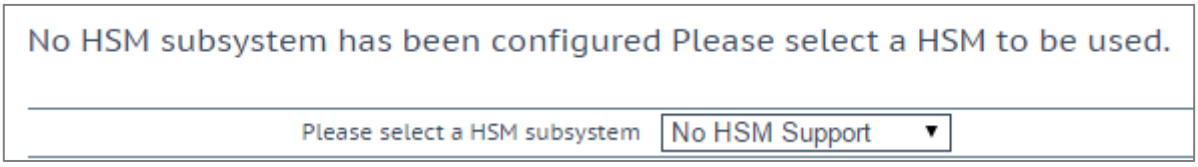
Enable OCSP Stapling（OCSP ステープルを有効にする）

このチェックボックスを選択すると、LoadMaster は OCSP ステープリング要求に応答できるようになります。 クライアントが SSL を使用して接続し、OCSP 応答を要求すると、これを返信します。バーチャルサービスの証明書だけを検証します。システムは、クライアントに送り返される OCSP 応答のキャッシュを保持します。このキャッシュは OCSP デーモンによって管理されます。 OCSP デーモンがサーバに要求を送信すると、OCSP デーモンは証明書に指定された名前（[Authority Information Access] フィールド内）を使用します。 この名前を解決できない場合は、[OCSP Server] テキストボックスで指定しているデフォルトの OCSP サーバを使用します。

OCSP Refresh Interval（OCSP リフレッシュ インターバル）

LoadMaster が OCSP ステープル情報を更新する頻度を指定します。 OCSP デーモンは、ここで指定された時間までエントリをキャッシュし、その後、リフレッシュします。有効な値の範囲は 1 時間（デフォルト）から 24 時間です。

9.9 HSM の設定

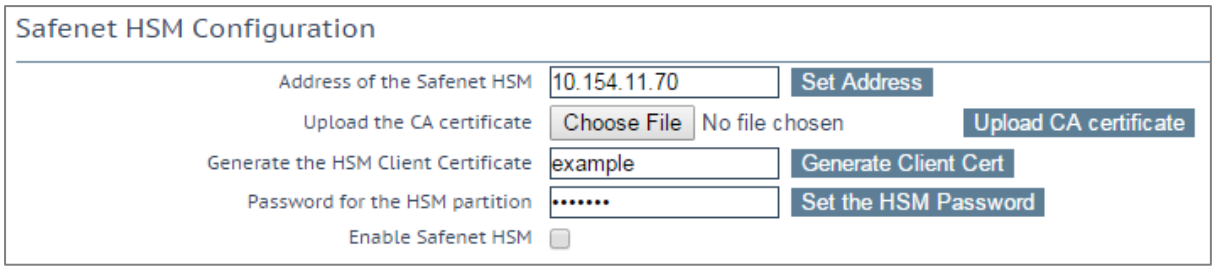


Please select a HSM subsystem（HSM サブシステムの選択）

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。



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、LoadMaster の FQDN 名である必要があります。この名前は、HSM の[client register] コマンドで使用します。

Password for the HSM partition（HSM パーティションのパスワード）

LoadMaster 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。

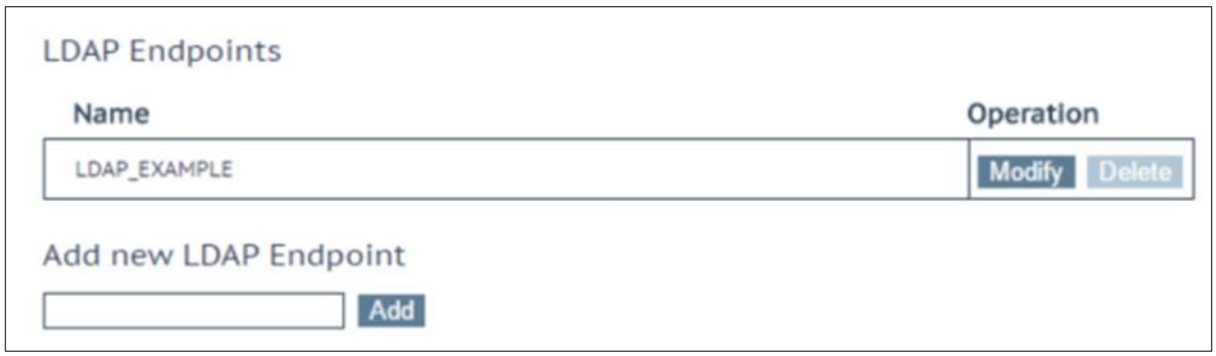
HSM を無効にすると、新たに HSM が追加されるか証明書の設定が変更されるまで、LoadMaster が新たな SSL（HTTPS）接続を作成できなくなり、既存の接続を直ちにドロップします。

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。

9.10 LDAP 設定

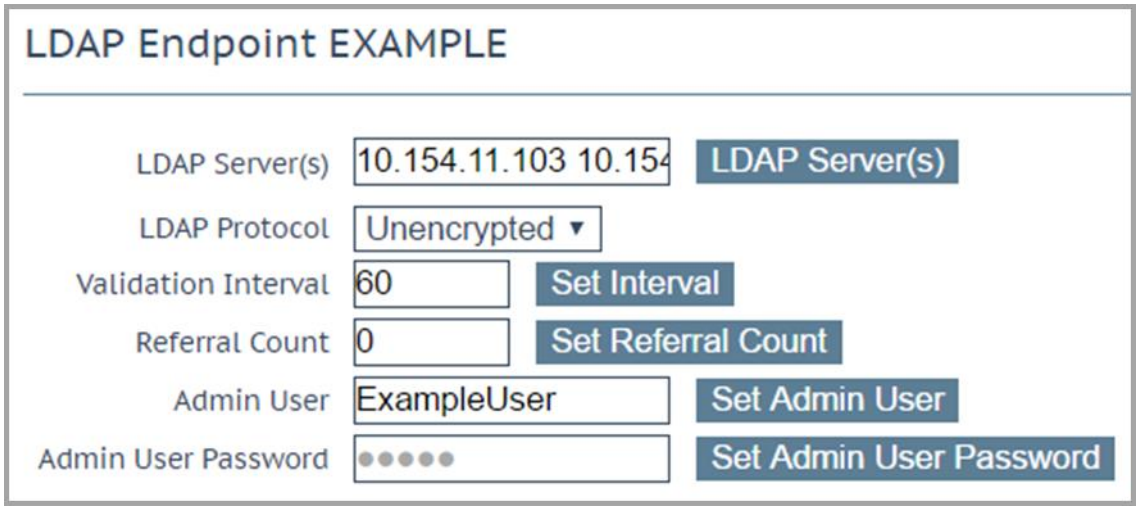
「LDAP 設定」画面を表示するには、[Certificates & Security] を展開し、[LDAP Configuration] をクリックします。この画面には、LDAP エンドポイントの管理インターフェイスを用意しています。LDAP エンドポイントは異なる 3 つの分野で使用できます。

Health checks（ヘルス チェック）
SSO domains（SSO ドメイン）
WUI authentication（WUI 認証）



既存の[LDAP Endpoints] を表示し、[Modify] と[Delete] オプションを表示します。LDAP エンドポイントが使用中の場合、削除はできません。

[Add a new LDAP Endpoin] にエンドポイントの名前を入力し[add] をクリックすると、新しい LDAP エンドポイントが追加できます。スペースと特殊文字は、LDAP エンドポイント名には入力できません。



LDAP Server(s)（LDAP サーバ）

LDAP サーバはスペース区切りを使用してリストを指定します。必要に応じてポート番号を指定します。マルチドメインで、許可されたグループを使用する場合、グローバル カタログ ポート番号を含める必要があります。そうしないと、許可されたグループは失敗します。 デフォルトのポートは 3628 です。例えば、10.110.20.23:3268 のように指定します。

LDAP Protocol（LDAP プロトコル）

LDAP サーバと通信するときに使用するトランスポートプロトコルを選択します。

Validation Interval（再検証インターバル）

Specify how often you should revalidate the user with the LDAP server.

LDAP サーバでユーザを再検証する頻度を指定します。

Referral Count（照会カウント）

LoadMaster は、アクティブディレクトリ ドメインコントローラからの LDAP 照会応答をサポートするためのベータ機能を提供します。 これを 0 に設定すると照会はサポートしません。このフィールドに 1～10 の値を設定すると、照会の追跡が可能になります。 指定した数は、ホップ数の制限になります。（照会の追跡）

複数のホップが認証待ち時間の増加を招く恐れがあります。構成内で要求する参照の深さとその数がパフォーマンスに影響します。

Active Directory 構造を十分に理解した上で、参照限度を適切に設定してください。同じ資格情報がすべてのルックアップなどに使用されます。

アクティブ ディレクトリのグローバルカタログ（GC）を使用するには、LDAP の照会追跡を有効にする代わりに、主要な解決手法を優先した構成にすることです。GC クエリは、LDAP と照会のプロセスに代わって GC キャッシュを問合せるために使用します。アクティブディレクトリの GC を使用すると LoadMaster のパフォーマンス低下を最小にできます。GC の追加/削除の手順は、TechNet の以下の記事を参照してください。
https://technet.microsoft.com/en-us/library/cc755257(v=ws.11).aspx

Admin User（Admin ユーザ）

管理者のユーザ名を入力します。

Admin User Password（Admin ユーザ パスワード）

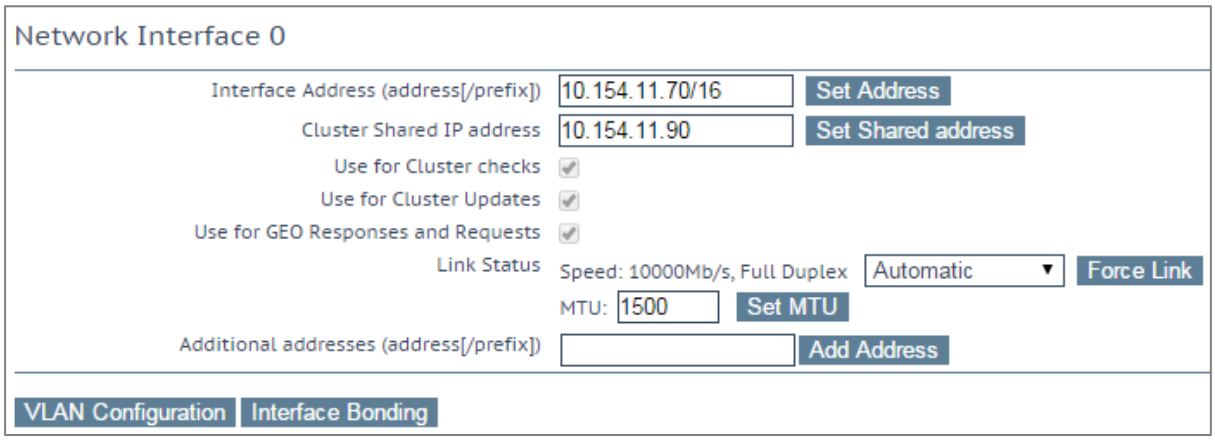
管理者ユーザのパスワードを入力します。

10　システム設定

10.1　　ネットワーク設定

10.1.1　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。



Interface Address（インターフェイス アドレス）

[Interface Address (address[/prefix])] テキストボックスで、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（クラスタの共有 IP アドレス）

クラスタ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] オプションは、LoadMaster にクラスタリング ライセンスを設定し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、FXC 株式会社の担当窓口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、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description」を参照してください。

Use for Cluster checks（クラスターチェック）

このオプションを使用すると、ノード間でクラスタ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（クラスタの更新）

これは、クラスタ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の使用）

[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] を選択している場合に限ります。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。

このオプションを設定すると、「Default Gateway」画面が現れます。ここで新しいデフォルトゲートウェイを設定します。デフォルトゲートウェイを変更すると注意のメッセージを表示します。

Allow Administrative WUI Access（管理用 WUI アクセスの許可）

このオプションは、>Certificates & Security >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、KEMP ドキュメントページの「SSL Accelerated Services, Feature Description」を参照してください。

システムは、最大で 64 個のネットワークインターフェイスを追跡で、1024 個のトータル アドレスでリスン状態を構成できます。

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。

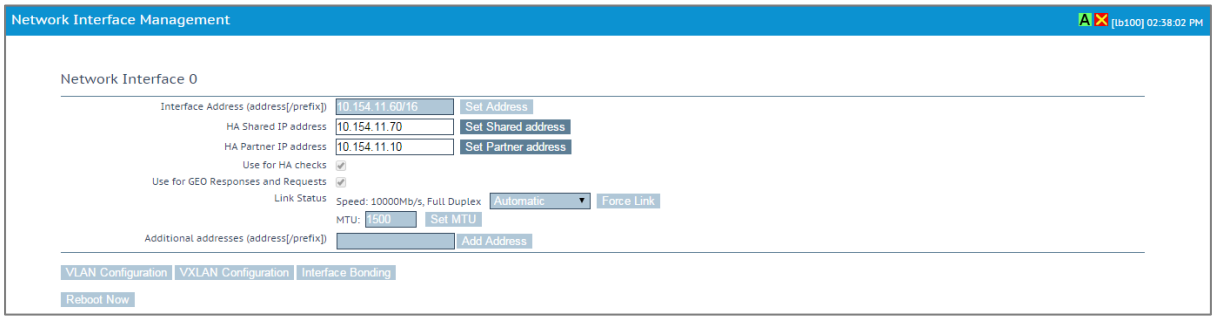
VLM の場合、VLM が実行されているハードウェアによって有効範囲が決まるため、512～9126 の範囲が必ず適用されるとは限りません。ハードウェアによる制約をチェックするようにしてください。

Additional addresses（追加アドレス）

[Additional addresses] フィールドを使用すると、LoadMaster 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「router on a stick」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 アドレスとリアルサーバ IP アドレスの両方で使用できます。

HA（ハイアベイラビリティ）

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。



この画面では、ユーザに下記を示唆します。

- 画面の左上のアイコンは HA ペアのマスター ユニットを意味します。
- 緑と赤のアイコンで、緑はシステムのアップ状態であり、ペアを組む相手ユニットはダウンしています。
- [Interface Address] はこのユニットの IP アドレスです。
- [HA Shared IP address] は HA ペア共通の IP アドレスです。
- [HA Partner IP address] はペアを組む相手ユニットの IP アドレス
- [Use for HA Check] は HA ヘルスチェックを有効にします。
- [Use for GEO Responses and Requests] では、このインターフェイスがデフォルトゲートウェイを使用することを意味します。
- [Link Status] はリンクの速度の設定です。[Automatic] で自動検出します。
- [Additional addresses] は代替アドレスの登録を行います。

Creating a Bond/Team（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。
- ボンディングし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。

Removing a Bond/Team（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] インターフェイスを表示しない場合、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。

[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。

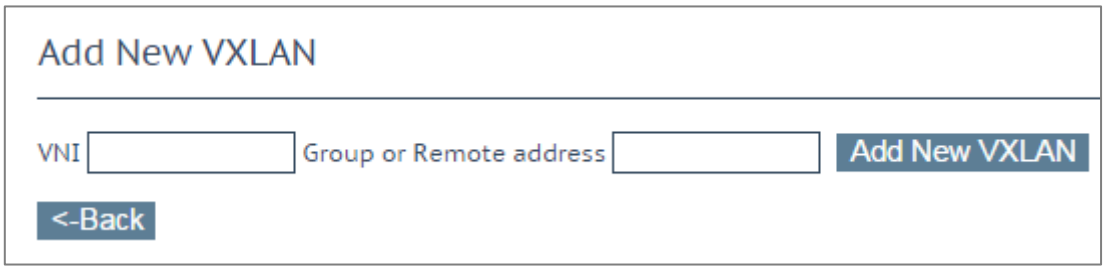
VLAN を削除するには、>System Configuration >Network Setup メニューオプションを選択し、プルダウンリストから目的の VLAN ID を選択します。

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] ボタンをクリックします。



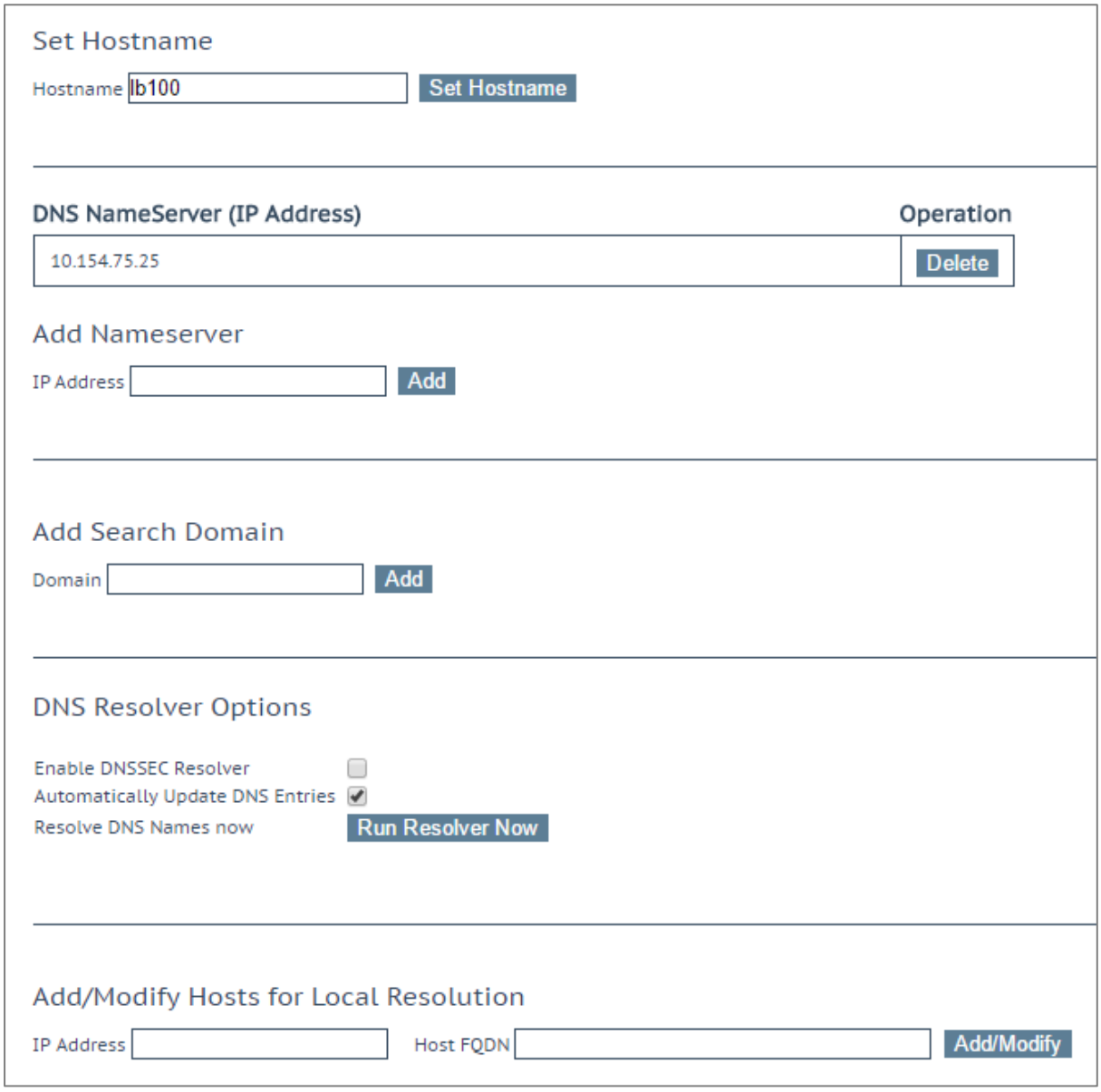
[VNI] テキストボックスに、新しい VXLAN ネットワーク識別子を入力します。[Group or Remote address] テキストボックスに、マルチキャストグループまたはリモートアドレスを入力し、[Add New VXLAN] をクリックします。

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。

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 パラメータの設定が行えます。

- [HA Shared IP address] 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



Set Hostname（ホスト名の設定）

[Hostname] テキストボックスにホスト名を入力し、[Set Hostname] 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)（ネームサーバの追加（IP アドレス））

LoadMaster にてローカルに名前解決する DNS サーバの 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 サーバを指定できます。

DNS SEC が有効な場合、最後に残ったネームサーバを削除することはできません。DNS SEC クライアントは、「ホストと DNS の設定」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、LoadMaster 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、LoadMaster 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、LoadMaster 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、LoadMaster 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 LoadMaster を再起動する必要があります。1 度設定を変更すると、LoadMaster 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、LoadMaster 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
- リアルサーバ

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、LoadMaster 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、リアルサーバ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。

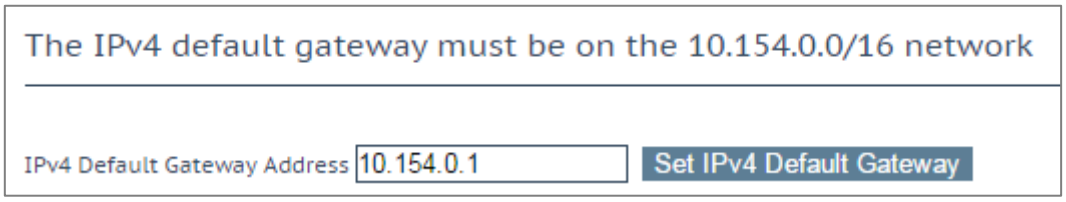
Resolve DNS Names now（DNS 名を直ちに解決する）

[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

ネットワークインターフェース アドレスはデフォルトゲートウェイを設定する前にセットしてください。

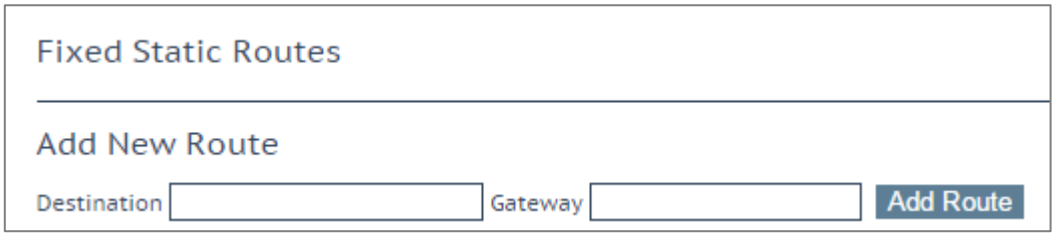
LoadMaster では、インターネットに接続するためのデフォルトゲートウェイを設定する必要があります。



LoadMaster 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。

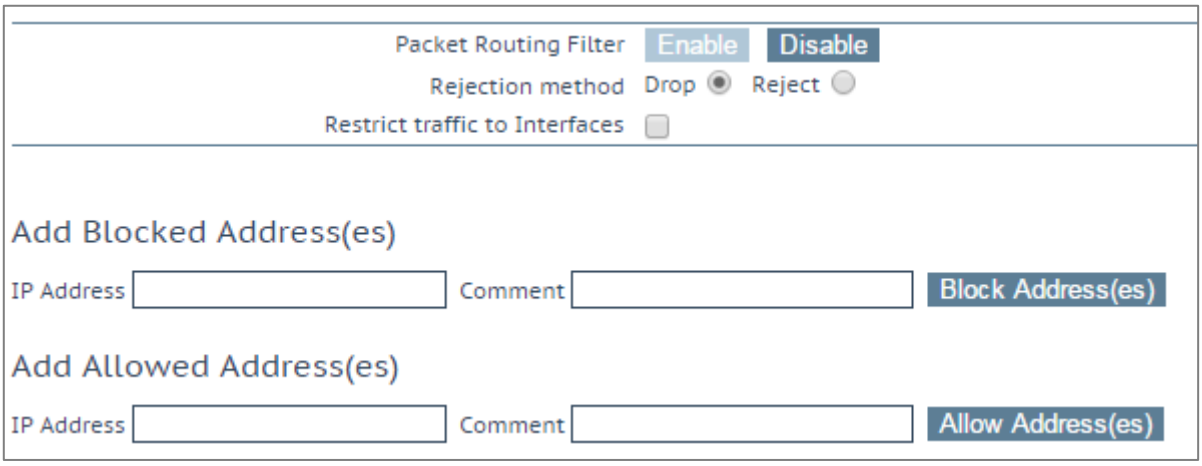
IPv4 および IPv6 のデフォルトゲートウェイは、同じインターフェイス上に存在している必要があります。

10.1.4 追加ルート



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 LoadMaster と同じネットワーク上になければなりません。なお、バーチャル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 ルーティング・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] 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] 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 LoadMaster 上で GEO を無効にするには、メインメニューで [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、LoadMaster 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 LoadMaster へのトラフィックが制限されますが、LoadMaster を経由したクライアントからバーチャルサービスへのアクセスは影響を受けません。また、リアルサーバから送信され、SNAT が設定された LoadMaster で処理されたトラフィックも影響を受けません。

フィルターを有効にすると LoadMaster にトラフィックの制限を与えますが、LoadMaster に設定しているサービス（SSH、HTTPS、SNMP、DNS）に対するクライアントアクセスには影響しません。SNAT を有効にすると、LoadMaster のデフォルトゲートウェイ インターフェースと同じ IP アドレスのバーチャルサービスで、トラフィックのブロッキングができなくなります。これは、単一の IP アドレスで構築する Azure やその他のクラウドプラットフォームで影響があります。

[Packet Routing Filter] が無効の場合、[Reject/Drop blocked packets] フィールドと[Restrict traffic to Interfaces] フィールドは表示しません。

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 LoadMaster 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）

LoadMaster は、[blacklist] （ブラックリスト）に基づく ACL（アクセス制御リスト）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、LoadMaster 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。[whitelist] （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。[whitelist] で指定されたアドレス（またはアドレス範囲）が、[blacklist] で指定された範囲に含まれる場合、[whitelist] の指定が優先されます。

[blacklist] にアドレスが指定されておらず、[whitelist] にのみアドレスが指定されている場合、[whitelist] 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 ACL 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。

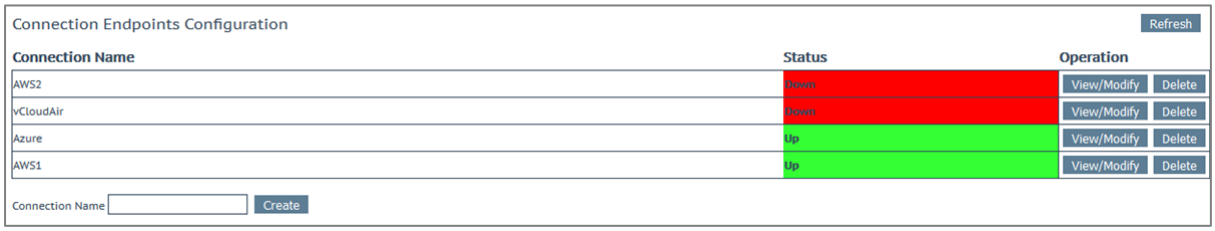
例えば、[blacklist] に 192.168.200.0/24 のアドレスを指定すると、192.168.200 のネットワーク上にあるすべてのホストがブロックされます。

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バーチャルサービスが設定されている場合、静的ポートのバーチャルサービスは正常に機能しません。静的ポートのバーチャルサービスにてそのトラフィックが拒否された後に、ワイルドカードのバーチャル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」リンク/画面は、LoadMaster 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 Tunneling, Feature Description（IPsec トンネリング機能説明を参照してください。



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）

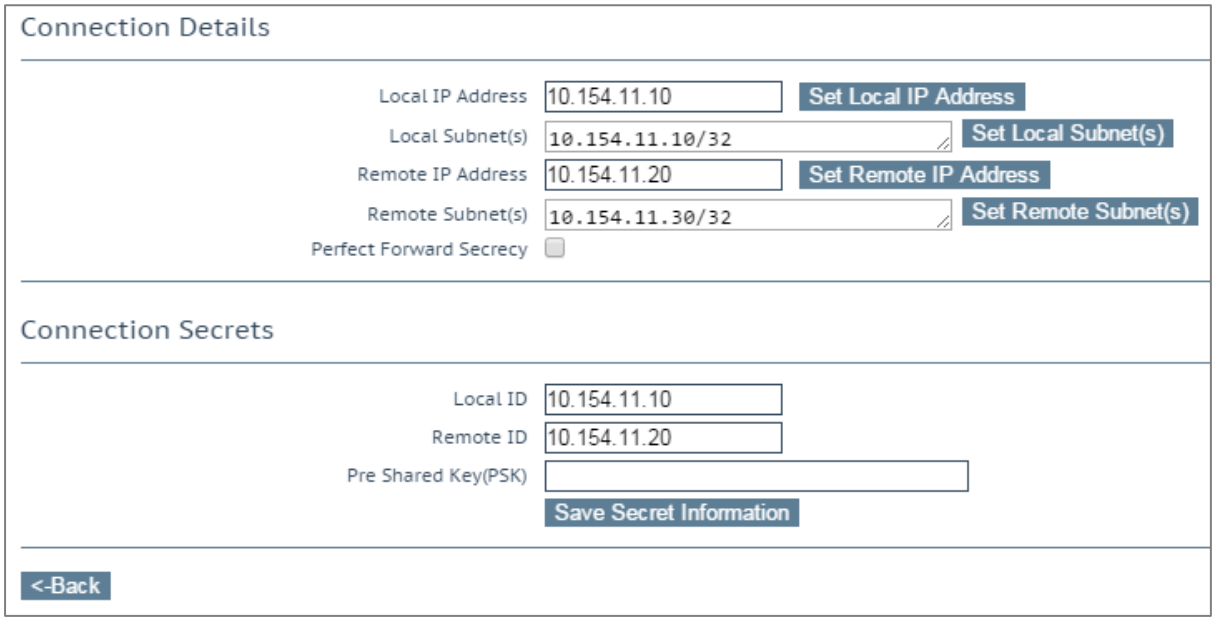
この接続の設定パラメータを表示/変更します。

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



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 LoadMaster 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] に設定している場合は、テキストボックスの値は自動設定されます。/32 CIDR が与えられている場合、ローカル IP が唯一設定可能です。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（パーフェクト フォワードセキュリティ）

PFS（パーフェクト フォワードセキュリティ）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] のどのオプションを設定すべきかが決まります。PFS 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、関連するドキュメント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。LoadMaster 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。

LoadMaster 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。LoadMaster 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。

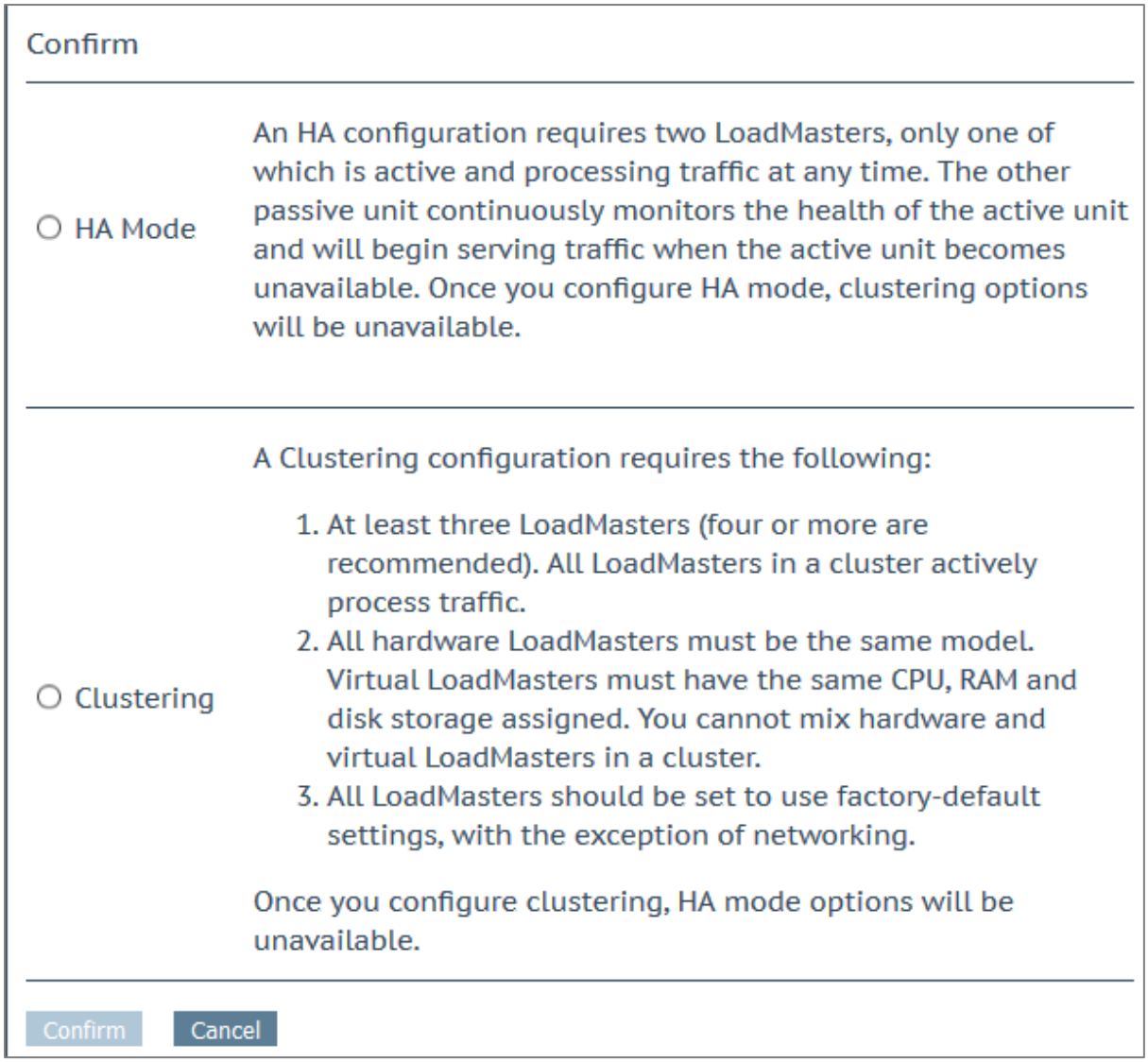
Pre Shared Key (PSK)（プレシェアードキー）

プレシェアードキーの文字列を入力します。

Save Secret Information（秘密情報の保存）

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



WUI のこのセクションは、LoadMaster 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）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] （クラスタ制御）と呼ばれます。

この画面では、HA モードと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。

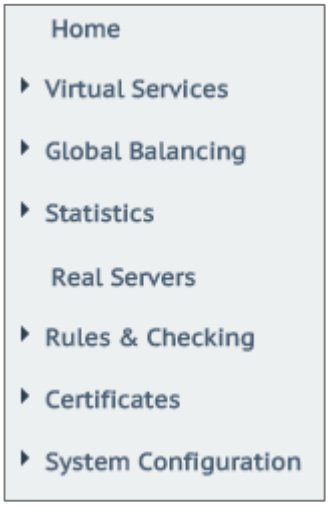
10.2.1 HA Mode（HA モード）

LoadMasterfor Azure を使用する場合は、「Azure HA パラメータ」を参照してください。

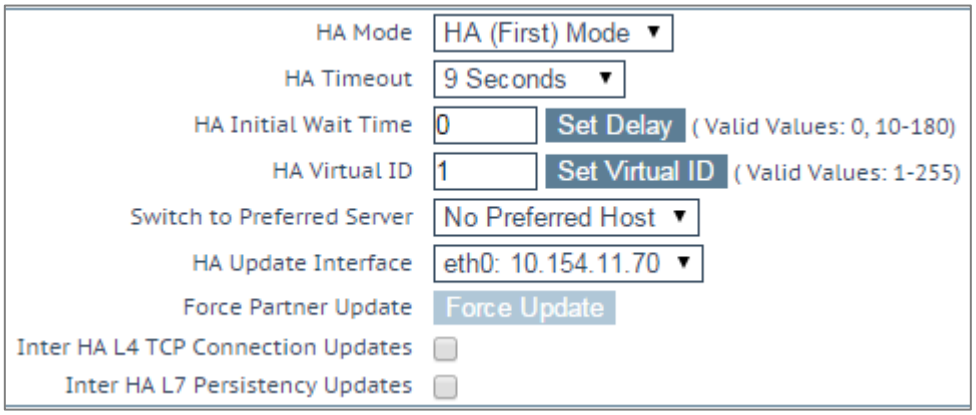
LoadMaster for AWS 製品を使用している場合は、「AWS HA パラメータ」を参照してください。

各ユニットのロールは、「HA Mode」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] か[HA (Second) Mode] を[HA Mode] で選択した場合、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。LoadMaster が再起動すると、HA モードが[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 台とも同じ値にすると正しいペアとして動作しません。

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 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。

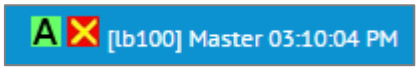


LoadMaster が HA モードになっている場合、[HA Parameters] メニューオプションを選択したときに以下の画面が表示されます。



HA Status（HA ステータス）

画面上部の時刻表示の隣にあるアイコンは、クラスタ内の LoadMaster 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 あり）	A	ユニットは、オンラインで正常に稼動しています。 「A」の文字表示は、マスター（アクティブ）ユニットであることを示しています。
緑 （A なし）		ユニットは、オンラインで正常に稼動しています。 「A」の文字表示がない四角は、スタンバイであることを示しています。
赤		ユニットは動作していません。オフラインか誤った構成になっています。 障害時にもう一方のユニットへ引き継ぐことができていません。もう一方のユニットの状態と設定の確認を行ってください。
青		ユニットが 5 分間で 3 回以上の再起動が発生したとき、緩やかな状態に移行します。この状態では、ユニットの IP がアドレス（共有 IP アドレスではなく）を使用したアクセスのみが可能で、HA アクティビティに接続できません。このため、マスターによる変更ができず、マスターに障害があっても切り替りません。この状態を解除するには、SSH かコンソールからログインして、ユニットを再起動します。
灰		マシンが不安定な状態にあり、正常な状態にするには再起動が必要です。この状態は、両方のユニットがマスターとしてアクティブ状態にあるか、重大な問題が発生している可能デイがあります。もし、再起動しても可決しない場合は、KEMP Technologies か FXC 株式会社に問い合わせてください。
アイコンなし		HA 状態のアイコンの表示がない場合は、HA が有効ではない可能性があります。>System configuration >HA andClustering の、[HA mode] が [HA (First) Mode] か[HA (Second) Mode] に設定されていることを確認してください。

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 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）

LoadMaster 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）LoadMaster 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 バーチャル 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）LoadMaster には、すべて一意の HA バーチャル ID 番号を割り当てる必要があります。

7.2.36 リリースから、LoadMaster は最初に設定したインターフェイス（最後の 8 ビット）の共有 IP アドレスに基づいてバーチャル ID を設定します。共有アドレスとパートナーアドレスが両方とも設定されると、値が選択

されて表示されます。値を任意の値（1～255 の範囲）に変更することも、すである値に保持することもできます。バーチャル ID がネットワーク上の各 LoadMaster で一意であることを確認してください。

Switch to Preferred Server（優先サーバの切替）

デフォルトでは、クラスタを構成するいずれのユニットにはのも優先権はありません。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 アップデイト 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（設定情報の強制更新）

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 接続での更新）

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 パーシステンス更新）

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 マルチキャストインターフェイス

HA 間のアップデイ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。

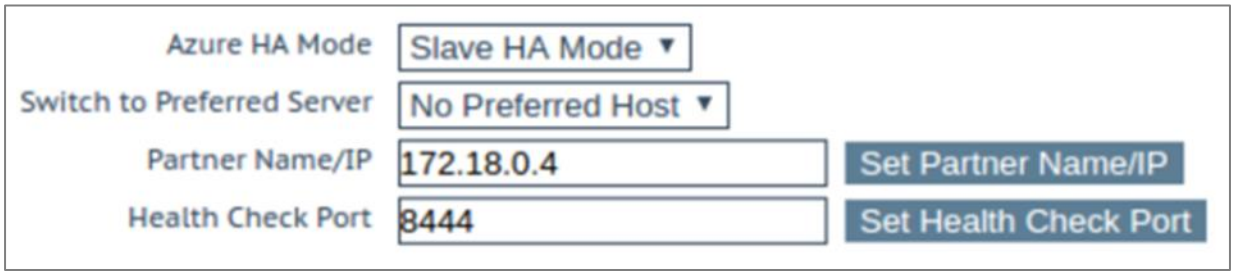
仮想 MAC アドレス

このオプションを有効にすると、HA の切替時に HA ペア間で MAC アドレスを強制的に交換します。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 GARP（gratuitous-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 LoadMaster に対してのみ利用可能です。

10.2.1.1 Azure HA パラメータ

この画面は、LoadMasterfor Azure でのみ利用できます。



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）

LoadMaster 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。

バーチャル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。

LoadMaster 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。

Switch to Preferred Server（優先サーバの切替）

以下の 2 つの値を設定でます。

No Preferred Host : 各ユニットは、他のユニットが故障したときに引き継ぎます。パートナーが再起動してもファイルオーバーは発生しません。

Prefer Master : HA1（マスター）ユニットは常に引き継ぎます。これはデフォルトのオプションです。

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。

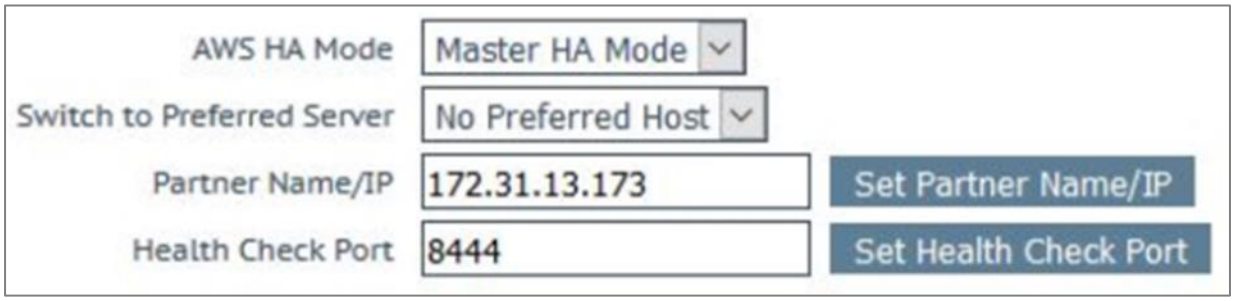
Health Check on All Interfaces（すべてのインターフェースのヘルスチェック）

このオプションを有効にすると、ヘルスチェックはすべてのインターフェースに対して応答を待機します。この設定はマルチアームの構成で使用します。この設定を無効にすると、ヘルスチェックの応答待機は Eth0 になります。

ユニットがスタンバイモードの場合、WUI アクセスはローカル管理に制限されます。 ユニットがアクティブかチェックがない状態であれば、完全な WUI アクセスが可能です。

10.2.1.2 AWS HA パラメータ

この画面は、LoadMaster for AWS のモデルでのみ利用できます。



AWS HA Mode（AWS 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）

LoadMaster 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。

バーチャル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。

LoadMaster 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。

Switch to Preferred Server（優先サーバの切替）

以下の 2 つの値を設定でます。

No Preferred Host : 各ユニットは、他のユニットが故障したときに引き継ぎます。パートナーが再起動してもファイルオーバーは発生しません。

Prefer Master : HA1（マスター）ユニットは常に引き継ぎます。これはデフォルトのオプションです。

Partner Name/IP（パートナー名/IP）

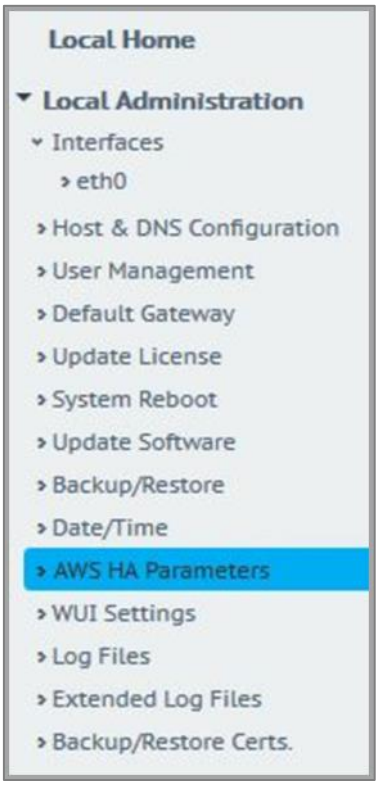
HA パートナーユニットのホスト名または IP アドレスを指定します。

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。

Health Check on All Interfaces（すべてのインターフェースのヘルスチェック）

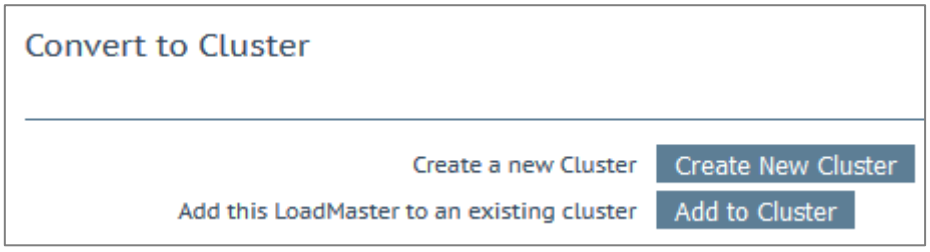
このオプションを有効にすると、ヘルスチェックはすべてのインターフェースに対して応答を待機します。この設定はマルチアームの構成で使用します。この設定を無効にすると、ヘルスチェックの応答待機は Eth0 になります。



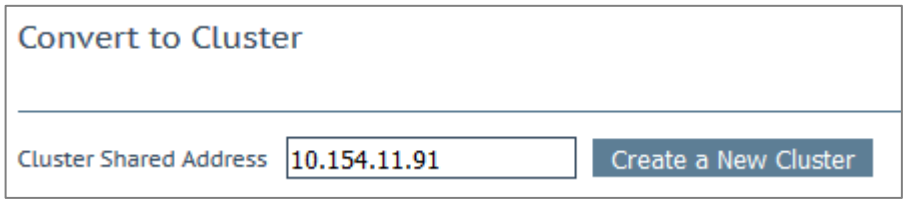
ユニットがスタンバイモードの場合、WUI アクセスはローカル管理に制限されます。 ユニットがアクティブかチェックがない状態であれば、完全な WUI アクセスが可能です。

10.2.2 クラスタ コントロール

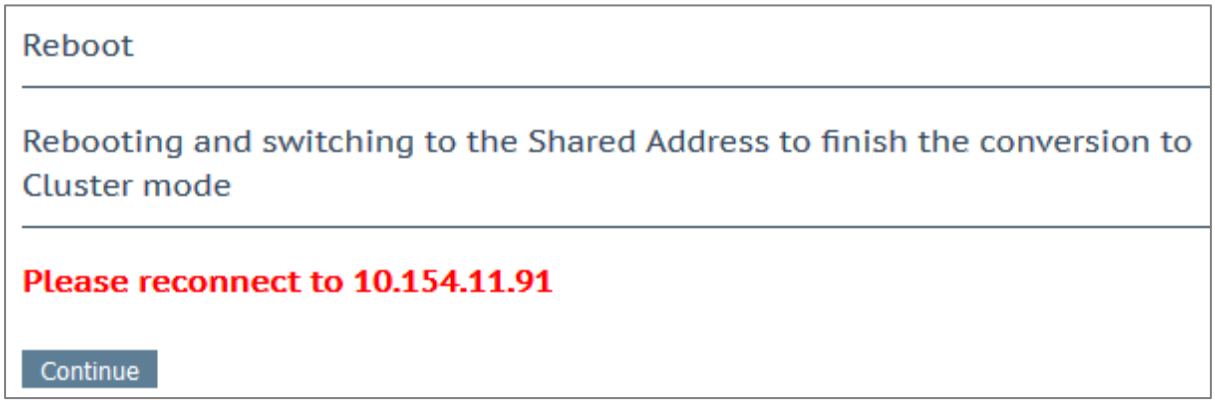
[Cluster Control] のオプションは、LoadMaster にクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、FXC 株式会社の担当窓口にお問い合わせください。クラスタリングについての詳細は、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description（LoadMaster のクラスタリング機能説明を参照してください。



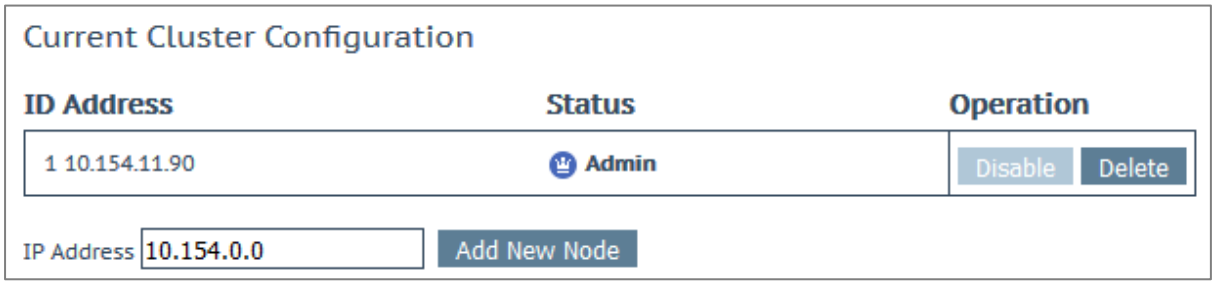
Create New Cluster : クラスタを新たに設定するには、このボタンをクリックします。
Add to Cluster : この LoadMaster を既存のクラスタに追加します。



[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、クラスタの管理に使用されます。

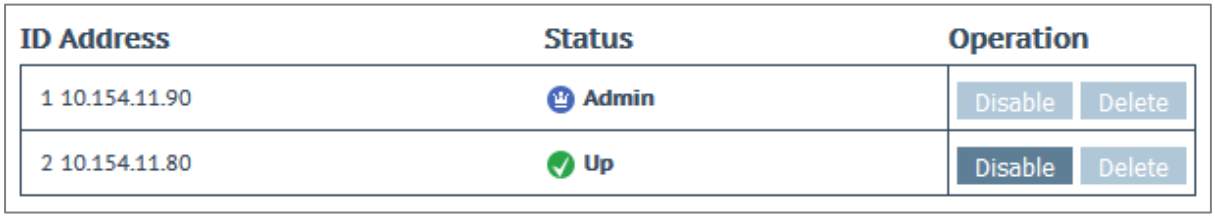


[Create a New Cluster] ボタンをクリックすると、LoadMaster が再起動されます。先ほど設定した共有 IP アドレスに再接続するか尋ねるメッセージが表示されます。



クラスタを作成すると、共有 IP アドレスの WUI の「クラスタ コントロール」画面で、LoadMaster のノードをクラスタに追加できるようになります。

LoadMaster の追加は、クラスターが利用可能であり、その LoadMaster 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、、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description」を参照してください。



共有 IP アドレスの WUI の[Cluster Control] 画面には、そのクラスタにある各ノードの詳細が表示されます。

Show Options : [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] と[Node Drain Time] 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、、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description（LoadMaster 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 ID

Address : LoadMaster 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。

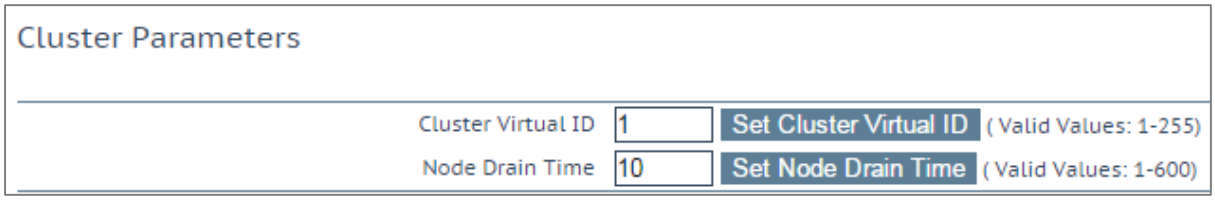
	ドレイン中	このノードは無効になっており、正しい手順で接続をシャットダウンしている最中です。ドレイン停止は、デフォルトで 10 秒間継続します。この値は、[Cluster Control] 画面の[Node Drain Time] の値を変更することで更新できます。詳細は、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description（LoadMaster のクラスタリング機能説明」を参照してください。

Operation：このノードに関して実行可能な各種動作

- Disable：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：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：クラスタ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 LoadMaster インスタンスになります。その後、LoadMaster をクラスタに戻すと、共有 IP アドレスに対して行われた変更が、ノードの LoadMaster に反映されます。
- Reboot：クラスタ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、、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description」を参照してください。

Add New Node：指定された IP を持つ新しいノードをこのクラスタに追加します。

10.2.2.1 クラスタ パラメータ



[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 バーチャル ID）

同じネットワーク上で複数のクラスタまたは LoadMaster HA システムを使用する場合、仮想 ID により各クラスタが識別されます。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 LoadMaster に対して行われた変更は、そのクラスタ内のすべてのノードに反映されます。

Node Drain Time（ノード ドレインタイム）

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[Draining]になります。

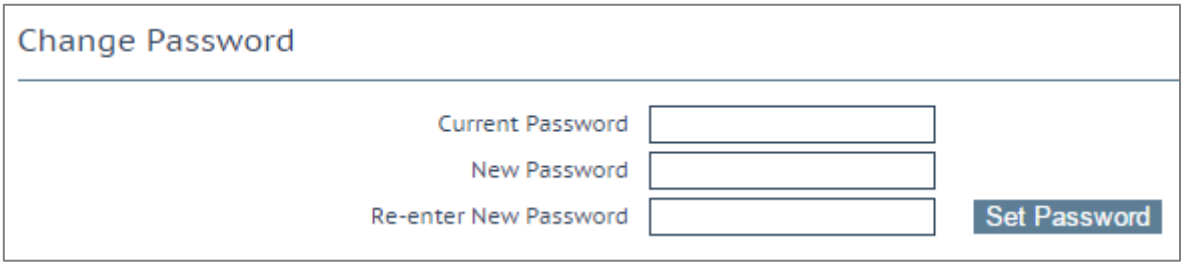
ドレイン時間が経過すると、ステータスが[disable] になります。

10.3 システム管理

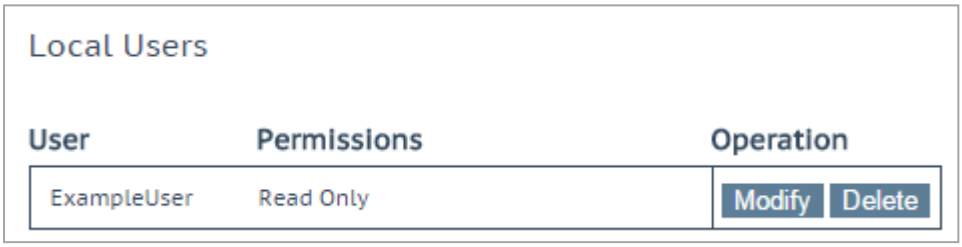
各オプションは、LoadMaster の基本レベルの運用を制御します。重要なポイントとして、HA ペアで各パラメータに変更を加えるには、フローティング管理 IP アドレスを使用する必要があります。これらのオプションの多くは、システムのリブートが必要になります。これらのパラメータを設定/変更した場合は、ペアで唯一のアクティブなシステムだけが影響を受けます。

10.3.1 ユーザの管理

以下、ユーザ管理用の各種 WUI フィールドについて説明します。ユーザ管理と WUI 認証の詳細については、KEMP ドキュメントページの「User Management, Feature Description」を参照してください。

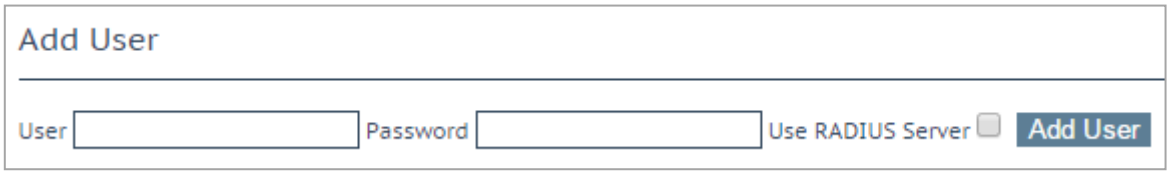


[Change Password] セクションでは、機器のパスワードを変更できます。これはローカルのアプライアンスにのみ適用され、HA 構成におけるパートナーのアプライアンスのパスワードには影響しません。



[Local Users] セクションには、既存のローカルユーザのリストが表示されます。既存のユーザに関して 2 つのオプションが用意されています。

- **Modify :** 既存のローカルユーザ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 :** 目的のユーザを削除します。



[Add User] セクションでは、新規ユーザを追加できます。

ユーザ名には最大 64 文字まで使用できます。ユーザ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。

=~^._+#@¥/-

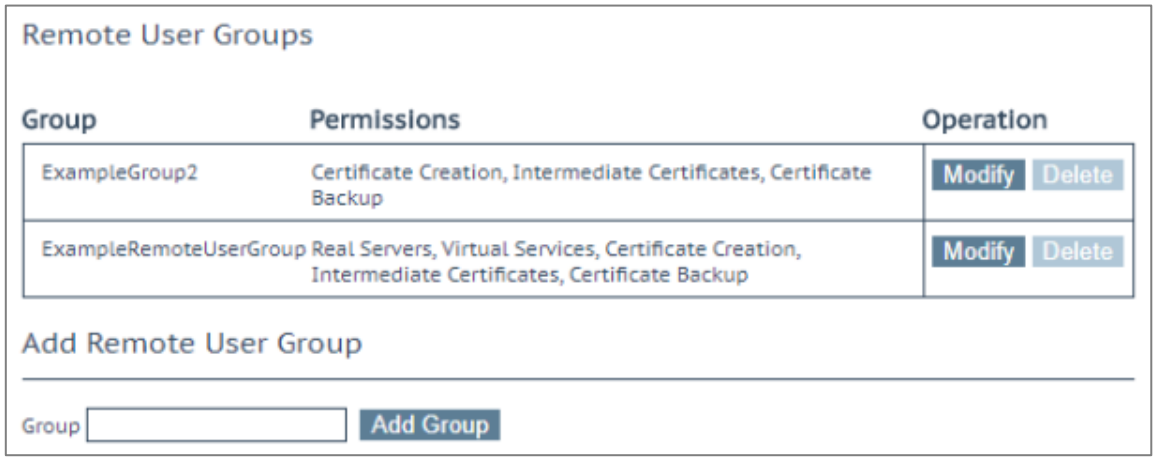
パスワードは 8 文字以上 64 文字以下でなければなりません。[¥] 、[”] 、[`] 、[’] を除いてすべての文字を使用できます。

[Use RADIUS Server] オプションを使用すると、ユーザが LoadMaster 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。

FRADIUS サーバによる認証を行う場合、LoadMaster から RADIUS サーバにユーザの情報が渡され、RADIUS サーバから LoadMaster にそのユーザが認証されたかどうかが通知されます。RADIUS サーバの設定に関する詳細は WUI の認証と権限設定セクションか、KEMP ドキュメントページの「the RADIUS Authentication and Authorization」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 サーバを設定する方法については、「WUI の認証と権限設定」セクションを参照してください。

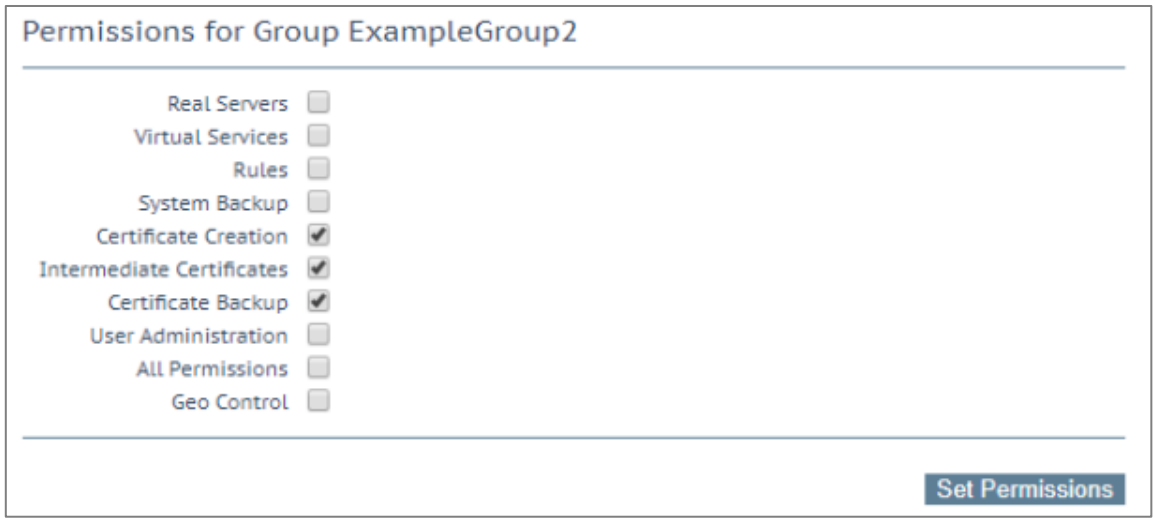
セッション管理が有効になっている場合、[Add User] セクションに[No Local Password] チェックボックスが表示されます。ユーザが LoadMaster にアクセスするときに、クライアント証明書を用いてそのユーザを認証する場合、このオプションを有効にできます。クライアント証明書による認証を有効にするには、[Remote Access] 画面で[Admin Login Method] を設定します。詳細はリモートアクセスセクションまたは、KEMP ドキュメントページの「User Management, Feature Description」を参照してください。



[Remote User Groups] セクション作成したリモートユーザグループを表示します。グループ名と関連する権限も併せて表示します。これらのグループは、>Certificates & Security >Remote Access >WUI Authorization Options 画面で LDAP WUI 認証を選択できます。詳細は WUI の認証と権限設定を参照してください。

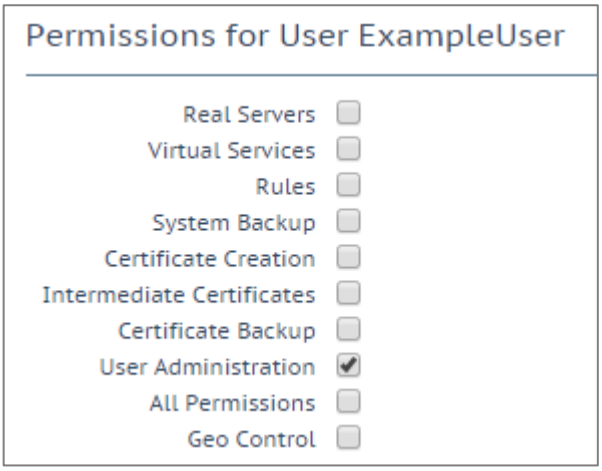
グループを選択し適用することが重要です。グループが選択していない場合、リモートユーザはグループチェックなしでログインできてしまいます。

新しいリモートユーザグループを作成する場合、グループ名を入力して[Add Group] をクリックしてください。[Modify] をクリックするとグループ権限を変更できます。



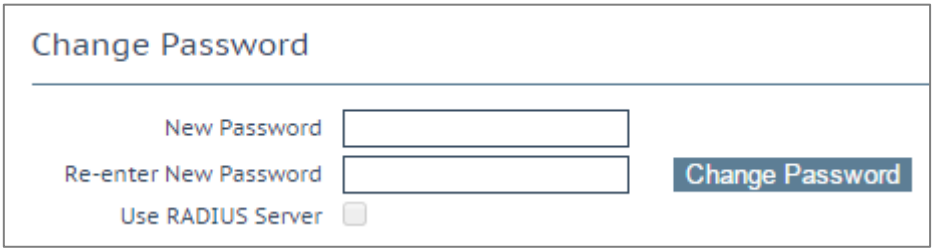
グループ権限についての詳しい情報 KEMP Documentation Page の User Management Feature Description を参照してください。

10.3.1.1 ユーザの編集



この画面では、ユーザ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「bal」は、常にすべての機能を使用する権限を持っています。セカンダリユーザは、一部の機能が制限される場合があります。

ユーザ権限の詳細については、KEMP ドキュメントページの「KEMP LoadMaster, Product Overview」を参照してください。

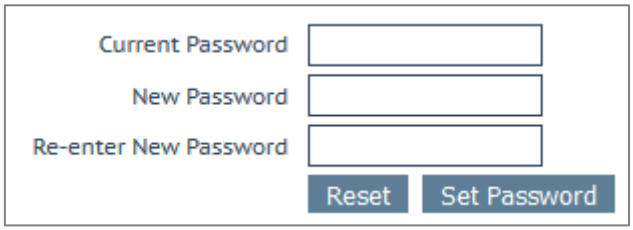


[Change Password] セクションでは、ユーザのパスワードの変更が行えます。また、RADIUS サーバによるユーザ認証を有効/無効にできます。

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 サーバを設定する方法については、「WUI の認証と権限設定」セクション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 LoadMaster 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「リモートアクセス」セクションまたは、KEMP ドキュメントページの「User Management, Feature Description」を参照してください。

名前付きユーザは、ユーザ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。名前付きユーザが >System Configuration >System Administration >User Management メニューオプションをクリックすると、[Change Password] 画面を表示します。



ユーザは、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、ユーザは、新しく設定したパスワードで LoadMaster に再度ログインするよう求められます。

[Local Certificate] セクションでは、そのユーザ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、LoadMaster 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は、自分または他のユーザ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 LoadMaster 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「リモート アクセス」セクションまたは KEMP ドキュメントページの「User Management, Feature Description」を参照してください。

10.3.2 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。[Update License] 機能で以下のようなライセンスの更新を行います。

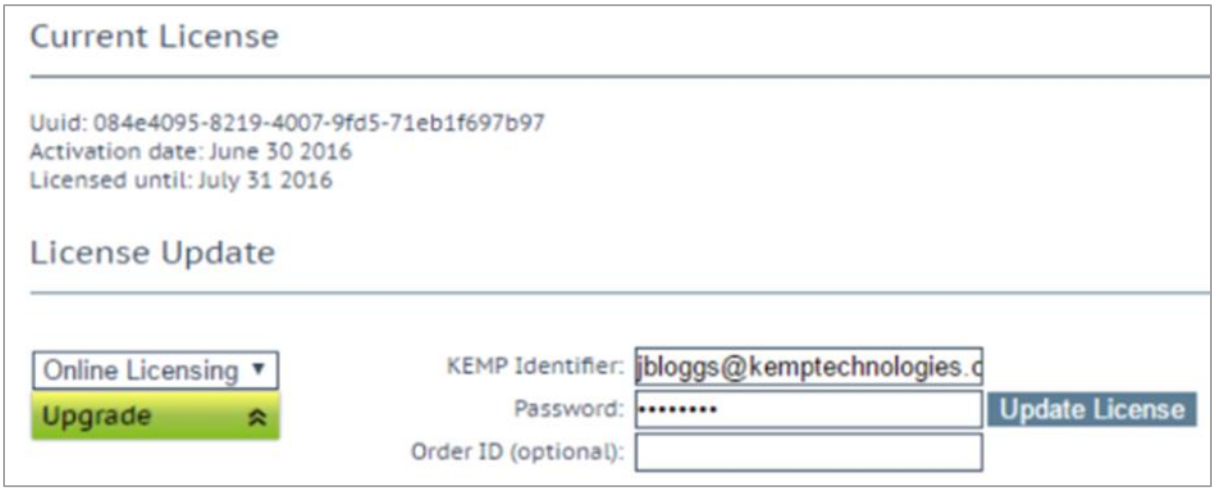
- You have renewed support（サポートの更新）
- You have renewed your license（ライセンスの更新）
- You have changed your license type（ライセンスタイプの変更）

LoadMaster 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、KEMP ドキュメントページの「Licensing, Feature Description」を参照してください。

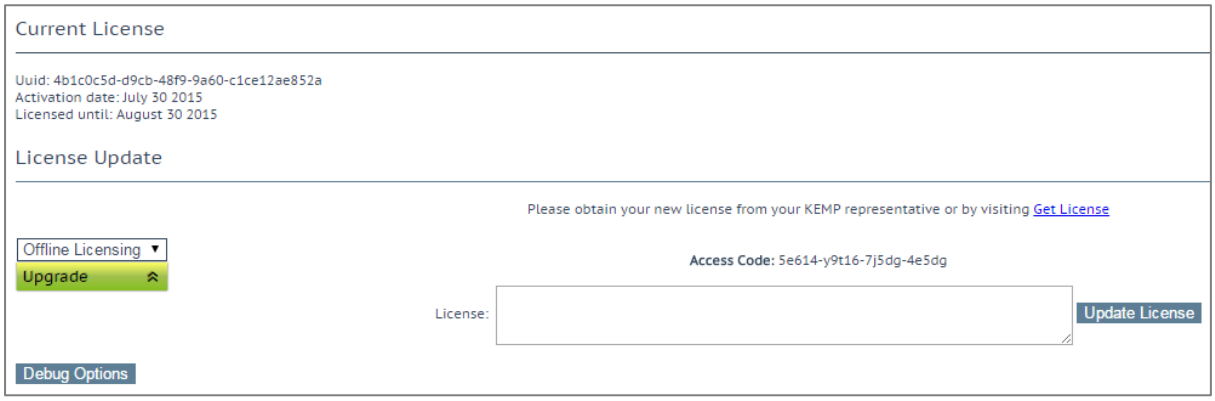
10.3.2.1 オンライン方式



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、LoadMaster 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 Identifier] （KEMP ID）と[Password] を入力する必要があります。

ライセンスのアップデイト後に再起動することをお薦めします。

10.3.2.2 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、LoadMaster 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 から直接入手するか、[Get License] 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。

ライセンスのアップデイト後に再起動することをお薦めします。ESP ライセンスの場合は、アップデイトの後に再起動を実施します。

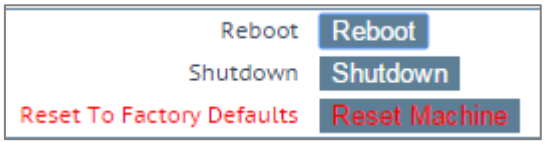
10.3.2.3 デバッグ チェック

ライセンスを取得で問題が発生すると、いくつかのチェックを自動実行し、結果と関連するエラーメッセージを表示します。

このチェックは、次のタスクを実行します。

- 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 サーバに ping を送信する）
- Ping Licensing Server（ライセンスサーバに ping を送信する）

10.3.3　システム リブート



Reboot

アプライアンスをリブートします。

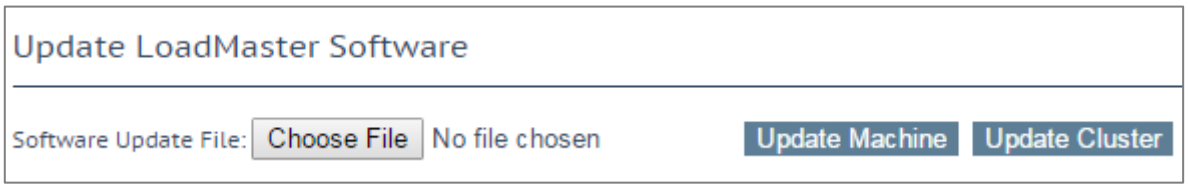
Shutdown

このボタンをクリックすると、LoadMaster 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

ライセンス、ユーザ名、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　ソフトウェアの更新



ソフトウェアの更新に関しては、FXC 株式会社の担当窓口までご連絡ください。

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次の url で確認できます。https://support.kemptechnologies.com/hc/en-us/sections/200428766-Firmware-Downloads

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、LoadMaster 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（クラスタの更新）

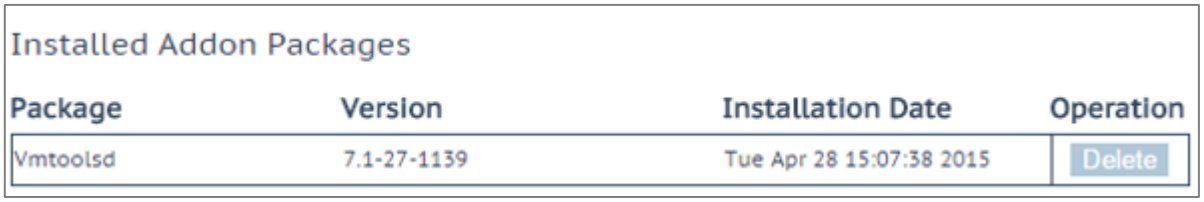
"Update Cluster"のオプションは、LoadMaster にクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMP の担当者にお問い合わせください。ク

ラスタリングについての詳細は、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description」を参照してください。

"Update Cluster"ボタンをクリックすると、クラスタにあるすべての LoadMaster 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、KEMP ドキュメントページの「LoadMaster Clustering, Feature Description（LoadMaster のクラスタリング機能説明」を参照してください。

Restore Software（ファームウェアのリストア）

LoadMaster 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。



Installed Addon Packages（アドオンパッケージのインストール）

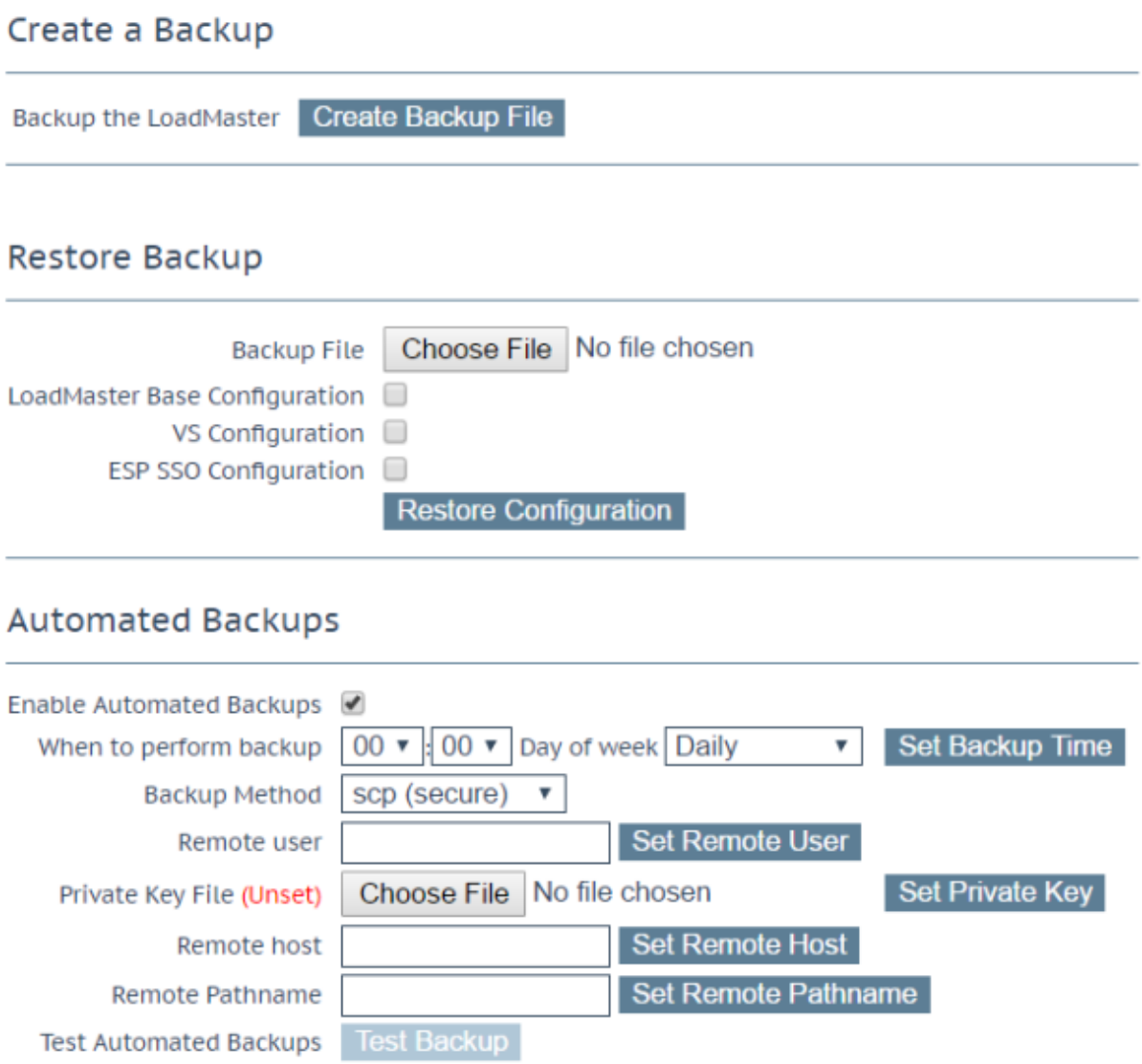
KEMP LoadMaster にはアドオンパッケージをインストールできます。アドオンパッケージでは、LoadMaster の追加機能が用意されています。今後、アドオン機能をさらに追加する予定です。

アドオンパッケージは、KEMP Technologies の Web サイトから入手できます。

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 バックアップとリストア



Create a Backup（クリエイト バックアップ）

バーチャル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 LoadMaster のホスト名が含まれています。

デフォルトでは、LoadMaster はバックアップの取得で「Netstat」の出力を含みます。このためバックアップの完了に時間がかかります。「Netstat」の出力を停止するには、「Debug Options」画面の[Include Netstat in Backups] オプションを無効にしてください。「Debug Options」画面は、>System Configuration >Logging Options >System Log Files >Debug Options にあります。

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、ユーザは復元する情報の種類を選択できます。

- **VS Configuration**（VS 設定を復元）
- **LoadMaster Base Configuration**（ネットワーク等のベース設定を復元）
- **Geo Configuration**（GSLB の設定を復元）
- **ESP SSO Configuration**（SSO ドメイン、LDAP エンドポイント、SSO カスタムイメージセットのリストア。VA 設定の復元は[VS Configuration] を使用して復元します。）

オプションの組合せについて

単一構成情報を HA 構成ユニットにリストア、HA 構成情報を単一構成ユニットにリストアすることはできません。

ESP が有効でないユニットに、ESP 対応のバーチャルサービス設定をリストアできません。

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 LoadMaster 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「日付/時刻」セクション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。

Backup Method（バックアップ方式）

自動バックアップのファイル転送方法を選択します。

Ftp（安全でない）
Scp（安全）

scp を使用している場合は、プライベートキーファイルが必要があります。

Remote user（リモートユーザ）

リモートホストにアクセスするユーザ名

Private Key File（プライベート キーファイル）

バックアップ方式で SCP を使う場合、プライベートキーファイルが必要です。これは、SSH のプライベートキーで、リモート SCP サーバの SSH-keygen で作成します。

Remote password（リモートパスワード）

リモートパスワードは、バックアップ方式が FTP の時に使用します。リモートホストにアクセスしてパスワード要求を設定します。このフィールドは、英数字と英数字以外も入力できます。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。

10.3.6 日付/時刻

時間、日付の設定が行えます。マニュアルで設定するか、NTP サーバを指定して精度の高い時刻を自動的に設定できます。

NTP host(s)（NTP ホスト）

NTP サーバ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/Disable NTP Authentication（NTP 認証パラメータと解除）

LoadMaster は、暗号化された署名を用いて安全な NTP サーバ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が表示されます。[Show NTP Authentication Parameters] を選択してしパラメータを変更する場合、チェックボックスの名称は[Disable NTP Authentication] に変わります。

NTP Key Type（NTP 鍵タイプ）

NTP の鍵として「MD5」か「SHA-1」を選択できます。

NTPv4 を機能させるには、サーバ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）

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。

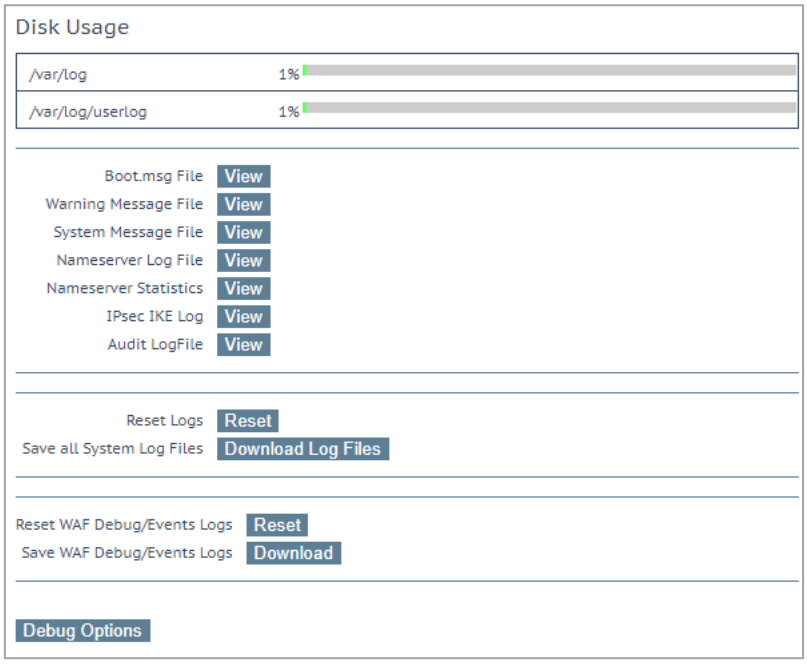
NTP Key ID（NTP 鍵 ID）

NTP 鍵 ID を選択します。値の範囲は 1～99 です。サーバごとに異なる鍵 ID を使用できます。

10.4 ログ オプション

LoadMaster 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。LoadMaster 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 マネージャ、Syslog サーバ、SMTP サーバ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 システム ログファイル



ディスク使用率：このセクションは、ログパーティションの使用状態をパーセンテージで表示します。使用レベルで色の表示が以下のように変化します。

- 0% ～ 50%：緑
- 50% ～ 90%：オレンジ
- 90% ～ 100%：赤

Boot.msg File（ブートメッセージ ファイル）

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（警告メッセージ ファイル）

LoadMaster の運用中に記録された警告を含んでいます。

System Message File（システムメッセージ ファイル）

LoadMaster 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 LoadMaster の内部イベントの両方が対象です。

Nameserver Log File（ネームサーバログ ファイル）

DNS ネームサーバのログを表示します。

Nameserver Statistics（ネームサーバ統計情報）

ネームサーバの最新の統計情報を表示します。

IPsec IKE Log（IPsec IKE ログ）

IPsec IKE のログを表示します。

WAF Event Log（WAF イベントログ）

最後にトリガーされた WAF ルールのログが格納されます。

WAF のイベントログが無いと、[WAF Event Log] ボタンを表示しません。

Audit LogFile（オーディットログ）

ユーザにより 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、「管理用 WUI のアクセス」セクションを参照してください。

Reset Logs（ログのリセット）

ワーニングとシステムメセージ ログファイルをクリアします。

Save all System Log Files（すべてのシステムログファイルを保存）

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。

Reset WAF Debug/Events Logs （WAF デバグ/イベント ログのリセット）

WAF のデバグ ログとイベント ログをすべてクリアします。

Save WAF Debug/Events Logs（WAF デバグ/イベント ログの保存）

WAF のデバグ ログとイベント ログを「.tar.gz」 形式のファイルに保存します。問題発生時にはこの形式のファイルを KEMP に送ってください。

WAF のイベント ログが無いと、[Reset WAF Debug/Events Logs] と[Save WAF Debug/Events Logs] ボタンを表示しません。

ログローテート情報は、https://linux.die.net/man/8/logrotate を参照してください。Linux で logrotate を実行することもできます。LoadMaster の logrotate 設定を確認するには、/etc/logrotate.d/ の設定ファイルを参照してください。

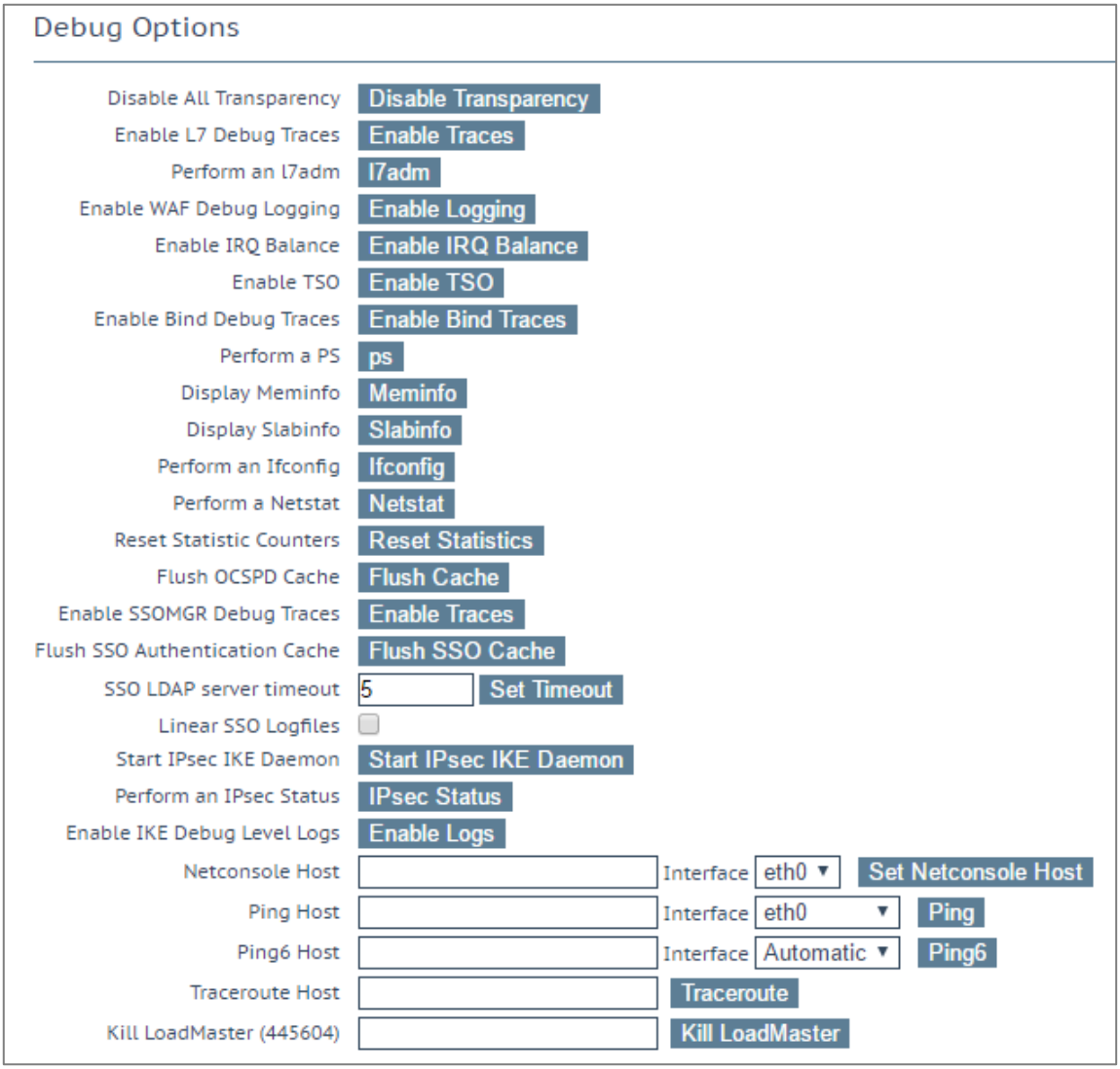
10.4.1.1 デバッグオプション

LoadMaster には、接続関連の問題を診断する際に、ユーザや 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。

ネットワーク接続がない状態でデバグが必要な場合、コンソールからログインした後に以下のコマンドを実行してデバグを行います。

echo "7" > /proc/sys/kernel/printk

実行するとデバグログをコンソールに出力します。このコマンドは充分な知識のある利用者により実行してください。利用にあたっては事前に KEMP サポートまでご連絡をお願いします。



【注意】KEMP は通常のオペレーションでデバグモードの利用を推奨していません。KEMP テクニカルサポートの指示により利用することが理想的です。
メモ：デバグコマンドは LoadMaster のパフォーマンスに影響をあたえます。さらに、このモードを実行している間は、セキュリティ上の脆弱性が増して余分な危険にさらされる恐れがあります。

Disable All Transparency（透過モードの無効化）

各バーチャル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。

このオプションはデバッグ用であり、バーチャルサービスごとに透過性を有効/無効にする通常コントロールに代わりにはなりません。

このオプションで透過性を無効にすると、無効になる前の設定をファイルにコピーして保存します。透過状態が戻ると元の設定が復元されます。ただし、バーチャルサービスは変更前の透過状態に戻らないことがあります。したがって、この間の構成変更は失われます。これには、新しい仮想サービスの作成も含まれます。

Enable L7 Debug Traces（L7 デバグトレースの有効化）

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（L7 アドミンの実行）

L7 のバーチャル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 のデバッグログの有効化）

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 が有効なすべてのバーチャル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、それらのバーチャル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 負荷分散の有効化）

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。

Perform a Top（top を実行）

[top] コマンドを実行すると LoadMaster のメモリ、CPU、I/O の利用状態を表示します。表示サンプル数とインターバルを指定できます。デフォルトはサンプル数が 10、インターバルが 1 秒です。また、チェックボックスの指定によりスレッドの表示やメモリの利用量で表示を切り替えます。

Include Top in Backups（バックアップに top を含める）

デフォルトでは、バックアップに[top] の出力を含みません。このチェックボックスを選択すると有効になります。バックアップに[top] を含む場合、[top] で指定しているパラメータは影響しません。ソートはメモリ利用量で行います。

Display Meminfo（メモリ情報の表示）

システムのメモリ使用状態を表示します。

Display Slabinfo（スラブ情報の表示）

システムのスラブ統計を表示します。

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。

Include Netstat in Backups（バックアップに Netstat を含める）

デフォルトのバックアップでは、Netstat の出力を含みます。これを含めると、バックアップの完了に時間がかかります。このオプションを無効にすると、Netstat を出力しません。

Reset Statistic Counters （リセット統計カウンタ）

すべての統計カウンタをゼロにリセットし、古いグラフも削除します。これにより、ラウンドロビンデータベース（RRD）ファイルも削除されますが、必要に応じて自動的で作成されます。

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。

Stop IPsec IKE Daemon

LoadMaster 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 ステータスを加工せずに表示します。

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、LoadMaster に保存されている SSO（シングルサインオン）のキャッシュを消去します。また、認証サーバ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 LoadMaster 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。

SSO LDAP server timeout（SSO LDAP サーバ タイムアウト）

SSO LDAP サーバのタイムアウト値を秒単位で設定します。デフォルトは 5 秒です。

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バーチャル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バーチャル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バーチャル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で、どのインターフェイスに Netconsole 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。

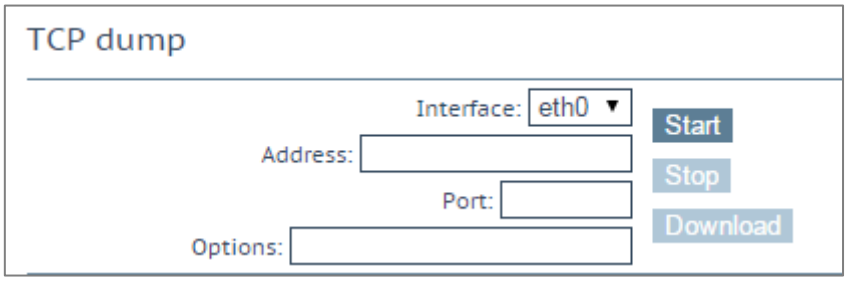
Traceroute Host（traceroute ホスト）

特定のホストのトレースルートを実行します。

Kill LoadMaster（LoadMaster の無効化）

LoadMaster 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、LoadMaster の機能を再度使用できるようになります。

KEMP テクニカルサポートに相談せずに LoadMaster を無効化しないでください。
[Kill LoadMaster] オプションは、KEMP Condor のテナントとしての LoadMaster では利用できません。



TCP dump（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。

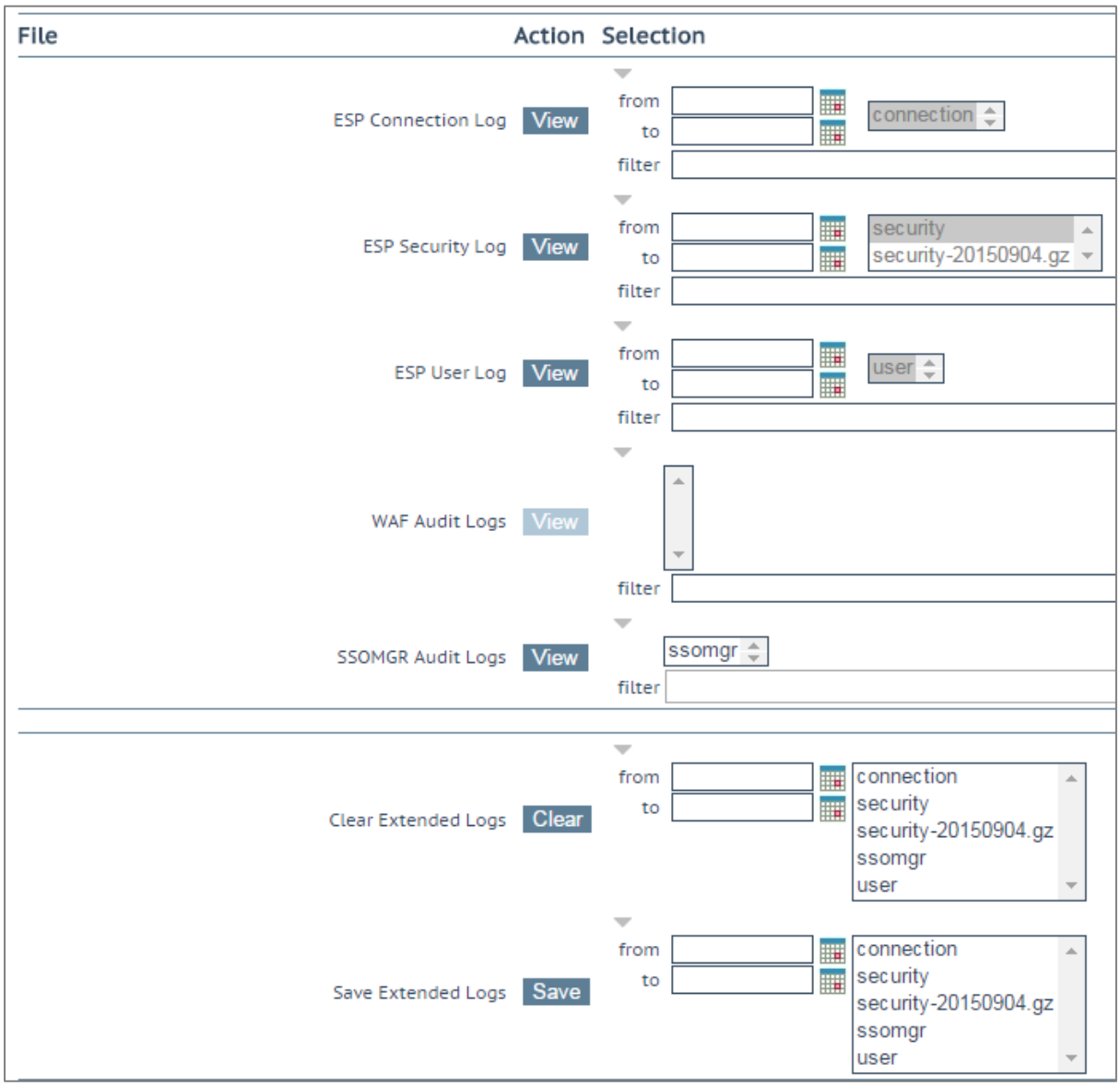
ユーザがダンプの停止および開始を切り替えることができます。また、ダンプを特定の場所にダウンロードすることもできます。TCP ダンプの結果は、Wireshark などのパケットトレース解析ツールで解析できます。

詳細は、KEMP ドキュメントページの「Packet Trace Guide, Technical Note」を参照してください。

10.4.2 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、LoadMaster 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。



さまざまなログファイルが LoadMaster に保存されます。

- **ESP Connection Log :** 各種の接続認証を行った結果を記録します
- **ESP Security Log :** すべてのセキュリティ アラートを記録します

- **ESP User Log :** すべてのユーザのログイン情報を記録します
- **WAF Audit Logs :** 「Virtual Service modify」設定画面の「WAF Options」セクションにある [Audit mode] ドロップダウンで選択した内容により 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、バーチャルサービス ID に対応します。バーチャルサービス 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てください（>Certificates & Security >Remote Access >Enable API Interface）。その後、Web ブラウザのアドレス バーに https://<LoadMasterIPAddress>/access/listvs と入力します。バーチャルサービスの[index] をチェックしてください。監査ログエントリの番号に対応します。

ログには表示のためのフィルターがあります。ログメッセージを日付順にするには、[from] と[to] に適切な日付を選択して[View] ボタンをクリックします。ESP ログの日付を選択するには、要求する日付のレコードを表示するには翌日の日付も含めます。これは、翌日のファイルに前の日付のログが含まれることがあるためです。

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。さらに、[filter] フィールドに単語や正規表現を入力して[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。

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）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。

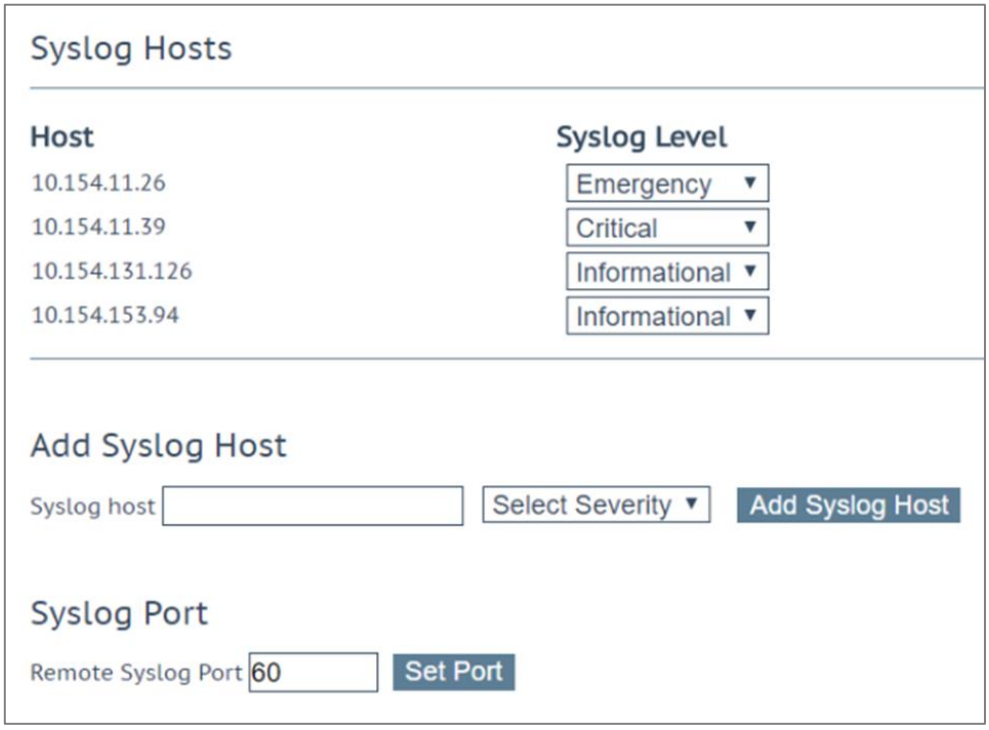
Save Extended Logs（拡張ログの保存）

矢印をクリックしてオプションを展開します。ファイルタイプを選択して日付の範囲を入力します。[Save] をクリックするとすべての拡張ログをダウンロードすることができます。

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）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 シスログ オプション

LoadMaster 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に蓄積されます。



また、LoadMaster は、これらのエラーメッセージをリモートの Syslog サーバに転送するようにに設定できます。Syslog サーバの登録は[Syslog host] に IP アドレスを入力、[Selecting Severity] で重要度を選択して[Add Syslog Host] をクリックします。

Syslog サーバの登録を削除するには、[Selecting Severity] で[None] を選択します。

エラーメッセージは、異なる 6 つのレベルがあり、各レベルを別のサーバに送信することができます。

「NOTICE」メッセージは情報として送信されます。「EMERGENCY」メッセージは通常、即時のユーザの処置が必要です。

最大 10 個までの IP アドレスを指定できます。以前の LoadMaster は 10 個以上の IP アドレス設定できましたが、アップグレード後は登録したエントリーを表示しますが追加はできません。

Syslog サーバのセットアップ後、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 の障害でユニット 2 がマスターを引き継いだ状態（HA 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 メッセージに関する注意点の 1 つは、それらが上方向にカスケードすることです。したがって、ホストが WARN メッセージを受信するように設定している場合、メッセージファイルには WARN レベル以上のすべてのレベルのメッセージを含みますが、以下のレベルは含まれません。

同じホストアドレスで再度入力すると、同じホストの古いエントリが置き換えられます。 同じホストで複数のエントリを持つ必要はありません。一つのエントリで定義する syslog レベルは、それより高いプライオリティ持つレベルをカバーするからです。このため、最低レベルのプライオリティを持つエントリを 1 つだけですべてが含まれます。

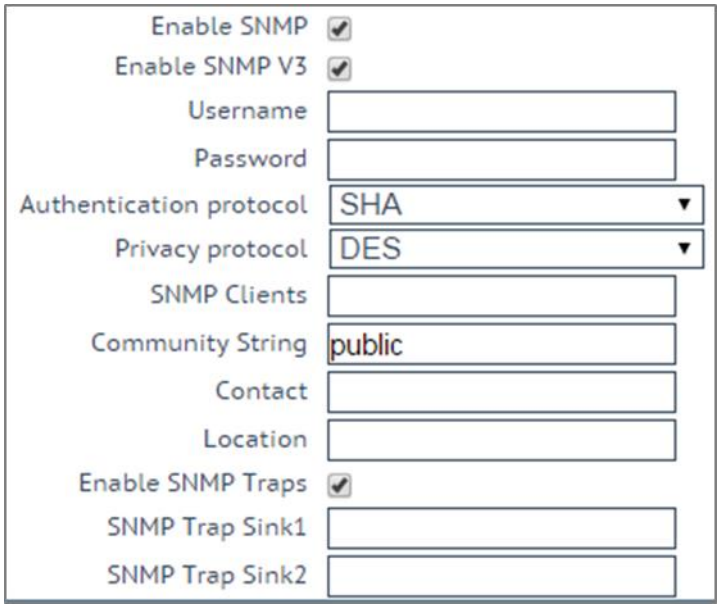
syslog 転送のために非標準ポートを設定するには、[Remote Syslog Port] テキストボックスに入力して、[Set Port] をクリックします。

リモート Linux サーバで LoadMaster 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 オプション

このメニューで SNMP の設定を変更できます。

Dell マシンの LoadMaster では、ハードウェア統計情報として温度、ファンスピード、電圧/電流等の情報を SNMP で収集することができます。これらの値は、SNMP でのみ確認できます。



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、LoadMaster 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 :** バーチャルサービス状態の変更
- **RsStateChange :** リアルサーバ状態の変化
- **HaStateChange :** HA 構成のみ：LoadMaster のフェイルオーバー

テンプレートを使って作成した、EPS が有効なバーチャルサービスの SNMP では、SubVS はマスターサービスで行わず、直接監視してください。これは、認証プロキシのサブサービスが常にアップ状態になり、結果としてマスタサービスもアップ状態になってしまうためです。

すべての LoadMaster 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	仮想サーバの統計
B-100-MIB.txt	L7 LoadMaster 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

SNMP で LoadMaster の性能と設定情報を要求できるようにするには、次のサイトから MIB ファイルをダウンロードして SNMP マネージャにインストールしてください。

カウンタの説明は、LoadMaster の MIB から取得できます。 MIB 情報を読むだけであれば、Linux の ucdsnmp を使って行うことができます。

snmptranslate -Td -OS <oid>

＜OID ：はオブジェクト識別子＞
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-ACCESSread-only

STATUScurrent

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。
LoadMasterMIB 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。

LoadMaster 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] と[Password] 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] と[Password] の設定が必要です。
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）

[Authentication protocol] で認証のプロトコルを選択します。[MD5] か[SHA] を選択できますが、推奨は[SHA] です。

Privacy protocol（プライバシープロトコル）

[Privacy protocol] でプライバシープロトコルを選択します。[AES] か[DES] を選択できますが、推奨は[AES] です。

SNMP Clients（SNMP クライアント）

このオプションでは、LoadMaster が応答するための SNMP マネージャ ホストを定義します。

クライアントを指定しない場合、LoadMaster は SNMP 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] 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、LoadMaster 管理者のメールアドレスなどです。

SNMP Location（SNMP ロケーション）

このオプションでは、LoadMaster が応答するための SNMP マネージャ ホストを定義します。

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）

LoadMaster のバーチャルサービスやリアルサーバ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、LoadMaster 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、LoadMaster 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）

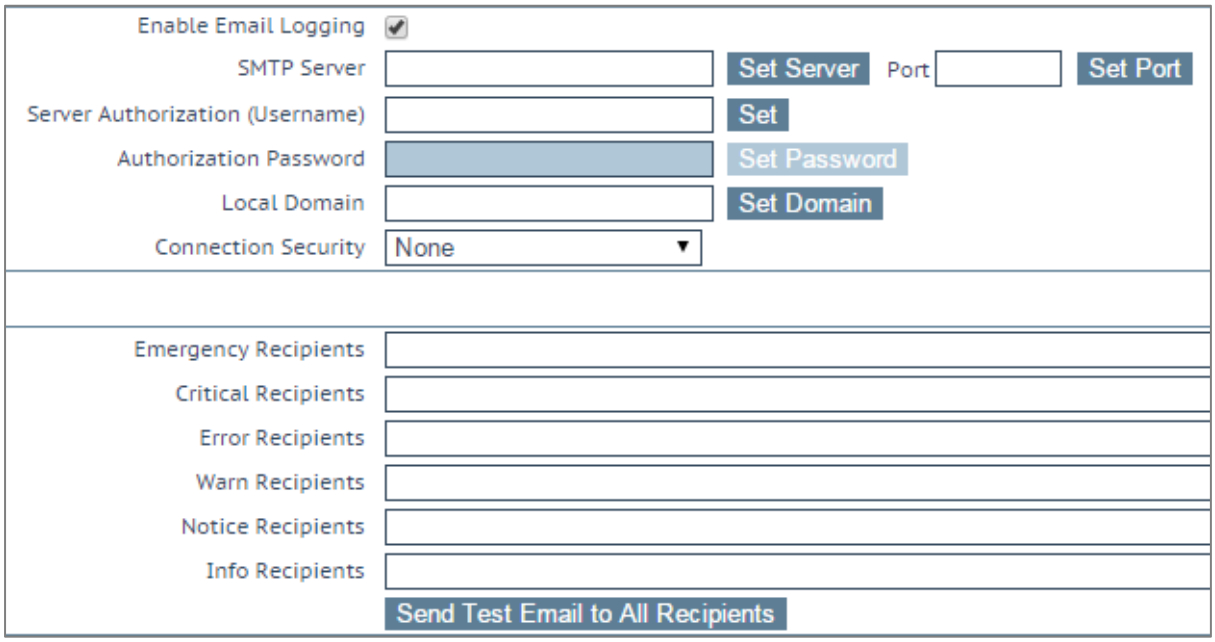
このオプションは、管理者がトラップの発生時に、SNMPv1 トラップをどのホストに送信するかを指定します。

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 メール オプション

この画面では、メールによる LoadMaster 関連イベントの警告通知を設定できます。メール通知は、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、メールサーバによりますが、ノンセキュアかセキュア両方の通信をサポートしています。



SMTP Server（SMTP サーバ）

メールサーバの 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 サーバを設定してください。

Port（ポート）

メールイベントを処理する SMTP サーバのポートを指定します。

Server Authorization (Username)（サーバ認証ユーザ名）

指定した SMTP サーバが、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
- STARTTLS, if available
- 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、それぞれ担当者のメール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。

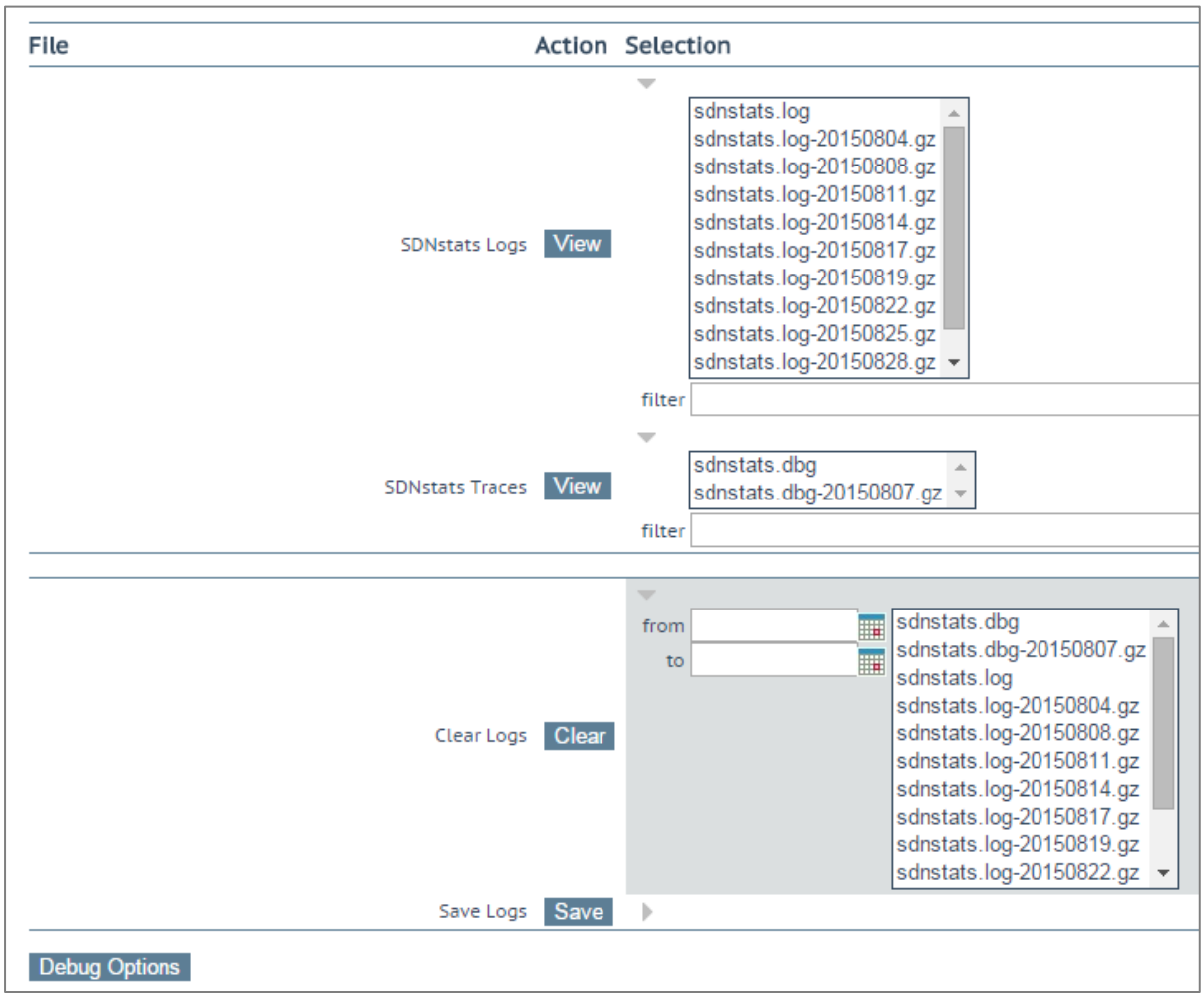
以下のように、コンマ区切りリストの形式で複数のメールアドレスを入力できます。

- 情報の受信者： info@kemptechnologies.com, sales@kemptechnologies.com
- エラー受信者： support@kemptechnologies.com

リストに登録されたすべての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。

上記はメールアラートの例です。メールの[Subject] はもっとも高いレベルに関連した内容を含みます。これらは、複数のアラートを一つのメールにまとめています。30 秒の間に発生したアラートの異同を照合して、インボックスの溢れを排除します。

10.4.6 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。

```
Apr 19 16:26:32 gstatsv2.py:iter:491 One minute timer
Apr 19 16:26:37 gstatsv2.py:run:506 Calling iter
Probing(10.35.7.10,8443,https=True):
        [HP VAN] SUCCESS [Version] 2.5.20.1227
```

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、LoadMaster が SDN コントローラ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] および[to] 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。

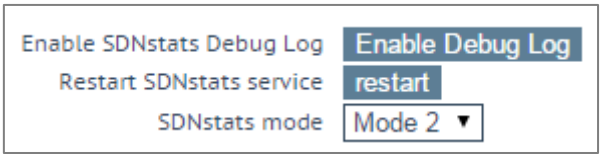
拡張ログの保存

[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 デバッグオプション

「SDN Debug Options」画面（SDN デバッグオプション画面）を開くには、「SDN Log Files」画面にある[Debug Options] ボタンをクリックします。



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] ボタンをクリックします。

デバッグログは LoadMaster 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）

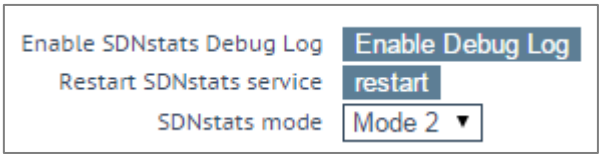
SDN の問題をトラブルシューティングする際、SDN サービス全体を再起動できます。この接続を再起動しても、トラフィックの接続には影響を与えません。このオプションは、LoadMaster と SDN コントローラとの接続のみ再起動します。

再起動すると、[Process ID] が新しい ID に変わります。[Process ID] を調べるには、 >System Configuration >Logging Options >System LogFiles の[Debug] 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。



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] 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 に設定すると、サーバ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 LoadMaster に返されます。
- **Mode 2 :** 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。

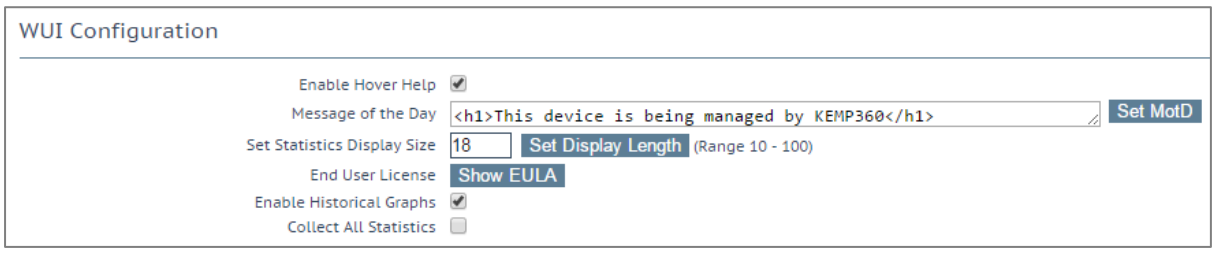
SDNstats HTTPlib timeout（SDNstats HTTPlib タイムアウト）

このフィールドで、SDN コントローラの応答待ち時間を長くすることができます。 これにより、環境による応答の遅れが原因のタイムアウトを抑制します。このフィールドの有効な値の範囲は 5～60 です。

10.5 その他のオプション

10.5.1 WUI Settings（WUI の設定）

「bal」ユーザまたは[All Permissions] の権限が設定されたユーザのみ、この機能を使用できます。それ以外のユーザの場合、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。



Enable Hover Help（ホバーヘルプ）

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、LoadMaster 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。例：&#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（エンドユーザライセンス）

"Show EULA"ボタンをクリックすると、LoadMaster のエンドユーザ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）

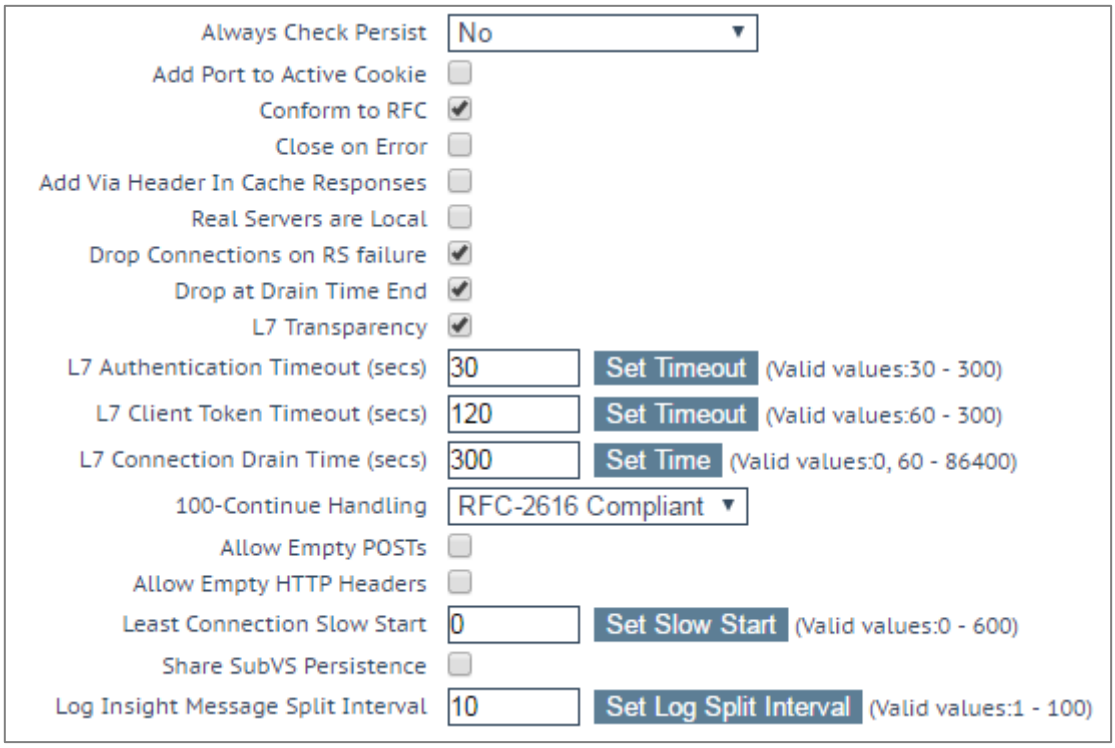
バーチャルサービスとリアルサーバに関する過去の統計情報の収集を有効にします。

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バーチャルサービスとリアルサーバ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、LoadMaster では、すべてのバーチャルサービスとリアルサーバを対象として統計情報が収集されます。

数多くのバーチャルサービスやリアルサーバ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 L7 コンフィグレーション



Allow Connection Scaling over 64K Connections

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、バーチャル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バーチャルサービスの IP アドレスを入力します。これにより、各バーチャル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。

透過バーチャル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、バーチャル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（常にパーシステンスをチェック）

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（ポートにアクティブクッキーを追加）

アクティブクッキーを使用している場合、LoadMaster はいくつかの情報の中から、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 で確認）

このオプションは、HTTP リクエストのヘッダ解析を RFC 1738 に準拠します。

このオプションをオンにすると、「GET / <パス名> HTTP/1.1」の 3 つの部分で構成する HTTP リクエスに対して、LoadMaster はスペースが表れるまで <パス名> をスキャンします。その後、HTTP/1.1 を確認します。パス名にスペースが含まれ、ブラウザが RFC に準拠している場合、そのスペースは「%20」にエスケープ処理されますので、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。これにより HTTP/1.x を見つけることができす、LoadMaster は要求を拒否します。

この機能をオフにすると、LoadMaster は強制的にスペースを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（エラーによる終了）

キャッシュ内のファイルの方が新しい場合など、LoadMaster 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 LoadMaster 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 ヘッダを追加する必要があると規定されています。残念ながら、LoadMaster 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（リアルサーバをローカルとみなす）

LoadMaster 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、クライアントがリアルサーバ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、リアルサーバがローカルであることを LoadMaster 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（クライアントとリアルサーバが 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、リアルサーバ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。リアルサーバが全く異なるネットワーク上にある場合、そのサーバ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（リアルサーバ障害時に接続をドロップする）

Microsoft Outlook ユーザに有用なオプションであり、リアルサーバ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、MS Exchange 2010, Deployment Guide を参照してください。

Drop at Drain Time End（ドレインタイム終了時にドロップ）

このオプションを有効にすると、無効化されたリアルサーバへのオープンな接続が、リアルサーバのドレイン停止時間終了時にすべてドロップします。（リアルサーバ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）

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）

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 コネクション ドレインタイム）

[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）、無効化されたリアルサーバ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、リアルサーバ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。

リアルサーバを無効にすると、直ちにすべての接続を閉鎖するわけではありません。これを穏やかなクローズといいます。

新しいパーシステンスは、有効な永続性レコードがない限り、排水時間中に実サーバに移動しません。 ドレインタイムが終了すると、Drain Time End で Drop が選択されると、既存のすべての接続が強制的に削除されます。 それ以外の場合、接続は開いたままです。 ドレン停止タイマーは、ドロップ時ドレインタイムエンドが有効になっていない限り、既存の接続に影響を与えません。

新しい接続では、有効なパーシステンス レコードがない限り、ドレイン時間ではリアルサーバに移動しません。もし、ドレイン時間の終了でドロップする、を選択した場合、すべての Drain は強制的に終了します。それ以外はコネクションはオープンの状態です。ドレイン終了タイマーが、ドロップ時のドレインタイムエンドで有効で無い場合、既存の接続に影響を与えません。

- Additional L7 Header（L7 ヘッダの追加）

HTTP/HTTPS バーチャルサービスのレイヤ 7 ヘッダ挿入を有効にします。ヘッダ挿入の設定は、「X-ClientSide」（KEMP LoadMaster 専用）、[X-Forwarded-For] または[None] のいずれかを選択できます。デフォルトは X-Forwarded-For です。

100-Continue Handling（100-Continue メッセージのハンドリング）

「100-Continue」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 で規定された動作に準拠します
- **Require 100-Continue :** 100-Continue メッセージを待機するよう、LoadMaster を設定
- **RFC-7231 Compliant :** LoadMaster 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（エンプティ POST の許可）

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 ヘッダまたは Transfer-Encoding ヘッダを含まない POST は、LoadMaster 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しません。

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。

Force Complete RS Match（強制的な RS マッチ）

デフォルトでは、LoadMaster はコンテンツスイッチを使用するリアルサーバを見つけようとするとき、ポートが同じではなくても、現在選択している同じリアルサーバを使用します。 このオプションを有効にすると、ポートも強制的に比較します。

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、リアルサーバがオンラインになったときにそのサーバ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、リアルサーバ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 SubVS パーシステンス）

デフォルトでは、バーチャルサービスの各 SubVS 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、SubVS 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、そのバーチャルサービス内にあるすべての SubVS 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 SubVS 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。

- SubVS のすべてのリアルサーバが同じでなければなりません
- すべての SubVS で、[Persistence Mode]（パーシステンスモード）が同じでなければなりません
- タイムアウト値を同じ値に設定する必要があります

上記の要件が満たされない場合、その SubVS または複数の SubVS 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。

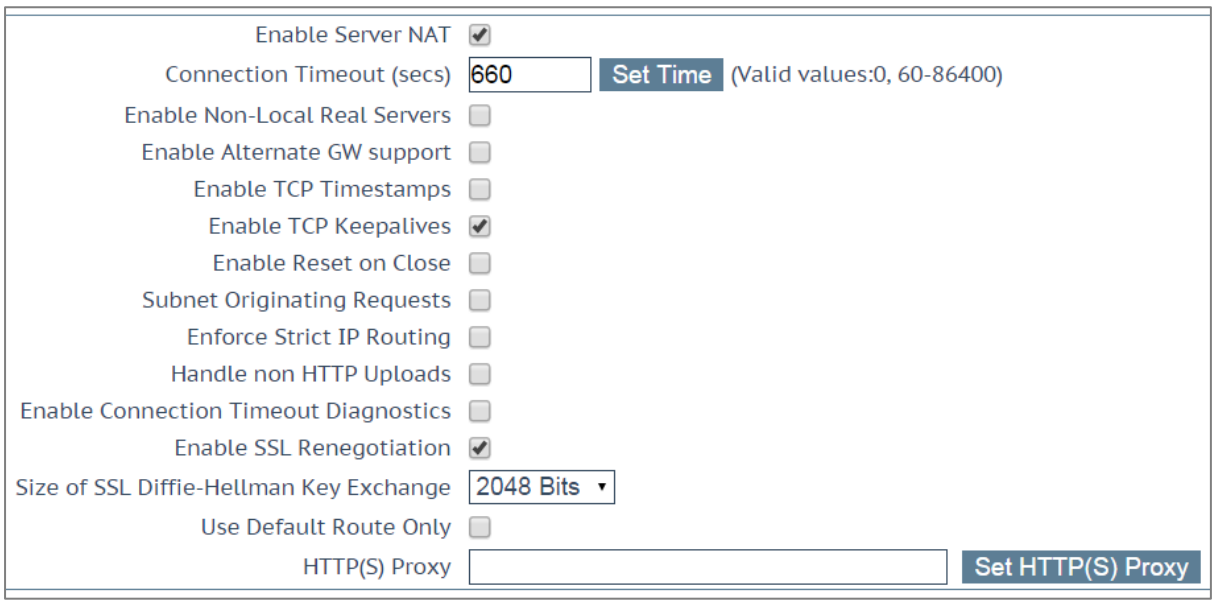
Log Insight Message Split Interval（ログインサイト メッセージ分割間隔）

[Log Insight Split Interval] の値はプール内のそれぞれのサーバに送信すべき Syslog メッセージ数をコントロールします。例えば、[Log Insight] ノードが 3 つで、[Log Insight Split Interval] が 1 を設定している場合、単一のメッセージはサーバ A に配信する前に、サーバ A、サーバ B、サーバ C の順で送ります。

Include User Agent Header in User Logs（ユーザエージェント ヘッダを含むユーザログ）

設定が有効な場合、ユーザエージェント ヘッダ フィールドにユーザログを追加します。

10.5.3 ネットワーク オプション



Enable Server NAT（サーバ NAT の有効化）

このオプションを選択すると、サーバ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、接続時にリアルサーバの 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。バーチャルサービスにおいて[Use Address for Server NAT] を有効にすると、バーチャル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、「スタンダード」セクション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（リモートサーバの有効化）

非透過モード（Non ransparent）バーチャルサービスで、ローカルサブネット以外のサーバを、リアルサーバとして追加できます。透過モード（Transparent）のバーチャル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。LoadMaster がインターフェイスを 1 つしか持つことができず、リアルサーバ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。

オプションのデフォルトは「有効」です。

Enable Alternate GW support（代替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 LoadMaster の画面に別途表示します。

Enable TCP Timestamps（TCP タイムスタンプの有効化）

LoadMaster は、クライアントからの接続とリアルサーバへの接続で、TCP の SYN パケットにタイムスタンプを含めることができます。

注意： これは NAT 接続に影響する可能性がありますので、KEMP テクニカルサポートと協議した上で、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、LoadMaster からリアルサーバ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（クローズでのリセットを有効化）

このオプションを有効にすると、LoadMaster 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、リアルサーバ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（サブネットアドレスでのリクエスト）

このオプションを有効にすると、IP アドレスを透過しないで、LoadMaster の IP アドレスをソース IP アドレスにします。ソース IP アドレスは、リアルサーバと同じサブネットか、リアルサーバへルーティングするゲイトウェイと同じサブネットになります。透過しない条件は、リアルサーバがローカルでない場合とスタティックルートを設定している場合です。詳細な情報は、詳細な情報とスタティックルートの設定は、KEMP ドキュメントページの Creating a Static Route を参照してください。

これはグローバル オプションの設定です。

バーチャルサービスごとに[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を無効にすると、各バーチャルサービスの[Subnet Originating Requests] オプションが優先されます。すなわち、バーチャルサービスごとに有効/無効にできます。このオプションは、バーチャル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）。バーチャルサービスごとのオプションに関する詳細は、「スタンダードオプション」セクションを参照してください。

SSL の再暗号化が有効なバーチャル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、そのバーチャル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] 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）

デフォルトでは、LoadMaster は、SSL トランザクションの間でクライアントとの自動のネゴシエーションを許可します。このオプションをオフにすると、クライアントからネゴシエーションの再要求があると SSL 接続を終了します。

Legacy TCP Timewait Handling（レガシーTCP タイムウェイト処理）

このオプションを有効にすると、TCP のタイムアウト接続のレガシーモードに復帰します。

Only enable the Legacy TCP Timewait Handling option after consulting with KEMP Support.

Enable SSL Renegotiation（SSL に再ネゴシエーションの有効化）

デフォルトでは、LoadMaster は SSL トランザクション期間中にクライアントが自動で再ネゴシエートを行うことを許可しています。このオプションをオフにすると、クライアントが再ネゴシエーションを要求しても、SSL 接続を終了します。

Force Real Server Certificate Checking（リアルサーバ証明書の強制チェック）

デフォルトでは、リクエストを再暗号化するとき、LoadMaster はリアルサーバが提供する証明書をチェックしません。 このオプションでは、LoadMaster がリアルサーバ上の証明書が有効であること（認証局と有効期限が正しいこと）を確認すします。これにはすべての中間証明書も含まれます。

Size of SSL Diffie-Hellman Key Exchange（SSL の Diffie-Hellman 鍵交換サイズ）

鍵の強度で Diffie-Hellman 鍵交換を使用できます。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）

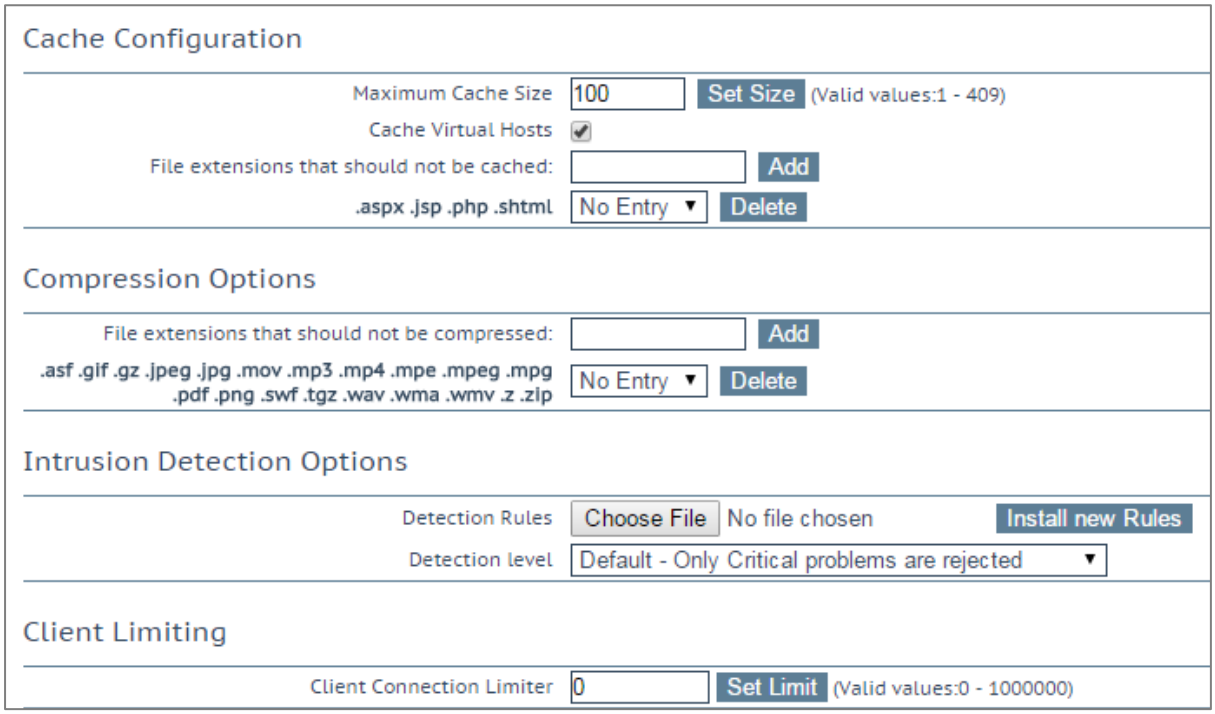
デフォルトのルートエントリセットを持つバーチャルサービスからのトラフィックを、バーチャルサービスのデフォルトルートが存在するインターフェイスにのみルーティングするようにします。この設定を使用すると、隣接するインターフェイスを使用してトラフィックを直接返送することなく、LoadMasterをクライアントネットワークに直接接続できます。

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バーチャル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、LoadMaster がインターネットに接続する際に使用する HTTP プロキシサーバとポートをクライアントが指定できます。

10.5.4 AFE コンフィグレーション



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、リアルサーバ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、リアルサーバ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

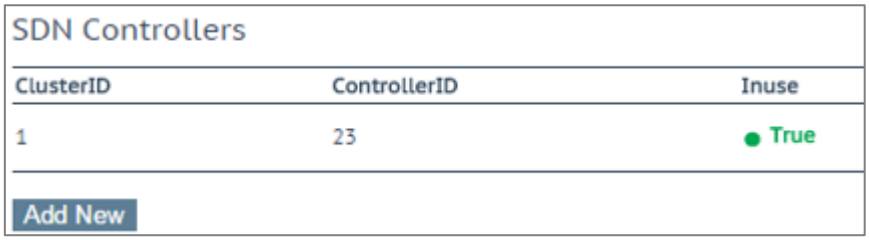
Client Limiting（クライアントの制限）

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 コンフィグレーション



新規追加

SDN コントローラ接続を新規に追加します。

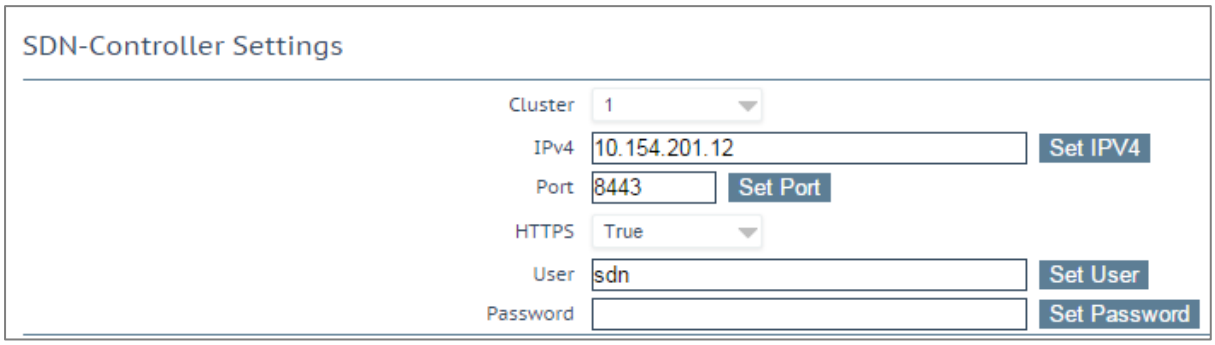
Modify（変更）

既存の SDN コントローラ接続を変更します。

Delete（削除）

既存の SDN コントローラ接続を削除します。

10.5.5.1 SDN コントローラの設定



SDN コントローラの接続を新たに追加する際、始めに、[Cluster] 、[IPv4] [Port] を入力する画面を表示します。SDN コントローラの接続を追加後、「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）

SDN コントローラがメンバーとなるクラスタです。

[Cluster] フィールドはデフォルトのままにしてください。

IPv4

SDN コントローラの IPv4 アドレス

Port（ポート）

SDN コントローラ 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 コントローラへのアクセスに HTTP/HTTPS を使用します。

User（ユーザ）

SDN コントローラへのアクセスで使用するユーザ名です。

Password（パスワード）

SDN コントローラへのアクセスで使用するパスワードです。

11 関連資料

11.1 Web サービス

Documentation

Technical documentation for LoadMaster including technical notes, configuration guides and deployment guides are available on KEMP's Help Center.
Documentation

Knowledge Base

Learn from KEMP Customer Support and your peers how to get the most out of your products and solve common challenges.
Knowledge Base

Customer Support

Engage with our customer support team to open a ticket or get help optimizing your application deployment.
Contact Support

Software Updates

Get the latest information about firmware releases, hotfixes and new application templates.
Get the Latest

Feature Requests

Have an idea about how to make KEMP products better? We'd love to hear about it.
Submit Feature Request

Give Us Feedback

Tell us about your experience working with KEMP products.
Tell Us About It

KEMP 360

Learn how KEMP 360 can help you streamline application delivery automation, management, outage prevention and time to resolution.
KEMP 360

ヘルプ画面は、外部 KEMP サービスへのアクセスのための統合された場所を提供します。

Documentation（技術ドキュメント）

KEMP の技術ドキュメントにアクセスしてください。Deployment Guides（デプロイメントガイド）、Installation Guides（インストールガイド）、Feature Descriptions（機能説明）、Technical Notes（テクニカルノート）、Overviews（概要）、Release Notes（リリースノート）、Interface Descriptions（インターフェイス説明）などがあります。

Knowledge Base（ナレッジベース）

SSO/ESP、Fault Tolerance（フォールトトレランス）、Operational Maintenance（運用保守）、Applications（アプリケーション）、Security（セキュリティ）、Platforms（プラットフォーム）、Routing/Switching（ルーティング/スイッチング）、Content Delivery（コンテンツ配信）など、さまざまなテーマのナレッジベース記事にアクセスできます。

Customer Support（カスタマーサポート）

KEMP のカスタマーサポートに問い合わせできます。

Software Updates（ソフトウェアアップデイト）

ファームウェアリリース、ホットフィックス、および新しいアプリケーションテンプレートに関する最新情報を入手できます。

Feature Requests（機能要求）

Take a look at existing feature requests submitted by other customers, and raise your own feature request.

他のお客様が発案した機能要求を確認したり、独自に機能を要求することができます。

Give Us Feedback（フィードバック）

製品の使用感などを KEMP に対して提言することができます。

KEMP 360

アプリケーション配信の自動化、停電対策、問題解決の短縮など、KEMP 360 製品についての各種ノウハウを提供しています。

11.2 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。

- Virtual Services and Templates, Feature Description（バーチャルサービスとテンプレート機能説明）
- RSA Two Factor Authentication, Feature Description（RSA の 2 要素認証 機能説明）
- Content Rules, Feature Description（コンテンツルール機能説明）
- LoadMaster 5.1 to 6.0 Migration, Technical Note（LoadMaster5.1 から 6.0 への移行テクニカルノート）
- Header Modification Guide, Technical Note（ヘッダ変更ガイド テクニカルノート）
- GEO, Feature Description（GEO 製品概要）
- GEO Sticky DNS, Feature Description（GEO Sticky DNS 機能説明）
- Packet Trace Guide, Technical Note（パケットトレースガイド テクニカルノート）
- VMware Tools Add-On Package, Feature Description （VMware ツールのアドオンパッケージ機能説明）
- Custom Authentication Form, Technical Note（カスタム認証フォーム テクニカルノート）
- Port Following, Feature Description（ポートフォローイング機能説明）
- SSL Accelerated Services, Feature Description（SSL アクセラレーションサービス機能説明）
- Kerberos Constrained Delegation, Feature Description（Kerberos Constrained Delegation 機能説明）
- Hardware Security Module (HSM), Feature Description（ハードウェアセキュリティモジュール（HSM）機能説明）
- IPsec Tunneling, Feature Description（IPsec トンネリング機能説明）
- KEMP LoadMaster, Product Overview（KEMP LoadMaster 製品概要）
- SDN Adaptive Load Balancing, Feature Description（SDN アダプティブ負荷分散 機能説明）
- DoD Common Access Card (CAC) Authentication, Feature Description（DoD 共通アクセスカード（CAC）認証 機能説明）
- RESTful API, Interface Description（RESTful API インターフェイス説明）
- Licensing, Feature Description（ライセンス機能説明）
- Radius Authentication and Authorization, Technical Note （RADIUS の認証と権限設定テクニカルノート）
- LoadMaster Clustering, Feature Description（LoadMaster のクラスタリング機能説明）
- MS Exchange 2010, Deployment Guide（Microsoft Exchange 2010 展開ガイド）
- RADIUS Authentication and Authorization, Technical Note（RADIUS の認証と権限設定 テクニカルノート）
- User Management, Feature Description（ユーザ管理 機能説明）

・改版履歴

- 改版履歴

Date	変更	Reason for Change	Ver	Resp
2016/10	アップデイト リリース	7.2.36 リリースに伴うアップデイト	12.0	LB
2017/01	アップデイト リリース	7.2.36 リリースに伴うアップデイト	13.0	LB
2017/03	アップデイト リリース	7.2.36 リリースに伴うアップデイト	14.0	LB
2017/07	アップデイト リリース	7.2.36 リリースに伴うアップデイト	15.0	LB
2018/03				