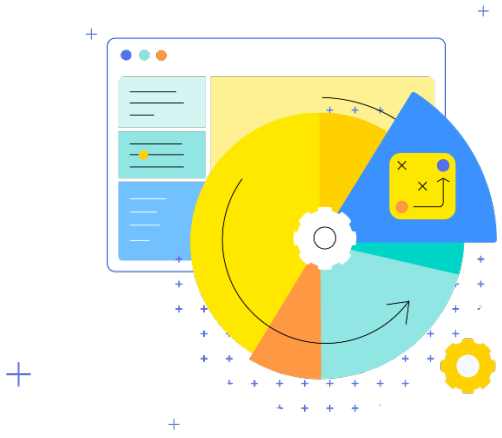
Kemp LoadMaster
Web User Interface (WUI)
構成ガイド



Updated 2022/9/19

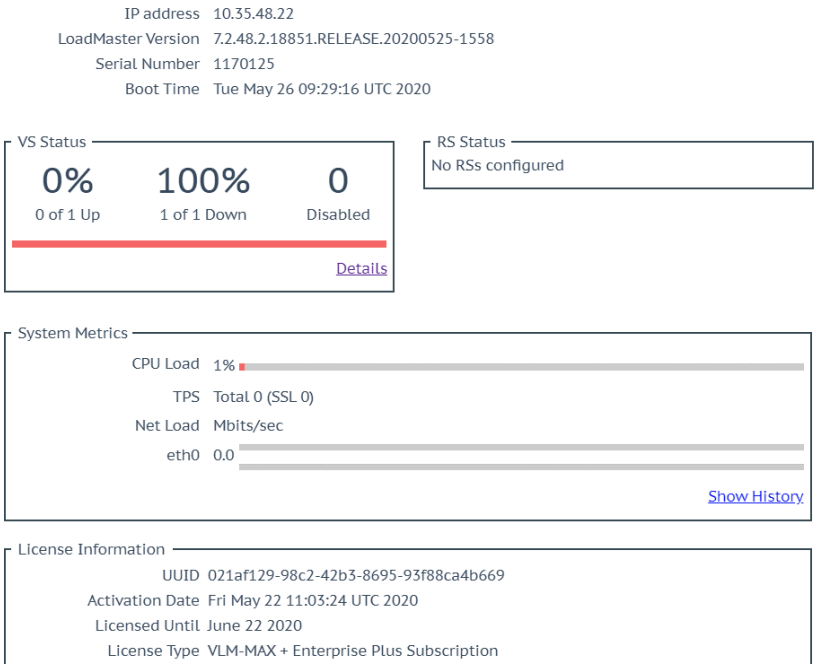
目次

1 はじめに

製品は、高可用性、高性能、柔軟なスケーラビリティ、セキュリティ、および管理の容易さによって定義されるように、Web およびアプリケーション インフラストラクチャを最適化します。 製品は、柔軟で包括的な展開オプションを可能にしながら、Web インフラストラクチャの総所有コストを最大化します。

2 ホーム

[Home] メニュー オプションをクリックすると、ロードマスターに関する基本情報のリストを示すホームページが表示されます。



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

2.1 ログイン情報

LoadMaster に最初にログインした後、セッション管理が有効になっている場合、いくつかのログイン情報が表示されます。

- 現在のユーザーの最終ログイン時刻と IP アドレス
- 現在のユーザーが過去 30 日間に成功したログインの数
- 前回のログイン成功以降に任意のユーザー (未知のユーザー名を含む) が失敗したログイン試行の総数

セッション管理の詳細については、OCSP Configuration Admin WUI Access セクションを参照してください。

2.2 一般情報

IP アドレス: LoadMaster の IP アドレス。

LoadMaster バージョン: LoadMaster のファームウェア バージョン。

シリアル番号: LoadMaster のシリアル番号。

起動時間: サーバーが最後に再起動された時間。

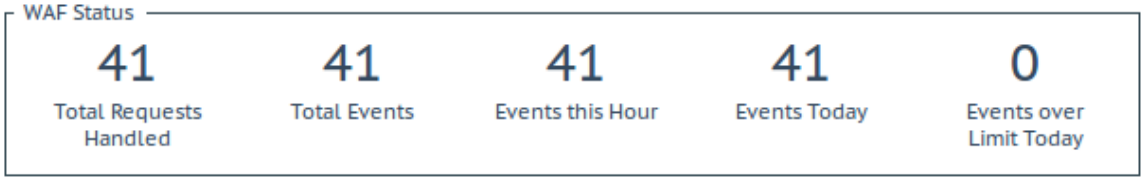
2.3 仮想サービスと実サーバーのステータス

VS ステータス

このセクションには、稼働中の仮想サービスのパーセンテージや無効な仮想サービスの数など、仮想サービスの監視情報が表示されます。 [Details] リンクをクリックすると、[View/Modify Services] 画面が表示されます。 稼働中/停止中の仮想サービス、SubVS、実サーバーの数などに関する syslog メッセージが 1 時間ごとに生成されます。 ステータスが変化すると、syslog メッセージも生成されます。

RS ステータス

このセクションには、稼働している実サーバーのパーセンテージや無効になっている実サーバーの数など、実サーバーの監視情報が表示されます。 詳細リンクをクリックすると、実サーバー画面が表示されます。



少なくとも 1 つの仮想サービスで WAF が有効になっている場合、[Web アプリケーション ファイアウォール (WAF) ステータス] セクションが表示されます。 ここに表示される値は次のとおりで

す。

- WAF によって処理されたリクエストの総数 (ブロックされたかどうかにかかわらず、すべてのリクエストを表示します)。 接続ごとに 2 つの要求が記録されます。 1 つの着信要求と 1 つの発信要求です。
- WAF によって処理されたイベント (つまり、ブロックされた要求) の総数
- 現在の時間に発生したイベントの数 (xx.00.00 以降)
- 午前 0 時 (現地時間) 以降に発生したイベントの数
- 今日、イベント カウンタが設定された警告しきい値を超えた回数。 たとえば、しきい値が 10 に設定され、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。 仮想サービスの変更画面。 詳細については、「レガシー Web アプリケーション ファイアウォール (WAF) オプション」セクションを参照してください。

2.5 システム指標

CPU 負荷: LoadMaster アプライアンスの CPU に対する負荷の割合。

TPS [conn/s]: 1 秒あたりの合計トランザクション数と 1 秒あたりの Secure Sockets Layer (SSL) トランザクション数。

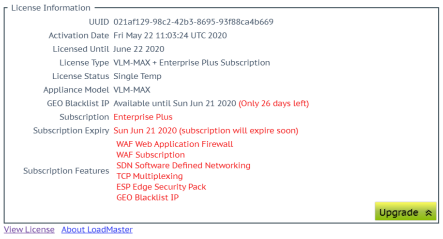
Net Load: ネットワーク負荷 (メガビット/秒)。構成されたインターフェースごとに表示されます。 Net Load は、構成済みのインターフェースについてのみ表示されます。

CPU 温度: サポートされているハードウェア プラットフォームの CPU の温度を表示します。

CPU 負荷とネット負荷のデータは 5 秒ごとに更新されます。

これらの値は、SNMP を使用してのみ使用できます。 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。

2.6 ライセンス情報



[View License] リンクをクリックして、モデル、サブスクリプションの有効期限、サブスクリプション機能の詳細 (LoadMaster ライセンスのアクティベーション日と終了日など) を表示します。

LoadMaster にトライアル ライセンスまたはサブスクリプション ライセンスがあり、有効期限が切れている場合は、[License Information] セクションにメッセージが表示されます。 サブスクリプションを更新するには、Kemp にお問い合わせください。

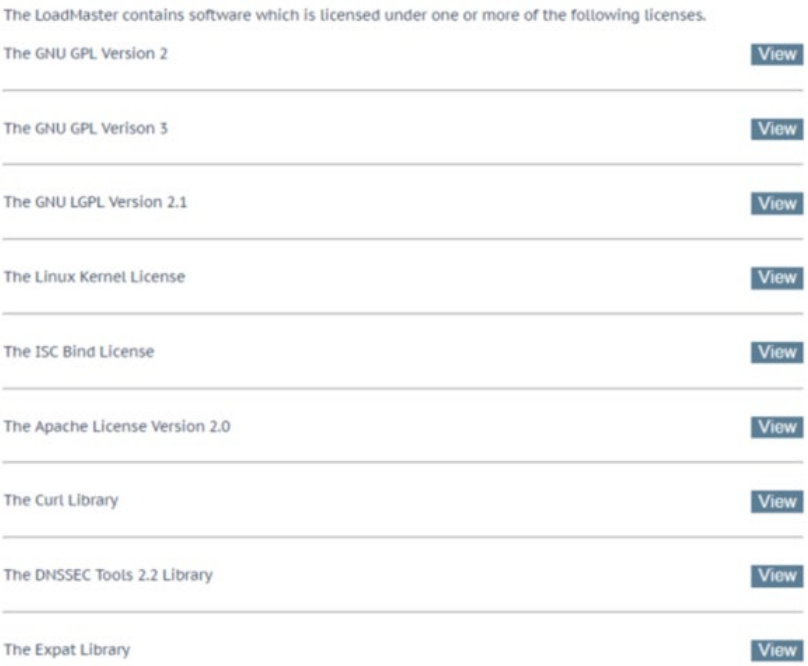
永久ライセンスと、Standard、Enterprise、または Enterprise Plus などのサポート サブスクリプションを持つ LoadMaster は、サポート サブスクリプションの有効期限が切れても引き続き機能します。 サポート サブスクリプションの有効期限が切れると、WAF や GEO の毎日のレピュテーション データなどの一部の機能のみが動作しなくなる場合があります。

ライセンスまたはサブスクリプションの有効期限の 13 日前から、有効期限を示すメッセージがホーム画面に表示されます。 アプライアンスのライセンスを再取得するか、サブスクリプションを更新するには、Kemp の営業担当者にお問い合わせください。

アップグレード: Progress Kemp 購入ポータルからライセンスを購入して、LoadMaster をアップグレードします。
Progress Kemp 購入ポータルは、米国のお客様のみが利用できます。

2.7 LoadMaster について

About LoadMaster ページでは、LoadMaster で使用されているサードパーティ ソフトウェアのライセンスを表示できます。

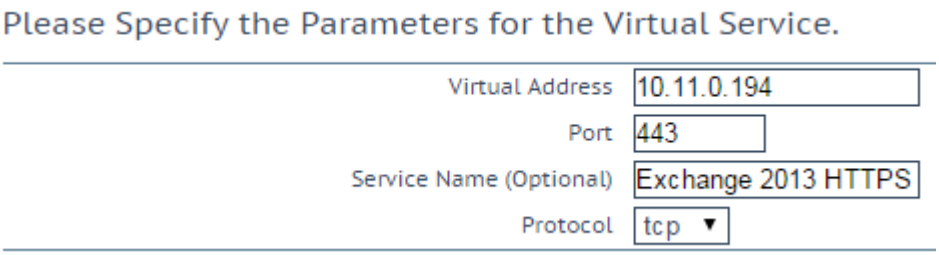


ライセンスを表示するには、関連する項目の横にある [View] ボタンをクリックします。

3 仮想サービス

仮想サービスこれ以降、このドキュメントの見出しは通常、LoadMaster WUI の左側にあるメインメニューのオプションに対応しています。

3.1 新しく追加する

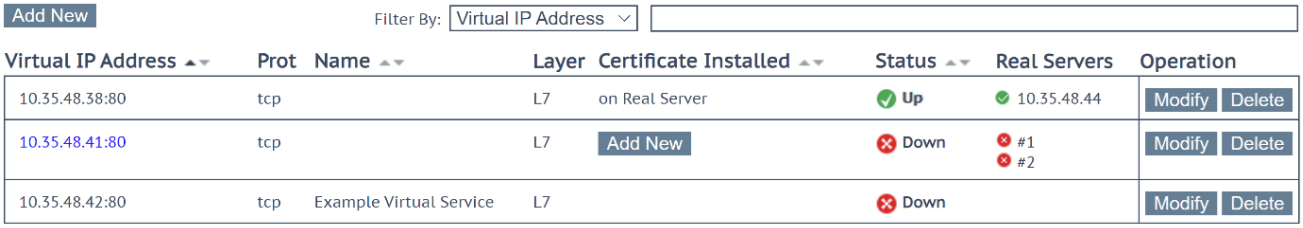


ここでは、仮想 IP (VIP) アドレス、ポート、プロトコル、および名前が定義されています。 VIP アドレス、名前、およびポートをテキスト ボックスに手動で入力し、ドロップダウン リストからプロトコルを選択します。

サービス名の最初の文字として特殊文字を使用することはできません。

テンプレートがマシンにインストールされている場合は、[Use Template] ドロップダウン リストが使用可能になり、テンプレートを選択して、ポートやプロトコルなどの仮想サービス パラメータを構成できます。
テンプレートの詳細については、仮想サービスとテンプレート機能の説明を参照してください。

3.2 表示/変更 (既存の HTTP サービス)



この画面から、仮想サービスを追加または変更できます。 フィルタ テキスト ボックスを使用して、仮想 IP アドレス、名前、およびステータスに基づいて仮想サービスをフィルタリングすることもできます。 詳細については、以下のセクションを参照してください。

3.2.1 仮想サービスのフィルタリングとソート

[Filter By] ドロップダウン リストから選択したオプションに基づいて、仮想サービスをフィルタリングできます。
使用可能なフィルタ オプションは次のとおりです。

- 仮想 IP アドレス
- 名前
- ステータス

デフォルトでは、[仮想 IP アドレス] オプションが選択されています。

[仮想 IP アドレス]、[Name]、または [Status] (ドロップダウンで選択した内容に応じて) に含まれるテキスト ボックスにテキストを入力すると、リストは即座にフィルター処理され、一致する結果が表示されます。 (ドロップダウンで選択したオプションに基づいて) 一致しないテキストを入力すると、テキスト ボックスが赤く点滅し、一致しないテキストが削除されます。 仮想サービス テーブルには、LoadMaster 上の仮想サービスのリストが表示され、それぞれの主なプロパティが要約され、

サービスを変更または削除したり、新しいサービスを作成したりするためのオプションが示されます。テーブル ヘッダーの上下矢印オプションを使用して、仮想 IP アドレス、名前、インストールされている証明書、およびステータスでエントリを並べ替えることができます。

- 仮想 IP アドレスの場合、エントリは最初に IP バージョン (IPv4 の次に IPv6) でソートされ、次に IP アドレス (昇順) またはその逆でソートされます。

  ページの表示中に仮想サービスが変更された場合、リストは再ソートされません。 また、並べ替えは SubVS には適用されません。
- Name のソート順は、最初に空白のエントリが表示され、その後に特殊文字が表示され、残りのエントリはアルファベット順 (またはその逆) で表示されます。
- 証明書がインストールされている場合、並べ替えの順序は次のとおりです (またはこの逆)。
  - 数値
  - 特殊文字
  - アルファベット順
  - 証明書を追加する必要がある SSL ベースの仮想サービス
  - 証明書のない仮想サービス (および SSL アクセラレーションが無効)
- ステータスの場合、並べ替えの順序は次のとおりです。
  各ステータスの意味については、後述の「仮想サービス ステータス」セクションで説明します。
  - アップ/チェックなし (どちらも同レベル)
  - 失敗メッセージ
  - リダイレクト
  - Sorry
  - WAF の設定ミス
  - セキュリティダウン
  - 下
  - 無効

  逆の順序で:
  - 無効
  - 下

- セキュリティダウン
- WAF の設定ミス
- sorry
- リダイレクト
- 失敗メッセージ
- アップ/チェックなし (どちらも同レベル)

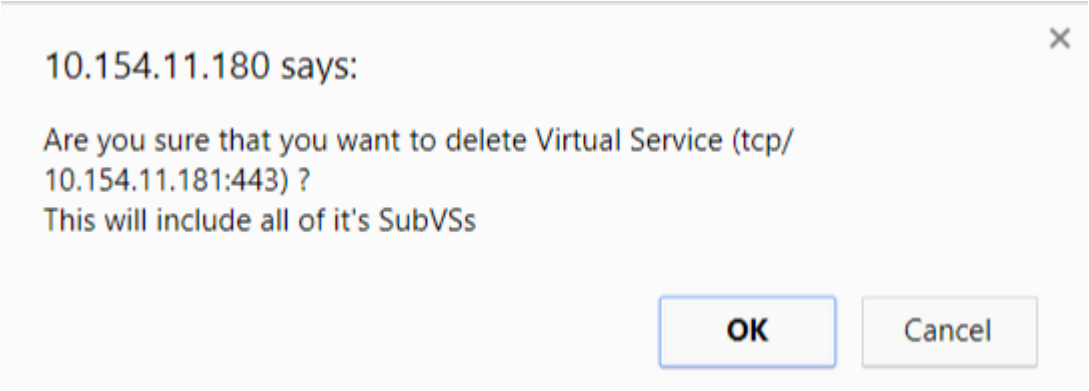
色が濃い矢印を確認することで、現在適用されているソートを確認できます。 一度に適用できる並べ替えは 1 つだけです。 明るい色の矢印の 1 つをクリックして、新しい並べ替えを適用します。

3.2.2 仮想サービスの変更と削除

注意

削除は永続的であり、UNDO 機能はありません。 注意して使用してください。

構成された各仮想サービスは、[Modify] ボタンをクリックして変更するか、[Delete] ボタンをクリックして削除できます。



SubVS を含む仮想サービスを削除しようとすると、確認の警告が表示されます。 [OK] をクリックして削除を確認します。

3.2.3 仮想サービスのステータス

仮想サービスのステータスが表示されます。 仮想サービスが作成されると、デフォルトでヘルスチェックが有効になります。 ヘルス チェックの詳細については、実サーバーのセクションを参照してください。 仮想サービスのステータスは、次のいずれかになります。

- Up – 少なくとも 1 つの実サーバーが利用可能です。
- Down – 使用できる実サーバーがありません。

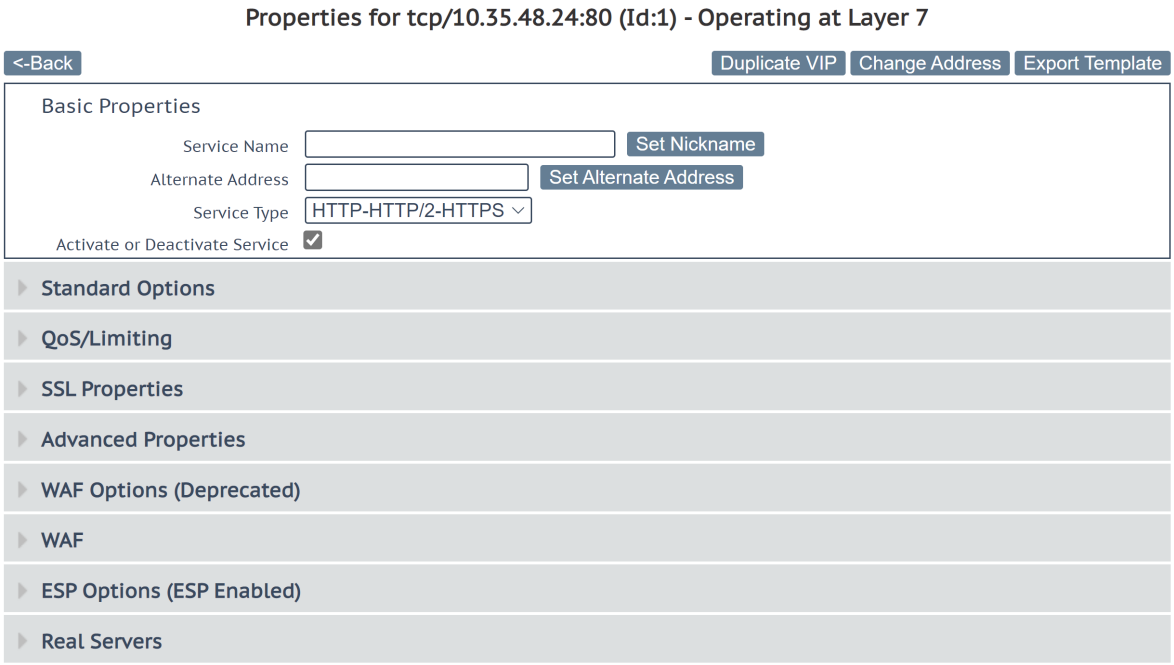
- Sorry – すべてのリアル サーバーがダウンしており、トラフィックは、ヘルス チェックなしで、リアル サーバー セットの一部ではない個別に構成されたソーリー サーバーにルーティングされます。
- Disabled - 仮想サービスの変更画面の [Basic Properties] セクションにある [サービスの有効化または無効化] チェック ボックスをオフにすることで、仮想サービスが管理上無効になっています。
- Redirect – 固定のリダイレクト応答が構成されています。 [Advanced Properties] セクションの [Add a Port 80 Redirector VS] オプションを使用して、リダイレクト仮想サービスを作成できます。

詳細については、「Advanced Properties」セクションを参照してください。

- Fail Message – 固定エラー メッセージが構成されています。 Not Available Redirection Handling オプションを使用して、固定エラー メッセージを指定できます。 詳細については、高度なプロパティのセクションを参照してください。
- Unchecked – 実サーバーのヘルスチェックが無効になっています。 すべての実サーバーがアクセスされ、稼働していると見なされます。
- Security Down – LoadMaster は認証サーバーに到達できず、Edge Security Pack (ESP) を含む仮想サービスへのアクセスを妨げます。
- WAF Misconfigured – 特定の仮想サービスの WAF が設定ミスの場合 (ルール ファイルに問題がある場合など)、ステータスは WAF の設定ミスに変わり、赤色になります。 仮想サービスがこの状態にある場合、すべてのトラフィックがブロックされます。 問題のトラブルシューティング中に、必要に応じてその仮想サービスの WAF を無効にして、ブロックされているトラフィックを停止できます。

3.2.4 仮想サービス設定セクション

以下の画像は、仮想サービスのプロパティ画面を示しています。 これは、いくつかのコンポーネントセクションで構成されています。



- Basic Properties - 通常の最も一般的な属性が設定されている場所
- Standard Options – 仮想サービスで最も広く使用されている機能
- QoS/Limiting - 速度制限接続/帯域幅に関連するオプションを LoadMaster に設定したり、特定のクライアント デバイスから設定したりできます。
- SSL Properties – SSL アクセラレーションが使用されている場合、Acceleration Enabled と表示され、画面のこのセクションを使用して SSL 機能を設定します。
- Advanced Properties – 仮想サービスの追加機能
- WAF Options – Web アプリケーション ファイアウォール (WAF) に関連するオプションを設定できます。
- ESP Options – ESP に関連するオプションが設定される場所
- Real Servers/SubVSs - 実サーバー/サブ VS が仮想サーバーに割り当てられている場合

サービス タイプ、および有効または無効な機能に応じて、特定のフィールドとオプションが WUI に表示されます。 このドキュメントのスクリーンショットは、考えられるすべての構成を表していない場合があります。

3.3 基本特性

[Basic Properties] 見出しの横に 3 つのボタンがあります。

Duplicate VIP

このオプションは、関連する SubVS を含む仮想サービスのコピーを作成します。 すべての仮想サービス構成設定が、複製された仮想サービスにコピーされます。 このボタンをクリックすると、コピーした仮想サービスの IP アドレスとポートを指定する画面が表示されます。

Change Address

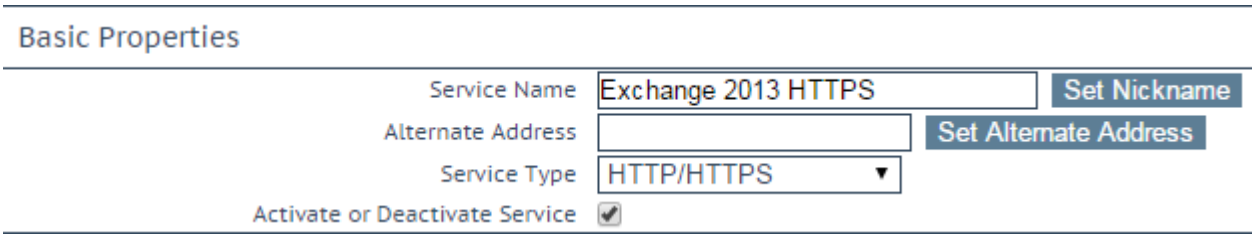
このボタンをクリックすると、仮想サービスの仮想 IP アドレスとポートを変更できる画面が開きます。

Export Template

仮想サービスの設定をテンプレートとしてエクスポートします。 テンプレートを使用して、仮想サービスをすばやく簡単に作成できます。

仮想サービスがカスタム暗号セットを使用する仮想サービス テンプレートをエクスポートする場合、テンプレートがインポートされる LoadMaster には、同じカスタム暗号セットが含まれている必要があります。

テンプレートから作成された仮想サービスには、テンプレートの設定に基づいてすべての設定が事前構成されています。 必要に応じて、仮想サービスの設定を変更できます。 テンプレートの詳細については、仮想サービスとテンプレート、機能の説明を参照してください。



Service Name

このテキスト ボックスでは、作成中の仮想サービスにニックネームを割り当てたり、既存のニックネームを変更したりできます。

通常の英数字に加えて、次の「特殊」文字をサービス名の一部として使用できます。 @ - _
ただし、サービス名の最初の文字として特殊文字を使用することはできません。

Alternate Address

ここで、必要に応じて、IPv6 または IPv4 形式でセカンダリ アドレスを指定します。

Service Type

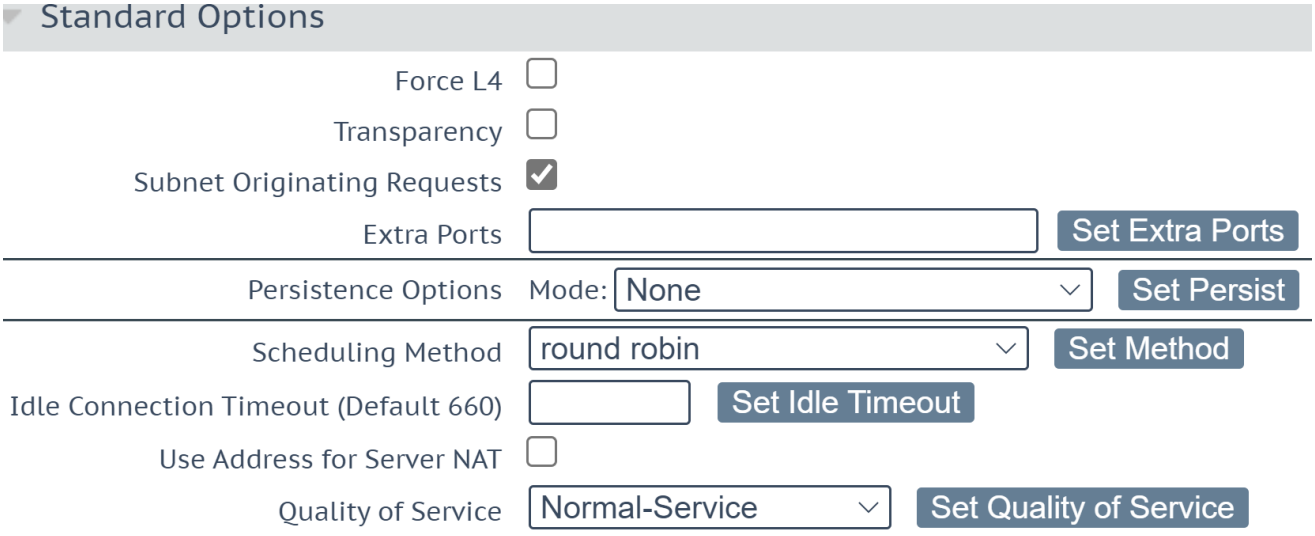
サービス タイプを設定すると、仮想サービスに表示されるオプションが制御されます。 負荷分散しているアプリケーションのタイプに応じてサービス タイプが設定されていることを確認することが重要です。

WebSocket 仮想サービスは、汎用サービス タイプに設定する必要があります。 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。
HTTP/2 は透過性をサポートしていません。 必要に応じて、サブネット発信、代替送信元アドレス機能、キャッシング、圧縮、本文の書き換えなど、すべての作業を行います。

Activate or Deactivate Service

このチェック ボックスでは、仮想サービスをアクティブ化または非アクティブ化するオプションが提供されます。 デフォルト（active）が選択されています。

3.4 標準オプション



Force L4

仮想サービスを強制的にレイヤー 7 ではなくレイヤー 4 で実行するには、このチェック ボックスをオンにします。これは、いくつかの特別な状況でのみ必要です。 疑わしい場合は、このオプションを

オフのままにしておきます。

L7 Transparency

L7 を使用すると、接続を透過的にすることができます。これは、実サーバーに到着する接続がクライアントから直接来ているように見えることを意味します。あるいは、接続が透過的でない場合、実サーバーでの接続は LoadMaster から来ているように見えます。 は、ほとんどの構成で透過性を無効にしておくことを推奨しています。透過性を有効にすると、仮想サービスが透過的になります (ネットワーク アドレス変換 (NAT) なし)。ただし、クライアントが仮想 IP および実サーバーと同じサブネット上に存在する場合、仮想サービスはソース IP を自動的に NAT します (非透過性を有効にします)。

実サーバーはローカル オプションが有効になっている場合、L7 透過性が有効になっていても、実サーバーは NATed (非透過) になります。これは、実サーバーが仮想サービスへの要求の発信元である場合にのみ発生します (他のクライアントからの要求に応答するだけではありません)。 Real Servers are local オプションの詳細については、「L7 構成」セクションを参照してください。

一般的な透明度の詳細については、透明度機能の説明を参照してください。

Subnet Originating Requests

このオプションは、透明度が無効になっている場合にのみ使用できます。

Subnet Originating Requests が有効になっている場合、実サーバーへの接続の送信元アドレスは LoadMaster のインターフェース アドレスです。このオプションを無効にすると、送信元アドレスは仮想サービスの IP アドレスになります。透過性が有効になっている場合、送信元アドレスはクライアントの IP アドレスであり、[Subnet Originating Requests] オプションは無視されます。リアル サーバーがサブネット上にあり、[Subnet Originating Requests] オプションが有効になっている場合、LoadMaster のサブネット アドレスがソース IP アドレスとして使用されます。 Subnet Originating Requests 機能は、「Local」実サーバー用に設計されました。実サーバーが非ローカルであり、デフォルト ゲートウェイ インターフェイス上にない場合を除き、再暗号化には問題なく機能します。この場合、[Alternate Source Address] フィールドにローカル アドレスを設定することで、ローカル アドレスを強制することができます。これは、通常の仮想サービスと再暗号化された仮想サービスの両方で機能します。このスイッチを使用すると、仮想サービスごとにサブネットからの要求を制御できます。グローバル スイッチ (メイン メニューの [System Configuration] > [Miscellaneous Options] > [Network Options] の [Subnet Originating Requests]) が有効になっている場合は、すべての仮想サービスに対して有効になります。

Subnet Originating Requests オプションを仮想サービスごとに有効にすることをお勧めします。

グローバル オプションの詳細については、「Network Options」セクションを参照してください。 グローバル オプションが有効になっていない場合は、仮想サービスごとに制御できます。

SSL 再暗号化が有効になっている仮想サービスに対してこのオプションをオンにすると、その仮想サービスを現在使用しているすべての接続が終了します。

Extra Ports

仮想サービス用にすでに構成されている基本ポートから始まるポートの範囲を、シーケンシャルまたはそれ以外で指定できます。 ポート番号はフィールドに入力され、スペースで区切られます。最大範囲は 510 ポートです。 追加のポートは、ポート範囲またはスペースまたはカンマで区切られた単一のポートとして任意の順序で入力できます。たとえば、リスト 8000-8080、9002、80、8050、9000 を入力すると、ポート 80、8000 から 8080、9000 および 9002 が追加されます。

追加ポートは、SSL 再暗号化では使用できません。

Server Initiating Protocols

デフォルトでは、LoadMaster はクライアントからデータを受信するまでリアル サーバーとの接続を開始しません。 これにより、データを送信する前にリアルサーバーと通信する必要がある特定のプロトコルが機能しなくなります。 仮想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
- その他のサーバー開始プロトコル

仮想サービスで指定されたポートが 80、8080、または 443 の場合、[Server Initiating Protocols] オプションは表示されません。

Persistence Options

Persistence は、仮想サービスごとに設定されます。 このセクションでは、このサービスに対して持続性を有効にするかどうかを選択し、持続性のタイプと持続性のタイムアウト値を設定できます。Persistence が有効になっている場合、LoadMaster を使用した特定のリアル サーバーへのクライアント接続が永続的であることを意味します。つまり、同じクライアントがその後同じリアル サーバーに接続します。 タイムアウト値は、この特定の接続が記憶される期間を決定します。 ドロップダウンリストには、持続性のタイプを選択するオプションがあります。 これらを以下にリストして説明します。

Source IP Address

この場合、（要求しているクライアントの）送信元 IP アドレスが永続性のキーとして使用されます。

Super HTTP

Super HTTP は、LoadMaster で HTTP および HTTPS サービスの永続性を実現するための推奨される方法です。 クライアント ブラウザの一意のフィンガープリントを作成し、そのフィンガープリントを使用して正しいリアル サーバーへの接続を維持します。 User-Agent 値に MSRPC 文字列が含まれていない場合、フィンガープリントは User-Agent フィールドの値に基づいています。 User-Agent 値に MSRPC 文字列が含まれている場合は、Authorization ヘッダーの値を使用して永続性を実現します。 Authorization ヘッダーが存在せず、ユーザー エージェント値に MSRPC 文字列が含まれている場合、持続値は長さ 0 の空白になります。

Server Cookie

LoadMaster は、HTTP ヘッダーに特別に設定された Cookie の値をチェックします。 同じ Cookie を使用した接続は、同じリアル サーバーに接続されます。

Server Cookie or Source IP

Cookie の persistence が失敗すると、ソースベースの永続性に戻ります。

Active Cookie

アクティブ Cookie persistence では、Cookie はサーバーではなく LoadMaster によって生成されます。アクティブ Cookie が設定された LoadMaster 仮想サービスに接続が入ると、LoadMaster は特定の Cookie を探します。その Cookie が存在しない場合、LoadMaster は Set-Cookie ディレクティブを使用して HTTP ストリームに挿入します。既存の Cookie は影響を受けません。サーバー Cookie 永続化方式と同様に、LoadMaster が生成した Cookie の値は各ユーザーに固有であるた

め、LoadMaster はユーザーを区別できます。この方法の利点は、サーバーによって Cookie を管理または生成する必要がないため、サーバー構成の負担が軽減されることです。クライアント接続ごとの分散を改善するには、L7 構成でポートをアクティブな Cookie に追加する機能を有効にします。このオプションの詳細については、「L7 Configuration」セクションを参照してください。アクティブ Cookie persistence を使用すると、Cookie はセッションの間、または永続時間が期限切れになるまで有効です。たとえば、持続タイムアウトを 10 分に設定してアクティブ Cookie 持続を使用し、クライアントが午後 2 時に接続し、その後切断して午後 2 時 5 分に再接続する場合、持続タイムアウト値がリセットされます。永続性タイムアウトの期限が切れた後にクライアントが仮想サービスに接続しようとすると、古い Cookie が提示されます。 LoadMaster は永続性テーブルをチェックし、有効なエントリがないことを確認します。その後、LoadMaster はクライアント用の新しい Cookie を生成し、持続性テーブルを更新します。

Active Cookie or Source IP

アクティブ Cookie の永続化に失敗すると、ソースベースの persistence に戻ります。

Hash All Cookies

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

Hash All Cookies or Source IP

Hash All Cookies または Source IP は Hash All Cookies と同じですが、HTTP 文字列に Cookie が含まれていない場合に Source IP persistence にフォールバックするという追加機能があります。

Super HTTP and Source IP Address

これは Super HTTP と同じですが、送信元 IP アドレスも文字列に追加するため、結果の HASH の分散が改善されます。

URL Hash

URL ハッシュの persistence により、LoadMaster は同じ URL を持つリクエストを同じサーバーに送信します。

HTTP Host Header

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

Hash of HTTP Query Item

このメソッドは、検査される名前付きアイテムが URL のクエリ文字列内のクエリ アイテムであることを除いて、Server Persistence とまったく同じ方法で動作します。 同じクエリ アイテム値を持つすべてのクエリは、同じサーバーに送信されます。

Selected Header

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

SSL Session ID

SSL を介した各セッションには、persistence できる独自のセッション ID があります。

このオプションが永続化方法として表示されるようにするには、仮想サービスのサービス タイプが Generic であり、SSL アクセラレーションが無効になっている必要があります。

仮想サービスが SSL サービスであり、オフロードされていない場合、LoadMaster はレイヤー 7 でストリーム内のデータと意味のあるやり取りを行うことができません。その理由は、データが暗号化されており、LoadMaster がそれを復号化する方法がないためです。 上記のシナリオで、ソース IP に基づいていない persistence モードが必要な場合、これが唯一の他のオプションです。 SSL セッションが開始されると、接続用のセッション ID が生成されます。 このセッション ID を使用して、クライアントを正しいサーバーに持続させることができます。 ただし、これにはいくつかの欠点があります。ほとんどの最新のブラウザーはセッション ID を非常に短い間隔で再生成し、persist タイムアウトに長い間隔が設定されていても、基本的に上書きします。

UDP Session Initiation Protocol (SIP)

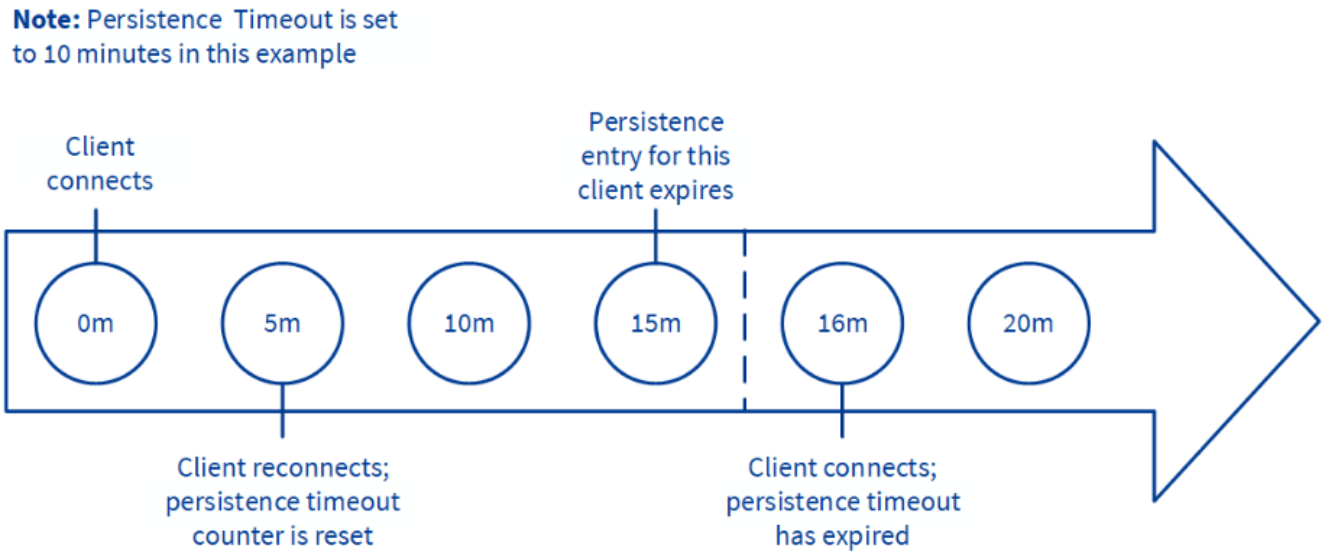
この永続性モードは、Force L4 が有効になっている場合に UDP 仮想サービスでのみ使用できます。SIP は、HTTP と同様に、要求と応答のトランザクションを使用します。 多数のヘッダー フィールドを含む最初の INVITE 要求が送信されます。 これらのヘッダー フィールドは永続化に使用できます。

Timeout

persistence 方法ごとに、各ユーザーの persistence が受け入れられる期間を決定する構成可能なタイムアウト値があり、1 分から 7 日間まで選択できます。

LoadMaster ファームウェア バージョン 7.2.53 では、persistence タイムアウト設定の最大値が 7 日から 28 日に増加しました。 persistence モードが選択されている場合、持続性タイムアウト ドロップダウン リストを構成できます。 persistence タイムアウトが 4 日以上に設定されている場合、[Refresh Persist] チェック ボックスが表示されます。 これはデフォルトで無効になっています。 Refresh Persist が有効になっている場合、存続期間の長い接続のために、持続エントリが毎日自動リフレッシュされます。

このタイムアウト クロックは、最初の接続が確立されたときに開始されます。 クライアントがタイムアウト期間内に再接続すると、persistence タイムアウト値が更新されます。 たとえば、persistence タイムアウトが 1 時間に設定されていて、クライアントが午後 2 時に接続を開始した場合、クライアントが切断して午後 3 時前に再接続した場合でも、クライアントは同じ実サーバーに持続します。 また、これを反映するために persistence レコードが更新され、このクライアントの persistence カウントダウン タイマーが 1 時間にリセットされます。



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

- persistence タイムアウトは 10 分に設定されています
- ユーザーは 20 分間に複数のリクエストを行いますが、接続間の時間は常に 1 分未満です

要求は、利用可能な (つまり、ヘルスチェックに合格している) 限り、正しい実サーバーに送信する必要があります。 アクティブな接続が 20 分間アイドル状態になると、次の接続は新しいセッションとしてカウントされ、スケジュールに応じて別のサーバーに送信される場合があります。 接続が 10 分

以上開かれ、クライアントが切断して再接続した場合、永続レコードは期限切れになり、LoadMaster はそのクライアントの新しい永続エントリを作成し、場合によってはクライアントを新しい実サーバーに送信します。 これは、接続の終了時ではなく、接続が確立されると持続カウントダウンが開始されるためです。 持続性の問題が発生している場合は、持続性タイムアウトが十分に長くないことが原因である可能性があります。 これが十分な長さでない場合は、タイムアウト値をより大きな値に設定する必要があります。 一般に、この値をサーバーのタイムアウト値と一致させることをお勧めします。

Header field name

LoadMaster で持続性モードとして UDP Session Initiation Protocol を選択すると、Header field name というテキスト ボックスが表示されます。 永続化情報のベースとして使用されるヘッダー フィールドをここに入力する必要があります。

Scheduling Methods

このセクションでは、この特定のサービスに対して LoadMaster が実サーバーを選択する方法を選択できます。 スケジューリング方法は次のとおりです。

- ラウンドロビン：

ラウンド ロビンにより、LoadMaster は実サーバーを順番にセッションに割り当てます。たとえば、最初のセッションは実サーバー 1 に接続し、2 番目のセッションは実サーバー 2 に接続するなどです。 実サーバーの割り当て方法に偏りはありません。

- 重み付けラウンドロビン:

このメソッドは、実サーバーの重みプロパティを使用して、どの実サーバーが優先されるかを決定します。 実サーバーの重みが高いほど、受信する接続の割合が高くなります。

- 最小接続:

この方法では、開いている接続が最も少ない現在の実サーバーがセッションに割り当てられます。

- 重み付け最小結合:

最小接続と同様ですが、重みに対する偏りがあります。

- リソースベース (適応型):

アダプティブ スケジューリングとは、リアル サーバーの負荷が定期的に監視され、すべてのマシンの負荷がほぼ等しくなるようにパケットが分散されることを意味します。

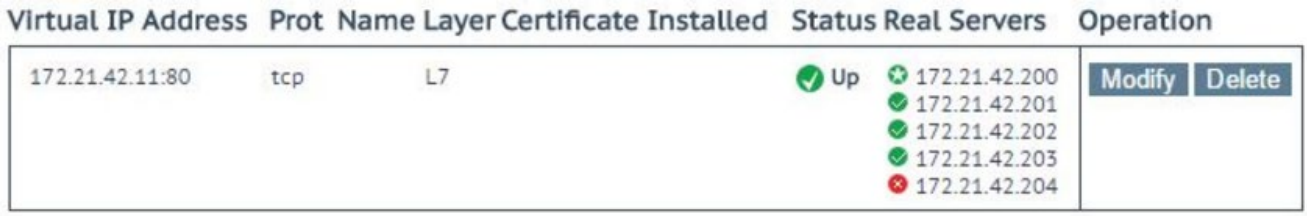
最初にアダプティブ スケジューリングを有効にし、実サーバー上で実行されている HTTP サーバーがない場合、実サーバーの重みは 100 (負荷が高い) に設定されます。

- リソースベース (SDN アダプティブ):

アダプティブ スケジューリング方式を使用する仮想サービス (SDN を使用するかどうかに関係なく) は、制御システムと見なすことができます。 その目的は、実サーバー上で均等に分散された負荷を実現することであり、コントローラーはこれからエラー値を計算します (これは、望ましい均等な分散からの偏差を表します)。 また、エラー値を減らす方法でシステムにフィードバックされる一連の制御値 (実サーバーの重み) も計算します。

- 固定加重:

すべてのトラフィックは、利用可能な最も重みの高い Real Server に送られます。 実サーバーは作成時に重み付けする必要があり、 2 つの実サーバーが同じ重みを持つべきではありません。そうしないと、予測不能な結果が生じる可能性があります。



固定加重を使用している場合、加重が大きい実サーバーは緑色の星のアイコンで示されます。

- 加重応答時間:

LoadMaster は 15 秒ごとに、ヘルス チェック プローブの応答が到着するまでの時間を測定し、この時間を使用して、それに応じて実サーバーの重みを調整します。つまり、他の実サーバーに比べて応答時間が速いほど、 重みが高くなると、そのサーバーに送信されるトラフィックが増加します。

- ソース IP ハッシュ:

重みを使用したり、ラウンド ロビンを実行したりする代わりに、ソース IP のハッシュが生成され、正しい実サーバーを見つけるために使用されます。 これは、同じホストからの実サーバーが常に同じであることを意味します。 ソース IP の永続性は必要ありません。

この方法はクライアント (送信元) IP アドレスのみに依存し、現在のサーバー負荷を無視するため、この方法を使用すると、特定の実サーバーが過負荷になったり、すべての実サーバー間で一般的なトラフィックの不均衡が発生したりする可能性があります。

- URL ハッシュ:

URL ハッシュ方式は、クライアント リクエストの URL で参照されるオブジェクトと、仮想サービス内の実サーバーまたはサブ VS の数に基づいてハッシュ値を作成することによって機能します。 特定

の URL に対するすべてのリクエストは、実サーバーまたはサブ VS が追加または削除されない限り、同じ実サーバーまたはサブ VS に送信されます。この場合、すべてのハッシュ値が再計算され、それに応じて後続のトラフィックが再分配されます。 書き込みは、障害に関係なく常に成功します (すべてがダウンしていない限り)。 URL ハッシュ方式は、SubVS がダウンしたときに、次に使用可能な SubVS に書き込み要求を送信します。 例えば：

- 仮想サービスには 3 つの SubVS があります。 SubVS 2 に書き込みを送信することを示す既存のハッシュがある書き込み要求が受信されます。
- SubVS 2 がダウンしています。 リクエストは SubVS 3 に送信されます。
- SubVS 3 がダウンしている場合は、SubVS 1 に送信します (ラウンドロビン方式で)。
- SubVS 2 がオンラインに戻ったら、ハッシュの尊重に戻り、今後の要求を SubVS 2 に送信します。

このスケジューリング方法は、主に Dell EMC Elastic Cloud Storage (ECS) アプリケーションと ECS ベースのリソースの効率的な使用をサポートするために開発されましたが、ストレージ効率が主な目標である他のワークロードをサポートするためにも使用できます。 Dell ECS 展開の場合、ロード トラフィックは展開内の仮想データ センター (VDC) に分散され、それぞれが LoadMaster で SubVS として表されます。 各 VDC 内で、トラフィックは SubVS 内の実サーバーに分散されます。

Idle Connection Timeout (Default 660)

アイドル状態の接続が閉じられるまでの秒数。 0 に設定すると、デフォルトの L7 接続タイムアウトが使用されます。 [System Configuration] > Miscellaneous Options [] > [Network Options] に移動して、デフォルトの接続タイムアウト値を変更できます。

Use Address for Server NAT

デフォルトでは、LoadMaster が SNAT 実サーバーに使用されている場合、インターネットで使用されるソース IP アドレスは LoadMaster のものです。 Use Address for Server NAT オプションを使用すると、実サーバーが仮想サービスと同じポートを使用してアウトバウンド要求を行う場合、仮想サービスで構成された実サーバーが代わりにソース IP アドレスとして仮想サービスを使用できます。 LoadMaster は、すべてのアウトバウンド ポートを NAT するわけではありません。

Use Address for Server NAT オプションは、LoadMaster がパブリック ドメインにあり、LoadMaster から送信されたソース アドレスがメール エクスチェンジャーと同じかどうかを確認す

るために逆引き DNS チェックが必要な場合に、SMTP などのサービスに最も役立ちます（MX）送信者のレコード。

このオプションが設定された複数の仮想サービスで実サーバーが構成されている場合、LoadMaster はサーバーの要求の宛先ポートを調べてから、一致するポートを持つ仮想サービスを選択します。 LoadMaster は、この仮想サービスをソース IP アドレスとして使用します。 要求されたポートに一致するものが見つからない場合、LoadMaster の IP アドレスがソース IP アドレスとして使用されます。

[User Address for Server NAT] オプションは、デフォルト ゲートウェイで動作している仮想サービスでのみ機能します。 このオプションは、デフォルト ゲートウェイ インターフェイス以外ではサポートされていません。

Quality of Service

Quality of Service ドロップダウンでは、仮想サービスから出るパケットの IP ヘッダーに Type of Service (ToS) を設定します。 これは、パケットを処理する次のデバイスまたはサービスが、このトラフィックを処理して優先順位を付ける方法を知っていることを意味します。 優先度の高いパケットは、優先度の低いパケットの前に LoadMaster から送信されます。
さまざまなオプションについて以下に説明します。

- Normal-Service: トラフィックに特別な優先順位はありません
- Minimize-Cost: より低い「コスト」を持つリンクを介してデータを転送する必要がある場合に使用されます。
- Maximize-Reliability: データが信頼できるリンクを介して宛先に移動する必要があり、再送信がほとんどまたはまったくない場合に使用されます。
- Maximize-Throughput: リンク上のレイテンシーが高い場合でも、間隔中に転送されるデータ量が重要な場合に使用されます
- Minimize-Delay: パケットが宛先に到達するまでの所要時間（レイテンシ）を短くする必要がある場合に使用されます。 このオプションには、各サービス品質の選択肢の中で最も速いキューがあります。
- Pass Through: LoadMaster ファームウェア バージョン 7.2.52 では、Pass Through 値が導入されました。 これを選択すると、Quality Of Service (QOS) フラグを含む接続が実サーバーに渡されます。 SubVS に関して注意すべき点がいくつかあります。

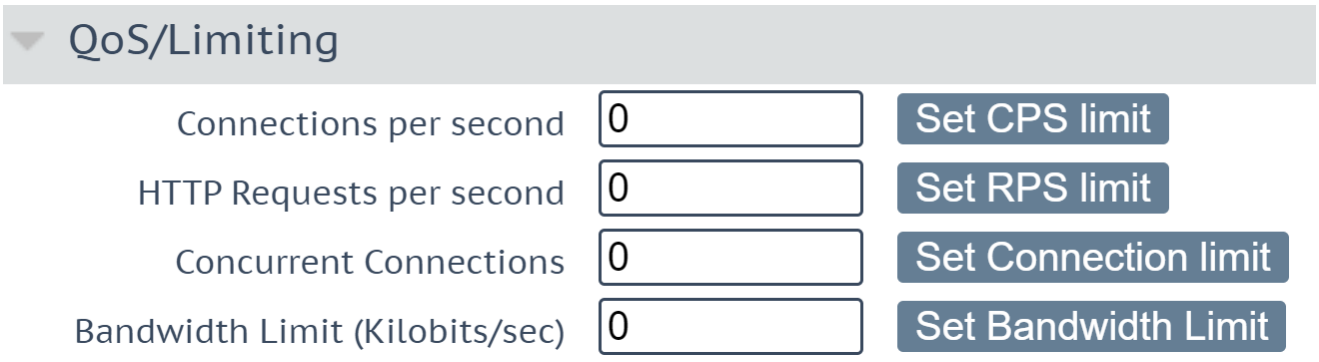
- - 親仮想サービスのサービス品質としてパス スルーを選択すると、親仮想サービスの下にあるすべてのサブ VS がパス スルーを使用します。 SubVS には Quality of Service フィールドが表示されず、アプリケーション プログラミング インターフェイス (API) を使用して Quality of Service の値を変更することはできません。
- - 親仮想サービスのサービス品質としてパス スルー以外のオプションを選択した場合、その仮想サービスの下にあるサブ VS のサービス品質ドロップダウン リストにパス スルー オプションが表示されず、次のことができなくなります。 API を使用してサービスの品質をパススルーに設定します。

次の表に、各オプションの ToS 値を示します。

Bits	Decimals	Importance
1000	8th	最小限の遅延
0100	4	最大スループット
0010	2	最高の信頼性
0001	1	最小限の費用（金額）
0000	0	通常のサービス

Quality of Service 機能は、レイヤ 7 トラフィックでのみ機能します。 レイヤ 4 トラフィックでは機能しません。

3.5 QoS/制限



Connections per second: この仮想サービスの 1 秒あたりの最大接続数を設定します。 制限を 0 に設定すると、このオプションが無効になります。 有効な値は 0 ～ 100000000 です。

HTTP Requests per second: この仮想サービスの 1 秒あたりの最大 HTTP 要求を設定します。制限

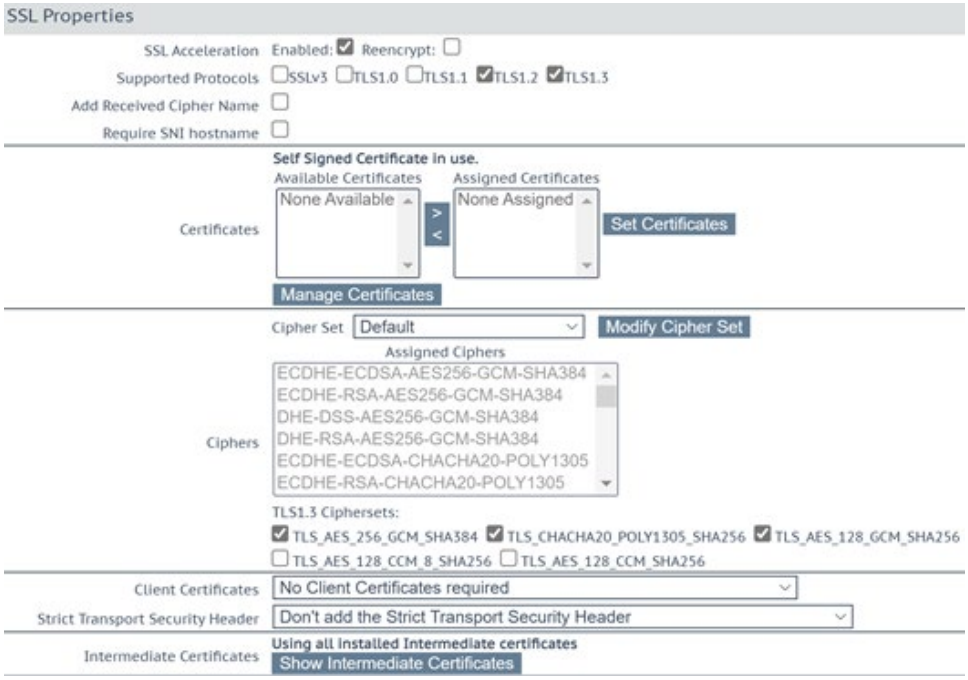
を 0 に設定すると、このオプションが無効になります。 有効な値は 0 ～ 1000000 です。

443 ポートで作成された仮想サービスの場合、HTTP リクエスト/秒オプションは、SSL アクセラレーション オプションが有効になっている場合にのみ使用できます。

Concurrent Connections: この仮想サービスの最大同時接続数を設定します。 制限を 0 に設定すると、このオプションが無効になります。 有効な値は 0 ～ 1000000 です。

Bandwidth Limit (Kilobits/sec): この仮想サービスの最大帯域幅を設定します。 値はキロビット/秒。 最小値は 16 です。最大値は 99999999 です。この値を 0 に設定すると、帯域幅の制限がなくなります。 これにより、仮想サービスを通過するすべてのトラフィックが制限されます。 仮想サービスに帯域幅制限が設定されている場合、強制的に Layer7 (L7) サービスになります。

3.6 SSL プロパティ



SSL Acceleration

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た場合に表示されます。 SSL アクセラレーションを有効にするには、このチェック ボックスをオンにします。

Enabled: [Enabled] チェック ボックスが選択されていて、仮想サービスの証明書がない場合は、証

明書をインストールするように求められます。 [Manage Certificates] をクリックし、証明書をインポートまたは追加することで、証明書を追加できます。

Reencrypt: [Reencrypt] チェック ボックスをオンにすると、実サーバーに送信する前に SSL データ ストリームが再暗号化されます。

SSL 再暗号化では、Extra Ports または Transparency を使用できません。

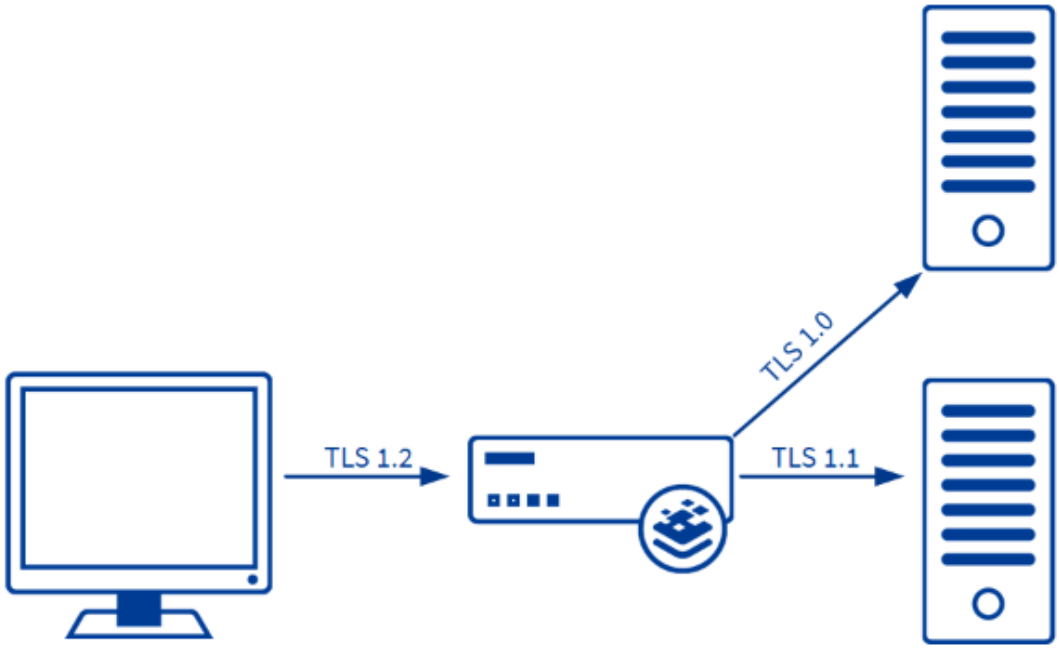
Reversed: このチェックボックスを選択すると、ロードマスターからリアルサーバーへのデータが再暗号化されます。 入力ストリームは暗号化しないでください。たとえば、クライアントは HTTP ポート 80 トラフィックをロードマスターに送信し、ロードマスターは HTTPS ポート 443 トラフィックをリアル サーバーに送信します。 これは、SSL トラフィックを復号化し、この仮想サービスを実サービスとして使用してデータをループバックする別の仮想サービスとの接続でのみ役立ちます。このようにして、クライアントから Real Server へのデータ パスは常にネットワーク上で暗号化されます。

Supported Protocols

[Supported Protocols] セクションのチェック ボックスを使用すると、仮想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、TLS1.2、および TLS1.3 が有効になっており、SSLv3 と TLS1.0 は無効になっています。

[Certificates & Security] > [SSL Options] の [OpenSSL Version] 設定が [Use older SSL Library]-no TLS1.3 に設定されている場合、[TLS1.3] チェック ボックスは表示されません。

バージョン 7.2.37 以降、再暗号化が有効になっている場合、LoadMaster とその背後にあるリアルサーバー間でネゴシエートできる TLS バージョンは、クライアント側で構成された TLS バージョン設定によって制限されなくなりました。 LoadMaster でサポートされているすべての TLS バージョンと暗号は、実サーバーによる制限なしでネゴシエートできます。 このようにして、LoadMaster は、たとえば、クライアント側のアプリケーション アクセスに厳格なセキュリティを提供しながら、特定の安全性の低い TLS バージョンと暗号のみをサポートするレガシー サーバーへのサーバー側接続を引き続きサポートできます。 これを以下の例に示します。



サーバー接続は、クライアント側で選択された TLS バージョンに関係なく、実サーバーの構成によってのみ制限されます。 各実サーバーは、他とは独立して構成できます。 LoadMaster は、各リアルサーバーの要件に従って接続をネゴシエートします。

Add Received Cipher Name

LoadMaster バージョン 7.2.52 以降では、[Add Received Cypher Name] という新しいチェックボックスが追加されました。 このオプションはデフォルトで無効になっています。 このオプションを有効にすると、LoadMaster は、次の表に示すように、TLS バージョン、TLS 暗号、クライアント証明書のシリアル番号、SNI ホストなどのクライアント SSL 情報を含む X-SSL ヘッダーを追加します。 これらのヘッダーに含まれる情報は、ルールで適切なヘッダー名を参照することにより、コンテンツ ルールで使用できます (下の表を参照)。 これにより、使用する暗号などに基づいて負荷分散の決定を行うことができます。 この情報は、たとえば、暗号セットを長期間維持する場合にも役立ちます。 どの暗号が使用されているかを確認でき、暗号セットでどの暗号を変更または削除するかを計画するのに役立ちます。 次の表のヘッダーをコンテンツ ルールで使用するには、[Add Received cypher Name] チェック ボックスをオンにする必要があります。

Header	Description	Example Value
X-SSL-Cipher	使用される暗号	X-SSL-Cipher: ECDHE-RSA-AES256-GCM-SHA384
X-SSL-Protocol	使用される SSL プロトコルのバージョン	X-SSL-Protocol: TLSv1.2
X-SSL-Serialid	仮想サービス証明書のシリアル番号	X-SSL-Serialid: 4900000006A2ABDC165ACEAD55000000000006
X-SSL-ClientSerialid	クライアント証明書のシリアル番号	X-SSL-ClientSerialid: 490000005D6898F3C7E590536100010000005D
X-SSL-SNIHost	受信した SNI 名の値	X-SSL-SNIHost: sni.test.com

Require SNI hostname

[Required SNI hostname] が選択されている場合、ホスト名は常に TLS クライアントの hello メッセージで送信される必要があります。

[Required SNI hostname] が無効になっている場合、一致するホスト ヘッダーが見つからない場合は、最初の証明書が使用されます。

[Required SNI hostname] が有効になっている場合、共通名が一致する証明書が見つかる必要があります。見つからない場合、SSL エラーが発生します。 ワイルドカード証明書も SNI でサポートされています。

サブジェクト代替名 (SAN) 証明書を使用する場合、代替ソース名はホスト ヘッダーと照合されません。

ワイルドカード証明書はサポートされていますが、ルート ドメイン名は RFC 2459 に従って一致しないことに注意してください。ドットの左側にあるものだけが一致します。 ルート ドメイン名と一致するように、追加の証明書を追加する必要があります。 たとえば、www.kemptechnologies.com は、*.kemptechnologies.com のワイルドカードまで一致します。 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、関連する仮想サービスの [Real Server] セクションで [Use HTTP/1.1] を有効にし、ホスト ヘッダーを指定します。 これが設定されていない場合、実サーバーの IP アドレスが使用されます。

Pass through SNI hostname

LoadMaster ファームウェア バージョン 7.2.52 以降では、このオプションを有効にして再暗号化すると、受信した SNI ホスト名が SNI として渡され、リアル サーバーへの接続に使用されます。 仮想サーバーに再暗号化 SNI ホスト名が設定されている場合、これは受信した SNI を上書きします。

このフィールドは、SSL 再暗号化が有効になっている場合にのみ表示されます。

Certificates

使用可能な証明書は、左側の [available Certificates] 選択リストに表示されます。 証明書を割り当てたり、割り当てを解除したりするには、証明書を選択して右矢印または左矢印ボタンをクリックします。 次に、[Set Certificates] をクリックします。 キーボードで Ctrl を押しながら必要な各証明書をクリックすると、複数の証明書を選択できます。

WUI を使用して仮想サービスに証明書を割り当てる場合、8171 文字の制限があります。

仮想サービスは、RSA 証明書と ECC 証明書の両方を使用して構成できます。 ただし、RSA 証明書と ECC 証明書の共通名が同じ場合 (kemp.com など)、最初の証明書が優先されます。 ECC 証明書がリストの最初にあり、クライアントに ECC 暗号がない場合、接続は失敗します。 逆に、RSA 証明書がリストの最初にあり、クライアントに RSA 暗号がない場合、接続は失敗します。

仮想サービスに追加できる証明書の総数は 256 ですが、この数は、使用される証明書ファイル名のサイズによってさらに制限される場合があります。 LMOS バージョン 7.2.47 以降のリリースでは、各証明書ファイル名と拡張子 (その間のピリオドはカウントしない) の文字数と、複数のファイル名を区切るために使用されるすべてのスペースの合計が 8176 文字以下になる必要があります (以前のリリースでは、制限は 1023 文字です。)

[Manage Certificates] をクリックすると、[SSL Certificates] 画面が表示されます。

バージョン 7.2.51 以降 (または 7.2.48.3 LTS 以降の LTS バージョン) の LoadMaster に証明書を追加してから、7.2.50 以前のバージョン (または 7.2.48.2 LTS 以降のバージョン) にダウングレードする場合 - 証明書は機能しません。 これを回避するには、ダウングレードする前にすべての SSL 証明書のバックアップを作成し、ダウングレード後に証明書を復元します ([Certificates & Security] > [Backup/Retore Certs])。 ダウングレードする前にバックアップを取るのを忘れた場合: ファームウェアを再度アップグレードし、証明書のバックアップを取り、ダウングレードしてから、証明書のバックアップを復元します。

Reencryption Client Certificate

SSL 接続では、LoadMaster はクライアントから証明書を取得し、サーバーからも証明書を取得します。 LoadMaster はクライアント証明書をヘッダーに転記し、データをサーバーに送信します。 サーバーはまだ証明書を期待しています。 これが、LoadMaster に事前認証済みの証明書をインストールすることが望ましい理由です。

Reencryption SNI Hostname

LoadMaster ファームウェア バージョン 7.2.52 以降では、再暗号化 SNI ホスト名を SubVS レベルで設定できます。 これが SubVS で設定されている場合、これは親仮想サービスの値および/または受信した SNI 値を上書きします。

このフィールドは、SSL 再暗号化が有効になっている場合にのみ表示されます。

Cipher Set

暗号は、暗号化または復号化を実行するためのアルゴリズムです。
各仮想サービス (SSL アクセラレーションが有効になっている) には、暗号セットが割り当てられています。 これは、システム定義の暗号セットまたはユーザーがカスタマイズした暗号セットのいずれかです。 システム定義の暗号セットを選択して、関連する暗号をすばやく簡単に選択して適用できます。 [Modify Cypher Set] をクリックして、カスタム暗号セットを作成および変更できます。

TLS1.3 プロトコルのみが選択されている場合、TLS1.2 以下のプロトコル暗号の選択は使用できなくなります。

Ciphers

暗号リストは読み取り専用で、現在割り当てられている暗号のリストが表示されます。 [Modify Cipher Set] をクリックすると、[Cipher Set Management] 画面が表示されます。 この画面では、

新しいカスタム暗号セットを作成したり、既存のカスタム暗号セットを変更したりできます。

TLS1.3 Cipher Sets

SSL 対応の仮想サービス上で、サポートされている暗号の任意の組み合わせを使用して許可される TLS1.3 プロトコルの暗号セットを選択します。 デフォルトでは、次の 3 つの暗号セットが有効になっています。

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

すべての暗号セットを無効にすることはできません。

TLS1.3 暗号セットは、TLS1.3 プロトコルが有効になっている場合にのみ使用可能になります。

Client Certificates

- No Client Certificates required: LoadMaster が任意のクライアントからの HTTPS 要求を受け入れることができるようにします。 これは推奨オプションです。

デフォルトでは、LoadMaster は任意のクライアントからの HTTPS リクエストを受け入れます。 以下のその他の値を選択するには、すべてのクライアントが有効なクライアント証明書を提示する必要があります。 さらに、LoadMaster は証明書に関する情報もアプリケーションに渡します。

このオプションは、デフォルトの [クライアント証明書は必要ありません] から変更しないでください。 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ことが確実な場合にのみ、デフォルト オプションから変更してください。

- Client Certificates required: HTTPS 要求を転送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提示する必要があります。
- Client Certificates and add Header: HTTPS 要求を転送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提示する必要があります。 LoadMaster は、ヘッダーを追加することによって、証明書に関する情報もアプリケーションに渡します。 クライアント証明書を使用する場合、X-SSLClientSerialid ヘッダーが設定されます。
- 以下のオプションは、証明書を元の生の形式で送信します。 さまざまなオプションを使用して、証明書を送信する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

仮想サービスの場合:

- SSL アクセラレーションが有効になっており、かつ
- [Client Certificates] ドロップダウン リストで、[SSL-CLIENT-CERT/XCLIENT-CERT としてパス スルー] を含むクライアント証明書に必要なオプションのいずれかが選択されている。
- ヘッダーの削除ルールがその仮想サービスに適用され、SSL/X-CLIENT-CERT ヘッダー フィールドが削除されます。

  ヘッダーの削除コンテンツ ルールは、ロードマスターが挿入したクライアント証明書ヘッダーを保持します。フィールドを削除し、クライアントから渡されたその名前のヘッダーを削除します。

Verify Client using OCSP

クライアント証明書が有効であることを (オンライン証明書ステータス プロトコル (OCSP) を使用して) 確認します。

このオプションは、ESP が有効になっている場合にのみ表示されます。

Strict Transport Security Header

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 Strict-Transport-Security ヘッダーを追加するには、このオプションを有効にします。 このドロップダウン リストのオプションは次のとおりです。

- Don't add the Strict Transport Security Header
- Add the Strict Transport Security Header - no subdomains
- Add the Strict Transport Security Header - include subdomains
- Add the Strict Transport Security Header - no subdomains + preload
- Add the Strict Transport Security Header - include subdomains + preload

Intermediate Certificates

中間証明書フィールドが SSL プロパティ セクションに追加される前は、中間証明書またはルート証明書を仮想サービスに割り当てる機能がありませんでした。 クライアント証明書の認証局 (CA) はグローバル証明書ストアに保持されていたため、次のことが発生する可能性があります。

- 2 つの異なる CA からのクライアント証明書が LoadMaster にインストールされている
- クライアント A は CA 1 から発行された証明書を提示し、ネットワーク管理者として、仮想

サービス 1 のみにアクセスできるようにしたいと考えています。

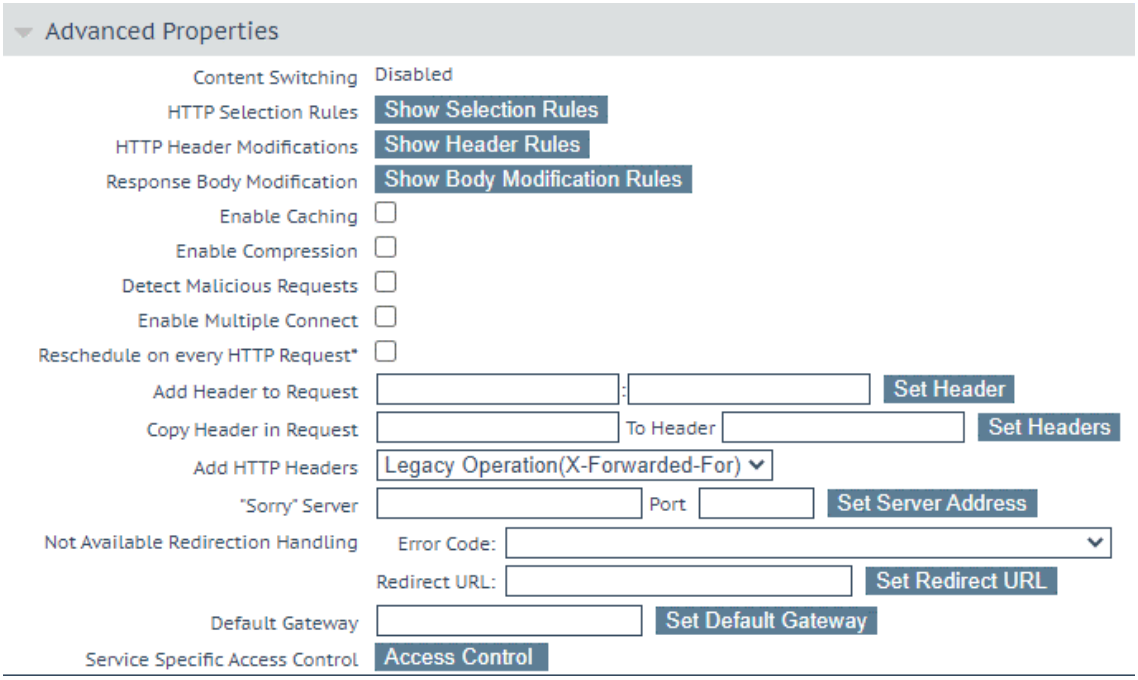
- クライアント B は CA 2 から発行された証明書を提示し、ネットワーク管理者として、仮想サービス 2 にのみアクセスできるようにしたいと考えています。
- 両方のクライアント証明書がグローバル LoadMaster トラスト ストアに対して検証されるため、クライアント A は仮想サービス 2 へのアクセスも許可され、クライアント B も仮想サービス 1 へのアクセスが許可されます。

中間証明書フィールドでは、中間証明書とルート証明書を特定の仮想サービスに割り当てることができます。 これにより、アクセスを制限する機能が提供されます。 また、複数の機関によって署名された複数のクライアント証明書を使用する環境で役立つサービスに接続するときに、どのクライアント証明書を使用する資格があるかを制御できます。 たとえば、これが上記のシナリオで正しく構成されている場合、クライアント A は仮想サービス 1 にのみアクセスでき、クライアント B は仮想サービス 2 にのみアクセスできます。これを構成するには、次の手順に従います。

- 関連する証明書をアップロードします。
- LoadMaster ユーザー インターフェイス (UI) で、[Virtual Services] > [View/Modify Services] に移動します。
- 関連する仮想サービスで [Modify] をクリックします。
- [SSL Property] セクションを展開します。
- [Show Intermediate Certificates] をクリックします。
- ボックスから関連する証明書を選択し、矢印をクリックしてそれらを削除/割り当てます。
- 仮想サービス。
- 次に、[Set Intermediate Certificates] をクリックします。

仮想サービスからすべての証明書の割り当てを解除することはできません。 クライアント証明書を要求しない場合は、[Client Certificates] ドロップダウン リストで [No Client Certificates required] を選択します。

3.7 詳細プロパティ



Content Switching

[Enable] ボタンをクリックすると、この仮想サービスでルールベースのコンテンツ スイッチングが有効になります。 有効にしたら、さまざまな実サーバーにルールを割り当てる必要があります。 実サーバーの横にある [なし] ボタンをクリックすると、ルールを実サーバーに関連付けることができます。 ルールが実サーバーにアタッチされると、[None] ボタンにアタッチされたルールの数が表示されます。

Rules Precedence

[Rules Precedence] ボタンをクリックすると、コンテンツ スイッチング ルールが適用される順序が表示されます。 このオプションは、コンテンツ スイッチングとルールが実サーバーに割り当てられている場合にのみ表示されます。

Rules assigned to Virtual Service tcp/10.35.48.24:80 (Id:1)

	Name	Match Type	Options	Header	Pattern	Operation
1	Rule1	RegEx	Ignore Case Include Query		/^\/owa.*/	
2	Rule2	RegEx	Ignore Case Include Query		/^\/owa.*/	Move
3	Rule3	RegEx			/^\/owa.*/	Move

この画面には、仮想サービスの実サーバーに割り当てられたコンテンツ スイッチング ルールと、それ

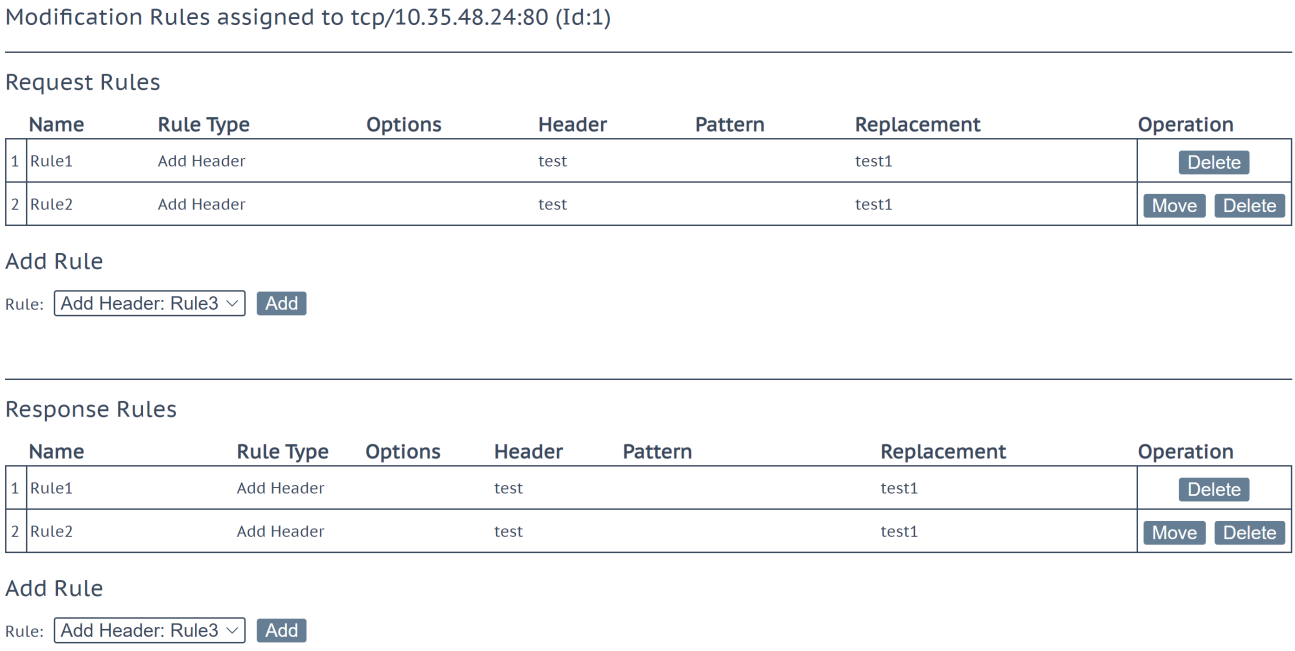
らが適用される順序が表示されます。 ルールは、対応する [Move] ボタンをクリックすることにより、優先順位に従って昇格できます。 LoadMaster ファームウェア 7.2.52 以降では、仮想サービス内のルールの優先順位を簡単に並べ替えることができます。ルールを移動する位置を指定できる移動オプションがあります。

HTTP Selection Rules

仮想サービスに関連付けられている選択ルールを表示します。

HTTP Header Modifications

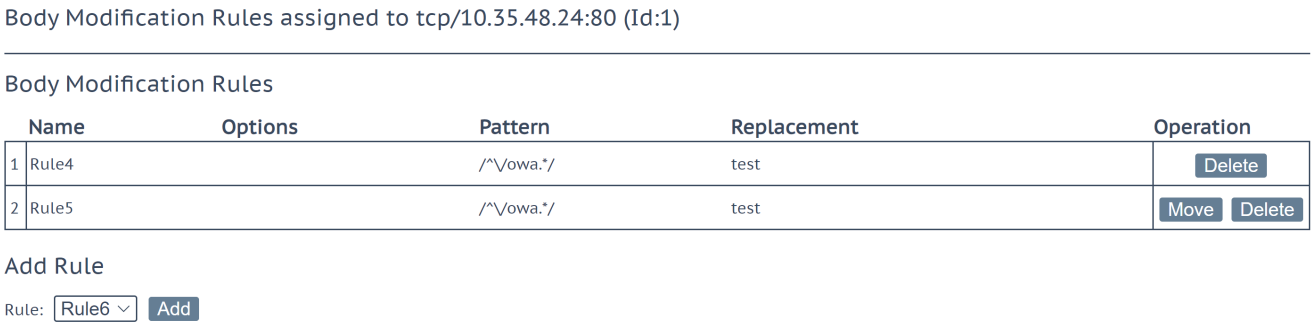
[Show Header Rules] をクリックすると、ヘッダー変更ルールが実装されている順序が表示されます。 実際のボタンには、(リクエスト タイプとレスポンス タイプの両方の) ルールの数が表示されます。



画面内から、ヘッダー変更ルールを追加および削除できます。 ルールが適用される順序は、[Move] ボタンをクリックして変更できます。 LoadMaster ファームウェア 7.2.52 以降では、仮想サービス内のルールの優先順位を簡単に並べ替えることができます。ルールを移動する位置を指定できる移動オプションがあります。 優先度を示すために、仮想サービスに割り当てられたコンテンツ ルールを示すページにも番号が表示されるようになりました。 LoadMaster ファームウェア バージョン 7.2.51 以降では、Response Rules [] セクションで関連する [Modify Response] ルールを選択することで、レスポンスに URL 変更ルールを割り当てることができます。

Response Body Modification

Show Body Modification Rules ボタンをクリックすると、仮想サービスに割り当てられたレスポンスボディの変更ルールが表示されます。 割り当てられたルールの数は、ボタン ラベルに表示されます。



この画面から、仮想サービスへの、または仮想サービスからの応答本文変更ルールの追加および削除を行うことができます。 [Move] ボタンをクリックすると、ルールが適用される順序を変更できます。 LoadMaster ファームウェア 7.2.52 以降では、仮想サービス内のルールの優先順位を簡単に並べ替えることができます。ルールを移動する位置を指定できる移動オプションがあります。 優先度を示すために、仮想サービスに割り当てられたコンテンツ ルールを示すページにも番号が表示されるようになりました。

応答本文の規則は、Kerberos Constrained Delegation (KCD) と互換性がありません。 仮想サービスで KCD が有効になっている場合、本文ルールを割り当てることはできません。

Enable HTTP/2 Stack

HTTP/2 クライアント リクエストが LoadMaster によって直接処理されるようにします。 HTTP/2 リクエストは、安全な接続を使用して行われます。 このオプションを有効にする場合は、SSL プロパティが構成され、BestPractices 暗号セットが選択されていることを確認してください。 エンド ユーザー エクスペリエンスを最適化するには、[キャッシュを有効にする] チェック ボックスもオンにする必要があります。

Enable Caching

このオプションは、静的コンテンツのキャッシュを有効にします。 これにより、Real Server の貴重な処理能力と帯域幅が節約されます。 キャッシングは、HTTP およびオフロードされた HTTPS 仮想サービスごとに有効にできます。 アイテムは 15 分間 (または、ページを更新して (たとえば、キー

ボードで Ctrl + F5 を押して) キャッシュがフラッシュされるまで) キャッシュに保持されます。

キャッシュできるファイルのタイプは、[Virtual Services] メニューの [Cache Configuration] で定義できます。

Maximum Cache Usage

仮想サービスでキャッシュを有効にすると、そのサービスで使用されるキャッシュの量を制限できます。 LoadMaster は、システム メモリ全体の 20% をグローバル キャッシュ値用に予約します。 たとえば、LoadMaster に 1GB の RAM がある場合、20% (または 204MB) がキャッシュと圧縮用に予約されます。 仮想サービスでキャッシュを有効にすると、制限なし (デフォルト値) または使用率の値を設定するオプションが表示されます。 [No Limit] を選択すると、使用可能なすべてのキャッシュを使用できます。 または、1 ～ 99% のパーセンテージを指定できます。 これにより、上記の例の 204MB をパーセンテージに分割できます。 たとえば、仮想サービス レベルで 20% を設定した場合、仮想サービスでは、サーバー応答をキャッシュするために合計 40MB を使用できます (204MB の 20% = 40.8MB)。 これにより、約 160MB が他の仮想サービスに使用できるようになります。

このメモリは、LoadMaster によってコンテンツの切り替えと本文の応答ルールにも使用されます。

パーセンテージを選択すると、LoadMaster は割り当てられた現在の使用量の合計を表示します。 これは、すべての仮想サービスに割り当てられている現在の使用量の組み合わせです。 たとえば、2 つの仮想サービスがあり、一方の最大キャッシュ使用率が 10% に設定され、もう一方の最大キャッシュ使用率が 7% に設定されている場合、現在の使用率の割り当て値は 17% と表示されます。 オーバー プロビジョニング/コミットすることが可能です。これを実行しようとすると、この値を設定するとキャッシュ メモリが N% オーバーコミットされるというメッセージが表示されます。 キャッシュ ストアの不均等な使用を防ぐために、キャッシュ サイズを制限することをお勧めします。 各仮想サービスが使用するキャッシュのパーセンテージを持つように、キャッシュの最大使用量が調整されていることを確認します。 キャッシュが有効な仮想サービスに割り当てる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

LoadMaster から送信されたファイルは Gzip で圧縮されています。

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。 キャッシュと圧縮の両方が有効になっている場合、キャッシュが優先されるため、最初のファイルはキャッシュされますが、圧縮されません。 2 回目以降の要求では、ファイルがキャッシュで検出され、圧縮されます。

圧縮できるファイルの種類は、LoadMaster WUI の [Virtual Services] メニューの [Compression Options] で定義できます。

サイズが 100MB 以上のファイルの圧縮はお勧めしません。 ハイパーバイザーを使用して大きなファイルを圧縮するには、仮想ロードマスターにさらに RAM を追加する必要がある場合があります。

Detect Malicious Requests

侵入防止システム (IPS) サービスは、攻撃をリアルタイムで軽減し、実サーバーを隔離することにより、実サーバー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、リアルタイムの侵入アラートを提供します。

更新またはカスタマイズされたルールを取得するには、SNORT Web サイト (https://www.snort.org/) 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選択すると、HTTP ごとの IPS およびオフロードされた HTTPS 仮想サービスが有効になります。 SNORT ルールに一致する要求の処理には 2 つのオプションがあります。 ルールが一致しても HTTP 応答が生成されないドロップ接続、またはルールが一致しても HTTP 400「無効な要求」のクライアントへの応答が生成される拒否の送信。 どちらのオプションも、要求が実サーバーに到達するのを防ぎます。

Enable Multiple Connect

このオプションを有効にすると、LoadMaster は LoadMaster とリアル サーバー間の接続処理を管理できます。 複数のクライアントからの要求は、同じ TCP 接続を介して送信されます。

多重化は、単純な HTTP GET 操作でのみ機能します。 [Enable Multiple Connect] チェック ボックスは、WAF、ESP、または SSL アクセラレーションが有効になっている場合など、特定の状況では使用できません。

Reschedule on every HTTP Request

これは実験的な機能です。 最初に　サポートに相談しない限り、有効にしないでください。

[Reschedule on every HTTP Request] オプションが有効で、コンテンツ スイッチングが使用されていない場合、リクエストごとに実サーバーの再選択が強制されます。 デフォルトでは、実サーバーは接続ごとに 1 回だけ選択されます。

HTTP 要求ごとに再スケジュール機能を使用するには、persistence を (標準オプションで) なしに設定する必要があります。

Port Following

２つのサービスが永続化レコードを共有する必要がある場合は、ポート フォローイングが設定されます。 通常、これは HTTP および HTTPS サービスに対して行われるため、安全に接続しているかどうかに関係なく、ユーザーはサーバー セッションを維持します。 いずれかの仮想サービスの実サーバーに障害が発生すると、他の仮想サービス上の同じ実サーバーの持続性レコードが消去されます。 ポートフォローイングにはいくつかの要件があります。

1. 仮想サービスには、同じ実サーバーのセットが必要です
2. 仮想サービスは同じ持続性オプションを使用している必要があります

これらの条件を満たすと、仮想サービスの変更画面で、[Port Following] の [Advanced Propeties] の下にオプションが表示されます。 ポート追跡が双方向で行われるように、両方の仮想サービスでこれを設定してください。 クライアントが HTTP を使用して接続するか HTTPS を使用して接続するかに関係なく、永続性とセッションが保存されるように、ポート追跡を双方向で設定する必要があります。

LoadMaster ファームウェア バージョン 7.2.51 より前では、サービス タイプが Generic に設定されている仮想サービスのポート フォローイングを構成することはできませんでした。 これは、バージョン 7.2.51 以降で可能です。

詳細については、Kemp ドキュメント ページのポート フォローイング、機能の説明を参照してください。

Add Header to Request

実サーバーに送信されるすべてのリクエストに挿入される追加ヘッダーのキーと値を入力します。 [Set Header] ボタンをクリックして、機能を実装します。

Copy Header in Request

これは、リクエストが実サーバーに送信される前に、新しいヘッダー フィールドにコピーするソース ヘッダー フィールドの名前です。 ソース ヘッダーをコピーするヘッダー フィールドの名前を [To Header] テキスト ボックスに入力します。

Add HTTP Headers

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ーを選択できます。 利用可能なオプションは次のとおりです。

- Legacy Operation(X-Forwarded-For)
- None
- X-Forwarded-For (+ Via)
- X-Forwarded-For (No Via)
- X-ClientSide (+ Via)
- X-ClientSide (No Via)
- Via Only

HTTP ヘッダーを使用すると、クライアントとサーバーは HTTP 要求または応答で追加情報を渡すことができます。 RDP 仮想サービスなど、すべての仮想サービスが HTTP データ (ヘッダー/本文) を処理できるわけではありません。 パフォーマンスを向上させ、不要な作業を節約するために、すべての HTTP 仮想サービスが HTTP データを参照する必要があるわけではありません。 単純なパススルー仮想サービスは、HTTP 要求を処理する必要はまったくありません。 仮想サービスでルールが定義されている場合、ヘッダーが追加されている場合、またはより複雑な機能が必要な場合、仮想サービスは HTTP データを確認する必要があります。 LoadMaster の古い (レガシー) バージョンでは、Add HTTP Headers の設定はグローバルのみであり、仮想サービスごとに設定することはできませんでした。 必要に応じて、特定の仮想サービスで HTTP ヘッダーの追加の設定を更新できるようになりました。 デフォルト値は、下位互換性の理由から Legacy Operation(XForwarded-For) です。

SubVS が存在する場合、[Add HTTP Headers] フィールドは親仮想サービスで構成できません。 は、SubVS を追加する場合は、親仮想サービスの Add HTTP Headers 値を変更しないことをお勧めします。 SubVS を追加した後に親仮想サービスでこれを変更する必要がある場合は、コンテンツ ル

ールを使用するか、API コマンドを実行して値を変更できます。

例: https://<LoadMasterIPAddress>/access/modvs?vs < VSIndex>&Addvia=5 Addvia パラメーターの有効な値を含む RESTful API の詳細については、RESTful API インターフェイスの説明を参照してください。

Sorry Server

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。 使用可能なリアル サーバーがない場合、LoadMaster はチェックなしで指定された場所にリダイレクトします。 ソーリー サーバーの IP アドレスは、ロードマスターで定義されたネットワークまたはサブネット上にある必要があります。

レイヤ 4 仮想サービスを使用する場合、Sorry Server は Real Server と同じサブネット上にある必要があります。 レイヤー 7 仮想サービスを使用する場合、Sorry Server は任意のローカル ネットワーク上に配置できます。 非ローカルのソーリー サーバーを追加することも可能です。 このためには、透過性を無効にする必要があり、Sorry Server へのルートが必要であり、[Enable Non-Local Real Servers] オプションを有効にする必要があります ([System Configuration] > [Miscellaneous Options] > [Network Options])。

Not Available Redirection Handling

リクエストを処理するために使用できる実サーバーがない場合、クライアントが受信するエラー コードと URL を定義できます。

- Error Code: 実サーバーが利用できない場合、LoadMaster は HTTP エラー コードで接続を終了できます。 適切なエラー コードを選択します。
- Redirect URL: 使用可能なリアル サーバーがなく、エラー応答がクライアントに返される場合、リダイレクト URL も指定できます。 このテキスト ボックスに入力された文字列に http:// または https:// が含まれていない場合、文字列は現在の場所に関連するものとして扱われるため、ホスト名がリダイレクト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と URI (Uniform Resource Identifier) をそれぞれ表す %h や %s などのワイルドカードの使用もサポートされています。
- Error Messages: 実サーバーが利用できず、エラー応答がクライアントに返される場合、指定されたエラー メッセージが応答に追加されます。

セキュリティ上の理由から、返された HTML ページはテキスト Document has moved のみを返します。 リクエスト提供の情報は返されません。

- Error File: 実サーバーが利用できず、エラー応答がクライアントに返される場合、指定されたファイルが応答に追加されます。 これにより、指定されたエラーに応答して単純なエラー HTML ページを送信できます。

このエラー ページの最大サイズは 16KB です。

Not Available Server/Port

UDP 仮想サービスには、利用できないサーバーとポートを指定するオプションがあります。 リクエストを処理できる実サーバーがない場合、このオプションはクライアントが受け取る URL を定義します。

サービスが現在 Not Available Server を使用していない場合、Not Available Server の値は UDP に対してのみ変更できます。

Add a Port 80 Redirector VS

ポート 80 の仮想サービスが構成されていない場合は、作成できます。 次に、リダイレクト URL: フィールドで指定された URL にクライアントをリダイレクトします。
Add HTTP Redirector ボタンをクリックして、リダイレクタを実装します。

[Add HTTP Redirector] ボタンをクリックすると、リダイレクト仮想サービスが作成され、この WUI オプションは関連する仮想サービスから消えます。

Default Gateway

クライアントに応答を返すために使用する仮想サービス固有のゲートウェイを指定します。 これが設定されていない場合、グローバル デフォルト ゲートウェイが使用されます。 [Set Default Gateway] ボタンをクリックして、デフォルト ゲートウェイを実装します。 仮想サービスのデフォルト ゲートウェイは、その仮想サービスに対してのみ使用されます。

[System Configuration] > [Miscellaneous Options] > [Network Options] でグローバルな [デフォルト ルートのみを使用] オプションが設定されている場合、デフォルト ゲートウェイが設定されている仮想サービスからのトラフィックは、仮想サービスのデフォルト ルートがあるインターフェイス

にのみルーティングされます。 これにより、隣接するインターフェイスを使用してトラフィックを直接返すことなく、LoadMaster をクライアント ネットワークに直接接続できます。

Alternate Default Gateway

このフィールドは、仮想サービスに代替アドレスが設定されている場合にのみ表示されます。 次の条件がすべて満たされている場合にのみ、代替デフォルト ゲートウェイ フィールドを使用してください。

- 代替アドレスには、メインの仮想サービス アドレスとは異なるアドレス ファミリがあります。たとえば、仮想サービス アドレスが IPv4 で代替アドレスが IPv6 である、またはその逆です。
- 仮想サービスのデフォルト ゲートウェイが設定されます。
- 2番目の仮想サービス デフォルト ゲートウェイが他のアドレス ファミリ用に設定されます。

Alternate Source Addresses

リストが指定されていない場合、LoadMaster は仮想サービスの IP アドレスをローカル アドレスとして使用します。 アドレスのリストを指定すると、LoadMaster はこれらのアドレスを代わりに使用するようになります。

Set Alternate Source Addresses ボタンをクリックして、Alternate Source Addresses を実装します。

このオプションは、[L7 Configuration] 画面で [Allow connection scaling over 64K Connections] オプションが有効になっている場合にのみ使用できます。

Service Specific Access Control

仮想サービス固有のアクセス コントロール リストを変更できます。

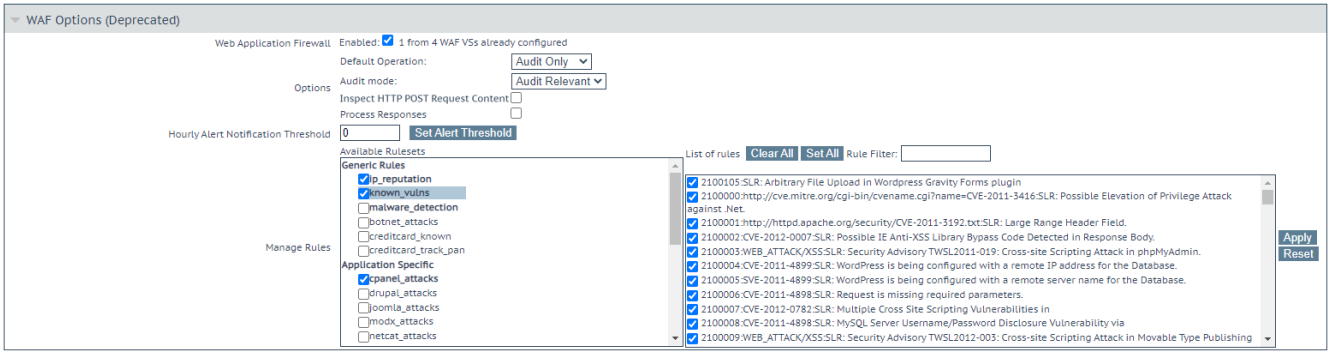
Access Control Lists オプションを実装すると、Extra Ports オプションは正しく機能しません。

インターフェイスと同じ IP アドレスを持つ仮想サービスでアクセス コントロール リストを使用する場合 (は推奨しません)、クライアントとして VS にアクセスする同じネットワーク インターフェイス上の実サーバーに対して、次のポートがブロックされることはありません。

- 443 (WUI)

- 22 (SSH)
- 53 (DNS)
- 161 (SNMP)

3.8 従来の Web アプリケーション ファイアウォール (WAF) オプション

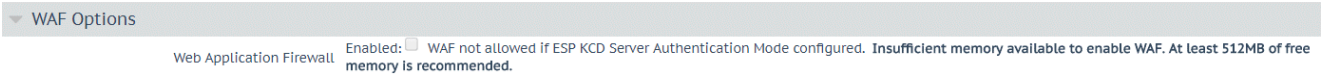


レガシー WAF ルールは 2021 年 6 月 29 日に廃止され、それ以上の更新は利用できません。は、ユーザーが構成を新しい WAF サービスに移行することを推奨しています。

これらのオプションを構成する前に、Web アプリケーション ファイアウォール (WAF) 機能を有効にする必要があります。

WAF は、すべてのサポート層で利用できるわけではありません。 各サポート層に含まれる機能の詳細については、次のページを参照してください。 LoadMaster サポート サブスクリプション

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。 [Enabled] チェック ボックスの横にメッセージが表示され、存在する WAF 対応の仮想サービスの数と、存在できる WAF 対応の仮想サービスの最大数が示されます。



WAF 対応の仮想サービスの最大数に達した場合、[Enabled] チェック ボックスはグレー表示されま

す。 WAF を有効にするために使用できるメモリが不足している場合は、メッセージが表示されます。

WAF を利用すると、LoadMaster の展開のパフォーマンスに大きな影響を与える可能性があります。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の LoadMaster インスタンスの場合、WAF の動作には最低 2GB の RAM が割り当てられている必要があります。 LoadMaster オペレーティング システム バージョン 7.1-22 より前の仮想 LoadMaster および LoadMaster ベア メタル インスタンスのデフォルトのメモリ割り当ては、1GB の RAM です。 このデフォルトの割り当てが変更されていない場合は、WAF 構成を続行する前にメモリ設定を変更してください。

Default Operation

WAF のデフォルトの動作を選択します。

1. Audit Only: これは監査のみのモードです。ログは作成されますが、要求と応答はブロックされません。
2. Block Mode: 要求または応答のいずれかがブロックされます。

Audit mode

記録するログを選択します。

- No Audit: データは記録されません。
- Audit Relevant: 警告レベル以上のデータをログに記録します。 これは、この設定のデフォルトのオプションです。
- Audit All: 仮想サービスを介してすべてのデータをログに記録します。

[Audit All] オプションを選択すると、大量のログ データが生成されます。 Progress Kemp は、通常の操作で [Audit All] オプションを選択することをお勧めしません。 ただし、特定の問題のトラブルシューティングを行う場合は、[Audit All] オプションが役立つ場合があります。

Inspect HTTP POST Request Content

このオプションを有効にすると、POST リクエストで提供されたデータも処理されます。

3 つの追加オプション (JSON パーサーを有効にする、XML パーサーを有効にする、およびその他の

コンテンツ タイプを有効にする) は、[HTTP ポスト リクエスト コンテンツの検査] が有効になっている場合にのみ使用可能になります。

Enable JSON Parser

JavaScript Object Notation (JSON) POST リクエストの検証を有効にします。

Enable XML Parser

XML POST リクエストの検証を有効にします。

Enable Other Content Types

POST コンテンツ タイプ (XML/JSON 以外) の検証を有効にします。

他のコンテンツ タイプの検査を有効にすると、システム リソースの使用率 (CPU とメモリ) が増加する可能性があります。 コンテンツ タイプの特定のリストを検討する必要があります。

このオプションを有効にすると、WAF 分析で許可される POST コンテンツ タイプのコンマ区切りリストを入力するためのテキスト ボックスが提供されます。 デフォルトでは、すべてのタイプ (XML/JSON 以外) が有効になっています。

Process Responses

実サーバーから送信された応答を検証するには、このオプションを有効にします。

これは、CPU とメモリを集中的に使用する可能性があります。 リアル サーバーが gzip エンコーディングの場合、プロセス レスポンスが有効になっていても、WAF はそのトラフィックをチェックしません。

Hourly Alert Notification Threshold

これは、アラートを送信する前の 1 時間あたりのインシデントのしきい値です。 これを 0 に設定すると、アラートが無効になります。 このしきい値は、WUI ホームページに表示される今日の制限を超えたイベント数にも関連しています。 たとえば、しきい値が 10 に設定されていて、20 のイベントがあった場合、カウンターは 2 に設定されます。

Rules

ここで、一般的なルール、アプリケーション固有のルール、アプリケーション固有のルール、およびカスタム ルールを仮想サービスとの間で割り当て/割り当て解除できます。

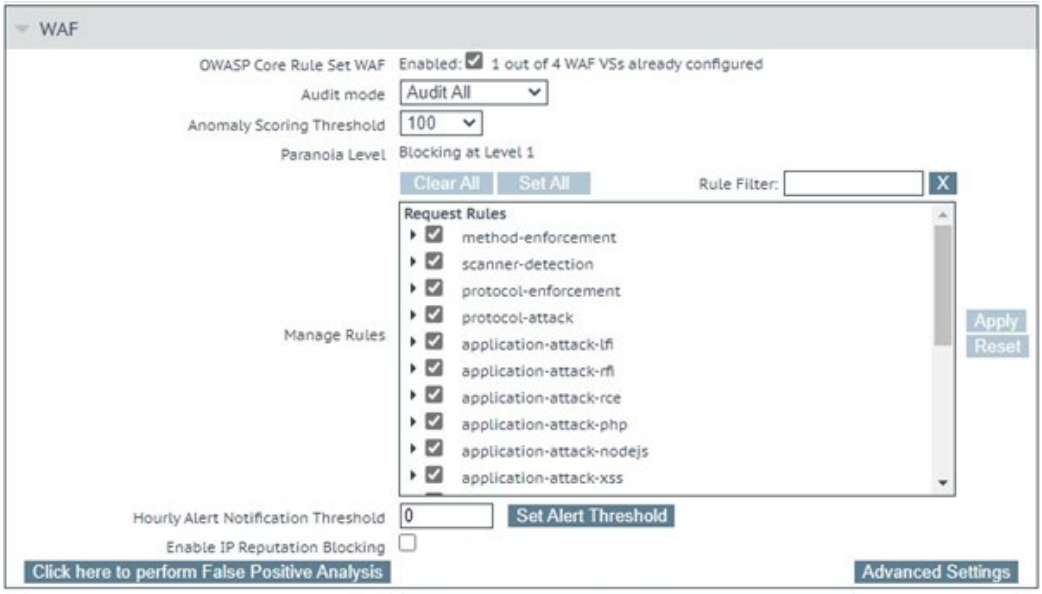
アプリケーション固有のルールとアプリケーション固有のルールを同じ仮想サービスに割り当てることはできません。

各ルールセット内の個々のルールは、必要に応じて有効/無効にすることができます。 ルールセットを有効にするには、関連するチェック ボックスをオンにします。 以前にそのルールセットでルールを有効/無効にしたことがない場合、すべてのルールがデフォルトで右側のボックスで有効になっています。 その仮想サービス内でそのルールセット内のルールを以前に有効化/無効化した場合、ルールは以前の設定を保持します。 必要に応じて、左側で関連するルールセットをチェックし、右側でルールをチェック/チェック解除することで、個々のルールを有効/無効にすることができます。

一部のルールまたはルール セットは、他のルールに依存する場合があります。 ルールが無効になっている場合、LoadMaster では依存関係のチェックは行われません。ルールを無効にする前に、ルール チェーン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 Al]l ボタンをクリックすると、選択したルールセットの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、選択したルールセットの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して、ルールをフィルタリングし、フィルタ テキストを含むルールのみを表示することができます。
[Reset] をクリックすると、すべてのルールセットとルールが無効になります。

3.9 ウェブ アプリケーション ファイアウォール (WAF) オプション



デフォルトでは、WAF は無効になっています。 WAF を有効にするには、[Enabled] を選択します。仮想サービスで WAF が有効になっている場合、仮想サービス オプションのセクションの見出しが WAF から WAF - Enabled に変わります。

WAF 対応の仮想サービスの最大数は、合計 (未使用または使用可能な) RAM (MB)/512 MB です。例: 8 GB/512 MB = 16 個の WAF 対応仮想サービス。 最大数に達すると、追加の仮想サービスを WAF で有効にすることはできません。 WAF を有効にするために使用できるメモリが不足している場合は、メッセージが表示されます。

[Enabled] チェック ボックスの横にメッセージが表示され、存在する WAF 対応の仮想サービスの数と、存在できる WAF 対応の仮想サービスの最大数が示されます。 WAF 対応の仮想サービスの最大数に達すると、[Enabled] チェック ボックスがグレー表示されます。

Audit mode.

次の 3 つの監査モードがあります。

- No Audit: データは記録されません。
- Audit Relevant 警告レベル以上のデータをログに記録します。 これは、この設定のデフォルトのオプションです。
- Audit All: 仮想サービスを介してすべてのデータをログに記録します。

[Audit All] オプションを選択すると、大量のログ データが生成されます。 Progress Kemp は、通常の操作で [Audit All] オプションを選択することをお勧めしません。 ただし、特定の問題のトラブルシューティングを行う場合は、[Audit All] オプションが役立つ場合があります。

Anomaly Scoring Threshold.

リクエストごとに、トリガーされた検出ごとに異常スコアが上昇し、ほとんどのルールのスコアは 5 です。リクエストごとの累積異常スコアが設定された制限に達すると、リクエストはブロックされます。 デフォルト値は 100 で、許容範囲は 1 ～ 10000 です。

パラノイア レベルは [Advanced Settings] で設定できますが、値は情報提供のためにここに表示されます。

Manage Rules

ルールは、OWASP 番号付けシステムに従って、リクエスト ルール セクションにグループ化されます。 各ルールセット内のルール グループまたは個々のルールは、必要に応じて有効/無効にすることができます。 ルールまたはルールのグループを有効にするには、関連するチェック ボックスをオンにします。 その仮想サービス内でそのルールセット内のルールを以前に有効化/無効化した場合、ルールは以前の設定を保持します。

一部のルールまたはルール セットは、他のルールに依存する場合があります。 ルールが無効になっている場合、LoadMaster では依存関係のチェックは行われません。ルールを無効にする前に、ルール チェーンまたは依存関係に注意してください。

ユーザーがカスタム ルールを作成した場合、[Customer Rules] セクション内でそれらを有効または無効にすることができます。 カスタム ルールに使用できる [Run first] チェック ボックスがあります。 最初に実行チェックボックスが有効になっている場合
カスタム ルールの場合、ルールは OWASP コア ルール セット (CRS) の前に最初に実行されます。カスタム ルールの [Run First] チェック ボックスが無効になっている場合、カスタム ルールは CRS の後に実行されます。 [Workloads] セクションには、利用可能ないくつかのワークロードがあります。 変更が完了したら、[Apply] ボタンをクリックします。 [Reset] をクリックすると、適用されていない変更が元に戻ります。 ルールをフィルタリングするには、[Rule Filter] テキスト ボッ

クスにテキストを入力すると、そのテキストを含むルールのみが表示されます。 [Set All] をクリックしてフィルタリングされたルールを選択するか、[Clear All] をクリックしてフィルタリングされたルールの選択を解除できます。 [Apply] ボタンをクリックして、変更を適用します。

Hourly Alert Notification Threshold

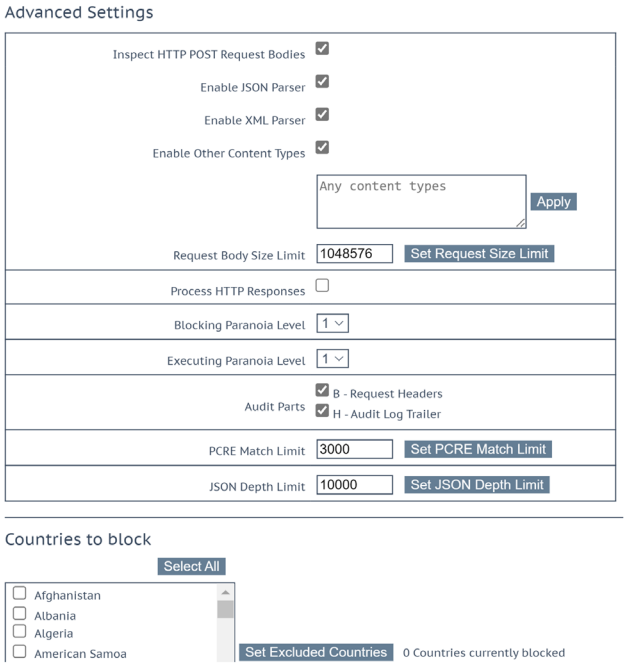
これは、アラートを送信する前の 1 時間あたりのインシデント数です。 これを 0 に設定すると、アラートが無効になります。

IP Reputation Blocking

このルール セットは、IP レピュテーション データベースに対するクライアント アドレスのチェックを有効にします。

3.9.1 高度な設定

[Advanced Settings]ボタンをクリックして、詳細な OWASP 設定を構成します。



Inspect HTTP POST Request Bodies

このオプションはデフォルトで無効になっています。 このオプションを有効にすると、さらに 3 つのチェック ボックスが使用可能になり、JavaScript Object Notation (JSON)、Extensible Markup Language (XML) 要求、およびその他のコンテンツ タイプの処理を有効にすることができます。

Request Body Size Limit

このオプションを使用すると、WAF エンジンが許可する POST リクエスト ボディの最大サイズを設定できます。 デフォルト値は 1048576 バイトです。 有効な値の範囲は 1024 ～ 52428800 バイト (50 MB) です。

値を大きくすると、より多くのメモリ リソースが必要になり、WAF エンジンのパフォーマンスに影響を与える可能性があります。

Process HTTP Responses

サーバーからクライアントへの応答のチェックを有効にします。
Process HTTP Responses オプションを有効にすると、さらに 2 つのオプション、E - Intended Response Body と F- Response Headers が、Audit Parts オプションで使用可能になります。

応答データの処理は、CPU とメモリを集中的に使用する可能性があり、パフォーマンスに影響を与える可能性があります。

Blocking Paranoia Level

ModSecurity エンジンが各ルールをどの程度厳密に実装するかを定義します。 デフォルトのパラノイア レベル値は 1 に設定されています。パラノイア レベルが上がるごとに、CRS はルールのより厳密な実装を有効にし、より高いレベルのセキュリティを提供します。 ただし、パラノイア レベルが高くなると、誤検知によって一部の正当なトラフィックがブロックされる可能性も高くなります。 より高いパラノイア レベルを使用する場合は、複雑な入力パターンを受け取る必要がある特定のアプリケーションに対して、いくつかの除外ルールを追加する必要がある可能性があります。

Executing Paranoia Level

ModSecurity エンジンがサーバーからのリクエストをチェック/検証するパラノイア レベルを定義します。 チェックの結果はログに記録されますが、実行パラノイア レベルは、ブロックされるトラフィックを決定するために使用されません。 実行パラノイア レベルはブロック パラノイア レベルより高くすることはできますが、低くすることはできません。 より高い実行パラノイア レベルでは、トラフィックをブロックすることなく、より高いパラノイア レベルでトリガーされるルールをユーザーが確認できます。

Audit Parts:

リクエストごとに WAF 監査ログに入力されるセクションを含む単一の文字列。 サポートされている値は A、B、E、F、H、K、Z ですが、有効または無効にできるのは B、E、F、H の値のみです。

監査パーツの詳細については、次を参照してください。

https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

PCRE Match Limit:

この設定は、一致に失敗する前に内部 PCRE エンジンが使用する最大反復回数を設定します。 値が低いと有効な一致が失敗する可能性があり、値が高いと WAF エンジンの実行が遅くなる可能性があります。 デフォルト値は 10000 です。最大値は 9999999 です。

JSON Depth Limit

この値は、JSON 解析中に受け入れられる最大深度を設定します。 値が低いと、有効な一致が失敗する可能性があります。 値を大きくすると、WAF エンジンの実行が遅くなる場合があります。 デフォルト値は 10000 です。有効な値の範囲は 1000 から 99999 です。

Workloads

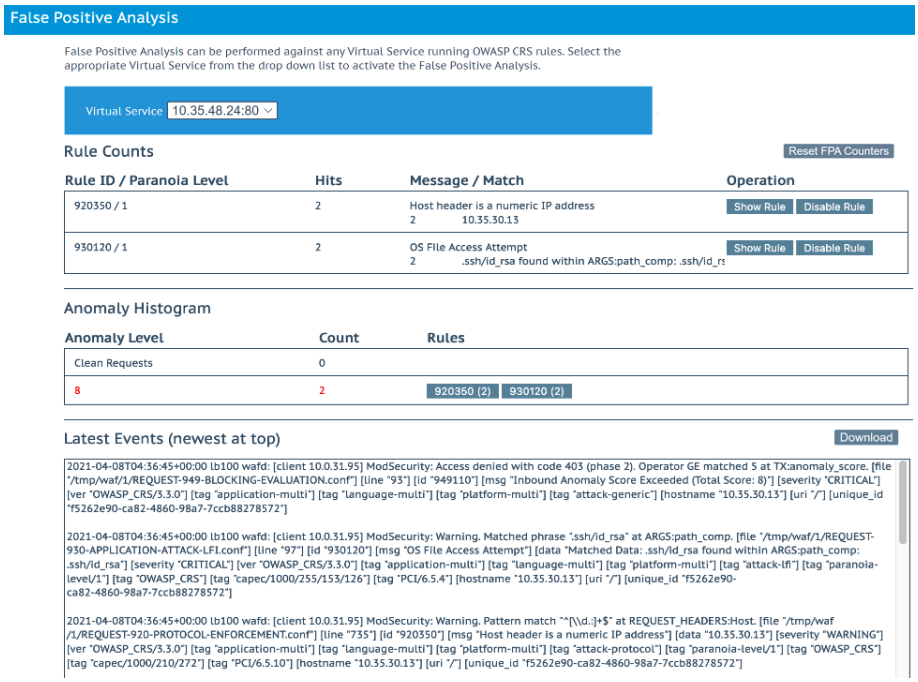
ワークロードが選択されると、OWASP CRS はルールを最適化し、既知の誤検知が返されないようにします。

Countries to block:

GEO IP 情報に基づいて、アクセスを許可しない国を選択できます。 [Select All] ボタンをクリックしてすべての国のアクセスをブロックするか、国リストからブロックする国を個別に選択して [Set Excluded Countries] ボタンをクリックします。

3.9.2 誤検知分析

この機能により、ユーザーはアプリケーションに対して誤検出分析を実行して、攻撃の可視性を高め、保護を微調整することができます。 OWASP CRS ルールを実行する仮想サービスに対して False Positive をチェックするには、ここをクリックして False Positive Analysis ボタンをクリックします。



Rule Counts

[Rule Counts] セクションには、リクエストによってトリガーされたすべてのルールに関する情報が表示されます。 ルール ID、ルールが実行されているパラノイア レベル、ルールをトリガーしたリクエストごとのヒット数、およびリクエストのメッセージまたは一致が、トリガーされたルールごとに表示されます。 [Operations] 列の [Show Rule] ボタンをクリックすると、トリガーされたルールに関連付けられているルール ファイルの内容が表示されます。 これは別のタブで開き、URL にはトリガーされたルール ID が含まれます。 [Disable Rule] ボタンをクリックすると、ルールを無効にすることができます。

Reset FPA Counter

仮想サービスのすべての誤検知分析カウンター (異常ヒストグラムと最新イベント) をリセットします。 最新のイベントをクリアしても、LoadMaster からログは削除されません。ログは、[System Configuration] > [Log Options] > [System Log Files] > [WAF Event Log File] で引き続き利用できます。

Anomaly Histogram

[異常ヒストグラム] セクションの最初の行には、ルールをトリガーせずに実行されたリクエストの数が表示されます。 後続の各行には、トリガーされ、異常スコアに影響を与えているルールの詳細が示されます。 各行には、累積異常スコア、ルールをトリガーしたリクエストの数、およびルールの詳細が表示されます。

Latest Events (newest at top)
トリガーされた各ルールのイベントの詳細を表示します。 これらのメッセージは標準の ModSecurity ログ形式であり、異常スコア、警告メッセージ、攻撃状態、パラノイア レベルが含まれています。

Download
[Download] ボタンをクリックして、表示されている WAF イベント ログの詳細をダウンロードします。

3.9.3 WAF が正しく構成されていない仮想サービスのステータス

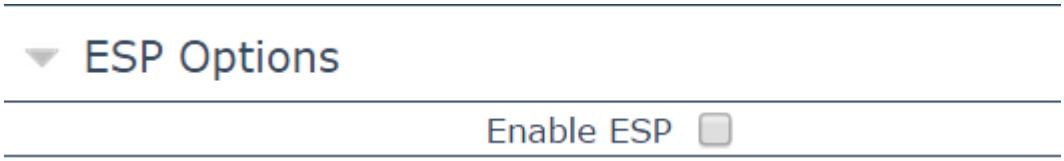
LoadMaster UI の View/Modify Services 画面では、各仮想サービスのステータスが表示されます。特定の仮想サービスの WAF が正しく構成されていない場合 (たとえば、ルール ファイルに問題がある場合)、ステータスは WAF の構成が正しくないに変わり、赤に変わります。

仮想サービスが WAF Misconfigured 状態にある場合、すべてのトラフィックの流れが停止します。問題のトラブルシューティング中に、必要に応じてその仮想サービスの WAF を無効にして、ブロックされているトラフィックを停止できます。

3.10 エッジ セキュリティ パック (ESP) オプション

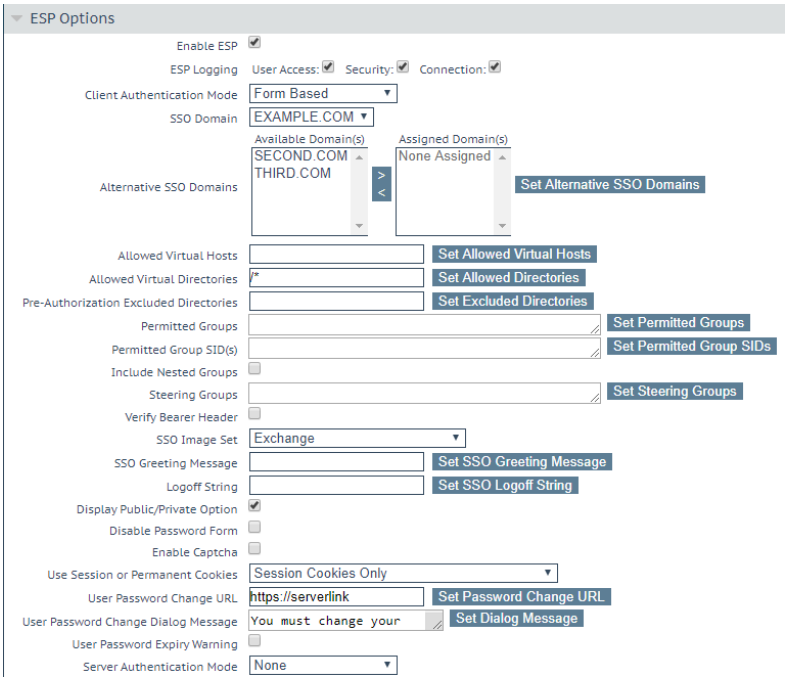
これらのオプションを構成する前に、ESP 機能を有効にする必要があります。 ESP 機能を有効にするには、ESP を有効にするチェックボックスを選択してください。

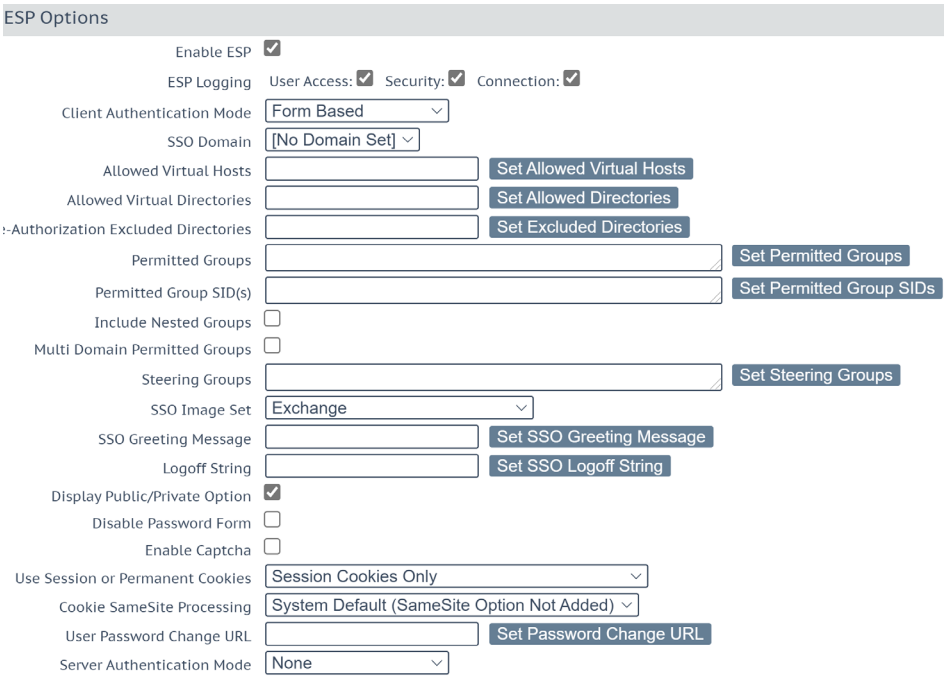
ESP はすべてのサポート層で利用できるわけではありません。 各サポート層に含まれる機能の詳細については、次のページを参照してください。 LoadMaster サポート サブスクリプション



完全な ESP オプション画面が表示されます。

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





Enable ESP

[ESP を有効にする] チェックボックスをオンまたはオフにして、ESP 機能セットを有効または無効にします。

ESP Logging

ESP 機能に関連して保存されるログには 3 つのタイプがあります。 これらの各ログは、関連するチェックボックスを選択または選択解除することで有効または無効にできます。 ログの種類は次のとおりです。

- User Access: すべてのユーザー ログインを記録するログ
- Security: すべてのセキュリティ アラートを記録するログ
- Connection: 各接続を記録するログ

ログは永続的であり、LoadMaster の再起動後にアクセスできます。 ログの詳細については、「Extended Log File」セクションを参照してください。

Client Authentication Mode

LoadMaster に接続しようとするクライアントを認証する方法を指定します。 次の種類のメソッドを使用できます。

- Delegate to Server: 認証はサーバーに委任されます
- Basic Authentication: 標準の基本認証が使用されます
- Form Bases: クライアントは、ロードマスターで認証されるためにフォーム内にユーザーの詳細を入力する必要があります
- Client Certificate: クライアントは、発行機関に対して検証された証明書を提示する必要があります

LoadMaster ファームウェア バージョン 7.2.53 では、サーバー側認証を使用しないクライアント証明書認証のサポートが追加されました。 詳細については、Progress Kemp ドキュメント ページの ESP 機能の説明を参照してください。

- NTLM/NTLM-Proxy: NTLM 資格情報は、対話型ログオン プロセス中に取得されたデータに基づいており、ドメイン名とユーザー名で構成されています。
- SAML: LoadMaster は、SAML サービス プロバイダーの役割を果たす SAML をサポートします。 サービス プロバイダーは、リソースへの安全なゲート付きアクセスを提供します。
- Pass Post: LoadMaster ファームウェア バージョン 7.2.53 では、パス ポストと呼ばれる新しいモードが導入されました。 この変更の導入により、Workspace クライアント アプリを使用する有効な資格情報を持つユーザーは、POST ベースを使用して (シングル サ

インオン（SSO）を使用して）正常にログインできます。クライアント側の認証とサーバー側のフォーム ベース認証（FBA）と、VDI ワークスペースへのアクセスが許可されます。

- OIDC/OAUTH: Open ID Connect (OIDC) は、OAuth2 プロトコルに基づく認証プロトコルであり、単一の ID プロバイダーを介して複数のアプリケーションでユーザーのシングル サインオンを有効にするために使用されます。 OIDC は、OAuth2 からの標準化されたメッセージ フローを使用して ID サービスを提供します。

ESP オプション セクションの残りのフィールドは、選択したクライアント認証モードに基づいて変更されます。

SSO Domain

仮想サービスが含まれるシングル サインオン（SSO）ドメインを選択します。 SSO ドメインの構成の詳細については、「SSO ドメインの管理」セクションを参照してください。 ESP 機能を正しく構成するには、SSO ドメインを構成する必要があります。

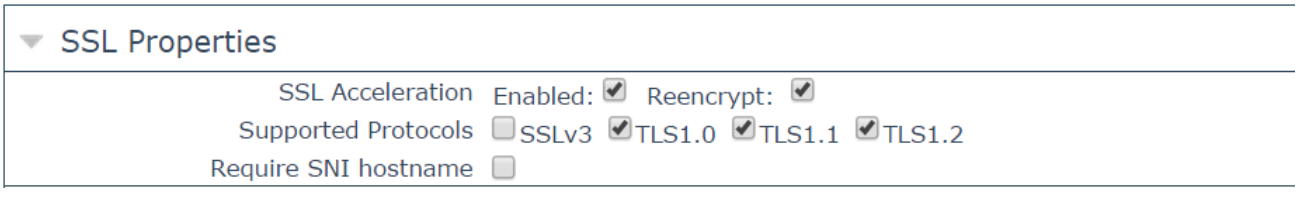
この [SSO Domain] フィールドには、構成タイプが [Inbound Configuration] の SSO ドメインのみがオプションとして表示されます。

Alternative SSO Domains

多くの組織は、エクストラネットを使用して顧客やパートナーと情報を共有しています。 エクストラネット ポータルには、 2 つ以上の Active Directory ドメインのユーザーがいる可能性があります。個々のドメインのユーザーを 1 人ずつ認証するのではなく、代替 SSO ドメインを割り当てると、 1 つの仮想サービスを使用して複数のドメインのユーザーを同時に認証できます。

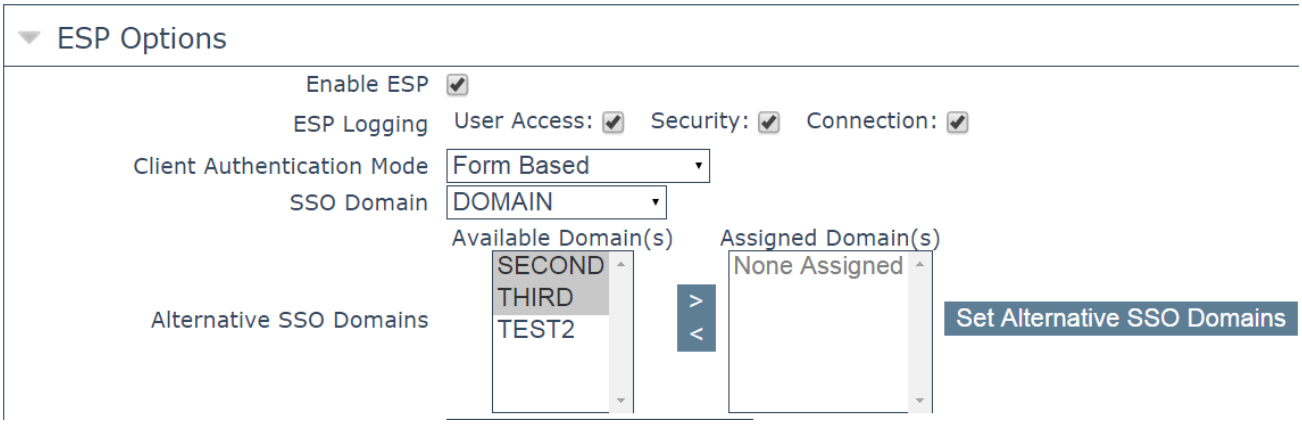
このオプションは、複数のドメインが構成されており、SSO ドメインの認証プロトコルが LDAP に設定されている場合にのみ表示されます。

SSO ドメインの構成の詳細については、「Manage SSO Domain」セクションを参照してください。

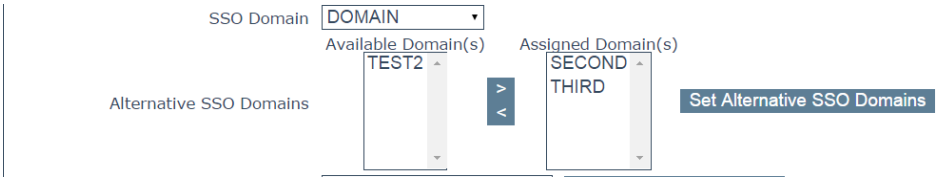


ESP を有効にする前に、SSL オフロードが HTTPS 仮想サービスに対して構成されていることを確認

してください。



[SSO Domain] ドロップダウン リストに表示されるドメイン名は、デフォルト ドメインです。 これは、 1 つだけが構成されている場合に使用されるドメインでもあります。 以前に構成された代替ドメインが [Available Domain(s)] リストに表示されます。



代替 SSO ドメインを割り当てるには:

- 割り当てたい各ドメインを強調表示し、[>] ボタンをクリックします。

割り当てられたドメインは、特定の仮想サービスを使用して認証できるドメインです。 利用可能として表示されるすべてのドメインは、仮想サービスに割り当てることができます。

- [Set Alternative SSO Domains] ボタンをクリックして、割り当てられたドメインの更新されたリストを確認します。
- [Server Authentication Mode] ドロップダウン リストから [Basic Authentication] を選択します。

ESP フォームを使用してドメインにログインするとき、別のドメインにアクセスする必要がある場合、ユーザーは SSO ドメインの名前を入力する必要があります。 ユーザー名にドメイン名が入力されていない場合、ユーザーはデフォルトで、デフォルトの SSO ドメイン ドロップダウン リストに入力されたドメインにログオンします。

仮想サービスのステータスを表示するには、メイン メニューで [Virtual Service] および [View /Modify Service] をクリックします。 各サービスの現在のステータスを示す仮想サービスのリストが表示されます。 代替ドメインが割り当てられ、特定のドメインに問題がある場合、影響を受けるドメイン名が [Status] 列に表示されます。

Allowed Virtual Hosts

仮想サービスは、指定された仮想ホストへのアクセスのみが許可されます。 指定されていない仮想ホストはすべてブロックされます。 [Allowed Virtual Host] 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て、許可された仮想ホストを指定します。 フィールド内に複数のドメインを指定して、多くのドメインをシングル サインオン ドメインに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。

LoadMaster WUI の正規表現で引用符を使用する場合、制限があります。詳細については、「Limitations of Using Regular Expressions」セクションを参照してください。 このフィールドを空白のままにすると、仮想サービスはブロックされます。 ESP オプションの Permitted Group] フィールドを使用する場合、ここで設定された 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。 たとえば、SSO ドメインが webmail.example に設定されていて、webmail が example.com 内の許可されたグループのディレクトリでない場合、それは機能しません。 代わりに、SSO ドメインを .example.com に設定する必要があります。

Allowed Virtual Directories

仮想サービスは、許可された仮想ホスト内の指定された仮想ディレクトリへのアクセスのみが許可されます。 指定されていない仮想ディレクトリはすべてブロックされます。 [Allowed Virtual Directories] フィールドに仮想ディレクトリ名を入力し、[Set Allowed Virtual Directories] ボタンをクリックして、許可された仮想ディレクトリを指定します。 このフィールドでは正規表現を使用できます。

Pre-Authorization Excluded Directories

このフィールド内で指定された仮想ディレクトリは、この仮想サービスで事前承認されず、関連する実サーバーに直接渡されます。

Permitted Groups

この仮想サービスへのアクセスを許可するグループを指定します。 設定されている場合、ユーザーがこの仮想サービスによって公開されたサービスにログインする場合、ユーザーは指定されたグループの

少なくとも 1つのメンバーである必要があります。 多数のグループが入力されると、パフォーマンスが影響を受ける場合があります。 このフィールドに入力されたグループは、LDAP クエリを使用して検証されます。 このフィールドに関するガイドラインは次のとおりです。

- 指定するグループは、仮想サービスに関連付けられた SSO ドメインの Active Directory で有効なグループである必要があります。 LoadMaster の SSO ドメインは、グループのディレクトリに設定する必要があります。 たとえば、LoadMaster の SSO ドメインが webmail.example に設定されていて、webmail がグループのディレクトリでない場合、機能しません。 代わりに、SSO ドメインを .example.com に設定する必要がある場合があります。
- リストされているグループは、セミコロンで区切る必要があります

IT ユーザーなど、ほとんどのグループには名前にスペースが含まれているため、スペース区切りのリストは機能しません。

1. ドメイン ユーザー グループは、新しいユーザーの既定のプライマリ グループであるため、使用しないでください。
2. 次の文字は許可されたグループ名に使用できません: / : + *
3. 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
4. グループは、完全な識別名ではなく、名前で指定する必要があります
5. [Permitted Group] フィールドと [Steering Group] フィールドの両方に同じグループ名を入力しないでください。 これにより、競合が発生します。 ステアリング グループを指定すると、許可されたグループのように動作すると見なされるため、[Permitted Group] フィールドと [Steering Group] フィールドの両方に同じグループを入力する必要はありません。

Permitted Group SID(s)

このフィールドは、許可されたグループ フィールドと同等です。 許可されたグループを指定する場合は、[Permitted Group] フィールドまたは [許可されたグループ SID(s)] フィールド (セキュリティ識別子) のいずれかに入力できます。

[Permitted Group SID(s)] フィールドで、この仮想サービスへのアクセスを許可するグループ SID を指定できます。 グループを入力したら、[Permitted Group SID(s)] をクリックします。

このフィールドには、長さが最大 64 バイト (NN NN NN の形式で 192 文字) のグループ SID のリストを指定できます。

各グループはセミコロンで区切ります。 特定のグループ SID では、バイトを区切るためにスペースが使用されます。
次に例を示します。
S-1-5-21-3763804817-1170992687-1336323834-1151
SID は、get-adgroup-Identity GroupName コマンドを使用して見つけることができます。

Include Nested Groups

このフィールドは、許可されたグループの設定に関連しています。 認証試行にネストされたグループを含めるには、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、最上位グループのユーザーのみがアクセスを許可されます。 このオプションを有効にすると、トップレベル グループと最初のサブレベル グループの両方のユーザーにアクセス権が付与されます。

Multi Domain Permitted Groups

LoadMaster ファームウェア バージョン 7.2.52 では、仮想サービスの変更画面の ESP オプション セクションに、Multi Domain Permitted Groups という新しいチェック ボックスが追加されました。 このチェック ボックスは、次のクライアント認証モードで構成できます。

- Basic Authentication
- Form Based
- Client Certificate
- NTLM

Multi Domain Permitted Groups が有効な場合、LoadMaster はトップレベル ドメインの下のすべてのサブドメイン内で許可されたグループ メンバーシップをチェックします。

[Multi Domain Permitted Groups] オプションは、[Permitted Group]、[Permitted Group SID(s)]、および [Include Nested Group] で機能します。

Multi Domain Permitted Groups が無効になっている場合、ユーザーは、ユーザー プロファイルが定義されているのと同じドメインまたはサブドメインに属している必要があります。そうでない場合、グループ チェックは失敗します。 Multi Domain Permitted Group オプションは、デフォルトで無効になっています。 [Include Nested Group] オプションは、マルチ ドメイン許可グループで機能します。 たとえば、server1 に group1 があり、同じサーバーの group1 内に group2 があり、ユーザーが異なる場合、Include Nested Groups と Multi Domain Permitted Groups の両方が有効になっていれば、それらのユーザーを認証できます。

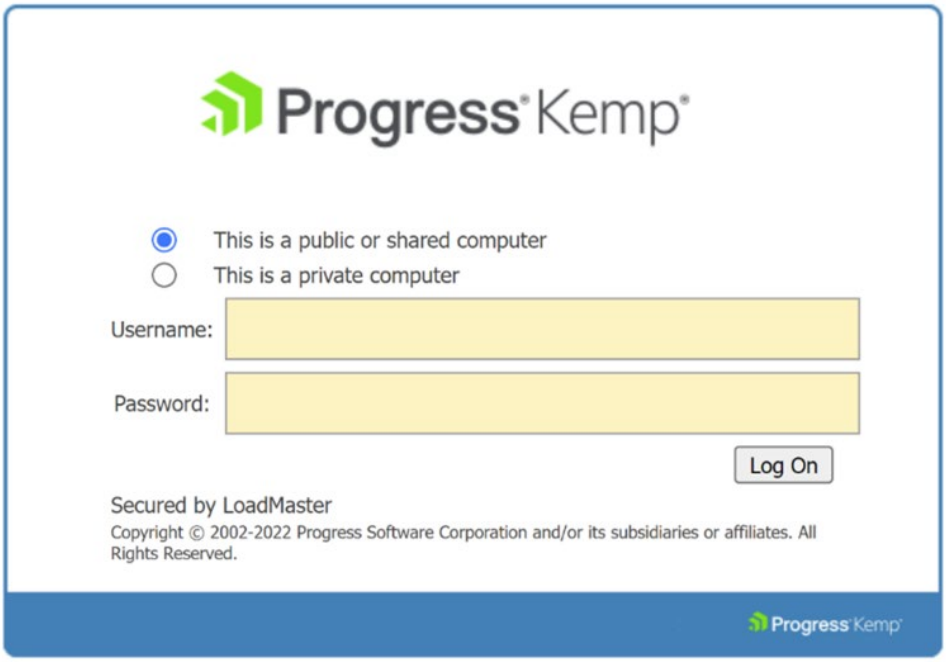
Steering Groups

ステアリング グループを使用すると、クライアント トラフィックを開始するユーザーの Active Directory (AD) グループ メンバーシップに基づいて、クライアント トラフィックを仮想サービス内の個々の実サーバーに誘導できます。 シナリオの例は、４つの実サーバーを持つ仮想サービスです。２つの実サーバーを Active Directory グループ 1 とのプライマリ アソシエーションを持つように構成し、２つの実サーバーを AD グループ 2 とのプライマリ アソシエーションを持つように構成することができます。ユーザーが仮想サービスにアクセスしようとすると、そのグループ メンバーシップが検証され、 リクエストを適切な実サーバーに誘導するために使用される情報。 グループ メンバーシップに基づいて選択された実サーバーが
使用できない場合、デフォルトの動作は、仮想サービスに割り当てられたスケジューリング方法にフォールバックすることです。 詳細については、ESP ステアリング グループのテクニカル ノートを参照してください。

基本認証または SAML 認証を使用している場合、ステアリング グループは使用できません。
[Permitted Group] フィールドと [Steering Group] フィールドの両方に同じグループ名を入力しないでください。 これにより、競合が発生します。 ステアリング グループを指定すると、許可されたグループのように動作すると見なされるため、[Permitted Group] フィールドと [Steering Group] フィールドの両方に同じグループを入力する必要はありません。

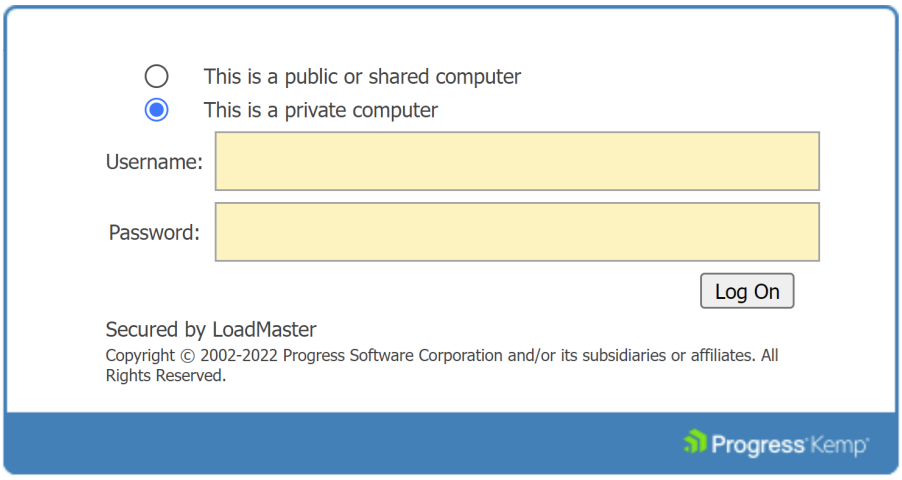
SSO Image Set

このオプションは、フォーム ベースがクライアント認証モードとして選択されている場合にのみ使用できます。 ユーザー名とパスワードの収集に使用するフォームを選択できます。 Exchange、Blank、および Dual Factor Authentication の ３つのフォーム オプションがあります。 フォームとエラー メッセージを他の言語で表示するオプションもあります。



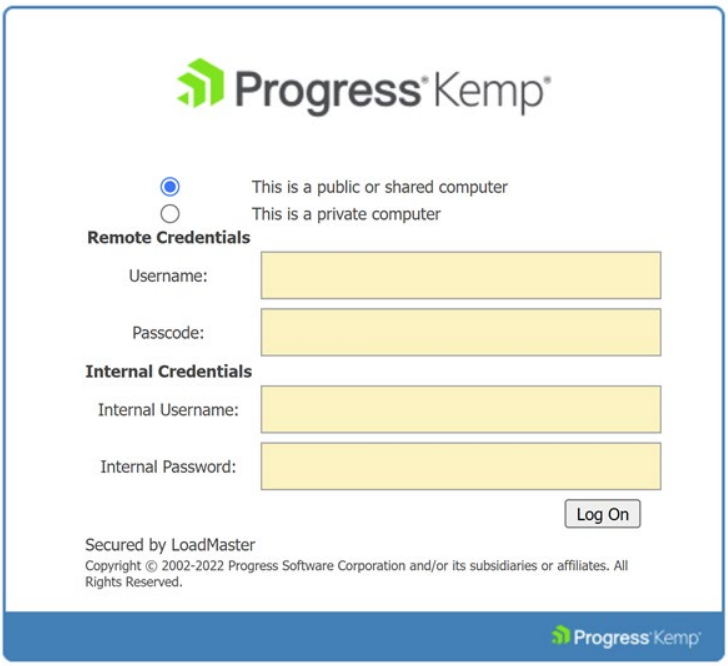
交換フォームにはケンプのロゴが含まれています。

- 空白のフォーム



空白のフォームには、大きなケンプのロゴは含まれていません。

- 二重要素認証



二重要素認証フォームには 4 つのフィールドが含まれます。2 つはリモート資格情報用で、2 つは内部資格情報用です。

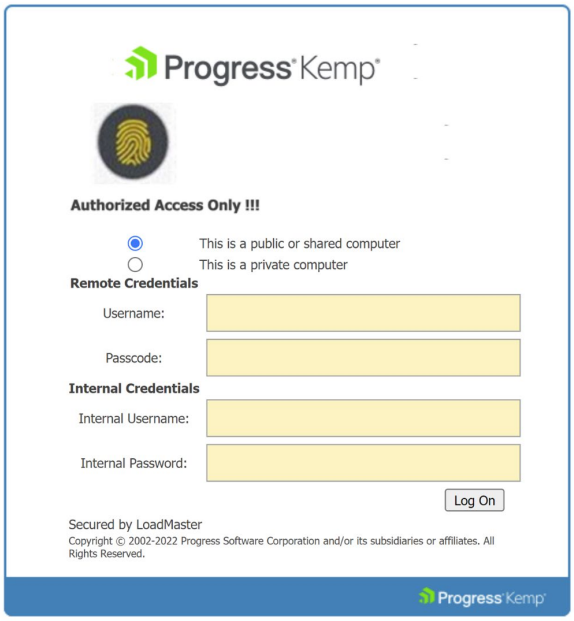
Remote Credentials は、ユーザーが Active Directory サーバーなどのドメイン サーバーに対して認証できるようにする前に、RADIUS などのリモート認証サーバーに対して認証するために使用される資格情報です。

Internal Credentials は、Active Directory サーバーなどの内部ドメイン サーバーに対する認証に使用される資格情報です。

関連する SSO ドメインの認証プロトコルが RADIUS および LDAP に設定されている場合、SSO イメージ セットは Dual Factor Authentication に設定する必要があります。

SSO Greeting Message

このオプションは、Form Based が Client Authentication Mode として選択されている場合にのみ使用できます。 ログインフォームは、テキストを追加してさらにカスタマイズできます。 フォームに表示するテキストを [SSO Greeting Message] フィールドに入力し、[Set SSO Greeting Message] をクリックします。 メッセージには最大 255 文字を使用できます。



SSO Greeting Message フィールドは HTML コードを受け入れるため、必要に応じて画像を挿入できます。

サポートされていない文字がいくつかあります。 これらは、グラーブ アクセント文字 (` ) と一重引用符 (') です。 SSO グリーティング メッセージでアクサン グラーブ文字が使用されている場合、その文字は出力に表示されません。たとえば、a`b`c は abc になります。 一重引用符を使用すると、ユーザーはログインできなくなります。

Logoff String

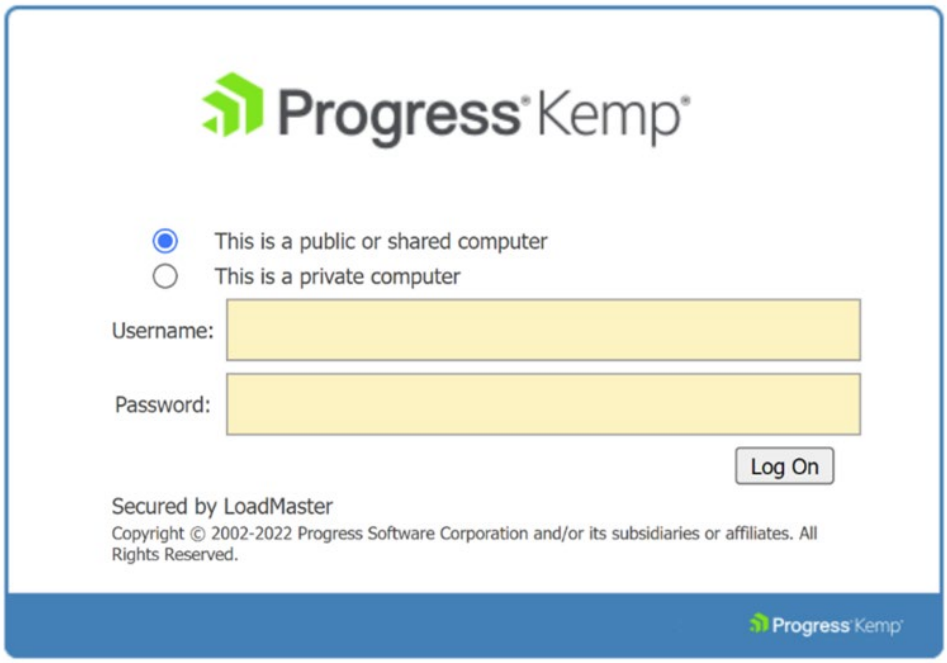
このオプションは、クライアント認証モードとしてフォーム ベースまたは SAML が選択されている場合にのみ使用できます。 通常、このフィールドは空白のままにしておく必要があります。 OWA 仮想サービスの場合、ログオフ文字列を /owa/logoff.owa に設定するか、カスタマイズされた環境では、変更したログオフ文字列をこのテキスト ボックスに指定する必要があります。 スペース区切りのリストを使用して、複数のログオフ文字列を入力できます。 このフィールドには最大 255 文字まで入力できます。

照合する URL に、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。 したがって、LoadMaster はユーザーをログオフしません。

Additional Authentication Header

このオプションは、クライアント認証モードとして SAML が選択されている場合にのみ使用できます。 HTTP ヘッダーの名前を指定します。 このヘッダーは、ロードマスターからリアル サーバーへの HTTP 要求に追加され、その値は認証済みセッションのユーザー ID に設定されます。 このフィールドには最大 255 文字まで入力できます。

Display Public/Private Option



このチェック ボックスを有効にすると、ESP ログイン ページにパブリック/プライベート オプションが表示されます。 ユーザーがログイン フォームで選択したオプションに基づいて、セッション タイムアウト値は、[Manage SSO Domain] 画面でパブリックまたはプライベートに指定された値に設定されます。 ユーザーがプライベート オプションを選択すると、ユーザー名がそのセッション用に保存されます。 これらのフィールドの詳細については、「Manage SSO Domain」セクションを参照してください。

Disable Password Form

このオプションを有効にすると、ログイン ページからパスワード フィールドが削除されます。 これは、RSA SecurID 認証を単一の方法で使用する場合など、パスワードの検証が必要ない場合に必要になることがあります。 デフォルトでは、このオプションは無効になっています。

Enable Captcha

ログイン ページで CAPTCHA 検証を許可するには、このチェック ボックスをオンにします。

LoadMaster は CAPTCHA v2 のみをサポートします。 [Enable Captcha] チェック ボックスを表示するには、[Client Authenticate Mode] を [Form Based] に設定する必要があります。

すべての CAPTCHA パラメータは、使用する前に設定する必要があります。 これが機能するには、LoadMaster とクライアント マシンの両方が Google にアクセスできる必要があります。

CAPTCHA が正しく回答されるまで、ログイン フォームの送信ボタンは無効になります。 ユーザーが CAPTCHA に回答してから 2 分以内にフォームを送信しない場合、CAPTCHA はタイムアウトになり (Google が指定したタイムアウト)、ユーザーは新しい CAPTCHA を検証する必要があります (新しい CAPTCHA が検証されるまで、送信ボタンは無効になります)。

Captcha Public Key

CAPTCHA サービスにサインアップしたときに公開鍵として提供された鍵。

Captcha Private Key

CAPTCHA サービスにサインアップしたときに秘密鍵として提供された鍵。

Captcha Access URL

CAPTCHA チャレンジを提供するサービスの URL。

通常: www.google.com/recaptcha/api.js

この URL を https で始めないでください。

現在、CAPTCHA V2 のみがサポートされています。

CAPTCHA Verification URL

CAPTCHA チャレンジへの応答を検証するサービスの URL。

通常: www.google.com/recaptcha/api/siteverify

この URL を https で始めないでください。

現在、CAPTCHA V2 のみがサポートされています。

Use Session or Permanent Cookies

このフィールドでは、次の 3 つのオプションを選択できます。

- Session Cookies Only: これはデフォルトで最も安全なオプションです。
- Permanent Cookies only on Private Computers: 個人のコンピューターでのみ永続的な

Cookie を送信します。

- Permanent Cookies Always: あらゆる状況で永続的な Cookie を送信します。

Permanent Cookies Only は Internet Explorer (IE) でのみ機能し、IE はサード パーティの Cookies を受け入れるように設定する必要があり、サイトを信頼済みサイトに追加する必要があります。 Permanent Cookies の有効期限は SSO の変更]画面の [Session Timeout] フィールドを構成することで設定できます。 最大値は 7 日 (604800 秒) です。

ログイン時に LoadMaster がユーザーのブラウザにセッション Cookie を送信するか、永久 Cookie を送信するかを指定します。

パーマネント Cookie は、SharePoint などの複数のアプリケーションにまたがるセッションを持つサービスでシングル サインオンを使用する場合にのみ使用してください。

Cookie SameSite Processing

このオプションを使用すると、LoadMaster Edge Security Pack が使用する Cookie に SameSite 属性を明示的に指定できます。 これは、ブラウザがサイト間で Cookie を使用する方法、特にファースト パーティとサード パーティのサイト間で異なる動作に影響を与えます。 (現在のサイトのドメイン、つまりブラウザのアドレス バーに表示されるものと一致する Cookie は、ファーストパーティ Cookie と呼ばれます。現在のサイト以外のドメインからの Cookie は、サードパーティ Cookie と呼ばれます。)

このフィールドで選択できるオプションは次のとおりです。

- SameSite option not added: このオプションの可用性は、グローバル レベルの構成、つまりデフォルトの ESP Cookie SameSite Processing に依存します。 SameSite Option Not Added 以外のオプションが Default ESP Cookie SameSite Processing フィールド ([System Configuration] > [Miscellaneous Options] > [L7 Configuration] ページ) に設定されている場合、SameSite Option Not Added オプションのみが VS のドロップダウン リストに表示されます。
- SameSite=None: Cookie データをサードパーティ/外部サイト (広告、埋め込みコンテンツなど) と共有できることを示します。
- SameSite=LAX: Cookie がファースト パーティ Cookie として使用される可能性があることを示しますが、ユーザーがクリックしたリンクを介して外部サイトからサイトにアクセ

スするときにも使用される可能性があります。

- SameSite=Strict: これは lax のサブセットであり、Cookie をファースト パーティ コンテキストでのみ使用できるようにし、外部サイトからの着信リンクを介してアクセスする場合はその使用を除外します。
- System Default: デフォルトでは、このオプションが選択されており、VS はグローバル レベルの設定を使用します。

LoadMaster で新しい仮想サービスが作成され、ESP でフォームベースが有効になっている場合、Cookie SameSite Processing オプションは常にシステム デフォルトに設定されます。この場合、Virtual Service は LoadMaster で構成されたデフォルトのグローバル設定を使用します。 ユーザーが仮想サービスの構成済みシステム デフォルト設定を他のオプションに変更すると、選択した仮想サービス オプションの構成がグローバル SameSite 構成をオーバーライドします。

User Password Change URL

これは、クライアント側のフォームベース認証と LDAP を使用する場合に関連します。 ユーザーがパスワードの変更に使用できる URL を指定します。

例えば

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

ユーザーのパスワードの有効期限が切れている場合、またはパスワードをリセットする必要がある場合は、この URL とユーザー パスワードの変更ダイアログ メッセージがログイン フォームに表示されます。 この URL は、ESP Pre Authorization Excluded Directories フィールドに入力する必要があります。これは、事前認証をバイパスするために必要です。 この期限切れパスワード機能を Exchange 2010 環境で使用する場合:

- 事前承認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 サーバーのサブパスです。
- パスワードを変更する場合、ユーザーはパスワードの変更ウィンドウの [domain¥user name] フィールドでユーザー プリンシパル名 (UPN) (例: joebloggs@example.com) を使用できません。Exchange 2010 SP1 RU3 以降がクライアント アクセス サーバーに展開されている場合を除きます。

詳細については、次の Microsoft TechNet 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

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。 ユーザー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。 このフィールドでは特殊文字は使用できません。

User Password Expiry Warning

デフォルトでは、SSO ユーザーには、パスワードの変更が必要になるまでの日数が通知されます。 このオプションを無効にすると、パスワードの有効期限通知はログイン フォームに表示されません。
パスワードの有効期限が切れる前に警告を表示する日数を指定できます。 このフィールドのデフォルト値は 15 日です。 このフィールドは、クライアント認証モードがフォーム ベースに設定され、ユーザー パスワード変更 URL が設定されている場合にのみ表示されます。 警告テキストの言語は、選択した SSO イメージ セットに基づいています (英語、フランス語、またはポルトガル語)。

Verify Bearer Header

着信クライアント要求の Authorizations ヘッダーに含まれる JSON Web トークン (JWT) の信頼性を検証するには、このチェック ボックスをオンにします。 トークンの署名の有効性を確認するか (証明書が必要)、トークン内の特定のテキストを確認することで、信頼性を確認できます。 または両方。

Verify Bearer Header フィールド (および以下に詳述する 2 つのフィールド) は、Client Authentication Mode が Delegate to Server に設定されている場合にのみ使用できます。

Bearer Header Validation Certificate

このオプションは、Verify Bearer Header チェックボックスが選択されている場合にのみ表示されます。 Bearer Header Validation Certificate ドロップダウン リストから関連する証明書の名前を指定します (Certificates & Security > SSL に移動して、これを最初に LoadMaster にアップロードする必要があります。
Certificates > Import Certificate) には、ベアラー ヘッダー トークン署名の信頼性を検証するために使用される公開キーが含まれています。 署名の検証を実行しない場合は、証明書を [None] に設定できます。

Bearer Header Validation Text

このオプションは、Verify Bearer Header チェックボックスが選択されている場合にのみ表示されます。 必要に応じて、最大 5 つのカンマ区切りの文字列を入力して、トークンの Audience Claim

Field (aud) と照合できます。 指定した場合、少なくとも 1 つの文字列が Audience Claim Field の内容と一致する必要があります。一致しない場合、トークンは拒否されます。

Server Authentication Mode

LoadMaster がリアル サーバーによって認証される方法を指定します。 次の種類のメソッドを使用できます。

- None: クライアント認証は必要ありません
- Basic Authentication: 標準の基本認証が使用されます
- KCD: KCD 認証を使用
- Server Token: SAML 応答の受信と検証時に、LoadMaster は長期間有効なトークンを要求します。 LoadMaster は、指定されたトークンを使用してリダイレクト URL を作成します。

SAML がクライアント認証モードとして選択されている場合、サーバー認証モードとしてサーバー トークンのみを選択できます。

- Form Based: フォーム ベース認証を選択すると、[Form Authentication Path] フィールドが表示されます。

フォーム ベースがクライアント認証モードとして選択されている場合、サーバー認証モードとしてフォーム ベースのみを選択できます。

- [From Authentication Path] フィールドに値を入力して [Set Path] ボタンをクリックすると、[Form POST Format] フィールドと [Post Format Username Only] フィールドが表示されます。 クライアント側のフォームベース認証からのユーザー名とパスワードは、POST 本文を作成するためにフォーム POST 形式に挿入されます。
- この機能は主に Microsoft Exchange 展開で使用され、Exchange 2013 および 2016 でのみテストされています。したがって、次の文字列を Exchange 2013/2016 用に明示的に構成する必要はありません。 これらはでデフォルトで使用されます。
  - 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、フォーム認証パスが設定されている場合にのみ表示さ

れます。

デプロイメントが Exchange でない場合、Progress Kemp は、実サーバーとの必要な対話に基づいて設定を評価し、その後適切に設定することをお勧めします。

POST Format Username Only

このオプションを有効にすると、サーバー側のフォーム ベースの認証 POST 要求でユーザー名のみ (ドメイン部分なし) が送信されます。

[Client Authentication Mode] として [Delegate to Server] が選択されている場合、[Server Authentication Mode] として [None] が自動的に選択されます。 同様に、基本認証がクライアント認証モードとして選択されている場合、基本認証がサーバー認証モードとして自動的に選択されます。特定のクライアント認証モード プロトコルを選択する場合、互換性のあるサーバー認証モード プロトコルを理解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	KCD
	Form Based
	None
NTLM	KCD
	None
Client Certificate	KCD
SAML	KCD
	None
	Server Token

Server Side configuration

このオプションは、サーバー認証モードの値が KCD に設定されている場合にのみ表示されます。

サーバー側構成の SSO ドメインを選択します。 構成タイプがアウトバウンド構成に設定されている SSO ドメインのみがここに表示されます。

Token Server FQDN

このオプションは、サーバー認証モードの値がサーバー トークンに設定されている場合にのみ表示されます。

トークン サーバーの FQDN を設定します。 設定すると、LoadMaster はサインオン時に特定の FQDN でトークン サーバーに接続し、そのトークン サーバーから永続的なアクセス トークンを取得します。 このパラメーターが設定されていない場合、LoadMaster は実サーバーからトークンを取得します (以前のリリースと同様)。

3.10.1 SMTP 仮想サービスと ESP

SMTP 仮想サービス (ポートとして 25 を使用) を作成する場合、[Enable ESP] チェックボックスをオンにすると、ESP 機能が使用可能になりますが、オプションのセットは少なくなります。

Enable ESP

[Enable ESP] チェックボックスを選択または選択解除して、ESP 機能セットを有効または無効にします。

Connection Logging

[Connection Logging] チェックボックスを選択または選択解除することで、接続のログを有効または無効にできます。

Permitted Domains

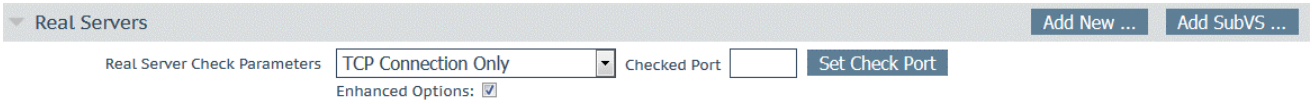
この仮想サービスによる受信が許可されているすべての許可ドメインをここで指定する必要があります。 たとえば、仮想サービスが john@kemp.com からの SMTP トラフィックを受信するようにするには、このフィールドに kemp.com ドメインを指定する必要があります。

3.11 サブ仮想サービス

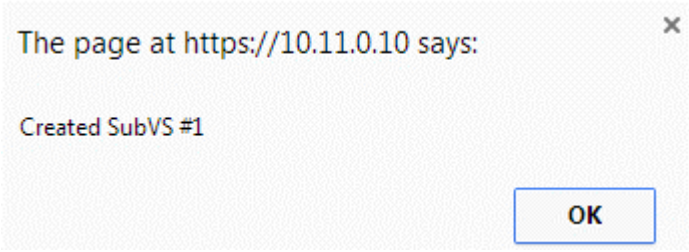
仮想サービス内から、 1 つ以上の「サブ仮想サービス」(SubVS) を作成できます。 SubVS は「Parent」仮想サービスにリンクされ、その IP アドレスを使用します。 サブ VS は、親仮想サービスに対して、および相互に異なる設定 (ヘルス チェック メソッドやコンテンツ ルールなど) を持っ

ている場合があります。 これにより、すべて同じ IP アドレスを使用して、関連する仮想サービスをグループ化できます。 これは、通常、多数の仮想サービスで構成される Exchange や Lync などの特定の構成に役立ちます。

仮想サービス権限を持つユーザーは、SubVS を追加できます。
実サーバー権限を持つユーザーは、SubVS を追加できません。

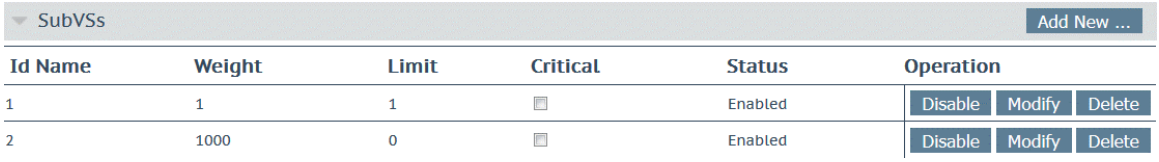


SubVS を作成するには、仮想サービスの構成画面で、[Real Server] セクションを展開し、[Add SubVS] ボタンをクリックします。



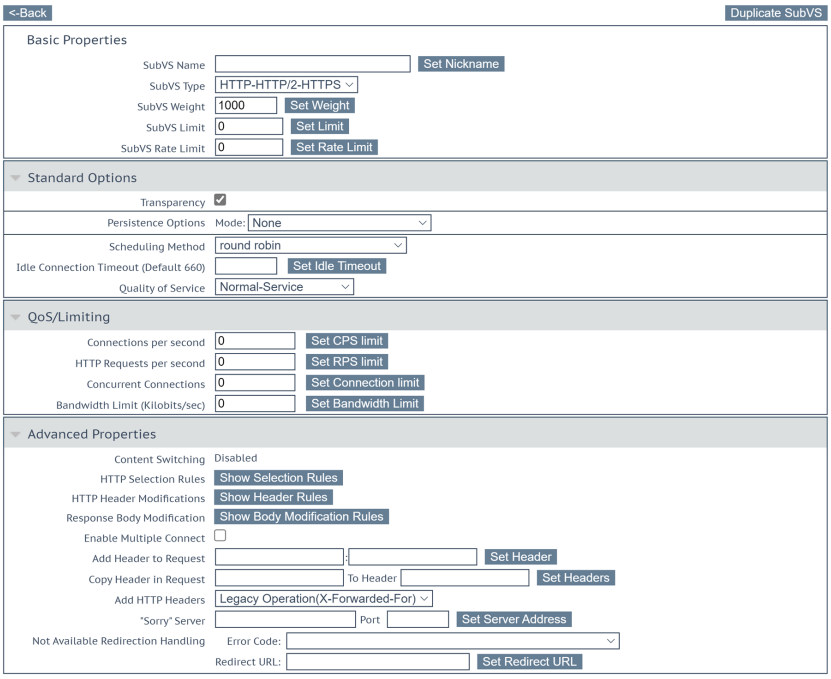
SubVS が作成されたことを示すメッセージが表示されます。

実サーバーと SubVS を同じ仮想サービスに関連付けることはできません。 ただし、実サーバーを SubVS に関連付けることはできます。



SubVS が作成されると、Virtual Services 設定画面の Real Servers セクションが SubVSs セクションに置き換えられます。
仮想サービスのすべての SubVS がここに一覧表示されます。 [Critical] チェック ボックスを有効にすると、仮想サービスが利用可能と見なされるために SubVS が必要であることを示すことができます。重要でないサブ VS が停止している場合、仮想サービスは稼働していると報告され、警告がログに記録されます。重要な SubVS がダウンしている場合、重要なログが生成され、仮想サービスはダウンとしてマークされます。電子メール オプションが設定されている場合、関連する受信者に電子メ

ールが送信されます。電子メール オプションの詳細については、「Email Options」セクションを参照してください。いずれの場合も、仮想サービスがダウンしていると見なされ、仮想サービスにソーリー サーバーまたはエラー メッセージが設定されている場合、これらが使用されます。 SubVS を変更するには、関連する [Modify] ボタンをクリックします。 SubVS の設定画面が表示されます。これには、通常の仮想サービスで使用できる構成オプションのサブセットが含まれています。



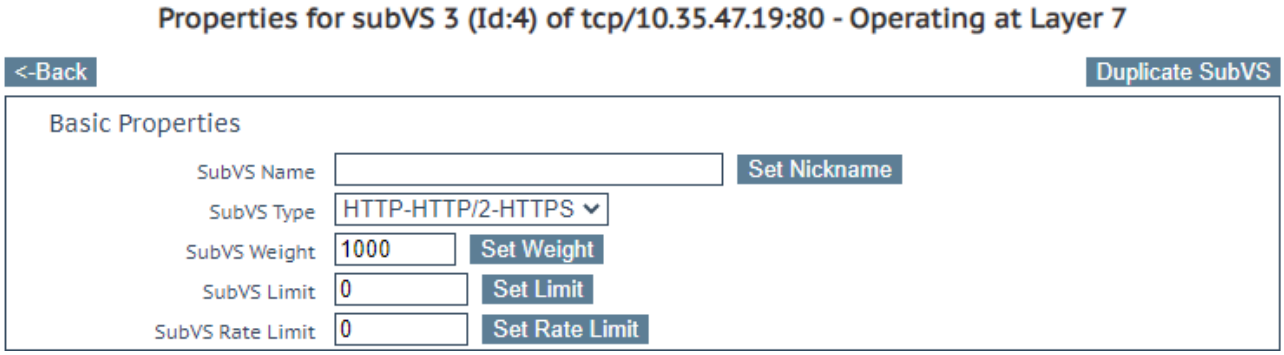
LoadMaster ファームウェア バージョン 7.2.52 以降では、再暗号化 SNI ホスト名を SubVS レベルで設定できます。 これが SubVS で設定されている場合、これは親仮想サービスの値および/または受信した SNI 値を上書きします。

SubVS は、メインの [Virtual Services] ビュー内から関連する [Modify] ボタンをクリックして変更することもできます。 SubVS を含む仮想サービスは、仮想 IP アドレス セクション内で異なる色で表示され、SubVS は実サーバー セクションに一覧表示されます。 SubVS の詳細は、「Parent」の仮想サービスをクリックしてビューを展開し、SubVS を含めることで表示できます。

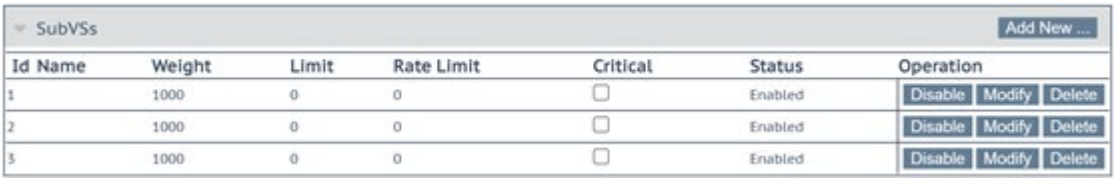
Duplicate SubVS

[Duplicate SubVS] をクリックして、同じ仮想サービス内にサブ VS の複製を作成できます。 すべての SubVS 構成設定は、複製された SubVS にコピーされます。

Duplicate SubVS をクリックすると、「SubVS duplicated, SubVS Id:4, RS Id: 3」のようなポップアップ メッセージが表示されます。 [OK] をクリックしてポップアップを閉じます。 SubVS には、仮想サービス ID (SubVS Id) と実サーバー ID (RS Id) の両方があります。



メッセージ内の SubVS Id は、仮想サービス ID を参照しています。 この ID は、関連する SubVS の SubVS 変更画面の上部にある見出しに表示されます。



RS Id は「Real Server」ID を参照します。 SubVS の場合、この実サーバー ID は、仮想サービス変更画面の SubVS セクションで SubVS を識別するために使用されます。

SubVS には、SubVS 変更画面の [Basic Properties] セクションに 2 つの追加制限フィールドがあります。

- SubVS 制限: この SubVS がメインの仮想サービスからローテーションから除外される前に、この SubVS に送信できる接続の最大数。 上限は 1000000 です。
- SubVS レート制限: この SubVS がメインの仮想サービスからローテーションから除外される前に、この SubVS に送信できる 1 秒あたりの最大接続数。 上限は 1000000 です。

可能な制限 (グローバル、クライアント、仮想サービス、およびサブ VS) のうち、最初に到達した最も低いものが適用されます。 グローバル制限はすべての仮想サービスに対するものであり、仮想サービス制限は複数のクライアントを持つ現在の仮想サービスに対するものであり、クライアント制限は構成に応じてすべてのクライアント、複数のクライアント、または単一のクライアントに適用できることに注意してください。 使用中の仮想サービスに関係なく、クライアント制限が適用されます。 SubVS を含む仮想サービスを削除する場合は、メイン サービスを削除する前に、まず SubVS を削除する必要があります。 SubVS は、その親仮想サービスとは異なる ESP 構成を持つ場合がありますが、親仮想サービスと SubVS ESP オプションが競合しないように注意する必要があります。

3.12 表示/変更 (リモート ターミナル サービス)

仮想サービスのプロパティには、汎用タイプが含まれ、リモート ターミナル固有のオプションも提供されます。

Persistence

ターミナル サーバーがセッション ディレクトリをサポートしている場合、LoadMaster はセッション ディレクトリによって提供される Routing を使用して、接続先の正しいホストを決定します。 LoadMaster の持続性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 ディレクトリの機能です。

これを機能させるには、セッション ディレクトリ構成のスイッチ「IP address redirect」を選択しないでください。

持続性の観点から、LoadMaster でのセッション ディレクトリの使用はオプションです。 クライアントが最初のリクエストでユーザー名とパスワードのフィールドを事前入力した場合、この値は LoadMaster に保存されます。 これらのフィールドが再接続時に入力されている限り、LoadMaster

は名前を検索し、元の接続と同じサーバーに再接続します。 持続タイムアウトは、情報が LoadMaster に保持される時間を制限するために使用されます。ターミナル サービス モードまたはソース IP モードを使用している場合、これら 2 つのモードのどちらも成功しない場合は persistence のためにソース IP アドレスが使用されます。

Service Check for the Virtual Service

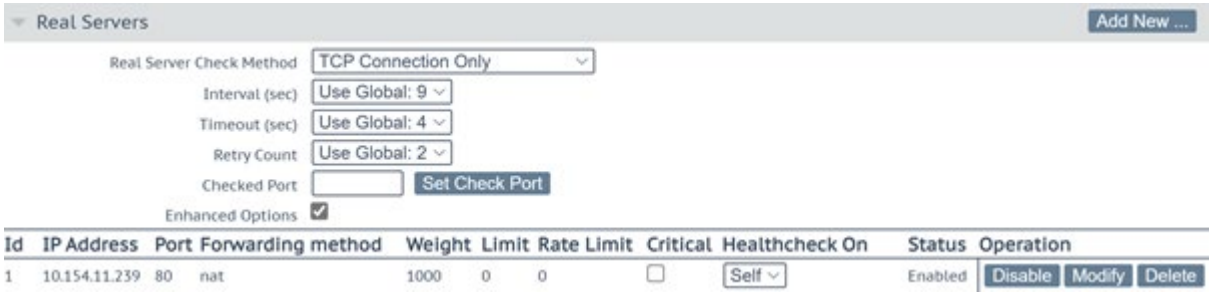
利用できるオプションは 3 つだけです。 ICMP、TCP、および RDP。 リモート ターミナル プロトコル (RDP) は、サービス ポート (ポート 3389) で実サーバーへの TCP 接続を開きます。 LoadMaster は a1110 コード (接続要求) をサーバーに送信します。 サーバーが a1101 コード (Connection request) を送信すると、LoadMaster は接続を閉じ、サーバーをアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しなかった場合、または別のステータス コードで応答した場合、サーバーは停止していると見なされます。

3.13 Real Server

このセクションでは、Real Server を作成し、仮想サービスに割り当てられている実サーバーを一覧表示できます。 Real Server のプロパティが要約されており、Real Server を追加または削除したり、実サーバーのプロパティを変更したりすることもできます。 コンテンツ スイッチングが有効になっている場合は、Real Server にルールを追加したり、実サーバーからルールを削除したりすることもできます (「ルールの追加」を参照)。

Real Server Check Method

これは、よく知られているサービスのヘルス チェックのリストと、TCP/UDP または ICMP の下位レベルのチェックを提供します。 サービス ヘルス チェックでは、選択したサービスの可用性について実サーバーがチェックされます。 TCP/UDP では、チェックは単に接続試行です。



以下の表は、Real Server の状態を確認するために使用できるオプションを示しています。 実サーバーのヘルス チェック ポートを指定することもできます。 ここで何も指定されていない場合は、デフ

ォルトで Real Server ポートになります。

HTTP/HTTPS、Generic、および STARTTLS プロトコルのサービス タイプが選択されている場合、次のヘルス チェック オプションを使用できます。

メソッド	アクション
ICMP Ping	ICMP ping が Real Server に送信されます
HTTP	HTTP チェックが有効になっています
HTTPS	HTTPS (SSL) チェックが有効になっています
TCP	基本的な TCP 接続がチェックされます
Mail	SMTP (Simple Mail Transfer Protocol) が使用されます。
NNTP	NNTP (Network News Transfer Protocol) が使用されます。
FTP	FTP (ファイル転送プロトコル) が使用されます。
Telnet	Telnet プロトコルが使用されます
POP3	POP3 (Post Office Protocol – メール クライアント プロトコル) が使用されます。
IMAP	IMAP (インターネット メッセージ アクセス プロトコル – メール クライアント プロトコル) が使用されます。
Name Service (DNS) Protocol	ネーム サーバー (DNS) プロトコルの値は、仮想サービス プロトコルが UDP に設定されている場合、[Real Server Check Method] ドロップダウンリストでのみ使用できます。 LoadMaster は、UDP ポート 53 を介してサーバー上の A レコードに対して nslookups を実行します。サーバーが DNS クエリに正常に応答すると、LoadMaster はそれをアクティブとしてマークします。 サーバーが構成された応答時間内に構成された回数応答しない場合、または A レコード要求への応答に失敗した場合、サーバーはダウンしていると見なされます。
Binary Data	送信する 16 進文字列を指定し、応答で確認する 16 進文字列を指定します
LDAP	ヘルスチェックに使用する LDAP エンドポイントを選択します。 LDAP ヘルス チェックでは、LDAP エンドポイントで指定された LDAP クレデンシャルとプロトコルが使用されます。 ヘルス チェックは、Real Server

	の IP アドレスとポートに対して実行されます。 LDAP ヘルス チェックは、ロードマスターが Real Server に接続し、指定されたユーザー資格情報を検証することで構成されます。 ヘルスチェックは次の 2 つのステップで実行されます。 ステップ 1: Real Server の指定されたポートが稼働しており、使用可能かどうかを確認します。 ステップ 2: LDAP で指定された資格情報を使用して Real Server へのログインを試みます。 ステップ 1 とステップ 2 が true の場合、ヘルスチェックは合格です。 ステップ 1 またはステップ 2 が失敗した場合、ヘルスチェックは失敗します。 LDAP エンドポイントの詳細については、「LDAP Configuration」セクションを参照してください。
None	チェックは実行されません

リモート ターミナル サービス タイプを選択すると、次のヘルス チェック オプションを使用できます。

メソッド	アクション
ICMP Ping	ICMP ping が Real Server に送信されます
TCP	基本的な TCP 接続がチェックされます
Remote Terminal Protocol	RDP ルーティング トークンが Real Server に渡されます。 このヘルスチェックは、ネットワークレベルの認証をサポートしています。
None	チェックは実行されません

UDP 仮想サービスの場合、ICMP Ping およびネーム サービス (DNS) プロトコル オプションのみを使用できます。

Check Parameters

LoadMaster ファームウェア バージョン 7.2.52 では、各仮想サービスまたは SubVs でチェック間隔、タイムアウト、および再試行回数の設定を構成できます。 以前は、これらは単なるグローバル設定でした。 [Rule & Checking] > [Check Parameters] でグローバル設定を構成できます。 グローバル設定は、デフォルトですべての仮想サービスに使用されます。

Interval (seconds): このフィールドは、連続するヘルス チェックの試行の間に経過する秒数を指定し、「ヘルス チェック サイクル」の長さを定義します。 グローバル間隔を上書きするには、ドロ

ップダウン リストから他の値を選択できます。 Timeout または Retry Count パラメータのいずれかがグローバル設定以外の値に設定されている場合、グローバル オプションは選択できません。

Timeout (seconds): これは、接続が確立され、ヘルスチェックへの応答が受信されるまでに許容される最大待機時間です。 タイムアウトになる前に応答が受信されない場合、再試行回数に達していない限り、接続が再試行されます。 ヘルス チェックに対する HTTP 応答が受信された場合、現在のヘルス チェック サイクルでは再試行は行われません。 グローバル タイムアウト値を上書きするには、ドロップダウン リストから他の値を選択できます。

Retry Count: これは、応答を受信する前に上記のタイムアウトに達した場合にヘルスチェックを再試行する回数を指定します。 グローバルな再試行回数の値を上書きするには、ドロップダウン リストから他の値を選択できます。 ヘルスチェックに対して応答があった場合、再試行回数は適用されません。 たとえば、200 または 404 応答を受信した場合、現在のサイクルでは再試行は行われません。

特定の仮想サービスに対してこれらの設定を構成するには、仮想サービスまたは SubVS の変更画面の [Real Server] セクションを展開します。 関連するフィールドを表示するには、Real Server Check Method を選択する必要があります。 これらの設定を構成して、グローバル値を使用するか、指定された範囲内で特定の値を設定するか、デフォルト値にリセットすることができます。 Parent 仮想サービスに対してこれらの設定を構成してから、その仮想サービス内にサブ VS を作成すると、グローバル値を使用するようにチェック値がリセットされます。

Enhanced Options

[Enhanced Options] チェック ボックスを有効にすると、追加のヘルス チェック オプションが提供されます。VS が稼働していると見なされるために必要な RS の最小数。 [Enhanced Options] チェック ボックスが無効 (デフォルト) の場合、少なくとも 1 つの Real Server が使用可能な場合、仮想サービスは使用可能と見なされます。 [Enhanced Options] チェック ボックスが有効になっている場合、仮想サービスが利用可能であると見なすために利用可能である必要がある実サーバーの最小数を指定できます。

VS が稼働していると見なされるために必要な RS の最小数

このオプションは、[Enhanced Options] チェック ボックスが有効になっており、実サーバーが複数ある場合にのみ表示されます。

仮想サービスが稼動していると見なされるために使用可能である必要がある実サーバーの最小数を選択

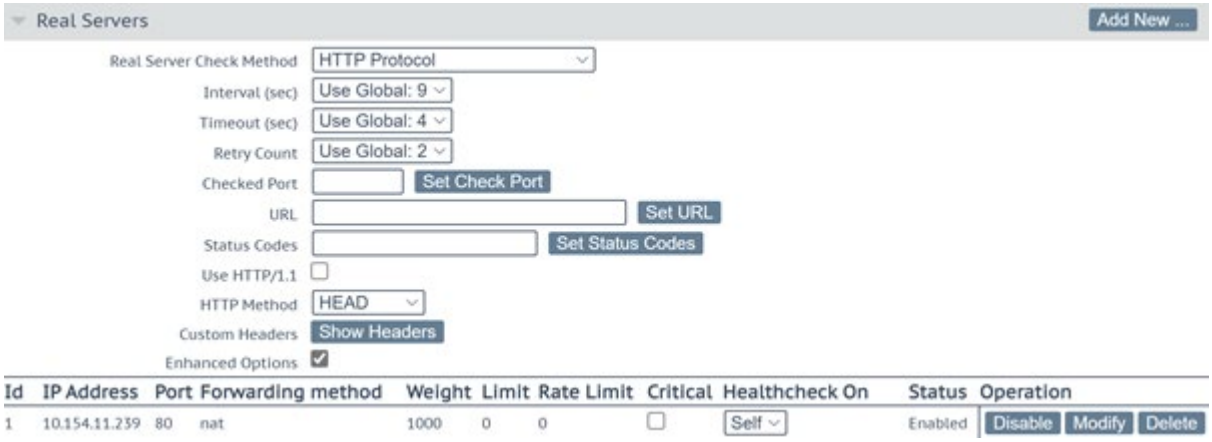
します。 使用可能な実サーバーが最小数よりも少ない場合、重大なログが生成されます。 一部の実サーバーがダウンしているが、指定された最小数に達していない場合、警告がログに記録されます。 電子メール オプションが設定されている場合、関連する受信者に電子メールが送信されます。 電子メール オプションの詳細については、「Email Options」セクションを参照してください。

クリティカルとしてマークされた実サーバーが利用できなくなると、システムは仮想サービスをダウンとしてマークすることに注意してください。たとえ拡張オプションが有効になっていて、指定された最小数よりも多くの実サーバーがまだ利用可能であった場合でも。

いずれの場合も、仮想サービスがダウンしていると見なされ、仮想サービスにソーリー サーバーまたはエラー メッセージが設定されている場合、これらが使用されます。 最小数が実サーバーの総数に設定されている場合、実サーバーの 1つが削除されると、最小数は自動的に 1減ります。
SubVS でコンテンツ ルールを使用する場合、必要な実サーバーの最小数の意味は少し異なります。ルールは利用可能であると言われ、そのルールが割り当てられた利用可能な実サーバーの数が制限を超えている場合にのみ一致します。 利用可能な実サーバーの数がこの制限を下回る場合、ルールは一致しません。SubVS はダウンとしてマークされ、これは適切にログに記録されます。 SubVS 上の実サーバーがクリティカルとしてマークされている場合、その実サーバーがダウンしている場合、SubVS はダウンとしてマークされます。 ただし、そのサブ VS がクリティカルとしてマークされていない限り、親仮想サービスはダウンとマークされません。

3.13.1 HTTP または HTTPS プロトコルのヘルス チェック

HTTP プロトコルまたは HTTPS プロトコルのいずれかのオプションを選択すると、以下で説明するように、いくつかの追加オプションを利用できます。



データの送信オプションは、POST HTTP メソッドが選択されている場合にのみ表示されます。

Reply 200 Pattern オプションは、POST または GET HTTP メソッドが選択されている場合にのみ表示されます。

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、マシンが使用可能かどうかを判断しようとします。 ここで別の URL を指定できます。

Status Codes

ヘルス チェック ステータス コードを設定して、デフォルトの機能を上書きできます。 ステータス コードが設定されていない場合、次の HTTP ステータス コードは Up と見なされます。

- 200-299
- 301
- 302
- 401

さらに、2xx ステータス コードは、構成されている場合、応答データのパターン マッチングの対象となります。 他のコードは、パターン マッチングが設定されていても、パターン マッチングなしでアップと見なされます。

カスタム ヘルス チェック コードが設定されている場合:

- チェック コードは、それぞれ 300 ～ 599 の数字のリストに設定できます
- チェックコードの長さは最大 127 文字です。これは、32 個の有効なコードを意味します
- リスト内のすべてのコードは、稼働中のヘルス チェック ステータスを持っていると見なされます
- 設定されたコードはデフォルトの設定を上書きします

- 2xx コードは常にすべてのケースで有効であると見なされ、設定されている場合はパターン マッチングの対象となります
- チェック コードは、300 ～ 599 の範囲にある限り、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のユーザー コードのいずれでもかまいません。
  - 公式の HTTP ステータス コードのリストについては、https://en.wikipedia.org/wiki/List_of_HTTP_status_codes を参照してください。
  - 非公式コードのリストについては、https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#Unofficial_codes を参照してください。
- 10 進数を使用した Microsoft サブコードをサポートできますが、最上位のステータス コードによってのみサポートされます。
  - 10 進数を使用した Microsoft サブコードのリストについては、https://support.microsoft.com/en-us/kb/943891 を参照してください。
  - サブコードはステータス コード フィールドで設定できない場合があります。3 桁のコードを使用してください
  - サブコードは最上位コードによってグループ化されます

デフォルトでは、LoadMaster は HTTP/1.0 を使用します。 ただし、より効率的に動作する HTTP/1.1 を使用することもできます。 HTTP/1.1 を使用する場合、ヘルスチェックは単一の接続に多重化されます。 これは、1 つの接続でより多くのヘルス チェックがサーバーに送信されることを意味します。これは、接続の観点からより効率的です。つまり、複数の接続ではなく 1 つの接続のみが存在します。

最適化は、HTTP (HTTPS ではなく) 接続でのみ機能します。

HTTP/1.1 Host

このフィールドは、[Use HTTP/1.1] が選択されている場合にのみ表示されます。

HTTP/1.1 チェックを使用する場合、リアル サーバーは各リクエストでホスト名を指定する必要があります。 値が設定されていない場合、この値は仮想サービスの IP アドレスです。 HTTPS ヘルス チェックで SNI ホスト情報を送信するには、関連する仮想サービスの [Real Server] セクションで [Use HTTP/1.1] を有効にし、ホスト ヘッダーを指定してください。 これが設定されていない場

合、実サーバーの IP アドレスが使用されます。

HTTP Method

ヘルスチェック URL にアクセスするとき、システムは HEAD、GET、または POST メソッドのいずれかを使用できます。 LoadMaster ファームウェア バージョン 7.2.52 では、HTTP および HTTPS ヘルス チェック タイプの OPTIONS メソッドのサポートが追加されました。 これは、LoadMaster が送信した HTTP (または HTTPS) OPTIONS リクエストに応答して LoadMaster が 200 OK を受信したときに、サーバーがマークアップされることを指定します。 OPTIONS HTTP メソッドは、許可された通信オプションの説明をサーバーに要求します。 サーバーからの 200 OK 応答には、追加のチェックを提供するために、オプションで特定のテキストを検索できる応答本文が含まれています。 レスポンスボディを検索するには、
OPTIONS HTTP メソッドを選択したときに表示される [Reply 200 Pattern] テキスト ボックスに検索テキストを指定します。 提供されたテキストが応答本文で見つかった場合、サーバーはマークアップされます。 それ以外の場合、サーバーはダウンとマークされます。

Post Data

このフィールドは、HTTP メソッドが POST に設定されている場合にのみ使用できます。 POST メソッドを使用する場合、最大 2047 文字の POST データをサーバーに渡すことができます。

Reply 200 Pattern

GET または POST メソッドを使用した場合、返された応答メッセージの内容を確認できます。この正規表現で指定された文字列が応答に含まれている場合、マシンは稼働していると判断されます。応答では、一致が実行される前にすべての HTML フォーマット情報が削除されます。応答データの最初の 4K のみを照合できます。 LoadMaster は、サーバーからの応答が 200 コードである場合にのみ、このフレーズをチェックします。返信がそれ以外の場合、そのページはフレーズをチェックせずにダウンとしてマークされます。ただし、応答がリダイレクト (コード 302) の場合、ページはダウンとしてマークされません。これは、LoadMaster がフレーズが存在しないと想定し、リダイレクトが役に立たなくなるため、サービスを停止できないためです。検索パターンの先頭にある感嘆符 (!) は、検索結果を否定します。たとえば、'fail' のパターンは、文字列 'fail' が応答に表示される場合に true を返します。一方、'!fail' のパターンは、応答に 'fail' が表示された場合に false を返します。文字列の指定には、正規表現と Perl 互換正規表現 (PCRE) の両方を使用できます。正規表現と PCRE の詳細については、コンテンツ ルール機能の説明を参照してください。

LoadMaster WUI の正規表現で引用符を使用する場合、制限があります。 詳細については、「Limitations of Using Regular Expressions in the LoadMaster WUI」セクションを参照してください。

Custom Headers

ここでは、ヘルスチェック要求ごとに送信される追加のヘッダー/フィールドを最大 4 つ指定できます。 [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。 最初のフィールドは、ヘルス チェック リクエストの一部となるカスタム ヘッダーのキーを定義する場所です。 2 番目のフィールドは、ヘルスチェック リクエストの一部として送信されるカスタム ヘッダーの値です。 情報を入力したら、[Set Header] ボタンをクリックします。 各ヘッダーは最大 20 文字、フィールドは最大 100 文字です。 ただし、4 つのヘッダー/フィールドの合計で許容される最大文字数は 256 です。

カスタム ヘッダー フィールドでは、次の特殊文字を使用できます。

; . ( ) / + = - _

ユーザーが HTTP/1.1 を指定した場合、ホスト フィールドは以前と同様にリアル サーバーに送信されます。 これは、追加のヘッダー セクションでホスト エントリを指定することによってオーバーライドできます。 User-Agent も同じ方法でオーバーライドできます。 実サーバーがアダプティブ スケジューリングを使用している場合、アダプティブ情報を取得するときに、ヘルス チェックで指定された追加のヘッダーも送信されます。 認証されたユーザーを使用してヘルスチェックを実行することができます: 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で Authorization ヘッダーを入力します。
Authorization フィールドは次のように構成されます。

- ユーザー名とパスワードは、文字列「username:password」に結合されます。
- 結果の文字列は、Base64 の RFC2045-MIME バリアントを使用してエンコードされます。ただし、76 文字/行に限定されません。
- 認証方法とスペース (「Basic」など) が、エンコードされた文字列の前に置かれます。

たとえば、ユーザー エージェントがユーザー名として 'Aladdin' を使用し、パスワードとして 'open sesame' を使用する場合、フィールドは次のように形成されます。

Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

HTTPS ヘルス チェックで SNI ホスト情報を送信するには、関連する仮想サービスの [Real Server] セクションで [HTTP/1.1 を使用] を有効にし、ホスト ヘッダーを指定してください。 これが設定されていない場合、実サーバーの IP アドレスが使用されます。

Rules

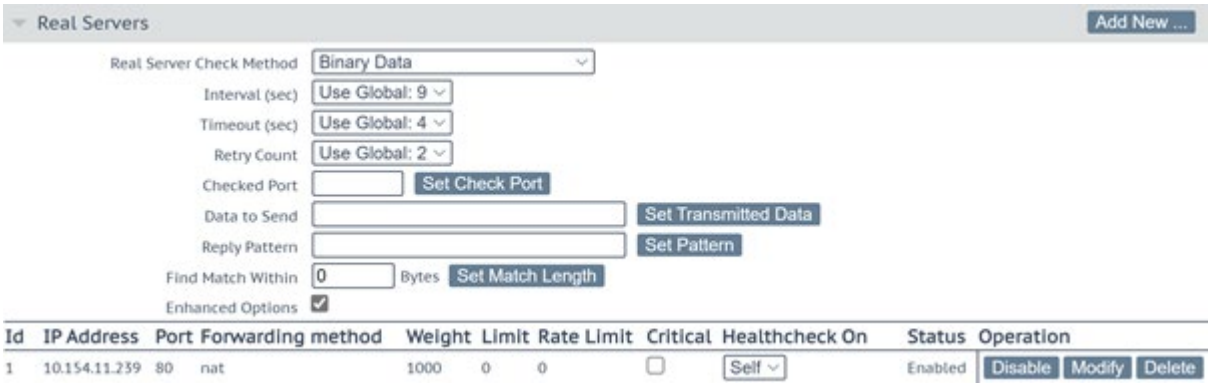
いずれかの実サーバーにコンテンツ スイッチング ルールが割り当てられている場合、[Real Server] セクションに [Rule] 列が表示されます。 各実サーバーに割り当てられたルールの数を示すボタン (ルールが割り当てられていない場合は [None] のボタン) が [ルール] 列に表示されます。

[Rule] 列内のボタンをクリックすると、[Manage Rule] 画面が開きます。

この画面から、Real Server に割り当てられたルールを追加または削除できます。

3.13.2 バイナリ データのヘルス チェック

バイナリ データがヘルス チェック方法として選択されている場合、以下で説明するように、他のいくつかのフィールドを使用できます。



Data to Send

Real Server 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、偶数の文字が含まれている必要があります。

Reply Pattern

Real Server から返される応答で検索される 16 進数の文字列を指定します。 LoadMaster が応答でこのパターンを検出すると、Real Server は稼働していると見なされます。 文字列が見つからない場合、Real Server は停止しているとマークされます。

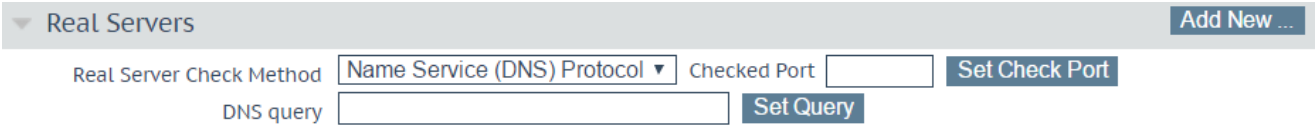
この 16 進文字列には、偶数の文字が含まれている必要があります。

Find Match Within

応答が返されると、LoadMaster は応答で応答パターンを検索します。 LoadMaster は、このフィールドで指定されたバイト数まで一致を検索します。 これを 0 に設定すると、検索が制限されないことを意味します。 一致するものが見つかるまで、Real Server からデータが読み取られます。 Real Server から最大 8 KB が読み取られます。 値を応答文字列の長さより短く設定すると、チェックは値が 0 に設定されているかのように動作します。つまり、すべてのパケット (最大 8 KB) が検索されます。

3.13.3 ネーム サーバー (DNS) プロトコルのヘルス チェック

Name Server (DNS) プロトコルのヘルス チェックは、UDP 仮想サービスを使用している場合にのみ使用できます。



Checked Port

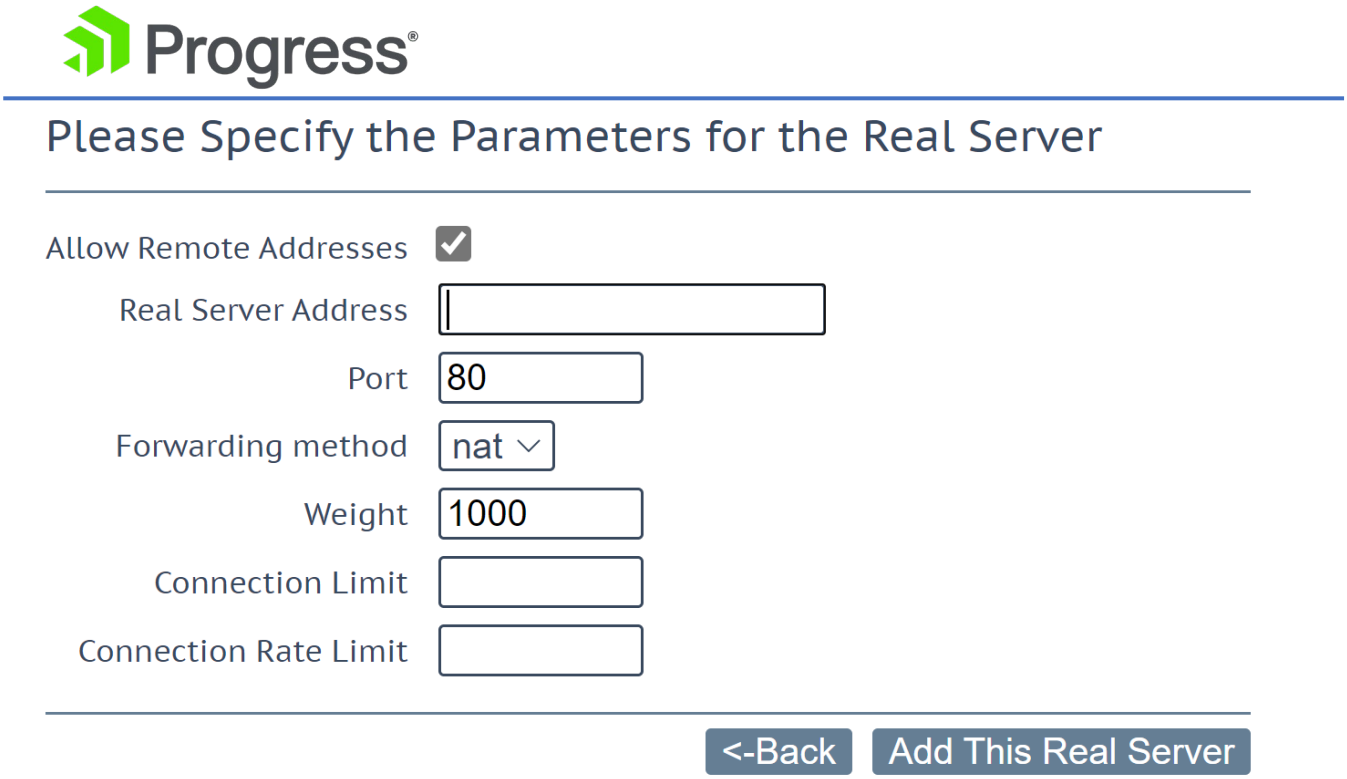
チェックするポート。 ポートが指定されていない場合、Real Server ポートが使用されます。

DNS query

ネームサーバーから要求す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。

3.13.4 Real Server を追加する

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



Allow Remote Addresses: デフォルトでは、ローカル ネットワーク上の Real server のみを仮想サービスに割り当てることができます。 このオプションを有効にすると、ローカル以外の Real Server を仮想サービスに割り当てることができます。 このオプションはデフォルトで有効になっています。

Allow Remote Addresses オプションを表示するには、Enable Non-Local Real Servers を選択する必要があります ([System Configuration] > [Miscellaneous Options] > [Network Options])。また、仮想サービスで Transparency を無効にする必要があります。 代替ゲートウェイ/非ローカル Real Server が設定されている場合、ヘルス チェックはデフォルト ゲートウェイを介してルーティングされます。

Real Server Address: これは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかです。Real Server を変更する場合、これは編集できません。 FQDN は、ネームサーバーが構成されている場合にのみ使用できます。 解決された名前は、括弧内の IP アドレスの横に表示されます。 詳細については、「Host & DNS Configuration」セクションを参照してください。 Real Server を追加するときに FQDN が使用される場合、名前は追加時に解決されます。 解決に失敗した場合、Real Server は作成されず、エラーが生成されます。 新しい Real Server のアドレスを入力するか、表示されるドロップダウン リストから既存の Real Server を選択できます。 ドロップダウン リストの行の前のエ

ントリは、既存の Real Server です。 行の下のエントリは、オートコンプリート フォーム オプションです。 この SubVS にすでに追加されている実サーバーは、ドロップダウン リストに表示されません。

ブラウザの制限により、このドロップダウン リストは Safari ブラウザには表示されません。

Add to all SubVSs

Real Server を SubVS に追加する場合、チェック ボックスを使用できます。これを選択すると、その仮想サービス内のすべての SubVS に Real Server が追加されます。

Port: Real Server の転送ポート。 このフィールドは編集可能であるため、ポートは必要に応じて後で変更できます。

Forwarding Method: NAT (ネットワーク アドレス変換) またはルート (直接) 転送のいずれか。利用可能なオプションは、サービスに対して選択された他のモードによって異なります。

Weight: Real Server の加重。 これは、加重ラウンド ロビン、加重最小接続、および適応スケジューリング方式で使用される Real Server の重みです。 重みのデフォルトの初期値は 1000 で、最大値は 65535、最小値は 1 です。たとえば、server1 が server2 の電力を計算するには、server1 に 4000 の重みを割り当て、server2 に 1000 の重みを割り当てます。

Connection Limit: ローテーションから除外される前に実サーバーが受け入れるオープン接続の最大数。 これは、レイヤ 7 トラフィックでのみ使用できます。 この制限により、新しい接続の作成が停止されますが、サーバーへの persistence な接続が既にある要求は許可されます。 persistence な接続には、コネクション ブローカによって設定されたセッション ブローカ Cookie を含むセッション ブローカの persistence を使用した仮想サービスへの接続が含まれます。 最大 1024 の異なる Real Server が許可されます。 たとえば、同じ Real Server プールを持つ 2 つの仮想サービスが必要な場合、各仮想サービスに 1024 の実サーバーを割り当てることができます。

LoadMaster Exchange の場合、構成できる実サーバーは 6 つに制限されています。

Add This Real Server ボタンをクリックすると、プールに追加されます。

Connection Rate Limit

LoadMaster ファームウェア バージョン 7.2.51 では、実サーバーを構成するときに [Connection Limit] フィールドがあります。これにより、ローテーションから除外される前に Real server に送信できる、1 秒あたりのオープン接続数 (CPS) の最大数を設定できます。上限は 100000 (100,000

CPS) です。 Connection Rate Limit が 0 (デフォルト) に設定されている場合、この機能は無効になります。つまり、レート制限はありません。
レート制限が有効になっている場合、LoadMaster は特定のリアル サーバーへの新しい接続数を制限します。制限に達すると、現在の期間が終了するまで、Real Server はローテーション/選択から外されます (つまり、負荷分散スケジューリング アルゴリズムから削除されます)。 「Rate Limit」は 0.1 秒です。 10 CPS 未満の値は、10 CPS として扱われます。実サーバーがローテーションから除外されると、現在の接続は仮想サービス (またはサブ VS) 内の別の実サーバーに移動するようにスケジュールされます。これには、レート制限された Real Server への持続性設定を伴う新しい接続が含まれます。レート制限を超えると、これらは別の Real Server にも送信されます。Real Server が見つからない場合は、通常の拒否方法が使用されます。現在の「Rate Limit」が満了し、Real Server が負荷分散スケジューリング プロセスに戻されるまで、新しい接続はレート制限された実サーバーに送信されません。リアル サーバーのレート値は、スロー スタートも考慮に入れます。 Real Server の再起動時に、CPS 制限は、スロー スタート期間の終わりに完全な値になります。スロー スタート機能の詳細については、「L7 Configuration Critical」セクションの「Latest Connection Slow Start」の見出しを参照してください。

このオプションは、[Enhanced Options] チェック ボックスが有効になっている場合にのみ表示されます。 [Enhanced Options] チェック ボックスの詳細については、Real Server のセクションを参照してください。

Virtual Service の変更画面の Real Servers セクションには、各 Real Server の Critical チェックボックスがあります。 このオプションを有効にすると、仮想サービスが利用可能であると見なされるために Real Server が必要であることを示します。 実サーバーに障害が発生したか無効になっている場合、仮想サービスは停止しているとマークされます。 SubVS 上の実サーバーがクリティカルとしてマークされている場合、その実サーバーがダウンしている場合、SubVS はダウンとしてマークされます。 ただし、そのサブ VS がクリティカルとしてマークされていない限り、親仮想サービスはダウン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] フィールドを上書きします。 たとえば、最小値が 2 に設定されていて、Real Server が 1 つだけダウンしているが、その Real Server がクリティカルに設定されている場合、仮想サービスはダウンとしてマークさ

れます。

いずれの場合も、仮想サービスがダウンしていると見なされ、仮想サービスにソーリー サーバーまたはエラー メッセージが設定されている場合、これらが使用されます。

Healthcheck On

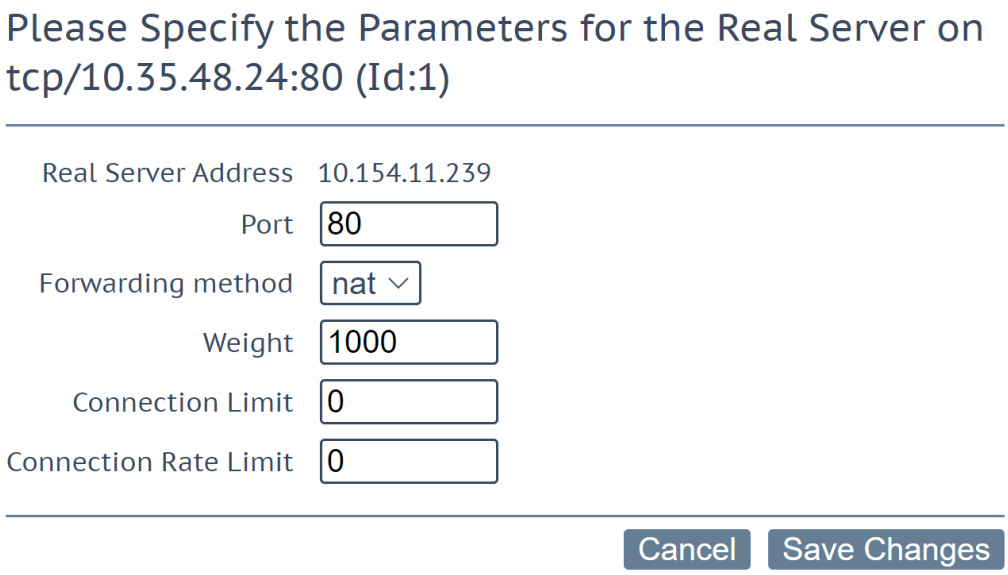
このオプションは、[Enhanced Options] チェック ボックスが有効になっている場合にのみ表示されます。 [Enhanced Options] チェック ボックスの詳細については、実サーバーのセクションを参照してください。

仮想サービス変更画面のリアル サーバー セクションには、各 Real Server のヘルスチェック オン ドロップダウン リストがあります。 これにより、ヘルスチェックのベースとなる Real Server を指定できます。 これを Self に設定して、特定の Real Server のステータスに基づいてヘルス チェックを実行するか、別の Real Server を選択することができます。 たとえば、リアル サーバー 1 がダウンしている場合、Real Server 1 に基づいてヘルス チェックを行っている Real Server も、実際の Real Server のステータスに関係なく、ダウンとしてマークされます。 注意すべき点を以下に示します。

- Real Server は、サブ VS ではなく、Real Server にのみ従うことができます。
- Real Server は、3 番目の Real Server もフォローしている Real Server をフォローできます。 最初の 2 つの Real Server のステータスは、3 番目の Real Server のステータスを反映します。
- Real Server のチェーンは許可されていますが、ループは許可されておらず、作成することもできません。
- Real Server が (単独で、または仮想サービスの一部として) 削除されると、Real Server に続くすべての Real Server は通常の動作にリセットされます (つまり、仮想サービスのヘルス チェック オプションを使用し始めます)。
- 仮想サービス内のすべての Real Server が別の仮想サービス上の Real Server をフォローしている場合、仮想サービスのヘルス チェック パラメータは WUI に表示されません (設定が Real Server に影響しないため)。
- [Enhanced Options] チェック ボックスを無効にすると、その仮想サービスに続くすべての実サーバー ヘルス チェックが無効になります。

3.15.5 Real Server の変更

Real Server の [Modify] ボタンをクリックすると、次のオプションが利用可能になります。



Real Server Address

このフィールドには、Real Server のアドレスが表示されます。 これは編集可能なフィールドではありません。

Port

これは、使用される Real Server のポートを詳述するフィールドです。

Forwarding Method

これは、使用する転送方法のタイプを詳述するフィールドです。 デフォルトは NAT です。 Direct Server Return は、L4 サービスでのみ使用できます。

Weight

加重ラウンド ロビン スケジューリングを使用する場合、Real Server の重みを使用して、サーバーに送信するトラフィックの相対的な割合を示します。 より高い値を持つサーバーは、より多くのトラフィックを受け取ります。

Connection Limit

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

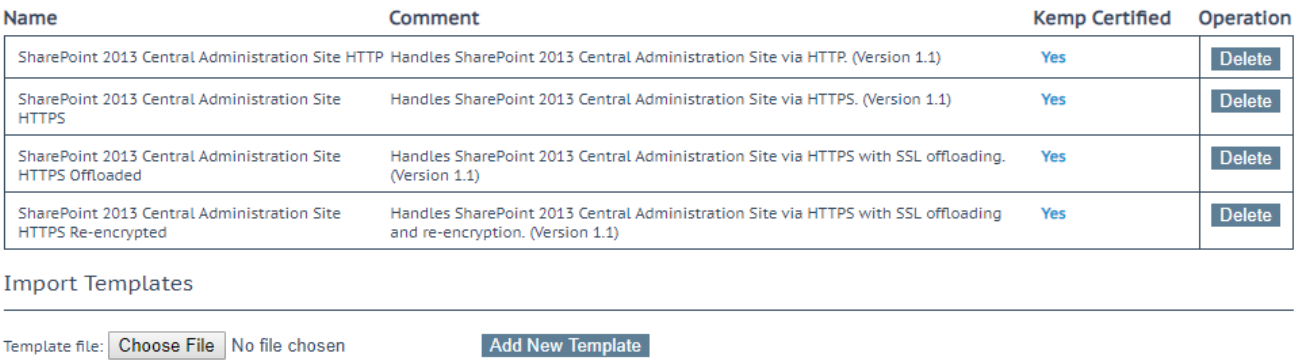
Connection Rate Limit

これは、ローテーションから除外される前に Real Server に送信できる、1 秒あたりのオープン接続

数（CPS）の最大数です。 上限は 100000 (100,000 CPS) です。

3.14 テンプレートの管理

テンプレートを使用すると、仮想サービスのパラメータが自動的に作成および構成されるため、仮想サービスの設定が簡単になります。 テンプレートを使用して仮想サービスを構成する前に、テンプレートをインポートして LoadMaster に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、インストールする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。 このテンプレートは、新しい仮想サービスを追加するときに使用できるようになりました。

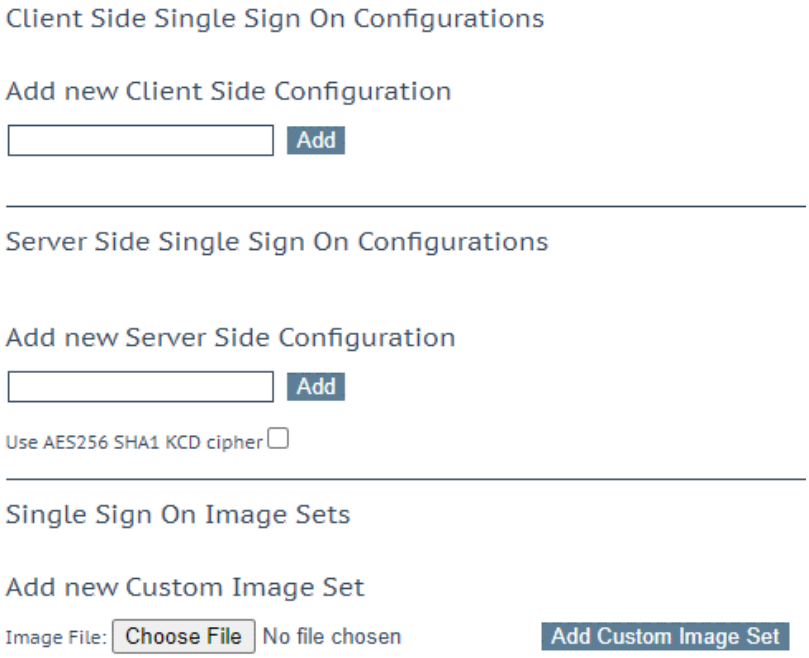
テンプレートを削除するには、[Delete] をクリックします。
Progress Kemp Certified 列には、テンプレートが Progress Kemp によって提供されたかどうかが示されます。 テンプレートが認定されている場合、それは Progress Kemp によって提供されています。 テンプレートが認定されていない場合は、(仮想サービスをエクスポートして) ユーザーが作成したテンプレートである可能性があります。
テンプレートを使用して新しい仮想サービスを作成および構成する方法や、Progress Kemp テンプレートを入手する場所など、テンプレートの詳細については、仮想サービスとテンプレートの機能の説明を参照してください。

3.15 SSO ドメインの管理

Edge Security Pack (ESP) を使用する前に、ユーザーは最初に LoadMaster でシングル サインオン (SSO) ドメインを設定する必要があります。 SSO ドメインは、LDAP サーバーによって認証される

仮想サービスの論理グループです。

許可される SSO ドメインの最大数は 128 です。



[Manage SSO Domain] メニュー オプションをクリックして、[Manage Single Sign On Options] 画面を開きます。

3.15.1 シングル サインオン ドメイン

クライアント側とサーバー側の 2 種類の SSO ドメインを作成できます。 クライアント側のシングル サインオン ドメインにより、使用されるプロトコルや認証エンドポイントなど、LoadMaster がクライアントを認証する方法を構成できます。 LoadMaster からサーバーへの接続の認証に Kerberos Constrained Delegation を使用する場合は、サーバー側ドメインが必要です。 クライアント側の構成では、認証プロトコルを LDAP、RADIUS、RSASecurID、証明書、RADIUS と LDAP、または RSA-SecurID と LDAP に設定できます。

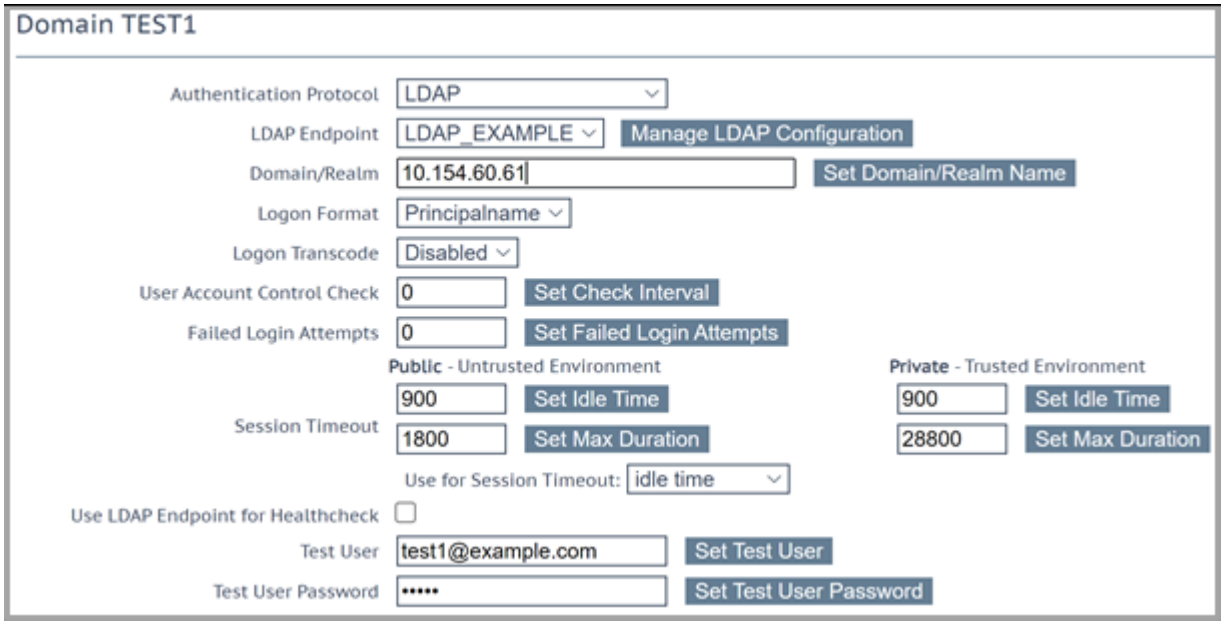
LoadMaster ファームウェア バージョン 7.2.52 では、RADIUS 2 要素認証と LDAP 認証がサポートされています。 ESP を参照してください。

詳細については、Progress Kemp ドキュメント ページの機能の説明を参照してください。

サーバー側の構成では、認証プロトコルを Kerberos Constrained Delegation (KCD) に設定できます。
新しい SSO ドメインを追加するには、[Name] フィールドにドメインの名前を入力し、[Add] をクリックします。 このフィールドには最大 64 文字まで入力できます。 ここに入力する名前は、Single Sign On ドメイン内の許可されたホストに関連付ける必要はありません。

ESP オプションの [Permitted Group] フィールドを使用する場合、ここで設定された 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。 たとえば、SSO ドメインが webmail.example に設定されていて、webmail が example.com 内の許可されたグループのディレクトリでない場合、それは機能しません。 代わりに、SSO ドメインを .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、最初に SSO ドメインを追加したときに設定されたドメイン名が Domain/Realm 名として使用されます。

3.15.1.1 クライアント側 (インバウンド) SSO ドメイン



Authentication Protocol
このドロップダウンでは、認証サーバーとの通信に使用するトランスポート プロトコルを選択できます。 オプションは次のとおりです。

1. LDAP

2. RADIUS
3. RSA-SecurID
4. Certificates

認証プロトコルを証明書に設定して SSO ドメインを作成する場合は、LDAP エンドポイントで LDAP プロトコルを LDAPS に設定してください。

- RADIUS and LDAP
- RSA-SecurID and LDAP
- SAML
- OIDC/OAUTH

この画面に表示されるフィールドは、選択した認証プロトコルによって異なります。

LDAP Endpoint

使用する LDAP エンドポイントを選択します。 [Manage LDAP Configuration] ボタンをクリックして、[LDAP Configuration] 画面に移動します。 LDAP エンドポイントの詳細については、「LDAP 構成」セクション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 および LDAP、または RSA-SecurID および 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)

ドメインの認証に使用するサーバーの IP アドレスを [Server] フィールドに入力し、[Set Servers] ボタンをクリックします。 このテキスト ボックスには、複数のサーバー アドレスを入力できます。各エントリはスペースで区切る必要があります。

IPv6 は、RADIUS 認証ではサポートされていません。

RADIUS Shared Secret

RADIUS サーバーと LoadMaster の間で使用される共有シークレット (48 文字の制限)。

このフィールドは、認証プロトコルが RADIUS または RADIUS と LDAP に設定されている場合にのみ使用できます。

Send NAS Identifier

このチェック ボックスが無効になっている場合 (デフォルト)、ネットワーク アクセス サーバー

(NAS) 識別子は RADIUS サーバーに送信されません。 有効にすると、NAS 識別子文字列が RADIUS サーバーに送信されます。 デフォルトでは、これはホスト名です。 または、[RADIUS NAS Identifier] テキスト ボックスに値が指定されている場合、この値が NAS 識別子として使用されます。 NAS 識別子を追加できない場合でも、RADIUS アクセス要求は処理されます。

このフィールドは、認証プロトコルが RADIUS または RADIUS と LDAP に設定されている場合にのみ使用できます。

NAS 識別子の送信には、次の 2 つの目的があります。

- 単にホスト IP アドレスを送信するのではなく、リクエストを送信しているデバイス タイプを分類するのに役立ちます。これにより、トラブルシューティングとログの使用が容易になります。
- 識別子に基づいて、カスタマイズされた認証応答をサーバーから送り返すことができます。

RADIUS NAS Identifier

Send NAS Identifier チェックボックスが選択されている場合、RADIUS NAS Identifier フィールドが表示されます。 指定すると、この値が NAS 識別子として使用されます。 それ以外の場合、ホスト名が NAS 識別子として使用されます。 NAS 識別子を追加できない場合でも、RADIUS アクセス要求は処理されます。

このフィールドは、認証プロトコルが RADIUS または RADIUS と LDAP に設定され、[NAS 識別子の送信] チェック ボックスが有効になっている場合にのみ使用できます。

Select Certificate to User Mapping

このオプションは、認証プロトコルが証明書に設定されている場合にのみ使用できます。 Select Certificate to User Mapping フィールドには、次の値があります。

- User Principal Name (default value)
- Subject
- Issuer and Subject
- Issuer and Serial Number

LoadMaster ファームウェア バージョン 7.2.53 では、Personal Identity Verification (PIV) スマート カード認証のサポートが追加されました。 詳細については、Progress Kemp ドキュメント ページの ESP 機能の説明を参照してください。

このオプションが有効で、チェックが失敗した場合、ログイン試行は失敗します。 このオプションが有効になっていない場合、ユーザーの altSecurityIdentities 属性が存在しないか一致しない場合でも、有効なクライアント証明書 (SubjectAltName (SAN) 内のユーザー名を持つ) のみがログインに必要です。 詳細については、Kerberos の制約付き委任機能の説明を参照してください。

Allow fallback to check Common Name

このオプションを有効にすると、SAN が使用できない場合にフォールバックで証明書の共通名 (CN) をチェックできます。

このフィールドは、認証プロトコルが証明書に設定されている場合にのみ表示されます。

Domain/Realm

使用するログイン ドメイン。 これは、たとえば、正規化されたユーザー名を作成するためにログオン形式でも使用されます。

- Principalname: <username>@<domain>
- Username: <domain>¥<username>

[Domain/Realm] フィールドが設定されていない場合、最初に SSO ドメインを追加したときに設定されたドメイン名がドメイン/レルム名として使用されます。

RSA Authentication Manager Config File

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

このファイルは、RSA Authentication Manager からエクスポートする必要があります。
構成方法を含む RSA 認証方法の詳細については、RSA 2 要素認証機能の説明を参照してください。

RSA Node Secret File

このオプションは、認証プロトコルが RSA-SecurID に設定されている場合にのみ使用できます。
ノード シークレットは、RSA Authentication Manager で生成およびエクスポートする必要があります。
RSA Authentication Manager 設定ファイルがアップロードされるまで、RSA ノード シークレット ファイルをアップロードすることはできません。 ノード シークレット ファイルは、構成ファイルに

依存します。

Logon Format

このドロップダウン リストでは、クライアントが入力する必要があるログイン情報の形式を指定できます。

使用可能なオプションは、選択した認証プロトコルによって異なります。

Not Specified: ユーザー名には正規化が適用されません。入力したとおりに取得されます。

Principalname: これをログオン形式として選択すると、クライアントはログイン時にドメイン (username@domain など) を入力する必要がなくなります。 この場合、対応するテキスト ボックスに追加された SSO ドメインがドメインとして使用されます。

RADIUS を認証プロトコルとして使用する場合、ログインが機能するには、この SSO ドメイン フィールドの値が正確に一致する必要があります。 大文字と小文字が区別されます。

Username: これをログオン形式として選択すると、クライアントはドメインとユーザー名を入力する必要があります (たとえば、domain¥username)。

Username Only: これをログオン形式として選択すると、入力したテキストがユーザー名のみに正規化されます (ドメインは削除されます)。

[Username Only] オプションは、RADIUS および RSA-SecurID プロトコルでのみ使用できます。

Logon Format (Phase 2 Real Server)

実サーバーへの認証に使用する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、認証プロトコルが次のいずれかのオプションに設定されている場合にのみ表示されます。

- RADIUS
- RSA-SecurID

Logon Format (Phase 2 LDAP)

LDAP への認証に使用するログオン文字列形式を指定します。

[Logon Format(Phase 2 LDAP)] フィールドは、認証プロトコルが次のいずれかのオプションに設定されている場合にのみ表示されます。

- RADIUS and LDAP

- RSA-SecurID and LDAP

Logon Transcode

必要に応じて、ログオン資格情報の ISO-8859-1 から UTF-8 へのトランスコードを有効または無効にします。 このオプションが無効になっている場合は、クライアントが指示する形式を使用してログインします。 このオプションが有効になっている場合は、クライアントが UTF-8 を使用しているかどうかを確認してください。 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。

User Account Control Check

UAC チェック間隔の値が 0 分 (デフォルト値) に設定されている場合、ログインが成功した後、UAC はユーザーに対して定期的に実行されません。 1 ～ 300 分の範囲の間隔値を指定すると、間隔の満了後に受信した要求に対して、定期的な UAC チェックがユーザーごとに実行されます。 UAC は以下を検出します。

- Unknown users
- Disabled accounts
- Locked accounts
- Expired passwords on accounts

拡張 ESP ユーザー ログは、UAC チェックの結果を提供します。 セッションの開始時間、合計継続時間、プロトコル情報、KCD 情報、ブロックされたユーザー イベントなど、ユーザーに関する追加情報がログに記録されます。 チェックは、新しい接続の確立時に、または既存のセッションの一部として発生する場合があります。 msDSUser Account-Control-Computed および userAccountControl 属性は、UAC の状態を判断するために使用されます。

Failed Login Attempts

ユーザーがロックアウトされるまでのログイン試行の連続失敗の最大回数。 有効な値の範囲は 0 ～ 99 です。これを 0 に設定すると、ユーザーはロックアウトされません。

ユーザーがロックアウトされると、そのユーザーの既存のログインはすべて終了し、今後のログインも終了します。

Reset Failed Login Attempt Counter after

認証試行が失敗してから (新しい試行なしで) この時間 (秒単位) が経過すると、失敗したログイン試行カウンターは 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、ブロック解除のタイムアウト値より小さくする必要があります。

Unblock timeout

ブロックされたアカウントが自動的にブロック解除されるまでの時間 (秒単位)。つまり、管理者の介入なしにブロック解除されます。 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、失敗したログイン試行カウンタのリセットの値より大きくする必要があります。

Session timeout

ここでは、信頼できる (プライベート) 環境と信頼できない (パブリック) 環境のアイドル時間と最大期間の値を設定できます。 使用される値は、ユーザーがログイン フォームで public または private のどちらを選択したかによって異なります。

- Idle time: セッションの最大アイドル時間 (秒単位)、つまりアイドル タイムアウト。
- Max duration: 秒単位のセッションの最大継続時間、つまりセッション タイムアウト。

これらのフィールドの有効な値の範囲は、60 ～ 604800 (秒) です。
Use for Session Timeout: セッション タイムアウトの動作 (最大期間またはアイドル時間) を選択するためのスイッチ。
明らかなユーザー操作がなくても、基礎となるネットワーク トラフィックによってセッションがアクティブなままになる場合があります。

Use LDAP Endpoint for Healthcheck

ヘルス チェックに LDAP エンドポイント管理者のユーザー名とパスワードを使用するには、このチェック ボックスをオンにします。 これが有効になっている場合、[Test User] および [Test User Password] テキストボックスは使用できません。 LDAP エンドポイントの詳細については、「LDAP Configuration」セクションを参照してください。

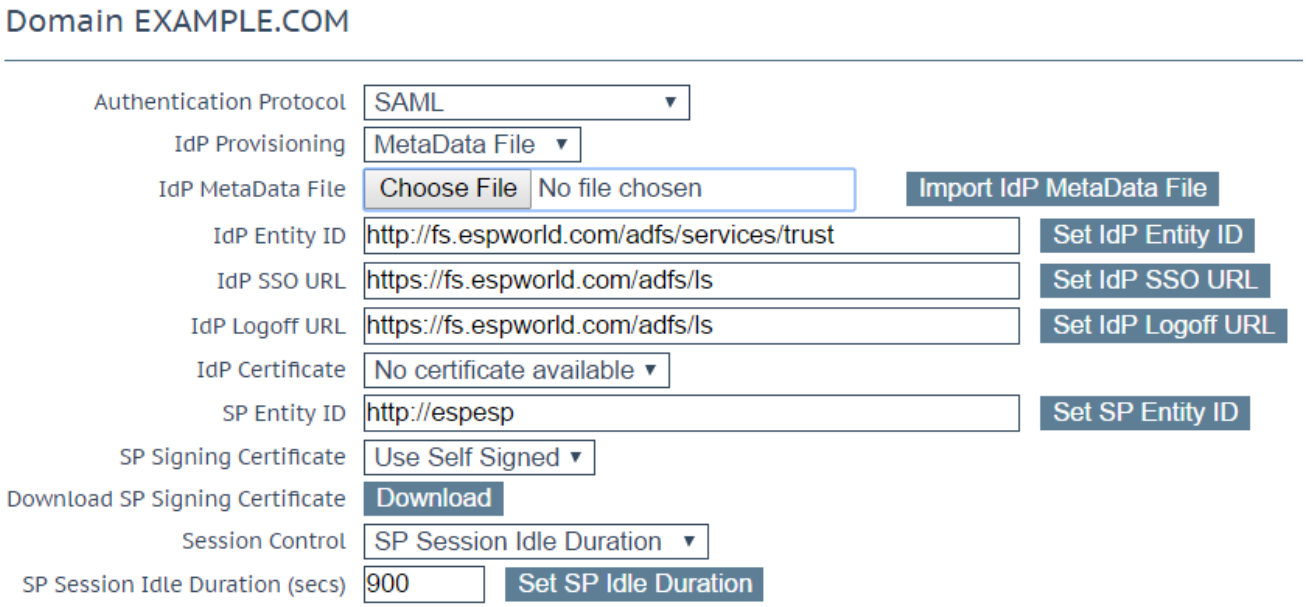
このオプションは、次のプロトコルでのみ使用できます。 LDAP、証明書、RADIUS と LDAP、RSA-SecurID と LDAP。

Test User and Test User Password

これら 2 つのフィールドに、SSO ドメインのユーザー アカウントの資格情報を入力します。
LoadMaster は、認証サーバーのヘルス チェックでこの情報を使用します。 このヘルス チェックは 20 秒ごとに実行されます。

3.15.1.1.1 クライアント側 (インバウンド) SAML SSO ドメイン

認証プロトコルが SAML に設定されている場合、フィールドは異なります。 SAML 固有のフィールドについて以下に説明します。



IdP Provisioning

手動オプションを使用すると、IdP フィールドに詳細を手動で入力できます。 メタデータ ファイル オプションを使用すると、IdP メタデータ ファイルをアップロードできます。 これにより、IdP エンティティ ID、IdP SSO URL、IdP ログオフ URL などの IdP 属性の構成が簡素化されます。 メタデータ ファイルは IdP からダウンロードできます。

IdP Metadata File

このフィールドは、IdP プロビジョニング フィールドがメタデータ ファイルに設定されている場合にのみ表示されます。 ファイルをアップロードするには、[Browse] をクリックし、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 エンティティ識別子を指定します。 このフィールドで許可される最大文字数は 255 です。

IdP SSO URL

Specify the IdP SSO URL. The maximum number of characters permitted in this field is 255.

IdP Logoff URL

IdP ログオフ URL を指定します。 このフィールドで許可される最大文字数は 255 です。

IdP Certificate

IdP 証明書は、IdP から受信する SAML 応答に含まれている必要があるアサーションの検証という点で非常に重要です。 証明書がないと、検証を続行できません。

IdP Certificate Match

このオプションが有効になっている場合、割り当てられた IdP 証明書は、IdP SAML 応答の証明書と一致する必要があります。

SP Entity 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 がエンティティを理解し、受け入れ、認識できるようにするために共有される識別子です。 これは、AD FS サーバー上の証明書利用者の識別子に関連付ける必要があります。 このフィールドで許可される最大文字数は 255 です。

SP Signing Certificate

ログオンのコンテキストで送信される要求に署名することはオプションです。 現在、LoadMaster はこれらのリクエストに署名していません。 ログオフ要求のコンテキストでは、これは必須であり、これらの要求に署名する必要があります。 これは、スプーフィングを回避し、ログオフ機能に関連する追加のセキュリティを提供するためです。 これにより、ユーザーがハッキングされたり、不必要にログオフされたりすることがなくなります。 [SP Signing Certificate] ドロップダウン リストで、自己署名証明書またはサード パーティ証明書を使用して署名を実行することを選択できます。

Download SP Signing Certificate

自己署名証明書を使用している場合は、[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、証明書利用者の署名に追加するために、IdP サーバー (AD FS など) にインストールする必要があります。 AD FS サーバーは、LoadMaster が生成する署名を検証するために公開キーを使用するために、この証明書を必要とします。

Session Control

関連するセッション制御オプションを選択します。 利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

LoadMaster で IdP の最大継続時間の値を設定することはできません。 値は IdP プロトコルから取得されます。 IdP 認証応答で値がまだ設定されていない場合、デフォルト値の 30 分が IdP の最大

期間として割り当てられます。

SP Session Idle Duration

セッションのアイドル期間を指定します (秒単位)。 このフィールドは、SP セッションのアイドル期間がセッション制御オプションとして設定されている場合にのみ表示されます。

SP Session Max Duration

セッションの最大継続時間を指定します (秒単位)。 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されます。

3.15.1.1.2 クライアント側 (インバウンド) OIDC / OAUTH SSO ドメイン

認証プロトコルが OIDC / OAUTH に設定されている場合、フィールドは異なります。 OIDC 固有のフィールドについて以下に説明します。

Application ID

アプリケーション (クライアント) 識別子を入力します。 このフィールドで許可される最大文字数は 255 です。

Redirect URI

リダイレクトの URI (Uniform Resource Identifier) または URI (応答 URL) を指定します。 複数の URI をスペースで区切って入力できます。 [Redirect URI] テキスト ボックスには最大 255 文字を指定できます。 このフィールドに値が設定されると、設定を解除することはできません。

Redirect URI フィールドが設定されたときに使用されるロジックの詳細については、OIDC 機能の説明を参照してください。

Authorization Endpoint URL

アプリケーションの OAuth 2.0 認証エンドポイント URL を入力します。 このフィールドで許可される最大文字数は 255 です。

Token Endpoint URL

アプリケーションの OAuth 2.0 トークン エンド ポイント URL を指定します。 このフィールドで許可される最大文字数は 255 です。

Logoff URL

アプリケーションのログアウト URL を指定します。 このフィールドで許可される最大文字数は 255 です。

Application Secret

アプリケーションのクライアント シークレットの値を指定します。

Session Control

セッション コントロールを選択します。

- Session Idle Duration
- Session Max Duration

Session Idle Duration/Session Max Duration

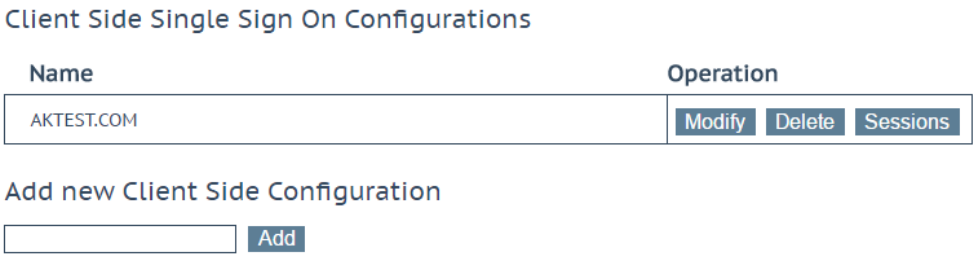
セッションのアイドル期間または最大期間を指定します (Session Control で選択されている内容に応じて異なります)。

3.15.1.1.3 RADIUS 二要素認証と LDAP 認証

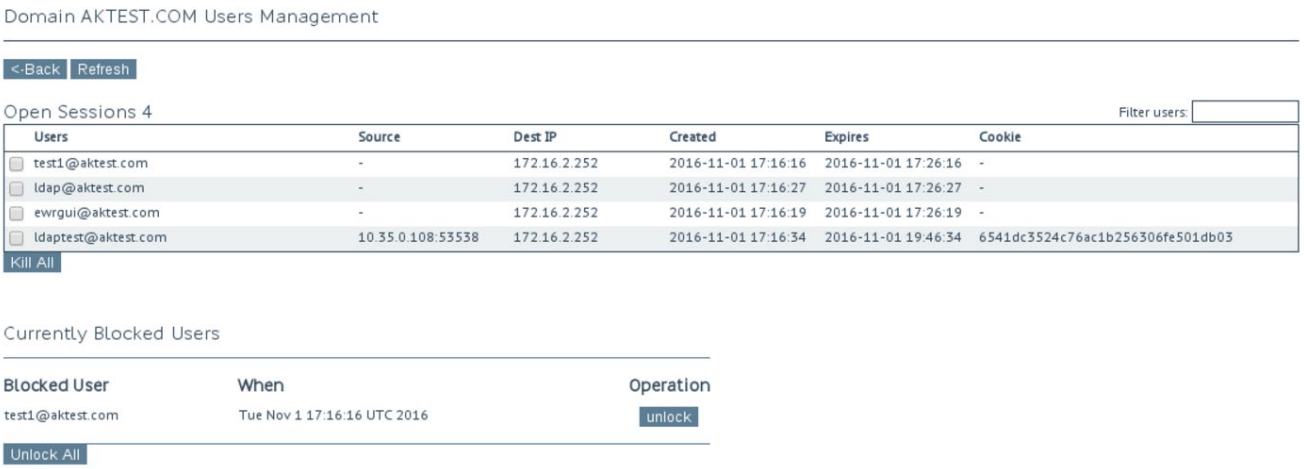
LoadMaster ファームウェア バージョン 7.2.52 では、RADIUS 2 要素認証と LDAP 認証がサポートされています。 これを構成するには:

- [Virtual Service] > [Manage SSO] でクライアント側のシングル サインオン (SSO) ドメインを追加または変更するときに、認証プロトコルとして RADIUS および LDAP を選択します。 RADIUS サーバーが 2 要素認証を使用するように構成されている場合、LoadMaster はこれを自動的に検出し、RADIUS 2 要素認証を実行します。
- この SSO ドメインの LDAP エンドポイントと RADIUS サーバーを設定します。
- [Virtual Service Modify] 画面の [ESP Options] セクションで、SSO イメージ セットとして [Exchange] または [Blank] を選択します。
- 構成に応じて他のパラメーターを設定します。

3.15.1.1.4 セッション



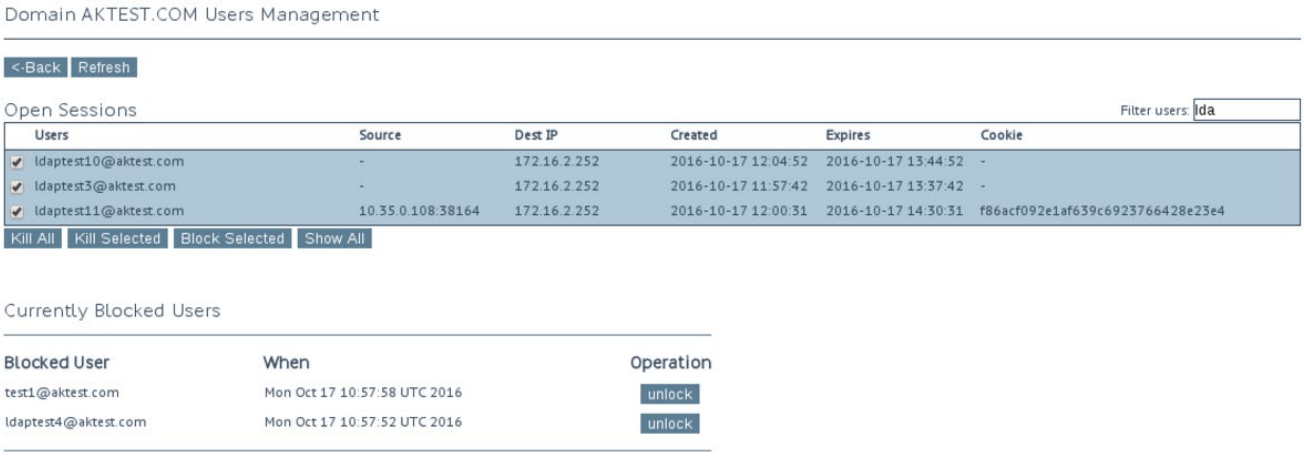
クライアント側 SSO ドメインの [Sessions] ボタンをクリックすると、そのドメインで現在開いているセッションを一覧表示する画面が開きます。



[Filter users] テキスト ボックスに検索語を入力して、リストをフィルター処理できます。 各セッションについて、次の情報が提供されます。

- User: クライアントのユーザー名/ドメイン。
- Source: クライアント (ホスト) の IP アドレスとソース ポート。
- Dest IP: 接続の宛先 IP アドレス。
- Created: 接続が作成された日時。
- Expires: 接続が期限切れになる日時。
- Cookie: 接続で使用される 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が強制終了されます (SSO キャッシュがフラッシュされます)。 Web ユーザー インターフェイス (WUI) 3 仮想サービス 120



1 つ以上のセッションを選択すると、さらにいくつかのオプションが提供されます。

- Kill Selected
- Block Selected

- Show All

ログは、セッションの強制終了操作ごとに監査ログに追加されます。 例えば：

1. Kill 'non-cookie' session log:

   Nov 9 16:47:31 LM ssomgr: Deleted a session tester@aktest.com:- for domain AKTEST.COM
2. Kill 'cookie' session log:

   Nov 9 16:47:31 LM ssomgr: Deleted a session ldaptest@aktest.com:420cf78373643b3c0171d95c757e7bf3 for domain AKTEST.COM
3. Kill all domain sessions log:

   Nov 9 16:48:46 LM ssomgr: Deleted all domain AKTEST.COM user sessions

Currently Blocked Users

このセクションには、現在ブロックされているユーザーのリストが表示され、ブロックが発生した日時も表示されます。 [Operation] ドロップダウン リストの [unlock] ボタンをクリックすると、ブロックを解除できます。

同じユーザー名の異なる形式は、同じユーザー名として扱われます。例えば、administrator@kemptech.net、kemptech¥administrator と kemptech.net¥administrator はすべて 1 つのユーザー名として扱われます。

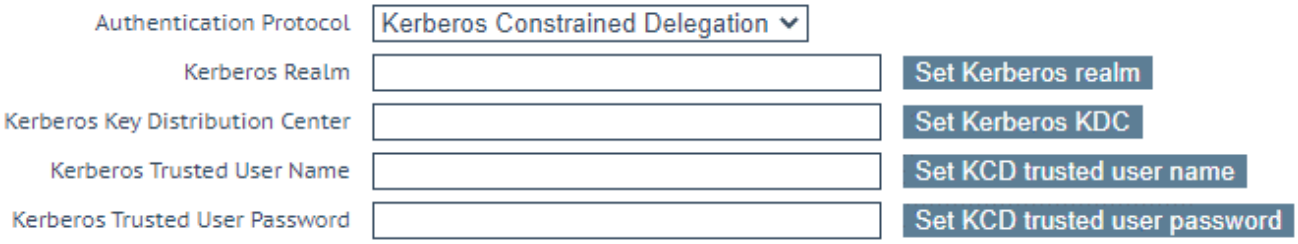
3.15.1.2 サーバー側 (アウトバウンド) SSO ドメイン

Kerberos Constrained Delegation をサーバー側認証プロトコルとして使用する場合、サーバー側 SSO ドメインを作成する必要があります。 これには、LoadMaster からサーバーへの接続で認証を完了するために必要なすべての構成が含まれています。

[Manage SSO] 画面の [Server Single Sign-on Configurations] セクションで、サーバー側 SSO の作成時に、チェックボックスを選択して [Use AES256 SHA1 KCD Cypher] を選択できます (デフォルトでは RC4 暗号が使用されます)。 Use AES256 SHA1 KCD cipher チェックボックスを Enabling/Disenabling にすると、ポップアップ メッセージが表示されます。 テーブルの有効期限が切れています。」 [OK] をクリックすると、SSO キャッシュがフラッシュされ、既存のセッションが停止します。 [キャンセル] をクリックすると、後で Kerberos キー テーブルの有効期限が切れたときに変更が有効になります。

Chrome ブラウザーを使用して [Use AES256 SHA1 KCD cipher] チェック ボックスの値を変更し、ポップアップ メッセージが表示されている間に別のタブに移動すると、ポップアップが消え、チェック ボックスの値が設定されます。 ポップアップで [OK] をクリックしなかったため、SSO キャッシュはフラッシュされません。

新しいサーバー側 SSO を追加するには、SSO 構成の名前を入力し、[Add] をクリックします。



Authentication Protocol

このドロップダウンでは、認証サーバーとの通信に使用するトランスポート プロトコルを選択できます。 アウトバウンド (サーバー側) 構成で使用できる唯一のオプションは、Kerberos Constrained Delegation (KCD) です。 KCD の詳細については、Progress Kemp ドキュメント ページの KCD 機能の説明を参照してください。

Kerberos Realm

Kerberos Realm のアドレス。

このフィールドでは、コロン、スラッシュ、および二重引用符は使用できません。 このフィールドは 1 つのアドレスのみをサポートします。

Kerberos Key Distribution Center (KDC)

Kerberos Key Distribution Center のホスト名または IP アドレス。 KDC は、Active Directory ドメイン内のユーザーとコンピューターにセッション チケットと一時的なセッション キーを提供するネットワーク サービスです。サーバー側の Kerberos Constrained Delegation (KCD) シングル サインオン (SSO) ドメインを構成するときは、ドメインの詳細を指定します。 LoadMaster ファームウェア バージョン 7.2.51 では、スペースで区切られた 2 つの Kerberos Key Distribution Center (KDC) を指定できます。これにより、アクティブな KDC が利用できなくなった場合のバックアップが提供されます。バージョン 7.2.51 より前では、指定できる KDC は 1 つだけでした。最初に入力した KDC は、失敗するまでアクティブになります。 KDC の可用性がチェックされ、KDC が 3 回正常に応答しない場合、または 5 秒間タイムアウトした場合、アクティブな KDC が切り替えられます。自動フェイルバック機能はありません。2 番目の KDC は、使用できなくなるまでアクティブになります。フェイルオーバーが発生し、最初の KDC が再び使用可能になった場合に最初の KDC に戻すには、[System Configuration] > [Logging Options] > [System Log Files] > [Flush SSO Cache] に移動して SSOMGR キャッシュをクリアします。 2 つの KDC を指定すると、アクティブな Kerberos KDC が [Kerberos Key Distribution Center] フィールドの下に表示されます。

複数の KDC を入力する場合、ユーザー名とパスワードは両方の KDC で同じでなければなりません。Kerberos Key Distribution Center フィールドでは、二重引用符と単一引用符は使用できません。

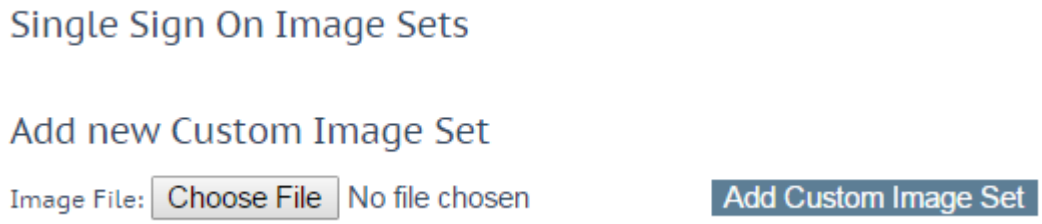
Kerberos Trusted User Name

LoadMaster を設定する前に、Windows ドメイン (Active Directory) でユーザーを作成し、信頼する必要があります。 このユーザーは、委任を使用するようにも設定する必要があります。 この信頼できる管理者ユーザー アカウントは、パスワードが提供されていない場合に、ユーザーとサービスに代わってチケットを取得するために使用されます。 この信頼できるユーザーのユーザー名をこのテキスト ボックスに入力する必要があります。

このフィールドでは、二重引用符と単一引用符は使用できません。

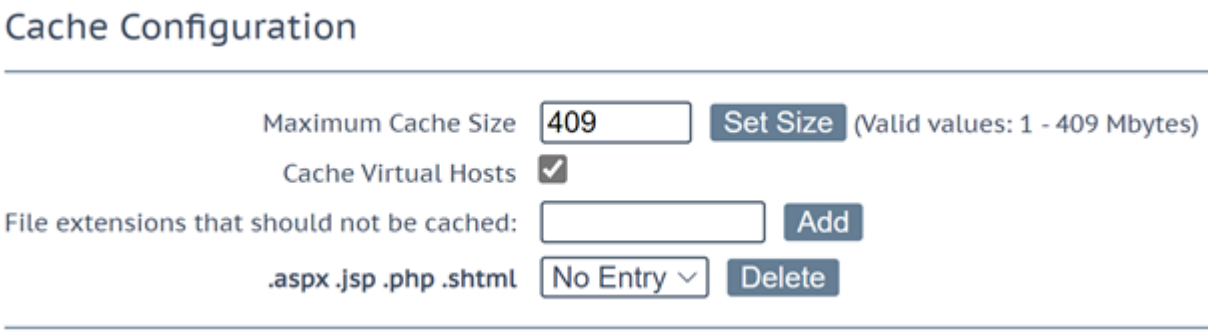
Kerberos Trusted User Password
Kerberos 信頼済みユーザーのパスワード。

3.15.2 シングル サインオン イメージ セット



新しい画像セットをアップロードするには、[Choose File] をクリックし、ファイルを参照して選択し、[Add Custom Image Set] をクリックします。 ファイルを追加すると、提供された画像セットがこのページに一覧表示されます。 仮想サービス変更画面の ESP オプション セクションの SSO イメージ セット ドロップダウン リストで選択することもできます。 .tar ファイルの構造を含む、SSO イメージ セットの詳細については、カスタム認証フォームのテクニカル ノートを参照してください。

3.16 キャッシュ構成



Maximum Cache Size

これは、キャッシュが使用できるメモリ量をメガバイト単位で定義します。 最大キャッシュ サイズは、キャッシュに割り当てられるメイン メモリの量を定義します。 マシンの総メモリの 5 分の 1 を超えることはありません。 キャッシュにより多くのメモリを割り当てると、接続に使用できるメモリの量が減り、エントリが保持されます。 正しく構成されたシステムでは、完全なキャッシュと、システムが処理すると予想されるすべての接続に十分なメモリが必要です。 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

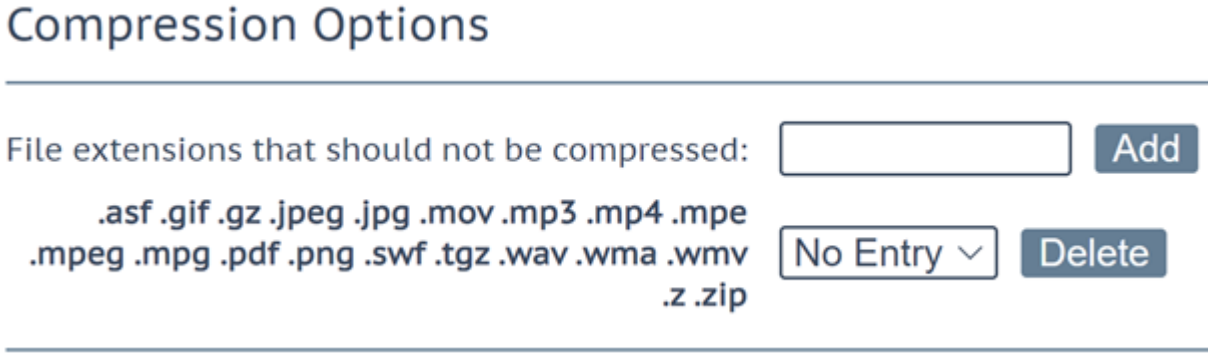
このオプションを無効にすると、キャッシュは、実サーバーでサポートされている仮想ホストが 1 つだけであると想定します。 このオプションを有効にすると、コンテンツが異なる複数の仮想ホストをキャッシュでサポートできます。

File Extensions Not to Cache

キャッシュしてはならないファイルの種類のリスト。

アイテムは 15 分間 (または、ページを更新して (たとえば、キーボードで Ctrl + F5 を押して) キャッシュがフラッシュされるまで) キャッシュに保持されます。

3.17 圧縮オプション



File Extensions Not to Compress
圧縮してはならないファイルの種類のリスト。

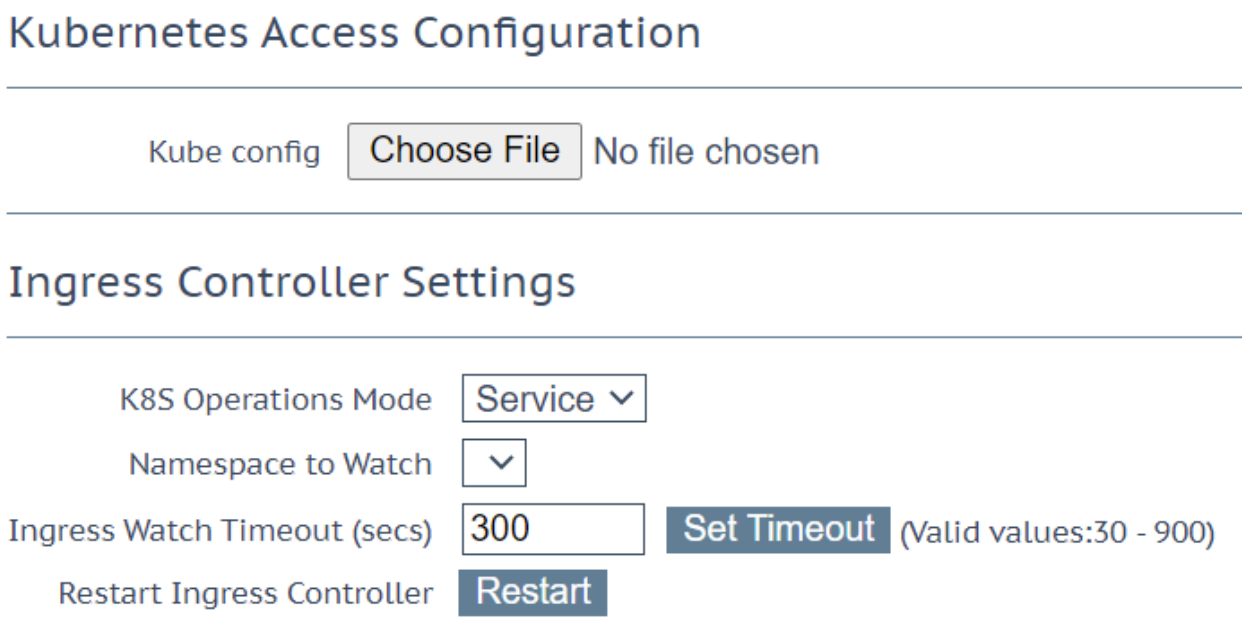
3.18 Kubernetes の設定

Ingress Controller は、デフォルトでは LoadMaster にインストールされていません。 次の手順に従って簡単にインストールできます。

1. LoadMaster ユーザー インターフェイス (UI) で、[Virtual Service] > [Kubernetes Settings] に移動します。
2. 2. [Install] をクリックします。
3. 3. インストールが完了するのを待ち、確認メッセージで [OK] をクリックします。
4. 4. LoadMaster を再起動して、必要なすべてのアドオンを有効にします - [System Configuration] > [System Administration] > [System Reboot] > [Reboot]。

再起動後、Kubernetes 設定構成ページを使用して、LoadMaster Kubernetes 統合を有効にすることができます。

高可用性ペアで AWS または Azure にデプロイされた LoadMaster の場合、アドオンが両方のデバイスにインストールされていることを確認してください。 LoadMaster ユーザー (デフォルトの admin bal ユーザーを除く) には、LoadMaster で Kubernetes 設定を変更するためのアクセスを許可するために、ユーザー権限で [すべての権限] オプションを割り当てる必要があります。



Kube Config

これにより、LoadMaster が Kubernetes と通信できるようになります。 Kube 構成ファイルのデフォルトの場所は ~/.kube/config です。たとえば、Azure Cloud Shell を使用している場合は、/home/<YourName>/.kube/config で [Download File] オプションを使用してアクセスできます。 Cloud Shell ウィンドウの上部。

Minikube を使用する場合は、認証に使用する証明書を kubeconfig ファイル内に埋め込むことをお勧めします。 これは、Minikube で次のコマンドを使用して行うことができます: minikube config set embedded-certs true

ある LoadMaster のバックアップを別の LoadMaster に復元する場合は、Kube 構成ファイルを復元した LoadMaster に個別にアップロードすることをお勧めします。

Kube 構成ファイルが正常にインストールされると、[Contexts] セクションにいくつかの情報が入力されます。 Name、Cluster、および User が表示されます。

K8S Operations Mode

Ingress Controller の操作モード (Ingress または Service) を決定します。 「K8S」は、仮想サービス リストで使用され、Kubernetes の制御下にある仮想サービスを示します。 Kubernetes で各モードを構成する方法を含む、各モードの詳細については、Progress Kemp ドキュメント ページの

Kemp Ingress Controller for Kubernetes Feature Description ドキュメントを参照してください。

Namespace to Watch
監視する K8s 名前空間。 このフィールドが設定されていない場合、すべての名前空間が監視されます。

Ingress Watch Timeout (secs)
Ingress コントローラーの監視タイムアウト (秒単位)。 有効な値の範囲は 30 から 900 です。正しく構成されている場合、Kubernetes ノードと関連オブジェクト (「kempLB」のイングレス クラス仕様を持つイングレス オブジェクトと「kempLB:Enabled」というラベルの付いたサービス オブジェクト) の詳細が画面の下部に表示されます。 .
詳細については、Progress Kemp ドキュメント ページの Kemp Ingress Controller for Kubernetes Feature Description ドキュメントを参照してください。

4 グローバルバランシング (GSLB)

このメニュー オプションは、構成によっては利用できない場合があります。 これらの機能は GSLB Feature Pack の一部であり、LoadMaster に適用されたライセンスに基づいて有効になります。 これらのオプションを利用したい場合は、Progress Kemp に連絡してライセンスをアップグレードしてください。

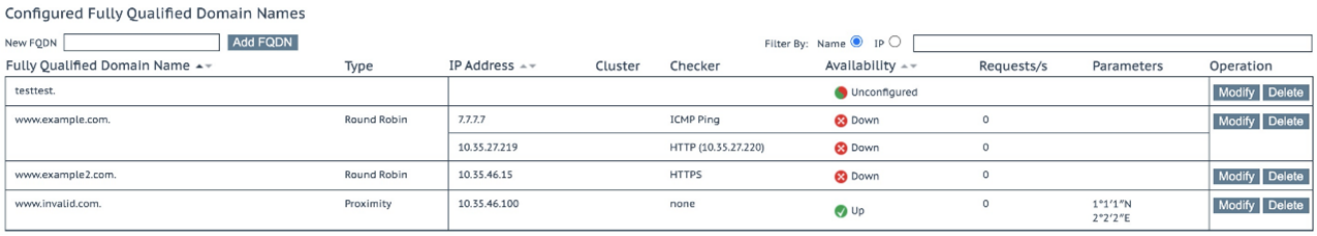
4.1 GSLB の有効化/無効化

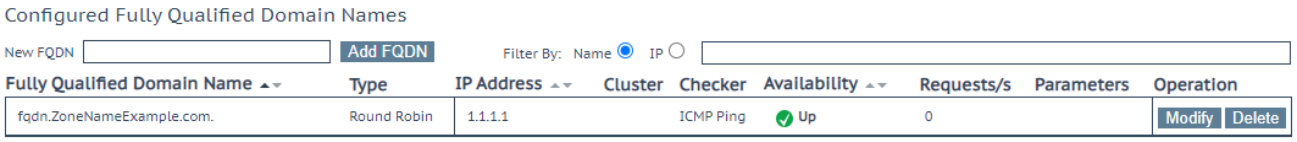
このメニュー オプションをクリックして、GEO 機能を有効または無効にします。 GEO が有効な場合、パケット ルーティング フィルタはデフォルトで有効になり、変更できません。 GEO が無効になっている場合は、[System Configuration] > [Access Control] > [Packet Filter] でパケット ルーティング フィルターを有効または無効にすることができます。

4.2 FQDN の管理

絶対ドメイン名とも呼ばれる完全修飾ドメイン名 (FQDN) は、ドメイン ネーム システム (DNS) のツリー階層内の正確な位置を指定するドメイン名です。 最上位ドメインとルート ゾーンを含むすべてのドメイン レベルを指定します。 完全修飾ドメイン名は、あいまいさがないという特徴があります。

つまり、一方向にしか解釈できません。 DNS ルート ドメインは名前がなく、空のラベルで表されるため、ドット文字で終わる FQDN になります。





この画面から、FQDN を追加または変更できます。 フィルタ テキスト ボックスを使用して、FQDN 名または IP アドレスに基づいて FQDN をフィルタリングすることもできます。

Filter By Name

デフォルトでは、FQDN 名のラジオ ボタンが選択されており、検索テキスト ボックスに FQDN 名を入力すると、関連する FQDN エントリの結果が表示されます。

Filter By IP

FQDN IP のラジオ ボタンを選択し、検索テキスト ボックスに任意の FQDN IP を入力すると、関連する IP アドレスを持つ FQDN エントリの結果が表示されます。 名前/IP に含まれるテキストをフィルター テキスト ボックスに入力すると、リストは即座にフィルター処理され、一致する結果が表示されます。 どの名前/IP にも含まれていないテキストをフィルタ テキスト ボックスに入力すると (選択したラジオ ボタンによって異なります)、テキスト ボックスが赤く点滅し、一致しないテキストが削除されます。 FQDN テーブルでは、FQDN テーブル ヘッダーの上/下矢印を使用して、FQDN 名、IP アドレス、および可用性オプションで使用可能な FQDN エントリを並べ替えることができます。

- FQDN 名の場合、エントリはアルファベット順または逆アルファベット順で並べ替えることができます。
- IP アドレスの場合、エントリは最初に IP バージョン (IPv4 の次に IPv6) で並べ替えられ、次に IP アドレスまたはアルファベットの逆順で並べ替えられます。
- 可用性については、エントリは最初にダウン ステータスでソートされ、リストに使用可能

なアップ ステータスとダウン ステータスの FQDN がある場合にのみ、残りの FQDN が続きます。 Up、Down、Disabled、Unconfigured などの複数のステータスを持つ複数の FQDN がリストに存在する場合、並べ替えは次の順序で行われます。

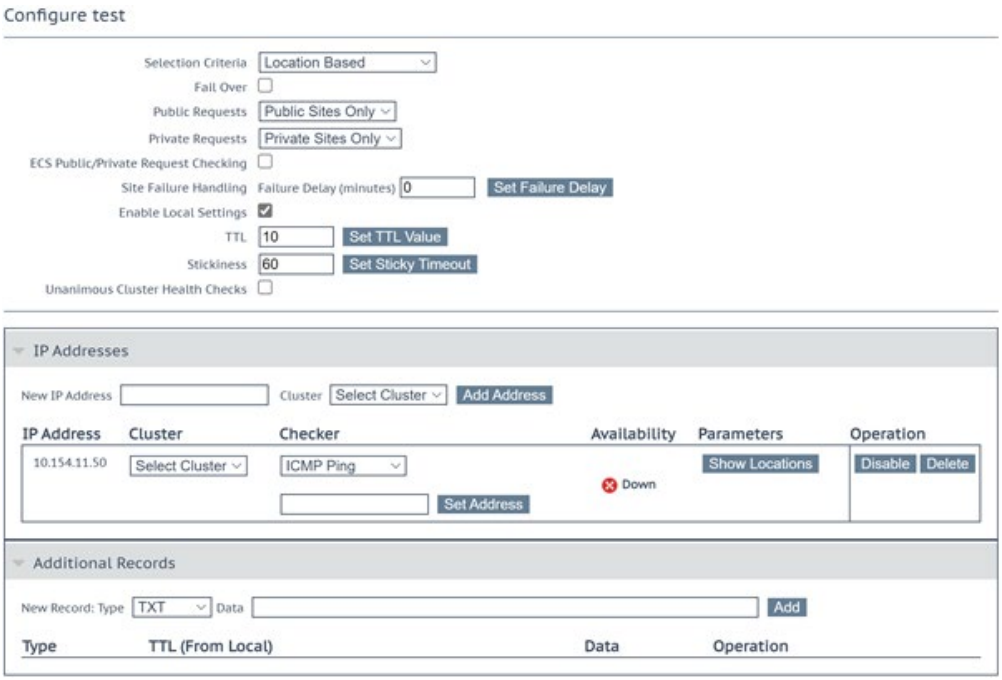
- Unconfigured
- Disabled
- Down
- Up

4.2.1 FQDN を追加する

New FQDN

www.example.com などの FQDN 名。 ワイルドカードがサポートされています。たとえば、*.example1.com は、.example1.com で終わるものすべてに一致します。

4.2.2 FQDN の追加/変更



Selection Criteria

解決要求の配布に使用される選択基準は、このドロップダウン リストから選択できます。 利用可能な選択基準は次のとおりです。

- Round Robin - サーバー ファーム (クラスター)、つまり使用可能なサーバー全体に順次分散されるトラフィック。
- Weighted Round Robin – サーバーごとに事前に割り当て可能な静的な「加重」を考慮しながら、着信要求がクラスター全体に順次分散されます。
- Fixed Weighting - 他の実サーバーに低い重み値が与えられている場合にのみ、最も高い重みの実サーバーが使用されます。
- Real Server Load - LoadMaster には、サーバーの状態を一定の間隔でチェックするロジックが含まれており、構成された重み付けとは無関係です。
- Proximity – トラフィックは、クライアントに最も近いサイトに分散されます。
  Proximity スケジューリングを使用すると、新しい公開サイトは GEO データベースに基づいて地理座標に自動的にマップされます。 新しいプライベート サイトは 0º0'0" にマップされ、期待どおりに機能します。正しいバランスを確保するために、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、IP アドレスによって決定されます。

LoadMaster ファームウェア バージョン 7.2.52 では、選択基準として Proximity を使用しているときに FQDN を作成または変更した後に GEO 位置座標が変更される原因となっていたバグが修正されました。 この問題は、バージョン 7.2.52 以降では発生しなくなりました。ただし、この問題が 7.2.52 より前のバージョンで発生し、7.2.52 以降にアップグレードした場合、座標は自動的に修正されません。 そのため、誤った座標がすでにロードマスターにある場合は、手動で修正する必要があります。

- Location Based - クライアントに最も近いサイトにトラフィックが分散されます。 サイトの配置は、セットアップ中にサイトの場所 (国または大陸) を入力することによって設定されます。 クライアントの位置は、IP アドレスによって決定されます。 同じ国コードを持つサイトが複数ある場合、要求はラウンド ロビン方式で各サイトに分散されます。
- All Available – A、AAAA、または ANY クエリ リクエストのすべての可能な正常な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。
  - - For Public Site Only-リストにはパブリック アドレスのみを含めることができます。 同様に、プライベート サイトのみの場合、リストにはプライベート アドレスの

みを含めることができます。

- - For Prefer Public-パブリック アドレスが使用できない場合を除き、リストにはパブリック アドレスのみが含まれます。この場合、リストにはプライベート アドレスが含まれます (使用可能な場合)。 同様に、Prefer Private の場合、プライベート アドレスが使用できない場合を除き、リストにはプライベート アドレスのみが含まれます。この場合、リストにはパブリック アドレスが含まれます (使用可能な場合)。
- For All Sites-リストには利用可能なすべてのアドレスが含まれます。

この目的は、使用可能な場合に優先アドレスのリストを提供することです。 それ以外の場合は、可用性を向上させるためのフェイルバック手段として、非優先アドレスのリストを提供してください。

Fail Over

[Fail Over] オプションは、[Selection Criteria] が [Location Based] に設定されている場合にのみ使用できます。 フェイルオーバー オプションが有効になっている場合、リクエストが特定のリージョンから送信され、ターゲットがダウンしている場合、接続はフェイルオーバーされ、階層内の次のレベルで応答されます。 これが利用できない場合、接続は最も近い (近接した) ターゲットによって応答されます。 これが不可能な場合は、リクエストが最も少ないターゲットが選択されます。 たとえば、アイルランドからの要求を受け取ったが、アイルランドに割り当てられたサイトが利用できない場合、ヨーロッパに割り当てられたサイトが選択されます。 ヨーロッパに割り当てられたサイトも使用できない場合は、Everywhere に割り当てられたサイトが選択されます。 これも利用できない場合は、同じ大陸で利用可能なサイトの中でリクエストが最も少ないサイトがラウンド ロビン方式で選択されます。 フェイルオーバー設定は、すべてのターゲットに影響します。

Public Requests & Private Requests

バージョン 7.1-30 では、パブリック/プライベート サイトの分離設定が強化されました。 チェックボックスは 2 つの個別のドロップダウン メニューに移行され、DNS 応答をより細かく制御できるようになりました。 既存の動作が保持され、現在の設定から移行されるため、DNS 応答が変更されることはありません。

これらの新しい設定により、管理者は、構成された FQDN への DNS 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 からのものかプライベート IP からのものかに基づいて、パブリック サイトまたはプライベート サイトで選択的に応答できます。 たとえば、管理者は、プライベート クライアントのみがプライベート サイトに送信されることを許可したい場合があります。

次の表に、設定とその構成可能な値の概要を示します。

Setting	Value	Client Type	Site Types Allowed
Public Request	Public Only	Public	Public
	Prefer Public	Public	Public, Private if no Public
	Prefer Public	Public	Private, Public if no Private
	All Sites	Public	Public and Private
Private Request	Private Only	Private	Private
	Prefer Private	Private	Private, Public if no Private
	Prefer Private	Private	Public, Public if no Public
	All Sites	Private	Public and Private

ECS Public/Private Request Checking

LoadMaster ファームウェア バージョン 7.2.58 では、ECS Public/Private Request Checking という新しいチェック ボックスが FQDN の変更画面に追加されました。 デフォルトでは、[ECS Public/Private Request Check] チェック ボックスは無効になっています。 無効にすると、デバイスはクライアント要求の送信元 IP アドレスを使用して、要求がパブリックかプライベートかを判断します。 有効にすると、デバイスは代わりに EDNS クライアント サブネット (ECS) 値を使用して (受信した場合)、要求がパブリックかプライベートかを判断します。 このオプションは、次のいずれかの条件で非アクティブになります。

- EDNS Client Subnet (ECS) Option (Global Balancing > Miscellaneous Params 内) が無効になっています。
- Public Requests と Private Requests の値は両方とも All Sites に設定されています。

EDNS Client Subnet (ECS) Setting	Public/Private Requests Settings	Public/Private Behavior	ECS Public/Private Request Checking Effect
Disabled	Any	ECS オプションが有効になっていない以前のリリースと同様に、ソース IP がチェックされます。	この新しいオプションは無視されます。
On	Public/private !=	ECS は無視されま	この新しいオプショ

	All Sites	す。 ソース IP がチェックされます。	ンが有効になっている場合、これは左側に記載されている動作をオーバーライドし、ECS が使用されます。
On	Public/private = All Site	ECS がチェックされます。 ソース IP は無視されます。	この新しいオプションは無視されます。

Site Failure Handling

デフォルトでは、フェールオーバーが自動的に発生します。 ただし、複数サイトの Exchange 2010 構成など、特定の状況では、これが最適ではない可能性があり、別の動作が必要になる場合があります。 失敗遅延は分単位で設定されます。 障害遅延が設定されている場合、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

このオプションは、Failure Delay が設定されている場合にのみ使用できます。 次の 2 つのオプションがあります。

このオプションは、Failure Delay が設定されている場合にのみ使用できます。 次の 2 つのオプションがあります。

- Automatic: サイトの復旧後、サイトはすぐに運用に戻されます
- Manual: サイトに障害が発生したら、サイトを無効にします。 通常の操作を復元するには、手動による介入が必要です。

Enable Local Settings

このオプションを選択すると、TTL と Stickiness の 2 つの追加フィールドが表示されます。 これらは、FQDN ごとに、またはグローバルに設定できます。 FQDN に設定するには、ローカル設定を有効にして、必要に応じて構成します。 FQDN ごとの設定は、FQDN の作成時にデフォルトでグローバル設定の値になります。

TTL

Time To Live (TTL) 値は、GEO LoadMaster からの応答が他の DNS サーバーまたはクライアントデバイスによってキャッシュされる期間を決定します。 時間間隔は秒単位で定義されます。 この値

は、実際にはできるだけ低く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

永続性とも呼ばれる「スティッキネス」は、指定された時間が経過するまで、個々のクライアントからのすべての名前解決要求を同じリソースに送信できるよう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

このオプションを有効にすると、IP アドレスがヘルス チェックに失敗した場合、同じクラスターに属する他の FQDN IP アドレスがダウンとしてマークされます。 Unanimous Cluster Health Checks が有効になっている場合、特定の FQDN 内の同じクラスターに属する IP アドレスは、すべてアップまたはすべてダウンしています。 たとえば、example.com にはアドレス 172.21.58.101、172.21.58.102、および 172.21.58.103 があり、これらはすべてクラスター cl58 に属しています。

- 172.21.58.101 に障害が発生すると、全会一致のポリシーにより 172.21.58.102 と 172.21.58.103 も強制的に停止されます。
- 172.21.58.101 が戻ってくると、全会一致のポリシーによって 172.21.58.102 と 172.21.58.103 が一緒に返されます。

手動復旧によるサイト障害モードにも同じアプローチが適用されます。 手動回復では、失敗したアドレスが無効になるため、管理者は問題を修正した後に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、 3 つのアドレスすべてが無効になります。 全会一致のポリシーでは、無効なアドレスは無視されます。 そのため、アドレスがダウンしていることがわかっていて、何らかの理由で同じクラスターに属する他のアドレスを引き続き使用したい場合は、失敗したアドレスを無効にすることができ、全会一致のポリシーによって他のアドレスが強制的にダウンされることはありません。

Unanimous Cluster Health Checks が有効になっている場合、一部の構成変更により、FQDN アドレスが強制的に停止または再起動されることがあります。 たとえば、アドレスが強制的にダウンされ、全会一致のポリシーが有効なときにクラスタから削除すると、アドレスは回復するはずです。 同様に、全会一致ポリシーが有効で、アドレスの 1 つがダウンしているクラスタにアドレスを追加すると、新しいアドレスは強制的にダウンされます。 この変更はすぐには発生しない可能性がありますが、次回ヘルス チェックが発生したときに発生するはずです。

Checker が [None] に設定されているアドレスと、ヘルス チェックが構成されているアドレスが組

み合わされている場合、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ダウンされませんが、Site Recovery Mode が [Manual] に設定されている場合は強制的に無効にすることができます。 たとえば、次の 3 つのアドレスがあるとします。

- 172.21.58.101 with a Checker of Cluster Checks
- 172.21.58.102 with a Checker of Cluster Checks
- 172.21.58.103 with a Checker of None

サイト障害処理がオフまたは自動の場合、172.21.58.101 の障害によって 172.21.58.102 が強制的にダウンされますが、172.21.58.103 はアップしたままです。 論理的根拠は、172.21.58.103 のヘルス チェックが不要な場合は、稼働したままにしておく必要があるということです。 ただし、Site Recovery Mode が Manual に設定されている場合、172.21.58.101 の障害により、172.21.58.102 と 172.21.58.103 の両方が 172.21.58.101 とともに無効になります。 サイト リカバリの場合 – ヘルス チェックが構成されていないアドレスも含め、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解決するまで、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。 これは、稼働しているが無効になっているアドレスを持つことができるため、ヘルス チェックのないアドレスを持つことと競合しません。
FQDN の IP アドレスを作成するには、[New IP Address] テキスト ボックスにドメインの IP アドレスを入力します。

7.2.57 より前のバージョンの LoadMaster ファームウェアでは、FQDN ごとに 64 個の IP アドレスのエントリ制限があります。 LoadMaster ファームウェア バージョン 7.2.57 では、エントリの制限が 256 IP アドレスに増加しました。 これ以上追加しようとすると、FQDN の IP アドレスが 256 の制限に達したことを示すエラー メッセージが表示されます。 LoadMaster には、FQDN ごとに最大 256 個の IP アドレスを構成するための十分なメモリ スペース (最小 8 GB の RAM) が必要です。 Progress Kemp は、LoadMaster ファームウェア バージョンを、FQDN ごとの IP アドレスのエンドポイント制限が構成済み FQDN の IP アドレス数よりも小さい以前のバージョンにダウングレードすることをお勧めしません。

Cluster

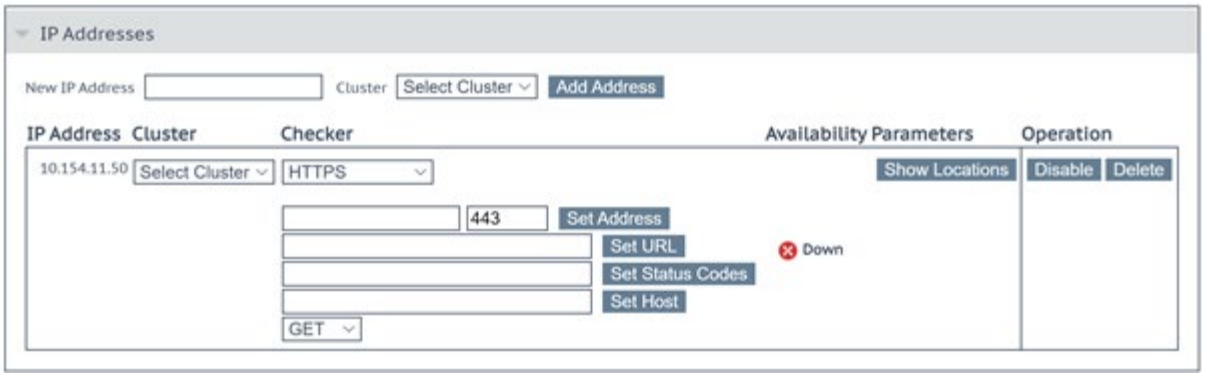
必要に応じて、IP アドレスを含むクラスターを選択できます。

Checker

これは、実行されるヘルスチェックのタイプを定義します。 オプションは次のとおりです。

- Nonce: これは、現在の FQDN に関連付けられているマシン (IP アドレス) のヘルス ステータスをチェックするヘルス チェックが実行されないことを意味します。
- ICMP Ping: IP アドレスに ping を実行して、ヘルス ステータスをテストします。
- TCP Connection: これは、指定されたポートの IP アドレスへの接続を試みることによって、正常性をテストします。
- Cluster Checks: これを選択すると、選択したクラスターに関連付けられたメソッドを使用してヘルス ステータス チェックが実行されます。
- HTTP/HTTPS: LoadMaster ファームウェア バージョン 7.2.53 では、アプリケーション配信のために LoadMaster から処理されない GEO「サイト」内のバックエンド サーバーで Layer7 (L7) HTTP および HTTPS ヘルス チェックを実行するためのサポートが追加されました。 つまり、LoadMaster によってヘルスチェックされていないバックエンド サーバーのヘルスをチェックすることで、GEO からサイトのヘルスの判断を直接強化することができます。

  HTTP/1.1 に対応しています (HTTP/1.0 には対応していません)。



HTTP または HTTPS が Checker として選択されたときに表示される使用可能なオプションは次のとおりです。

- Address: IP アドレスのヘルスチェックに使用するアドレスとポートを設定します。 デフォルトのポートは、HTTP を選択した場合は 80、HTTPS を選択した場合は 443 です。
- URL: デフォルトでは、ヘルス チェッカーは URL のスラッシュ (/) にアクセスして、マシンが使用可能かどうかを判断しようとします。 ここで別の URL を指定できます。
  - URL はスラッシュ (/) で始まる必要があります。
  - URL に http: または https: を含めることはできません。

- URL は最大 127 文字です。
- URL を空白のままにすると、デフォルトでスラッシュ (/) が送信されます。

- Status Code: サーバーから受信したときに成功として扱われる HTTP および HTTPS ステータス コードのスペース区切りのリスト。
  - コードは 300 ～ 599 の間である必要があります。
  - 最大 32 個のコードがあります。
  - 127 文字の制限があります。
- Host: サーバーへのリクエストでホスト名を指定できます。 これが設定されていない場合は、サーバー アドレスがホストとして送信されます。
  - 127 文字の制限があります。
  - 使用できる文字: 英数字および -._:
- Method: ヘルスチェック URL にアクセスするとき、システムは GET メソッドまたは POST メソッドのいずれかを使用できます。 POST を選択すると、POST データを設定する別のフィールドが表示されます。 最大 2047 文字の POST データをサーバーに渡すことができます。

ヘルスチェックのステータスが [Availability] 列に表示されます。

FQDN ごとに GEO ヘルス チェックを上書きすることはできません (仮想サービスでできるように)。 [Rules & Checking] > [Check Parameters] の [Check Parameters] は GEO には適用されません。 Global Balancing > Miscellaneous Params の設定のみが GEO に適用されます。

ヘルス チェックの詳細については、GEO 機能の説明を参照してください。

Parameters

選択基準のパラメータが説明されており、このセクション内で変更できます。 以下に説明するように、パラメータは使用中の選択基準によって異なります。

- Round Robin – 利用可能なパラメーターはありません
- Weighted Round Robin– IP アドレスの加重は、[Weight] テキスト ボックスの値を変更し、[Set Weight] ボタンをクリックして設定できます。
- Fixed Weighting – IP アドレスの重みは [Weight] テキスト ボックスで設定できます。
- Real Server Load – IP アドレスの重みは [Weight] テキスト ボックスで設定でき、測定される仮想サービスは [Mapping] フィールドから選択できます。

- Proximity – IP アドレスの物理的な位置は、[Show Coordinates] ボタンをクリックして設定できます。
- Location Based - IP アドレスに関連付けられた場所は、[Show Locations] ボタンをクリックして設定できます。

Delete IP address

該当する IP アドレスの [Operation] 列にある [Delete] ボタンをクリックすると、IP アドレスを削除できます。

Additional Records

LoadMaster ファームウェア バージョン 7.2.53 の時点で、特定の FQDN のレコードを構成するために、新しい追加レコード セクションが追加されました。 追加の TXT、CNAME、および MX レコードを FQDN に追加、変更、または削除できます。 これらのレコード タイプを使用すると、ドメイン リソースをクライアントに伝達できます。

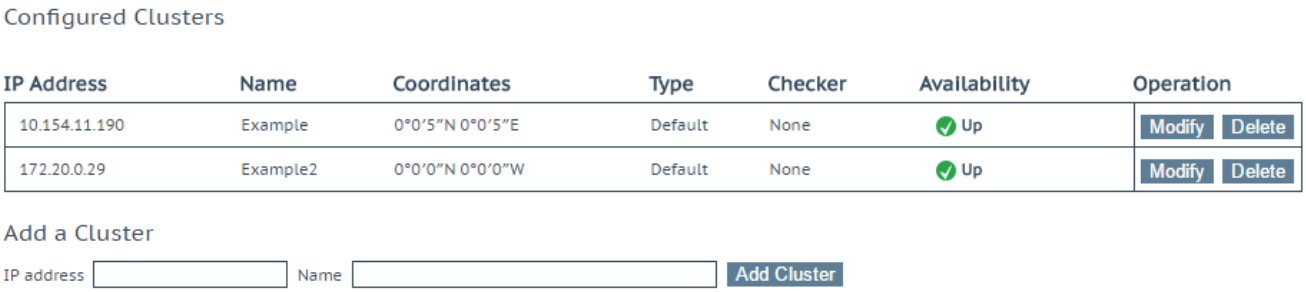
- TXT: TXT (テキスト) レコードは基本的にフォーマットされていないデータで、ほぼすべての目的に使用できますが、通常、何らかの方法でドメインを分類したり、ドメインに関する詳細を提供したり、ドメイン内で利用可能なリソースを指定したりするためにクライアントが使用する情報が含まれています。 ドメイン。
- CNAME: CNAME レコードは、DNS 名 (www.example.com など) を別の DNS 名 (lb.example.com など) にポイントします。 これは通常、Web サイトのエイリアスを定義するために使用されます。
- MX: メール エクスチェンジャー (MX) レコードは、ドメイン名に代わって電子メール メッセージを受け入れるメール サーバーを指定します。

Delete FQDN

[Modify (Configure) FQDN] 画面の下部にある [Delete] ボタンをクリックすると、FQDN を削除できます。

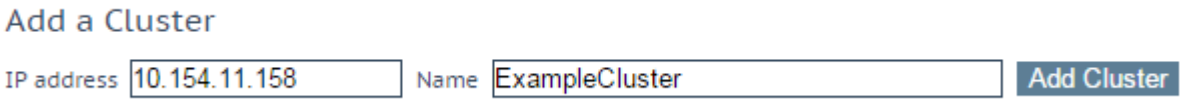
4.3 クラスターの管理

GEO クラスターは、主にデータセンター内で使用される機能です。 ヘルス チェックは、特定の FQDN に関連付けられたマシン (IP アドレス) で実行され、マシン自体ではなく、含まれているクラスター サーバーを使用します。



[Manage Cluster] 画面には、クラスターを追加、変更、および削除するためのオプションがあります。

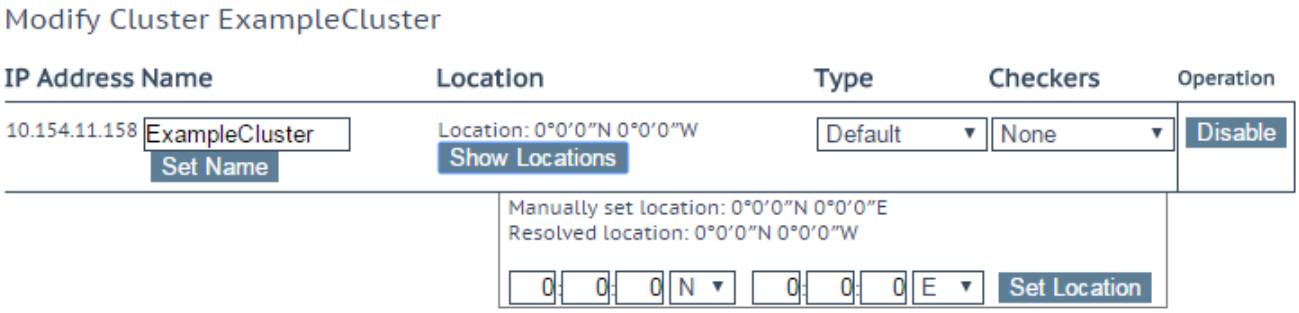
4.3.1 クラスターを追加する



クラスターを追加する場合、入力するテキスト ボックスが 2 つあります。

- IP Address – クラスターの IP アドレス
- Name – クラスターの名前。 この名前は、他の画面でクラスターを識別するために使用できます。

4.3.2 クラスターを変更する



Name

クラスターの名前。

Location

必要に応じて、[Show Locations] ボタンをクリックして、IP アドレスの場所の緯度と経度を入力で

きます。

Type

クラスタ タイプは、デフォルト、リモート LM、またはローカル LM のいずれかです。

- Default: クラスタのタイプがデフォルトに設定されている場合、次の 3 つの使用可能なヘルス チェックのいずれかを使用して、クラスタに対してチェックが実行されます。
  - None: ヘルスチェックは実行されません。 したがって、マシンは常に稼働しているように見えます。
  - ICMP Ping: クラスタ IP アドレスに対して ping を実行することにより、ヘルス チェックが実行されます。
  - TCP Connect: ヘルス チェックは、指定されたポートのクラスター IP アドレスに接続することによって実行されます。
- Local LM: Local LM が Type として選択されると、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ーのヘルスチェックは暗黙的です (SSH を使用して実行されます)。

選択基準としてリアル サーバー負荷を使用し、クラスタ タイプがローカル LM またはリモート LM に設定されている場合、[Mapping Menu] というドロップダウン リストが表示されます。マッピング メニューのドロップダウン リストには、その LoadMaster からの仮想サービス名 (利用可能な場合) と仮想サービス IP アドレスのリストが表示されます。ポートのない各仮想サービス IP アドレスと、すべての仮想 IP アドレスとポートの組み合わせが一覧表示されます。このマッピングに関連付けられている仮想 IP アドレスを選択します。ポートのない仮想サービスが選択されている場合、ヘルス チェックは、選択されたものと同じ IP アドレスを持つすべての仮想サービスをチェックします。それらのいずれかが「稼働中」ステータスの場合、FQDN は「Up」と表示されます。ポートは考慮されません。ポートを持つ仮想サービスが選択されている場合、ヘルス チェックは、FQDN のヘルスを更新するときに、その仮想サービスのヘルスに対してのみチェックします。リモート LM とローカル LM の唯一の違いは、TCP 経由ではなくローカルで情報を取得するため、TCP 接続が保存されることです。それ以外の機能は同じです。

Checkers

クラスタのステータスをチェックするために使用されるヘルス チェック メソッド。 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法は ICMP Ping と TCP Connect で

す。 [Type] として [Remote LM] または [Local LM] が選択されている場合、[Checker] ドロップダウン リストは使用できません。

Disable
必要に応じて、[Operation] 列の [Disable] ボタンをクリックしてクラスターを無効にすることができます。

4.3.3 クラスターを削除する

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

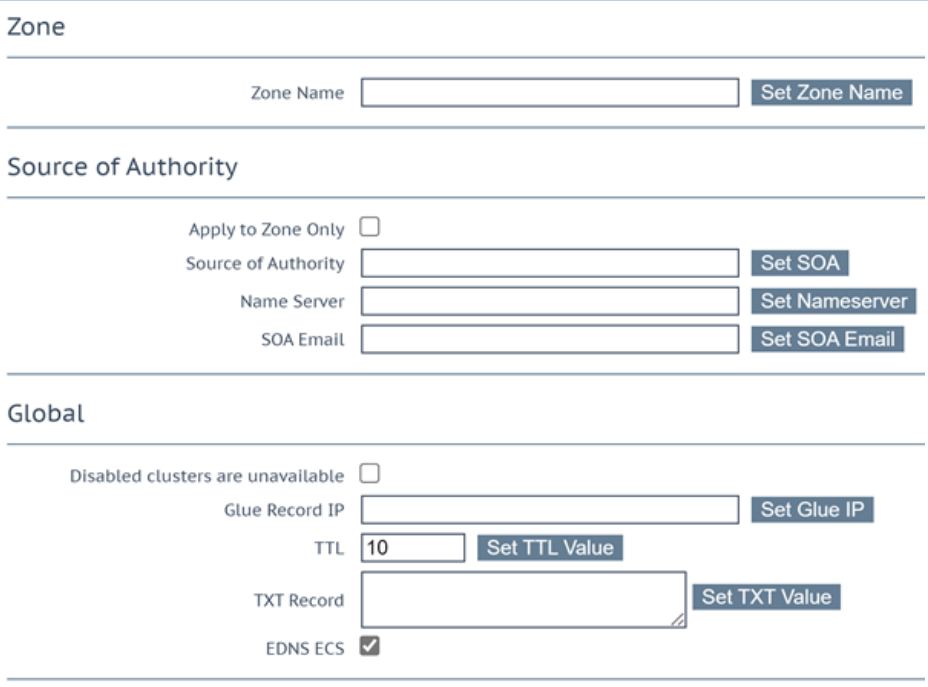
削除機能は慎重に使用してください。 この削除を元に戻す方法はありません。

4.3.4 GEO パートナーのアップグレード

GEO パートナーをアップグレードする場合は、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お勧めします。 GEO パートナーはアクティブ-アクティブ モードで動作するため、同時にアップグレードすることで、すべてのノードで一貫した動作が得られます。 バージョンが混在する GEO パートナーを運用する必要がある場合は、必ず最新バージョンからすべての変更を行ってください。 これにより、互換性のない構成による構成の損失を防ぐことができます。 さらに、古いバージョンに存在しない構成オプションを変更すると、異なる動作が発生します。

4.4 その他のパラメータ

[Miscellaneous Params] メニュー オプションのセクションとフィールドの説明を以下に示します。



Zone Name

使用するゾーン名を入力します。 DNSSEC 構成にはゾーン名が必要です。 ゾーン内のすべての FQDN は、提供されたキーを使用して署名されます。 ゾーン外のすべての FQDN は引き続き機能しますが、応答は署名されていません。

LoadMaster ファームウェア バージョン 7.2.52 では、[Zone Name] フィールドが新しい [Zone] セクションに移動し、[Apply to Zoon Only] チェック ボックスが [Source Authority] セクションに追加されました。 このオプションを有効にすると、Source of Authority (SOA) パラメータはゾーンにのみ適用されます。 無効にすると、SOA パラメータはすべての完全修飾ドメイン名 (FQDN) に適用されます。 [ゾーンのみに適用] オプションはデフォルトで無効になっています。

Source of Authority

これは 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 パラメータを定義します。 ゾーン ファイルで許可される SOA レコードは 1 つだけです。

Name Server

ネーム サーバーは、トップ レベル DNS で構成された正引き DNS エントリとして定義され、完全修飾ドメイン名 (FQDN で末尾がドット) として記述されます (例: lm1.example.com)。 HA 構成などで複数のネーム サーバーがある場合は、フィールドに 2 番目のネーム サーバーを空白で区切って追加します (例: lm1.example.com lm2.example.com)。

SOA Email

このテキストボックスは、「@」を「.」に変換して、このゾーンを扱う個人または役割アカウントのメールアドレスを公開するために使用されます。 ベスト プラクティスは、専用のメール エイリアスを定義 (および維持) することです。たとえば、「hostmaster」[RFC 2142] などの DNS 操作 (hostmaster@example.com など) を定義します。

Disabled clusters are unavailable

LoadMaster ファームウェア バージョン 7.2.53 の時点で、[Disabled clusters are unavailable] という名前の新しいチェック ボックスが導入されました。 このオプションはデフォルトで無効になっています。 有効にすると、GEO クラスターが無効になっている場合に、クラスターへの要求がドロップされます。 ユーザー インターフェイス (UI) の [Global Balancing] > [Manage FQDNs] ページのクラスター名も赤いテキストで表示されます。

Glue Record IP

LoadMaster ファームウェア バージョン 7.2.52 では、Glue Record IP と呼ばれる新しいテキスト ボックスが導入されました。これにより、ネーム サーバーの IP アドレスを設定して、DNS 応答の追加レコードで返すことができます。 [Glue Record IP] テキスト ボックスで IP アドレスが構成されていない場合、追加のレコードが必要な場合は常に 0.0.0.0 が返されます。 IPv4 と IPv6 の両方のアドレスがサポートされています。

Time To Live (TTL) 値は、GEO LoadMaster からの応答が他の DNS サーバーまたはクライアント デバイスによってキャッシュされる期間を決定します。 この値は、実際にはできるだけ低く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。このフィールドの有効範囲は 1 ～ 86400 です。時間間隔は秒単位で定義されます。

TXT Record

LoadMaster ファームウェア バージョン 7.2.52 では、TXT (テキスト) レコード タイプのサポートが GEO 機能に追加されました。 TXT (テキスト) レコードは、ほとんどすべての目的に使用できるフォーマットされていないデータですが、通常、何らかの方法でドメインを分類したり、ドメインに関する詳細を提供したり、ドメイン内で使用可能なリソースを指定したりするためにクライアントによって消費される情報が含まれています。 構成されたレコードは、完全修飾ドメイン名 (FQDN) での TXT 要求に対して返されます。 グローバル TXT レコードとして最大 127 文字を入力できます。以下は現在サポートされていません。

- レコード内の複数の文字列: 一部の DNS プロバイダーでは、"string 1" のように、引用

符を使用して 1 つのエントリに複数の文字列を入れることができます。

string 2" "string 3". Progress Kemp は現在これを許可していないため、"string 1" のみを使用できま

す。

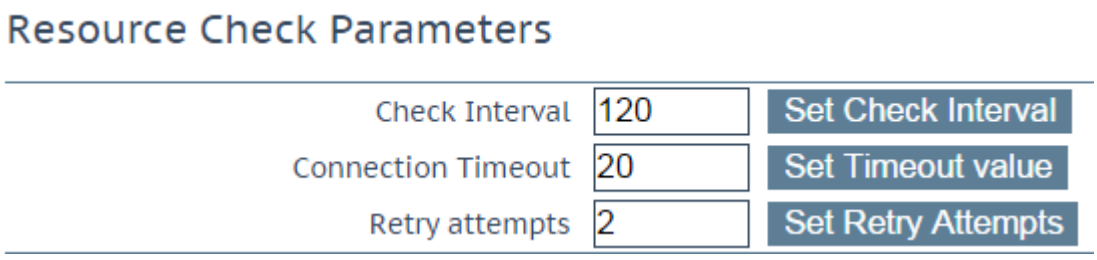
- 非 ASCII 文字。

EDNS Client Subnet (ECS)

LoadMaster ファームウェア バージョン 7.2.57 では、EDNS クライアント サブネット (ECS) という名前のチェックボックスが導入されました。 ECS は、ホストまたはクライアントに代わって DNS クエリを作成するときに、再帰的な DNS リゾルバーがサブネットワークを指定できるようにする DNS の拡張メカニズムのオプションです。 デフォルトでは、新しいインストールでは EDNS クライアント サブネット (ECS) チェックボックスが有効になっていますが、以前に GEO 機能を使用していた LoadMaster をアップグレードする場合、このオプションは無効になります。 有効にすると、ECS フィールド (リクエストに含まれている場合) を使用してクライアントの場所が特定されます。 無効にすると、このフィールドは無視されます。

EDNS が有効になっているクライアントが、EDNS が有効になっていない再帰 DNS サーバー経由で要求を送信している可能性があります。 つまり、LoadMaster が受信する UDP パケットからクライアント サブネットが削除されます。 EDNS クライアントのサブネット情報が削除された場合、LoadMaster はそれを利用できなくなります。

4.4.1 リソース チェック パラメータ



Check Interval (seconds)

ヘルスチェック試行間の秒数。 これは「Health Check Cycle」の長さを定義し、GEO クラスターと FQDN の両方に適用されます。 このフィールドの有効範囲は 9 ～ 3600 です。デフォルト値は

120 です。

間隔の値は、タイムアウト値に再試行の値を掛けた値よりも大きくする必要があります (間隔 > タイムアウト * 再試行 + 1)。 これは、前のヘルス 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。 タイムアウトまたは再試行の値がこの規則に違反する値まで増加すると、間隔の値が自動的に増加します。

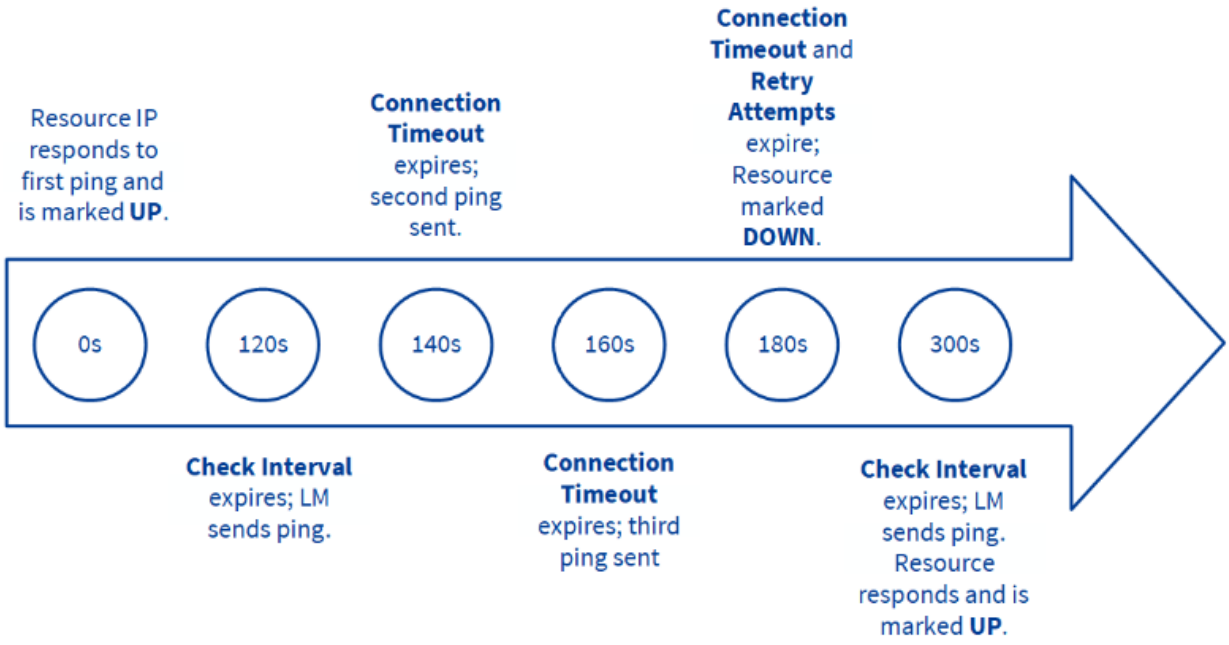
Connection Timeout (seconds)

これは、接続が確立され、ヘルスチェックへの応答が受信されるまでに許容される最大待機時間です。タイムアウトになる前に応答が受信されない場合、再試行回数に達していない限り、接続が再試行されます。 ヘルス チェックに対する HTTP 応答が受信された場合、現在のヘルス チェック サイクルでは再試行は行われません。 このフィールドの有効範囲は 4 ～ 60 です。デフォルト値は 20 です。

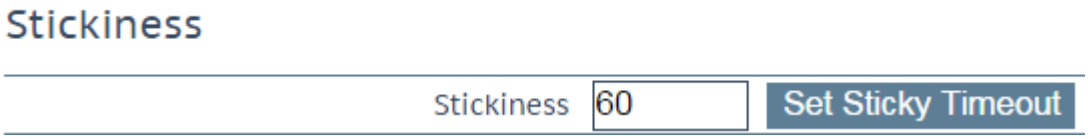
Retry Attempts

これは、応答を受信する前に上記のタイムアウトに達した場合にヘルスチェックを再試行する回数を指定します。 デフォルトの再試行回数は 2 回です。ヘルス チェックに対する応答が受信された場合、再試行回数は適用されません。 たとえば、200 または 404 応答を受信した場合、現在のサイクルでは再試行は行われません。 FQDN の失敗したクラスターの最大検出ウィンドウは、チェック間隔 (接続タイムアウト * (再試行回数 + 1)) です。 平均して、最大時間はその半分です。 以下のタイムライン ダイアグラムは、リソース IP が追加または有効化されてから、ダウンしてから再びアップするまでに何が起こるかを示しています。

1. リソース IP が有効化/作成されると、LoadMaster によって ICMP リクエストがリソース IP に送信されます。 応答すると仮定すると、リソースは UP とマークされます。
2. 120 秒 (デフォルトのチェック間隔) が経過すると、ICMP 要求がリソース IP に送信されます。 20 秒 (デフォルトの接続タイムアウト) が経過しても IP が応答しない場合、LoadMaster は最大 2 つの追加の要求 (デフォルトの再試行回数) を送信し、それぞれの間で 20 秒間待機します。 これらの 3 つの要求すべてが応答を受信しない場合、リソースはダウンとマークされ、チェック間隔タイマーがリセットされます。
3. 120 秒が経過すると、LoadMaster は ICMP リクエストをリソース IP に送信しようとします。 リソースが復旧し、接続タイムアウトが経過する前に応答した場合、LoadMaster はそれを UP とマークし、Check Interval タイマーをリセットします。

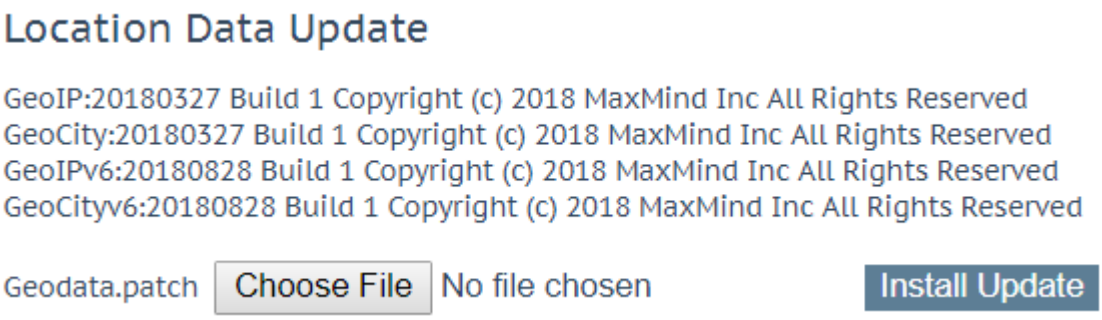


4.4.2 スティッキネス



Global Persistence とも呼ばれる「Stickiness」は、指定された時間が経過するまで、個々のクライアントからのすべての名前解決要求を同じリソースに送信できるよう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。

4.4.3 位置データの更新



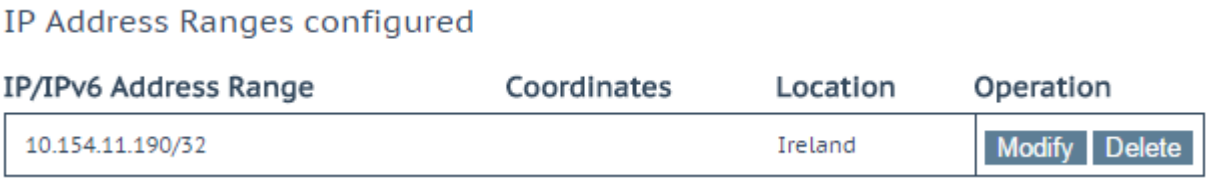
ロケーション パッチには、地理的にエンコードされた IP からロケーション データへのデータが含ま

れています。 データ ファイルは、通常のサポート チャネルを使用して Progress Kemp から直接取得できます。 これらのファイルは、MaxMind の再パッケージ化されたディストリビューションです。 GeoIP データベース。

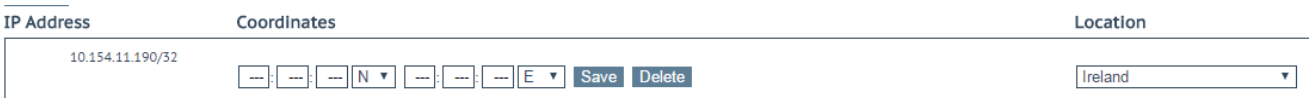
従来の MaxMind GeoLite データベースは、LoadMaster バージョン 7.2.44 以下でのみサポートされています。 新しい MaxMind GeoLite2 データベースは、LoadMaster バージョン 7.2.45 以降でのみサポートされています。
最新のリリースを入手するには、サポートにお問い合わせください:
https://kemptechnologies.com/support.

4.5 IP 範囲の選択基準

IP 範囲選択基準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。



アドレスを追加した後、[Modify] をクリックすると、設定の変更画面が開きます。 追加した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 の IP 範囲を定義できます。

IP Address

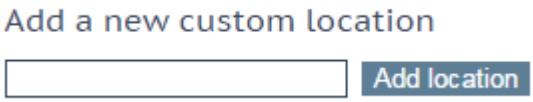
IP アドレスまたはネットワークを指定します。 ここで有効なエントリは、単一の IP (192.168.0.1 など)、または Classless Inter-Domain Routing (CIDR) 形式のネットワーク (192.168.0.0/24 など) です。

Coordinates

場所の緯度と経度を指定します。

Location

アドレスに割り当てる場所を指定します。



Add Custom Location

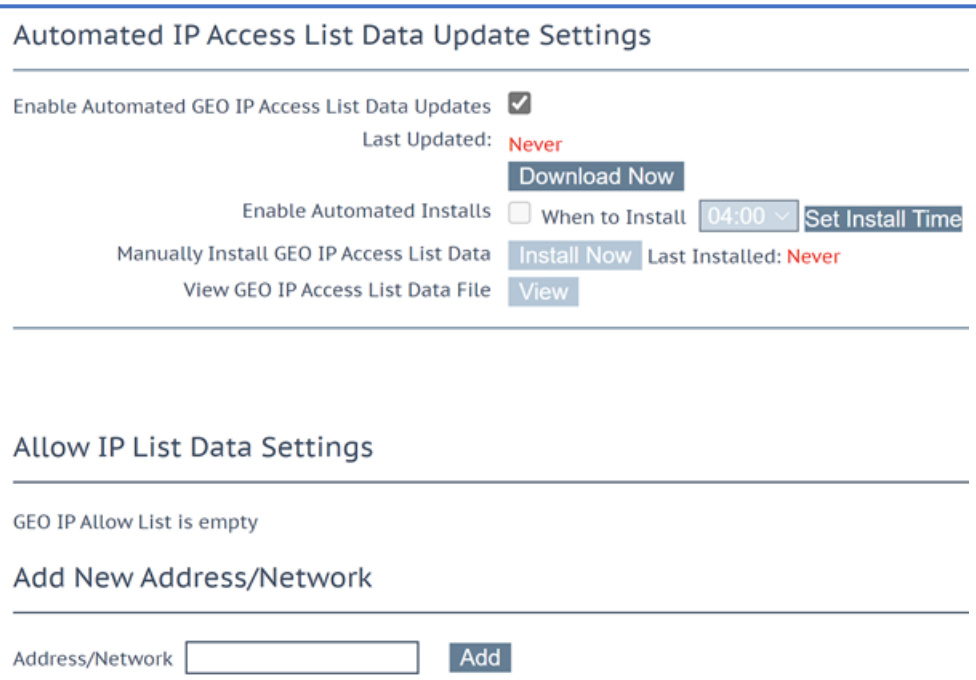
このセクションでは、カスタムの場所を追加できます。

既存のカスタム ロケーションも、このセクションで変更および削除できます。

4.6 IP アクセス リストの設定

Progress Kemp からアクセス リスト ルールをダウンロードして、アクセス リストにある IP アドレスからのアクセスをブロックすることができます。 アクセス リストを上書きする許可リストを手動で指定できます。

これはライセンス可能な機能です。 これらのオプションが表示されない場合、またはグレー表示されているフィールドがある場合は、Progress Kemp 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 Access List Data Updates

このオプションを有効にすると、GEO IP アクセス リストの更新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

最後のアップデートがダウンロードされた日付が表示されます。 GEO アクセス リスト データが 7 日以上経過している場合は、それを通知するメッセージが表示されます。

Download Now

このボタンをクリックして、アップデートを今すぐダウンロードします。

Enable Automated Installs

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

When to Install

毎日アップデートをインストールする時間を選択します。

Manually Install GEO IP Access List Data

このボタンを使用すると、更新を手動でインストールできます。 このセクションには、更新プログラムが最後にインストールされた日時も表示されます。 GEO アクセス リスト データが 7 日以上更新されていない場合、通知するメッセージが表示されます。

View GEO IP Access List Data File

[View] ボタンをクリックすると、現在の GEO IP アクセス リスト データ ファイルが表示されます。

Allow IP List Data Settings

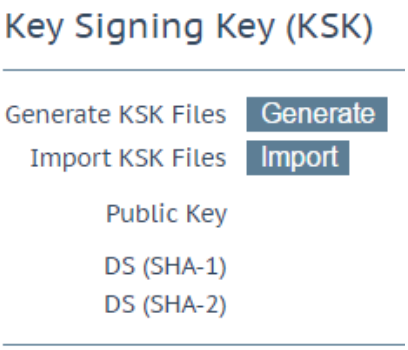
このセクションには、現在許可リストにある IP アドレスが表示されます。

Add New Address/Network

このセクションでは、新しいアドレスとネットワークを許可リストに追加できます。 許可リストは、アクセス リストを上書きします。

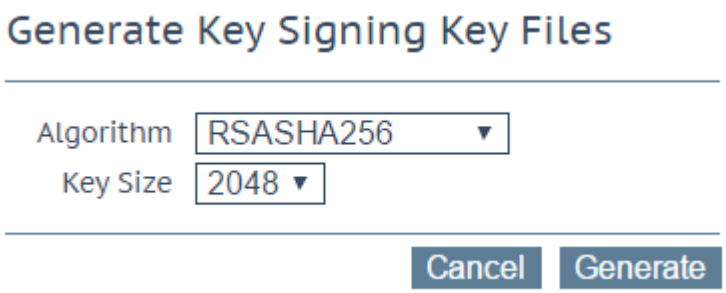
4.7 DNSSEC の構成

DNSSEC を構成する前に、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 のパラメータに移動し、ゾーン名を指定します。



ゾーン名を定義したら、鍵署名鍵 (KSK) を構成する必要があります。 2 つの選択肢があります。次のいずれかを実行できます。

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



生成画面で、暗号化アルゴリズムと鍵サイズを選択します。 次のアルゴリズムがサポートされています。

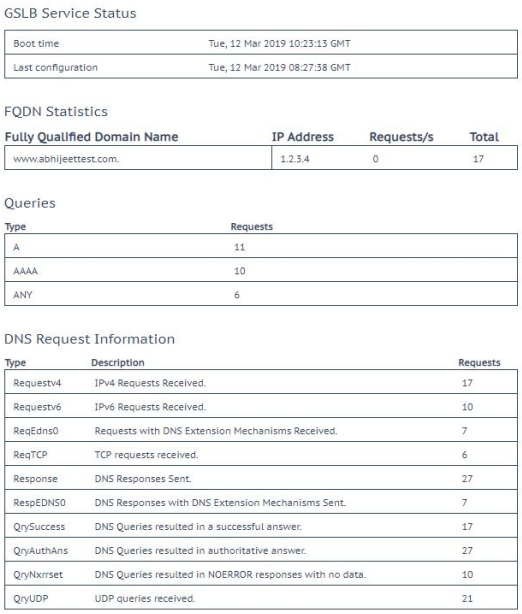
- NSEC3RSASHA1
- RSASHA256
- RSASHA512

デフォルトは RSASHA256 です。 サポートされている鍵のサイズは、1024、2048、および 4096 ビットです。 デフォルトは 2048 です。

KSK ファイルが生成/インポートされると、DNSSEC 画面に KSK の詳細が表示され、KSK ファイルを削除するオプションが表示されます。 最後のステップは、チェックボックスを選択して DNSSEC を有効にすることです。

4.8 GSLB 統計

GSLB 統計画面（メイン メニューの [Global Balancing] セクションからアクセス可能）は、サイトの回復力とハイブリッド トラフィック分散を可能にする GSLB コンポーネントの集中スナップショットです。



GSLB Service Status

Boot time	Tue, 12 Mar 2019 10:23:13 GMT
Last configuration	Tue, 12 Mar 2019 08:27:38 GMT

FQDN Statistics

Fully Qualified Domain Name	IP Address	Requests/s	Total
www.abhijeettest.com.	1.2.3.4	0	17

Queries

Type	Requests
A	11
AAAA	10
ANY	6

DNS Request Information

Type	Description	Requests
Requestv4	IPv4 Requests Received.	17
Requestv6	IPv6 Requests Received.	10
ReqEdns0	Requests with DNS Extension Mechanisms Received.	7
ReqTCP	TCP requests received.	6
Response	DNS Responses Sent.	27
RespEDNS0	DNS Responses with DNS Extension Mechanisms Sent.	7
QrySuccess	DNS Queries resulted in a successful answer.	17
QryAuthAns	DNS Queries resulted in authoritative answer.	27
QryNxrrset	DNS Queries resulted in NOERROR responses with no data.	10
QryUDP	UDP queries received.	21

次のセクションが GSLB 統計画面に表示されます。

- GSLB Service Status: 起動時間（バインド デバイスの開始時間）と最終構成（構成が最後に変更された日時）を表示します。
- FQDN：statistics: FQDN 構成と IP アドレス情報を表示します。
- Queries: 受信したさまざまな DNS クエリの種類を表示します。
- DNS Request Information: DNS リクエストのタイプを説明とリクエスト数とともに表示します。

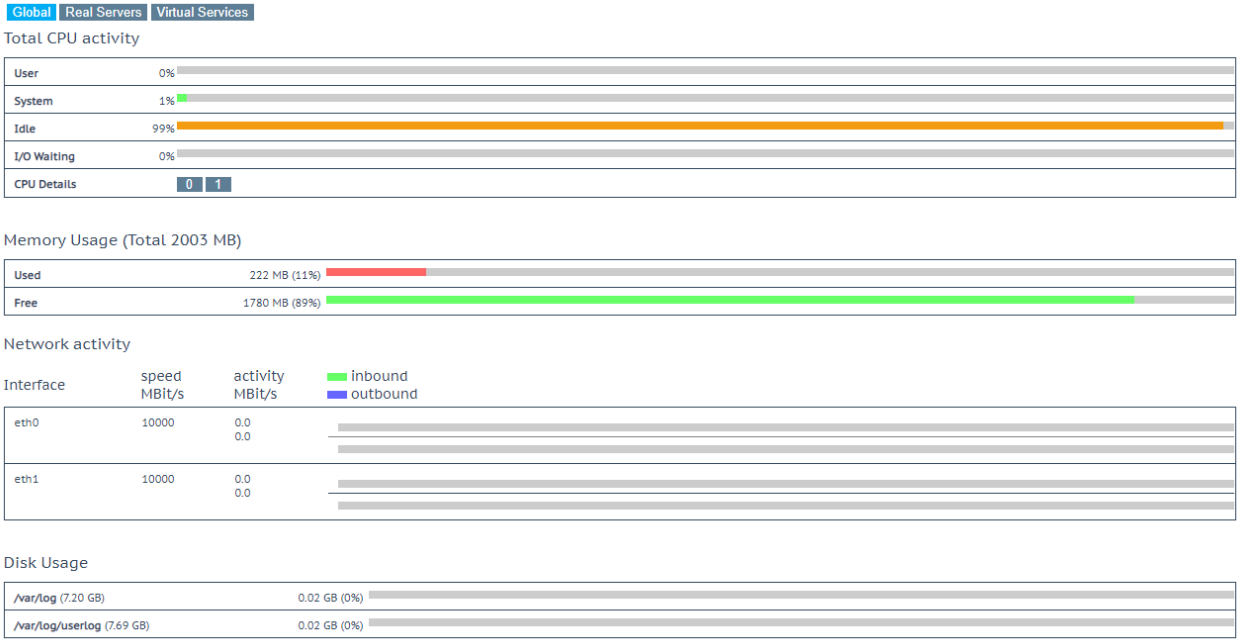
GSLB を無効にして再度有効にすると、GSLB 統計はゼロにリセットされます。

5 統計

5.1 リアルタイム統計

システム内のロードマスター（グローバル）、実サーバー、仮想サービス、WAF、およびクライアント制限のアクティビティを表示します。

5.1.1 グローバル



Total CPU Activity

このテーブルには、特定の LoadMaster の次の CPU 使用率情報が表示されます。

Statistic	説明
User	ユーザーモードで処理に費やされた CPU の割合
System	システム モードで処理に費やされた CPU の割合
Idle	アイドル状態の CPU の割合
I/O Waiting	I/O の完了を待機するために費やされた CPU の割合

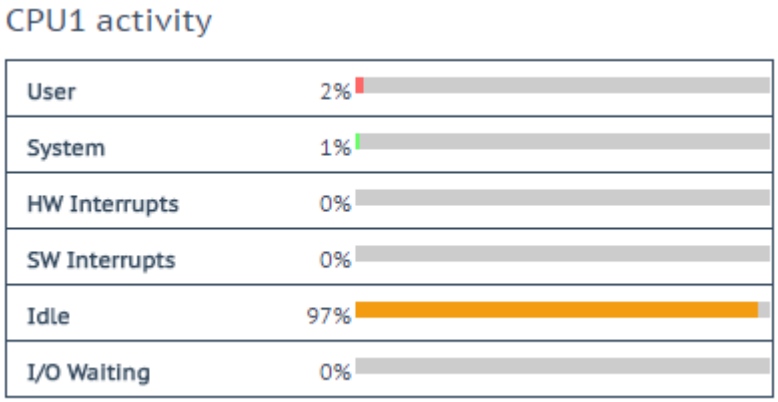
これら 4 つのパーセンテージの合計は 100% です。

Core Temperatures:

Core Temperatures: LoadMaster ハードウェア アプライアンスの各 CPU コアの温度が表示されます。 Virtual LoadMaster の統計画面に温度が表示されません。

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

CPU Details: 個々の CPU の統計を取得するには、[CPU Details] で関連する番号のボタンをクリックします。



CPU の詳細画面には、HW 割り込みと SW 割り込みの 2 つの追加統計が表示されます。

Memory usage

この棒グラフは、使用中のメモリ量と空きメモリ量のパーセンテージ (MB) を示しています。

Network activity

これらの棒グラフは、各インターフェイスの現在のネットワーク スループットを示します。

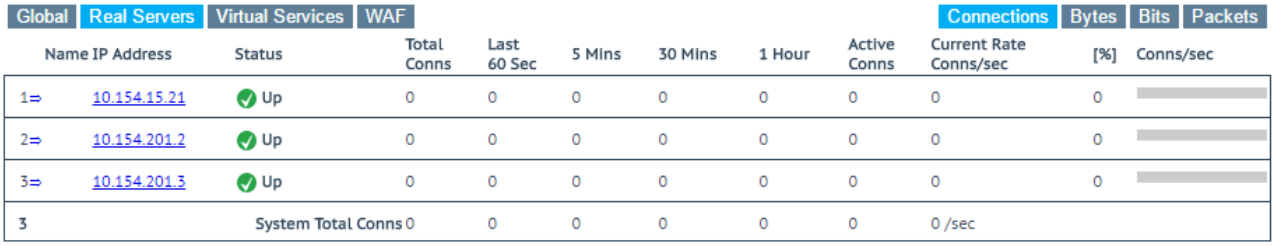
Elastic Network Adapter (ENA) ドライバー インターフェイスの場合、表示される速度は、インターフェイス全体の速度がそのインターフェイスで定義された個別の論理インターフェイスの数の総計であるという点で、結合されたインターフェイスと同様に動作します。

Disk Usage

このセクションには、ログ パーティションの使用済み/空きの割合 (GB) が表示されます。 色分けは、さまざまな使用レベルを強調するために使用されます。

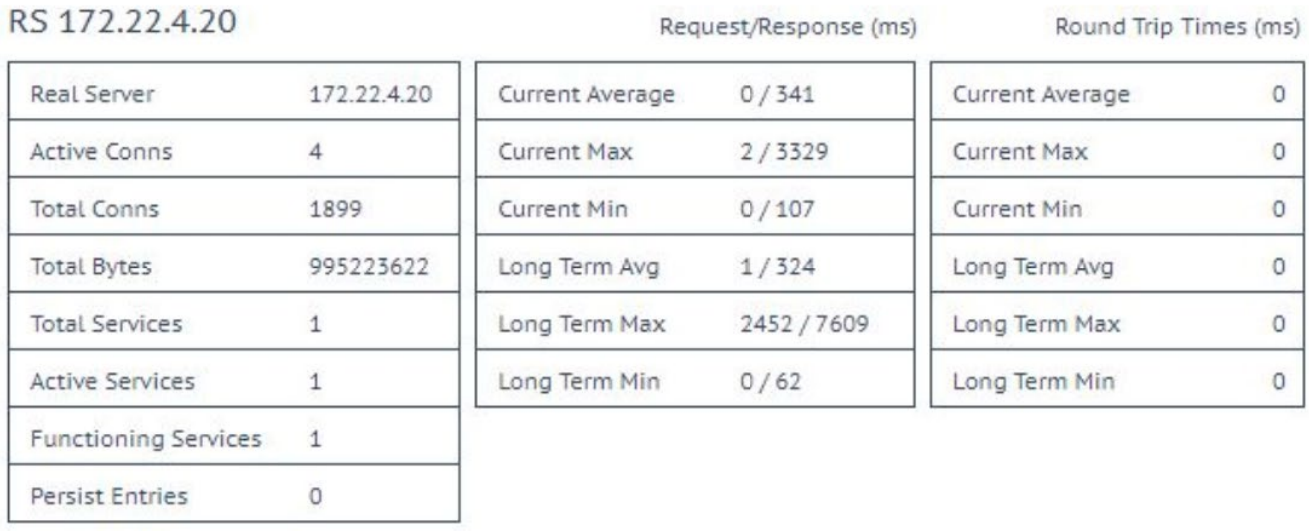
- 0% to 50%: 緑
- 50% to 90%: オレンジ
- 90% to 100%: 赤

5.1.2 リアルサーバー



これらのグラフには、選択に応じて、接続、バイト、ビット、またはパケットが表示されます。 ページの右上にあるボタンは、表示される値を切り替えます。 実サーバーに表示される値
実サーバーにアクセスするすべての仮想サービスの値で構成されます。 実サーバーが複数の仮想サービスに割り当てられている場合、最初の列の数字の右にある矢印（**=>** ）をクリックすると、仮想サービスごとに各実サーバーの統計を表示できます。 これにより、ビューが展開され、実サーバー上の各仮想サービスの統計が表示されます。

暗号化されたサービスの実装方法が原因で、暗号化された仮想サービスのパケット統計を表示することはできません。
Name: [Name] 列は、DNS ルックアップに基づいて自動的に入力されます。
IP Address: この列には、実サーバーの IP アドレスが表示されます。



[IP Address] 列のリンクをクリックすると、その実サーバーに固有の多数の統計を含む別の画面が表示されます。 LoadMaster と Real Server 間の往復時間が表示されます。 実サーバーのパフォーマ

ンスは、次の 2 つの測定値で監視されます。

- Real Server が要求に応答するのにかかる時間 (最初のバイト)。
- Real Server がすべてのデータ (最後のバイト) を送信するのにかかる時間 - 応答時間。

上の図では、リクエスト/レスポンスの現在の最大値は 2 / 3329 です。これは、実サーバーがリクエスト (最初のバイト) に応答するのに最大 2 ミリ秒かかり、すべてのデータを送信するのに最大 3329 ミリ秒かかったことを意味します。 応答時間の測定。

再暗号化を使用している場合、サーバーへのラウンドトリップ時間 (RTT) は測定できません。 使用されているサービスが HTTP-HTTP/2-HTTPS サービスでない場合、要求/応答時間は適用されません。 [Debug Options] 画面 ([System Configuration] > [System Administration] > [System Log Files] > [Debug Options]) で [Reset Statistics] をクリックすると、すべての値がクリアされます。

各 RTT または要求/応答時間について、次の値が測定されます。

- Current Avarage: 過去 5 秒間 (または統計が最後にリセットされてから) の平均時間 (ミリ秒 (ms))。
- Current Max: 現在の最大時間 (ミリ秒単位) - 過去 5 秒間 (または最後の統計のリセット以降)。
- Current Min: 現在の最小時間 (ミリ秒単位) - 過去 5 秒間 (または最後の統計のリセット以降)。
- Long Term Avg: 仮想サービスがトラフィックの処理を開始してから (または最後の統計がリセットされてから) の期間全体の平均時間。
- Long Term Max: 仮想サービスがトラフィックの処理を開始してから (または最後の統計がリセットされてから) の全時間の最大値 (ミリ秒単位)。
- Long Term Min: 史上最小値 (ミリ秒単位) (または最後の統計のリセット以降)。

値が記録されている場合にのみ、値が存在します。 たとえば、過去 5 秒間に仮想サービスを通過したトラフィックがない場合、または仮想サービスが特定の値を監視できない場合、現在の最大値は表示されません。

仮想サービスおよび実サーバーの現在の平均、現在の最大値、現在の最小値、長期の平均値、長期の最

大値、および長期の最小値も SNMP 経由で利用できます。

Status: 実サーバーのステータスを示します。
Adaptive: これは、仮想サービスに対して適応スケジューリング方法が選択されている場合にのみ表示されます。この列には適応値が表示されます。
Weight: これは、スケジューリング方法が仮想サービスでリソース ベース (SDN アダプティブ) に設定されている場合にのみ表示されます。コントローラーから収集された情報によって、適応値が何に設定されるかが決まります。適応値が上がると、実サーバーの重みが下がります。すべての適応値が同じ場合、すべての重みは同じです。適応値が異なると、重みが変わります。実サーバーの重みによって、トラフィックの送信先が決まります。実サーバーが複数の仮想サービスで構成されている場合、重みに対して 2 つの数値が表示されます。1 つ目は、実サーバーが構成されているすべての仮想サービスの現在の重みの平均を示します。2 つ目は、実サーバーが構成されている仮想サービスの数を示します。実サーバーはで構成されています。たとえば、972/2 の重量は、実サーバーの平均重量が 2 つの仮想サービスで構成されているのは 972 です。
Total Conns: 確立された接続の総数。

レイヤー 4 UDP 接続の場合、接続数は常に 0 と表示されます。

- Last 60 Sec: 過去 60 秒間の合計接続数。
- 5 Mins: 過去 5 分間の合計接続数。
- 30 Mins: 過去 30 分間の合計接続数。
- 1 Hour: 過去 1 時間の合計接続数。
- Active Conns: 現在アクティブな接続の総数。

ESP を使用する場合、ログイン プロセスを通過するすべての接続は、仮想サービスのアクティブな接続としてカウントされます。 それらは実サーバーへの実際の接続ではないため、実サーバーのアクティブな接続としてカウントされません。 WUI ページには実サーバーに関連付けられたアクティブな接続の数が表示され、SNMP には仮想サーバーのアクティブな接続の数が表示されます。
サービス。 API は、WUI に表示されるものと同じ値を返します。 ESP がない場合、これらの値は同一です。 ESP を使用する場合、上記の理由により、仮想サービスの数が実サーバーに送られる最終的な数よりもはるかに多くなる可能性があります。

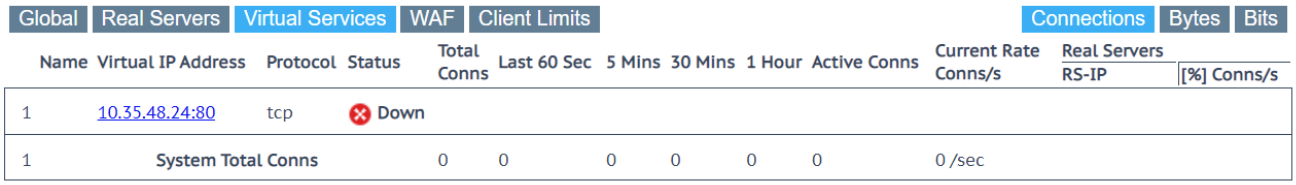
Current Rate Conns/sec: 現在の 1 秒あたりの接続数。

[%]: 1 秒あたりの接続数の割合。

Conns/sec: 1 秒あたりの接続数のグラフ表示。

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

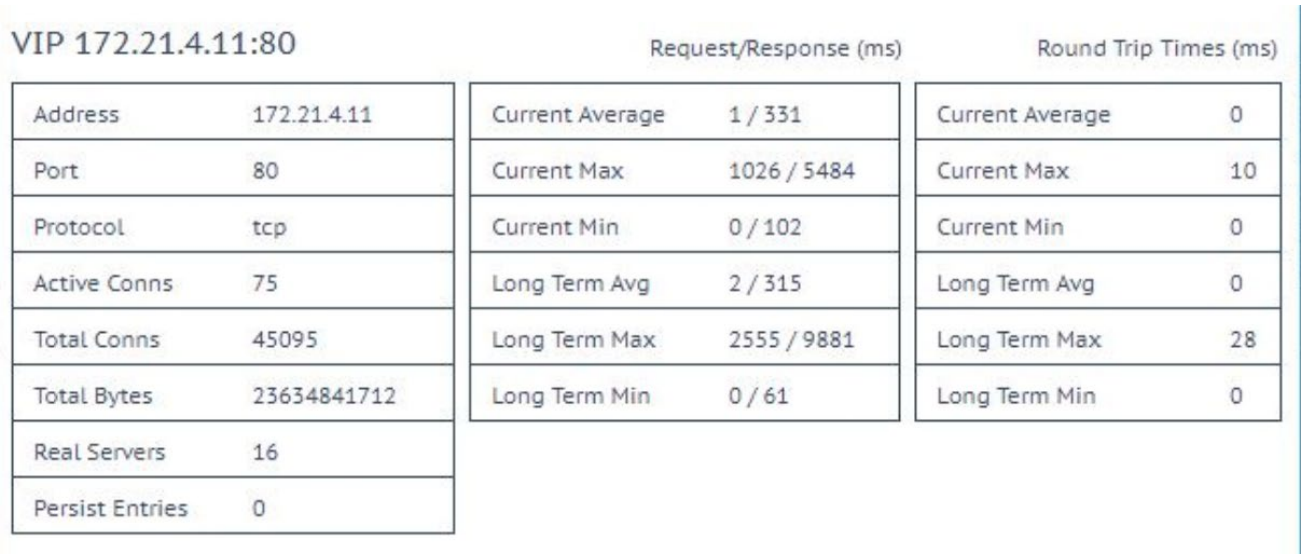
5.1.3 仮想サービス



これらのグラフには、選択に応じて、接続、バイト、ビット、またはパケットが表示されます。 ページの右上にあるボタンは、表示される値を切り替えます。 仮想サービスの実サーバー全体の分散のパーセンテージが表示されます。

Name: 仮想サービスの名前。

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



[Virtual IP Address] 列のリンクをクリックすると、その仮想サービスに固有の多数の統計を含む別の画面が表示されます。 クライアントと LoadMaster 間の往復時間が表示されます。 仮想サービスのパフォーマンスは、次の 2 つの測定値で監視されます。

- 仮想サービスがリクエストに応答するのにかかる時間 (最初のバイト)。
- 仮想サービスがすべてのデータ (最後のバイト) を送信するのにかかる時間 - 応答時間。

上の図では、要求/応答の現在の最大値は 1026 / 5484 です。これは、実サーバーが要求 (最初のバ

イト) に応答するのに最大 1026 ミリ秒かかり、すべてのデータを送信するのに最大 5484 ミリ秒かかったことを意味します。 応答時間の測定。 仮想サービス統計では、次の制限統計も利用できます。

- Conns/Sec Blocked
- Req/Sec Blocked
- MaxConns Blocked

[Debug Options] 画面 ([System Configuration] > [System Administration] > [System Log Files] > [Debug Options]) で [Reset Statistics] をクリックすると、すべての値がクリアされます。

各 RTT または要求/応答時間について、次の値が測定されます。

- Current Average: 過去 5 秒間 (または統計が最後にリセットされてから) の平均時間 (ミリ秒 (ms))。
- Current Max: 現在の最大時間 (ミリ秒単位) - 過去 5 秒間 (または最後の統計のリセット以降)。
- Current Min: 現在の最小時間 (ミリ秒単位) - 過去 5 秒間 (または最後の統計のリセット以降)。
- Long Term Avg: 仮想サービスがトラフィックの処理を開始してから (または最後の統計がリセットされてから) の期間全体の平均時間。
- Long Term Max: 仮想サービスがトラフィックの処理を開始してから (または最後の統計がリセットされてから) の全時間の最大値 (ミリ秒単位)。
- Long Term Min: 史上最小値 (ミリ秒単位) (または最後の統計のリセット以降)。

値が記録されている場合にのみ、値が存在します。 たとえば、過去 5 秒間に仮想サービスを通過したトラフィックがない場合、または仮想サービスが特定の値を監視できない場合、現在の最大値は表示されません。

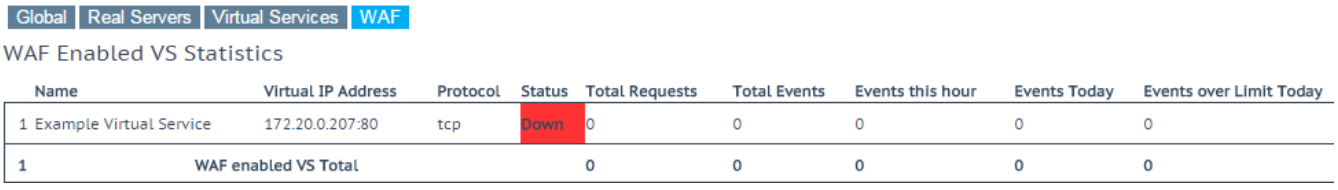
- Address: 仮想サービスの IP アドレス。
- Protocol: 仮想サービスのプロトコル。 これは、tcp または udp のいずれかになります。
- Active Conns: 現在アクティブな接続の総数。

ESP を使用する場合、ログイン プロセスを通過するすべての接続は、仮想サービスのアクティブな接

続としてカウントされます。 それらは実サーバーへの実際の接続ではないため、実サーバーのアクティブな接続としてカウントされません。 WUI ページには実サーバーに関連付けられたアクティブな接続の数が表示され、SNMP には仮想サーバーのアクティブな接続の数が表示されます。
サービス。 API は、WUI に表示されるものと同じ値を返します。 ESP がない場合、これらの値は同一です。 ESP を使用する場合、上記の理由により、仮想サービスの数が実サーバーに送られる最終的な数よりもはるかに多くなる可能性があります。

Total Conns: 確立された接続の総数。
Total Bytes: 送信された総バイト数。
Real Server: この仮想サービス内の実サーバーの総数。
Persist Entries: 作成された永続エントリの総数。
WAF: 仮想サービスで WAF が有効になっている場合、ステータスは、以下の他の WAF 統計とともに表示されます。
Request: WAF によって処理されたリクエストの総数 (ブロックされたかどうかにかかわらず、すべてのリクエストを表示します)。接続ごとに 2 つの要求が記録されます。1 つの着信要求と 1 つの発信要求です。
Incident: WAF によって処理されたイベント (つまり、ブロックされた要求) の総数。
インシデント/時間: 現在の時間 (xx.00.00 以降) に発生したイベントの数。
インシデント/日: 午前 0 時 (現地時間) 以降に発生したイベントの数。
Incidents/Dayover: 今日、イベント カウンターが設定された警告しきい値を超えた回数。たとえば、しきい値が 10 に設定され、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。仮想サービスの変更画面。詳細については、「レガシー Web アプリケーション ファイアウォール (WAF) オプション」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



これらの統計は、5 ～ 6 秒ごとに更新されます。 この画面には次の項目が表示されます。

Count: 一番左の列には、WAF 対応の仮想サービスの総数が表示されます。

Name: WAF 対応の仮想サービスの名前。

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

Protocol: 仮想サービスのプロトコル (tcp または udp)。

Status: 仮想サービスのステータス。考えられる各ステータスの詳細については、「表示/変更 (既存の HTTP サービス)」セクションを参照してください。

リクエストの総数: WAF によって処理されたリクエストの総数 (ブロックされたかどうかにかかわらず、すべてのリクエストを表示します)。接続ごとに 2 つの要求が記録されます。1 つの着信要求と 1 つの発信要求です。

Total Events: WAF によって処理されたイベント (ブロックされた要求) の総数。

この時間のイベント: 現在の時間 (xx.00.00 以降) に発生したイベントの数。

今日のイベント: 午前 0 時 (現地時間) 以降に発生したイベントの数。

Events over Limit Today: 今日、イベント カウンターが設定された警告しきい値を超えた回数。たとえば、しきい値が 10 に設定され、20 個のイベントが発生した場合、このカウンターは 2 に設定されます。仮想サービスの変更画面。詳細については、「レガシー Web アプリケーション ファイアウォール (WAF) オプション」セクションを参照してください。

5.1.5 クライアントの制限

[Client Limits] ボタン ([Statistics] > [Real statistics] の下) は、[System Configuration] >

[QoS/Limiting] 画面で少なくとも 1 つのクライアント制限が有効になっている場合にのみ表示されます。 統計は、[System Configuration] > [QoS/Limiting] > [Limiter Options] で [Generate Limiter Statistics] チェック ボックスがオンになっている場合にのみ生成されます。 統計は 10 秒ごとに更新されます。 Client Limits 統計画面の右側にあるボタンで、Total Connections と Bandwidth Usage の別のページを選択できます。

これらのボタンは、対応するクライアント制限が System Configuration >QoS/Limiting で設定されている場合にのみ表示されます。

過去 30 秒、過去 5 分間、および過去 30 分間の上位 10 クライアントが表示されます。 OK 接続とブロックされた接続の数を示す別の列があります。 これらの洞察に基づいて、特定のクライアント IP アドレスに対して特定のレート制御を構成できます。

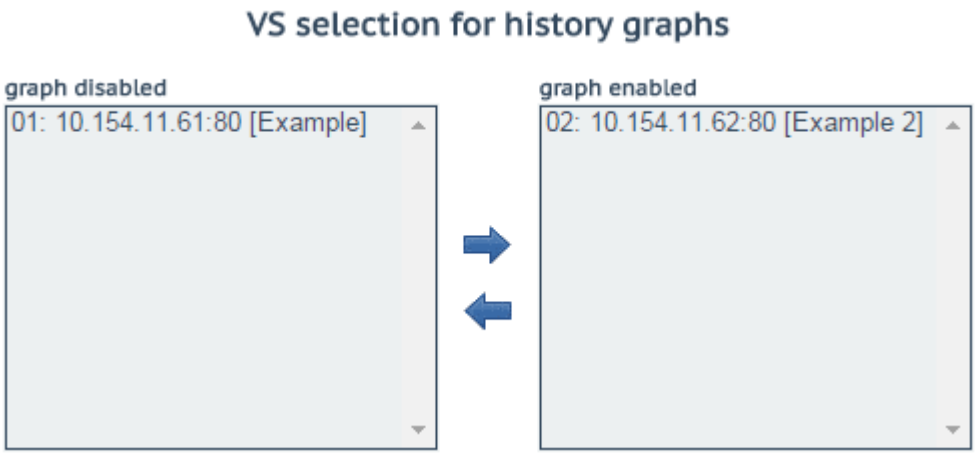
5.2 履歴グラフ

[Historical Graphs] 画面には、LoadMaster の統計がグラフィカルに表示されます。 これらの構成可能なグラフは、LoadMaster によって処理されているトラフィックを視覚的に示します。

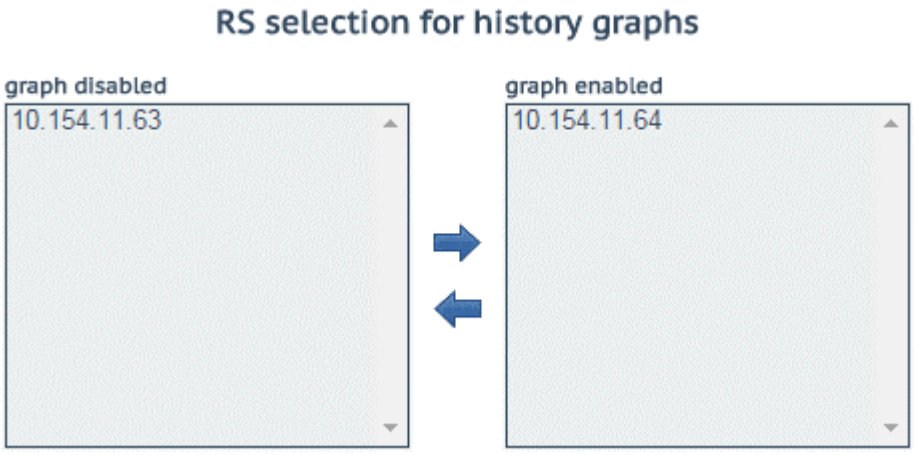
場合によっては、LoadMaster ファームウェアをバージョン 7.1.35 から新しいファームウェア バージョンにアップグレードした後、履歴グラフが表示されないことがあります。 これを修正するには、統計カウンターをリセットします ([System Configuration] > [Extended Log Files] > [System Log Files] > [Debug Options] > [Reset Statistics])。

各インターフェイスのネットワーク アクティビティのグラフがあります。 仮想サービス全体と個々の仮想サービス、および実サーバー全体と個々のグラフを表示するオプションもあります。 時間の粒度は、時間、日、月、四半期、または年のオプションのいずれかを選択して指定できます。 インターフェイス グラフのネットワーク アクティビティの場合、パケット、ビット、またはバイト オプションのいずれかを選択して、使用する測定単位のタイプを選択できます。
仮想サービスと実サーバーのグラフでは、接続、ビット、またはバイト オプションのいずれかを選択して、使用する測定単位のタイプを選択できます。 仮想サービス パネルの構成アイコン をクリックして、どの仮想サービス統計を表示するかを構成できます。 これにより、仮想サービスの構成ウ

ィンドウが開きます。



ここから、統計表示から仮想サービスを追加または削除できます。 これらのグラフを無効にするには、[WUI Settings] 画面の [Enable Historical Graphics] チェック ボックスを無効にします。 同時に最大 5 つの仮想サービスを表示できます。 ダイアログを閉じて変更を適用するには、必ずウィンドウ内のボタンをクリックしてください。



Real Servers パネルの設定アイコンをクリック すると、表示される Real Server 統計を設定できます。 これにより、実サーバー構成ダイアログが別のウィンドウで開きます。 ここから、Real Server を追加したり、統計表示から削除したりできます。

同時に最大 5 つのリアル サーバーを表示できます。

ダイアログを閉じて変更を適用するには、ウィンドウ内のボタンをクリックしてください。 デフォルトでは、仮想サービスと実サーバーの統計のみが統計に表示されます。
ページをまとめて保存します。 すべての仮想サービスと実サーバーの統計を表示するには、[System Configuration] > [Miscellaneous Options] > [WUI Settings] で Collect All Statistics [] オプションを有効にします。

多数の仮想サービスおよび実サーバーの統計を収集すると、CPU 使用率が非常に高くなる可能性があるため、このオプションはデフォルトで無効になっています。

LoadMaster WUI のグラフは自動スケーリングで、SI マグニチュード単位を使用して表示されます。 必要に応じて絶対値を計算できるように、使用される倍率の接頭辞がグラフに表示されます。 可能な倍率とそのプレフィックスを次の表に示します。

Symbol	Prefix	Factor
P	Peta	10^15
T	tera	0^12
G	giga	10^9
M	Mega	10^6
k	Kilo	10^3
m	Milli	10^(-3
µ	micro	10^(-6)

絶対的な「実際の」値を計算するには、グラフに示されている値にスケーリング値を掛けます。

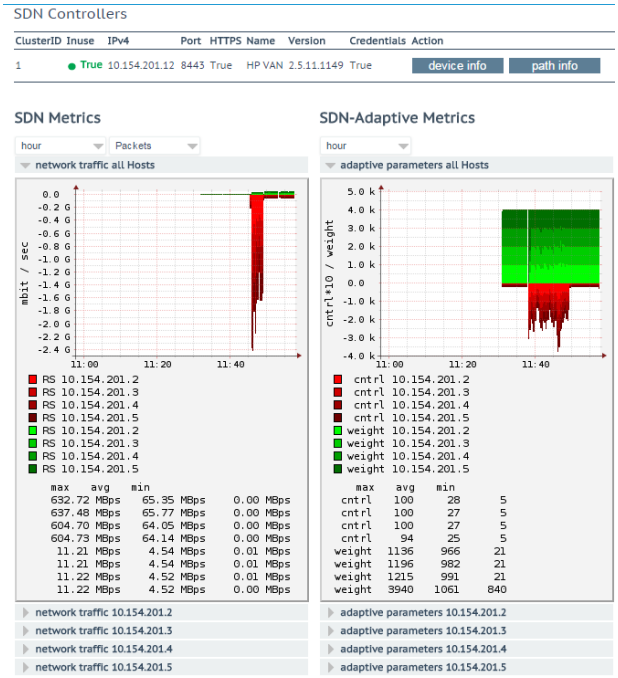
例
1 秒あたりの接続数のグラフでは、倍率「m」で 200 の値が示されています。 上の表にあるように、「m」は「ミリ」を表します。 したがって、その時間の 1 秒あたりの接続数の絶対値を求めるには、値 200 に係数 10^(-3) を掛ける必要があります。

- 10^(-3) = 0.001
- 200 x 0.001 = 1 秒あたり 0.2 接続

この計算は、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。また、接続率が非常に低いため、グラフが接続の絶対数を示している場合、ゼロの直線になり、有用な情報を提供しません。

6 SDN 統計

SDN 統計を表示するには、LoadMaster WUI のメイン メニューで [Statistics] > [SDN Statistics] に移動します。



LoadMaster が SDN コントローラに正常に接続されている場合、名前、バージョン、資格情報が表示されます。

Statistics section

SDN コントローラが追加されていて、LoadMaster と通信していない限り、統計は表示されません。Name、Version、および Credentials が表示されない場合は、LoadMaster が SDN コントローラに接続されていないことを意味します。 これは、構成が正しくないか、SDN コントローラーがダウンしていることを意味している可能性があります。

この画面には、ネットワーク トラフィックと適応パラメータの 2 種類の統計が表示されます。

- Network Traffic - 各実サーバーの 1 秒あたりの転送ビット数とバイト数を表示できます。 1 秒あたりの最大、平均、および最小のビット/バイト数が表示されます。
- Adaptive Parameters - 適応値 (ctrl) と重みが表示されます。 適応値が上がると、実サーバーの重みが下がります。

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

デバイス情報ボタンをクリックすると、OpenFlow が有効になっているコントローラのスイッチに関する情報を表示できます。

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

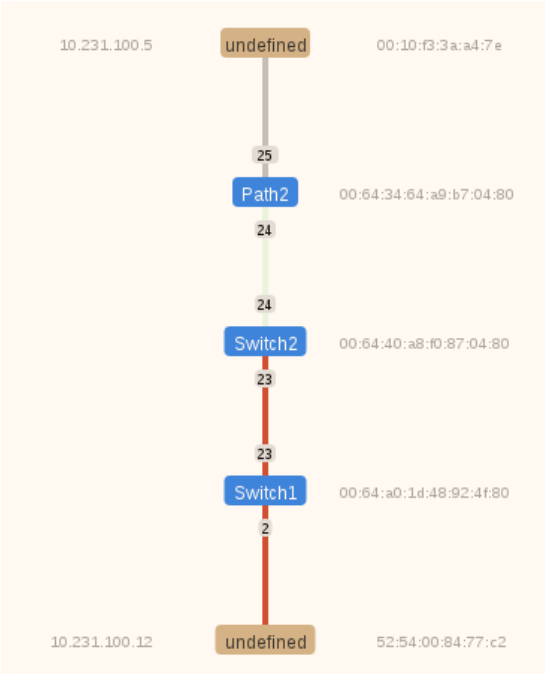
プラス (+) ボタンをクリックして各デバイスを展開すると、詳細情報が表示されます。

6.1.1 パス情報

パス情報は、Path Info ボタンをクリックして表示できます。

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

パスのグラフィック表現を表示するには、関連するパスの Dir 列にある => または <= アイコンをクリックします。



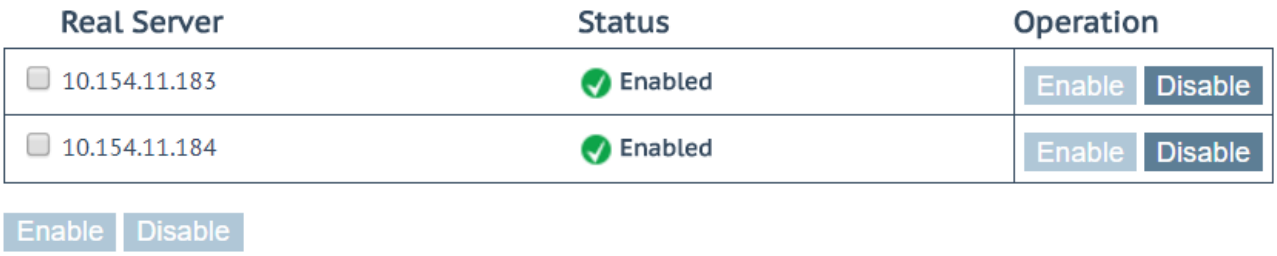
この画面には、LoadMaster、Real Server、およびその間のすべてのスイッチが表示されます。 LoadMaster と Real Server は茶色で表されます。 上がロードマスター、下が Real Server です。 スイッチは青色で表されます。 SDN コントローラがスイッチ名を取得すると、青色のボックスにスイッチ名が表示されます。 ネットワーク上の各スイッチのデータ パス識別子 (DPID) は、スイッチの右側に表示されます。 DPID は、コントローラがさまざまなスイッチを識別する方法です。 LoadMaster と Real Server の Media Access Control (MAC) アドレスは、これらのデバイスの右側に表示されます。 LoadMaster と Real Server の IP アドレスも左側に表示されます。 パスの色は次のとおりです。

- 薄緑色: トラフィックはアイドル状態で、リンクは正常です。
- 赤: パスがトラフィックで混雑しています。
- グレー: LoadMaster と最初のスイッチの間のパスはグレーで表示されます。

したがって、上記のスクリーンショットの例では、Path2 と Switch2 スイッチ間のパスは正常ですが、Switch2 と Switch1 およびリアル サーバー間のパスは輻輳しています。 パスが多かれ少なかれ混雑するにつれて、パスの色が変わる場合があります。 表示できる赤色の配列があります。赤色が

濃いほど、経路上の渋滞が多くなります。

7 リアルサーバー



この画面には、実サーバーの現在のステータスが表示され、各実サーバーを無効または有効にするオプションが表示されます。 各 Real Server には、Real Server を無効化 (オンライン サーバーをオフラインにする) および有効化するための対応するボタンがあります。 関連する Real Server を選択し、下部にある関連するボタンをクリックすることで、複数の Real Server を同時に有効または無効にすることもできます。 ステータスは、有効 (緑)、無効 (赤)、または部分的 (黄) のいずれかです。これは、 1 つの仮想サービスで実サーバーが有効になっていることを意味します。

注意

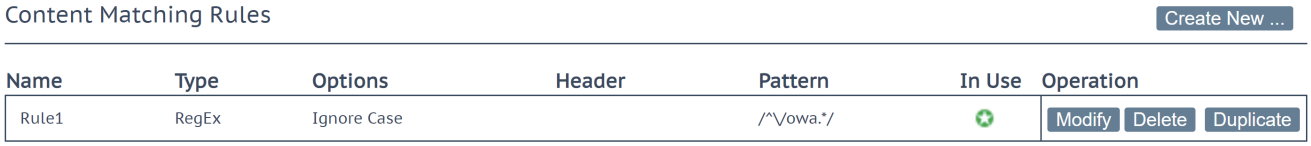
Real Server を無効にすると、それを使用するように構成されたすべての仮想サービスが無効になります。 それが利用可能な唯一の Real Server (つまり、最後の実サーバー) である場合、仮想サービスは実質的にダウンしており、トラフィックを通過させません。

DNS 名が割り当てられた Real Server は、DNS 名のない Real Server の上/下に表示されます。 [Real Server] または [Status] 列見出しをクリックして、実サーバーのリストを並べ替えることができます。

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 マッチング ルール



この画面には、構成されているルールが表示され、変更または削除のオプションが表示されます。 LoadMaster ファームウェア 7.2.52 以降では、コンテンツ ルールを複製できます。 コンテンツ ルール ページには、コンテンツ ルールが使用中かどうかを示す [In Use] 列もあります。

- スター アイコンは、コンテンツ ルールがどの仮想サービスにも割り当てられていないことを意味します。

- チェック アイコンは、コンテンツ ルールが少なくとも 1 つの仮想サービスに割り当てられていることを意味します。 割り当てられた仮想サービスの数は、チェック アイコンの横に表示されます。 チェック アイコンにカーソルを合わせると、このコンテンツ ルールが割り当てられている仮想サービスの詳細が表示されます。 ホバー テキストには、割り当てられた最初の 20 個の仮想サービスのみが表示されます。

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。 ルールに名前を付ける必要があります。 ルール名は、一意の英数字にする必要があり、スペースを含めることはできません。 ルールでは大文字と小文字が区別されるため、Rule1 と rule1 という 2 つの異なるルールが存在する可能性があります。 コンテンツ ルールのデフォルトに名前を付けることはできません。 使用可能なオプションは、選択したルール タイプによって異なります。 使用可能なルールは次のとおりです。

Rule Types

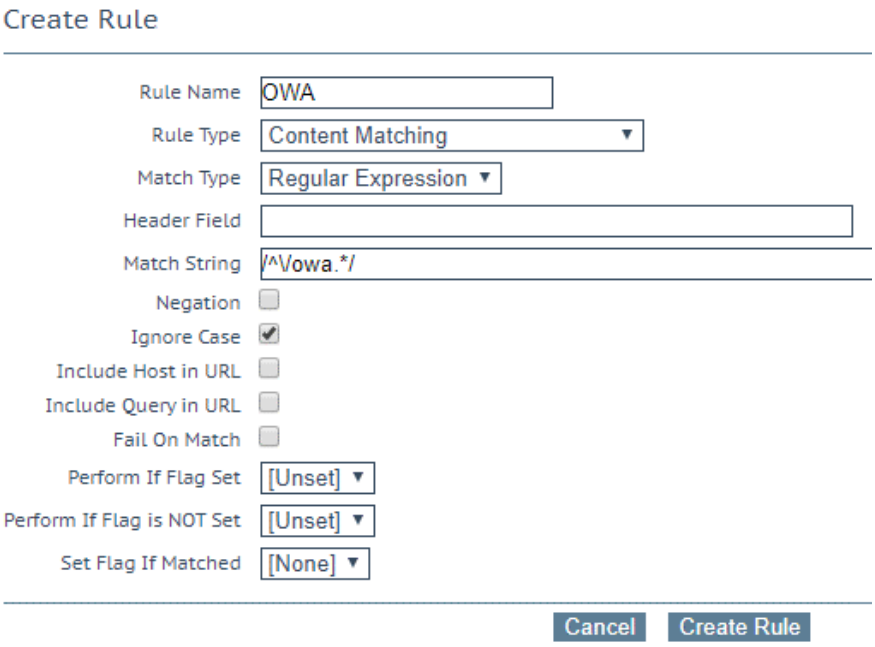
- Content Matching: ヘッダーまたは本文のコンテンツと一致します。

- Add Header: ルールに従ってヘッダーを追加します
- Delete Header: ルールに従ってヘッダーを削除します
- Replace Header: ルールに従ってヘッダーを置き換えます
- Modify URL: ルールに従って URL を変更します。
- Replace String in Response Body: 規則に従って本文のテキストを置換します

ルールの構成の詳細については、ドキュメントを参照してください。

8.1.2 コンテンツ マッチング

選択したルール タイプがコンテンツ マッチングの場合、以下に使用可能なオプションについて説明します。



Rule Name

ルールの名前。

Match Type

- Regular Expression: ヘッダーをルールと比較します。

  LoadMaster WUI の正規表現で引用符を使用する場合、制限があります。 詳細については、「Limitations of Using Regular Expressions in the LoadMaster WUI.」セクションを参照してください。
- Prefix: ルールに従ってヘッダーのプレフィックスを比較します

- Postfix: ルールに従ってヘッダーの接尾辞を比較します

Header Field

ヘッダー フィールド名が一致している必要があります。 ヘッダー フィールド名が設定されていない場合、デフォルトでは URL 内の文字列と一致します。 [Header Field] テキスト ボックスに src-ip を入力すると、クライアントの送信元 IP に基づいてルールを照合できます。 ヘッダー フィールドには、クライアントの送信元 IP が入力されます。 同様に、GET、POST、HEAD など、使用される HTTP メソッドに基づいてルールを照合することもできます。 照合するメソッドは大文字で記述する必要があります。 リクエストの本文は、[Header Field] テキスト ボックスに body と入力することでも照合できます。

Match String

照合するパターンを入力します。 正規表現と PCRE の両方がサポートされています。 許可される最大文字数は 250 です。

正規表現と PCRE の詳細については、Contents Rule 機能の説明を参照してください。

Negation

照合を反転します。

Ignore Case

文字列を比較するときに大文字と小文字を区別しません。

Include Host in URL

一致を実行する前に、ホスト名を要求 URL の先頭に追加します。

Include Query in URL

一致を実行する前に、クエリ文字列を URL に追加します。

Fail On Match

このルールが一致する場合、常に接続に失敗します。

Perform If Flag Set

指定されたフラグが設定されている場合にのみ、このルールの実行を試みます。

Perform If Flag is NOT Set

指定されたフラグが設定されていない場合にのみ、このルールを実行してみてください。

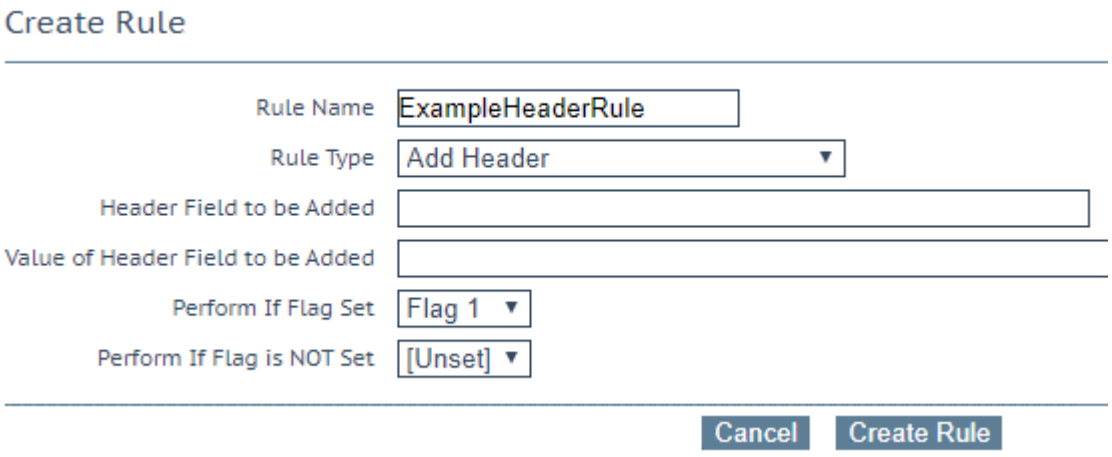
Set Flag If Matched

ルールが正常に一致した場合は、指定されたフラグを設定します。

[Perform If Flag Set] オプションと [Set Flag If Matched [] オプションを使用すると、ルールを相互に依存させることができます。つまり、別のルールが正常に一致した場合にのみ特定のルールを実行することができます。 「Chaining」ルールの詳細については、コンテンツ ルール機能の説明を参照してください。

8.1.3 ヘッダーを追加

選択したルール タイプが [Add Header] の場合に使用できるオプションを次に示します。



Rule Name

これは、ルールの名前を入力するためのテキスト ボックスです。

Header Field to be Added

追加するヘッダーフィールドの名前を入力するテキストボックスです。

Value of Header Field to be Added

追加するヘッダー フィールドの値を入力します。 このフィールドには最大 255 文字を入力できます。

Perform If Flag Set

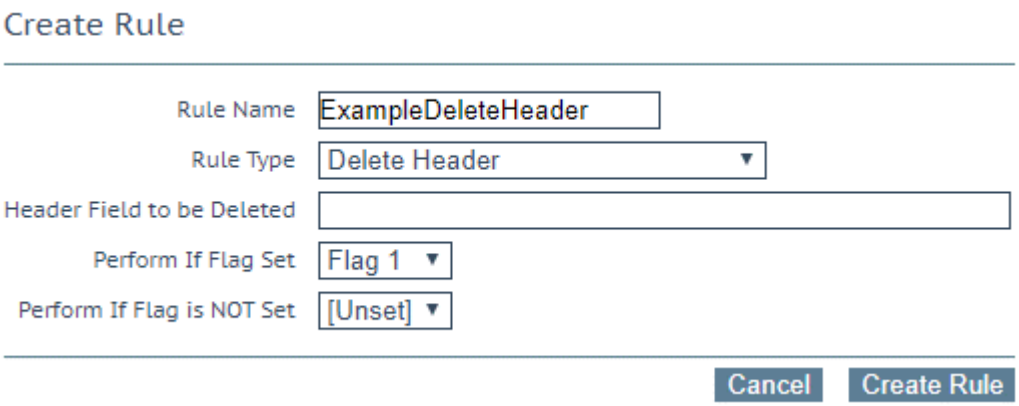
指定されたフラグが設定されている場合にのみ、このルールを実行します。 フラグは別のルールによって設定されます。 フラグの詳細については、コンテンツ マッチングのセクションを参照してください。

Perform If Flag is NOT Set

指定されたフラグが設定されていない場合にのみ、このルールを実行してみてください。

8.1.4 ヘッダーを削除

選択したルール タイプが [Delete Header] である場合に使用できるオプションを次に示します。



Rule Name

これは、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

これは、削除するヘッダー フィールドの名前を入力するテキスト ボックスです。

Perform If Flag Set

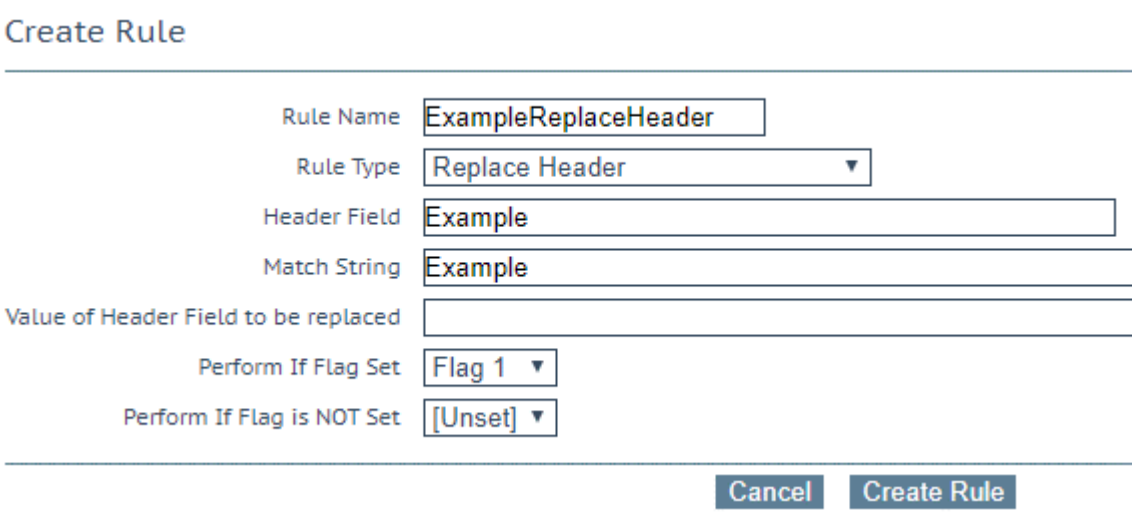
指定されたフラグが設定されている場合にのみ、このルールを実行します。 フラグは別のルールによって設定されます。 フラグの詳細については、Content Matching のセクションを参照してください。

Perform If Flag is NOT Set

指定されたフラグが設定されていない場合にのみ、このルールを実行してみてください。

8.1.5 ヘッダーを置換

選択したルール タイプが [Replace Header] の場合に使用できるオプションについて、以下に説明します。



Rule Name

これは、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

これは、置換が行われるヘッダー名フィールドを入力するためのテキストボックスです。

Match String

一致させるパターン。

Value of Header Field to be replaced

これは、置き換えられるヘッダー フィールドの値を入力するためのテキスト ボックスです。

Perform If Flag Set

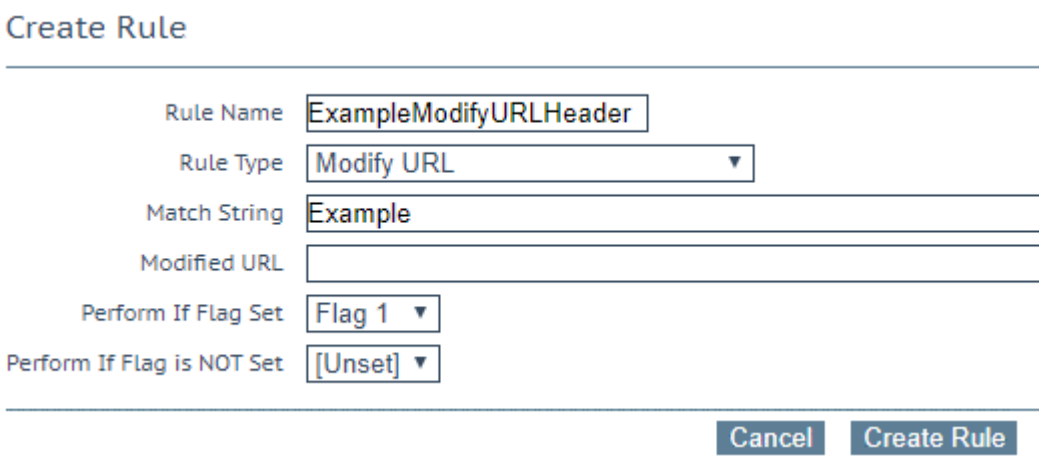
指定されたフラグが設定されている場合にのみ、このルールを実行します。 フラグは別のルールによって設定されます。 フラグの詳細については、コンテンツ マッチングのセクションを参照してください。

Perform If Flag is NOT Set

指定されたフラグが設定されていない場合にのみ、このルールを実行してみてください。

8.1.6 URL の変更

選択したルール タイプが [Modify URL] である場合に使用できるオプションを次に示します。



Rule Name

これは、ルールの名前を入力するためのテキスト ボックスです。

Match String

これは、一致させ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

これは、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

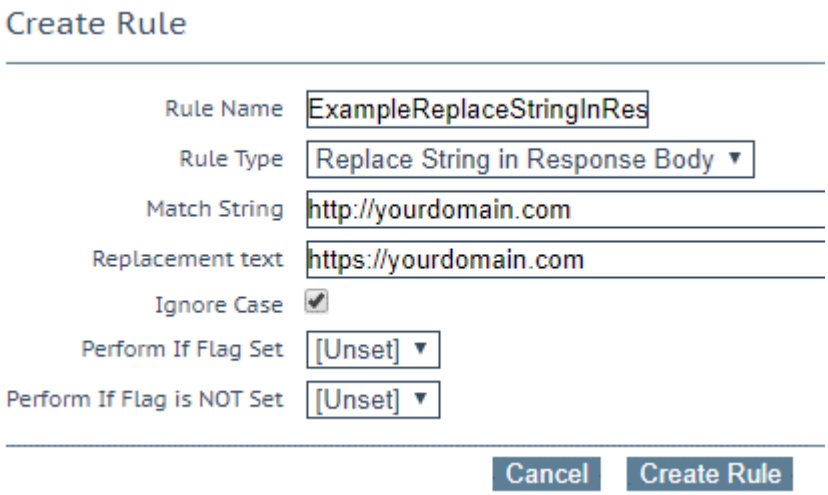
指定されたフラグが設定されている場合にのみ、このルールを実行します。 フラグは別のルールによって設定されます。 フラグの詳細については、コンテンツ マッチングのセクションを参照してください。

Perform If Flag is NOT Set

指定されたフラグが設定されていない場合にのみ、このルールを実行してみてください。

8.1.7 応答本文の文字列を置換

選択したルール タイプが [Replace String in Response Body] の場合、次のオプションを使用できます。



Rule Name

ルールの名前。 ルール名は一意である必要があります。

Match String

一致する文字列。

Replacement text

置換文字列。

Ignore Case

比較時に文字列の大文字と小文字を無視するには、このチェック ボックスをオンにします。

Perform If Flag Set

指定されたフラグが設定されている場合にのみ、このルールを実行します。 フラグは別のルールによって設定されます。

Perform If Flag is NOT Set

指定されたフラグが設定されていない場合にのみ、このルールを実行してみてください。

8.1.8 LoadMaster WUI で正規表現を使用する際の制限事項

LoadMaster WUI で正規表現を使用する場合、偶数の引用符 (一重または二重) を使用する必要があります。 引用符も正しく入れ子にする必要があります。たとえば、二重引用符内で単一引用符を使用する場合、単一引用符は二重引用符内で一致する必要があります。 正規表現で単一の " (二重引用符) 文字を使用するには、代わりに ¥22 (または単一引用符の場合は ¥27) を使用します。正規表現で奇数の引用符を使用する場合は、代わりに API を使用します。

ウィ。 たとえば、WUI で次の一致文字列を設定しようとすると、一致するパターンを指定してくださいというエラーが発生します。

/¥<img([^¥>¥/]*)¥ssrc¥=¥"([^¥"]*)¥"([^¥>¥/]*)¥/?>/

ただし、API を使用してこれを設定することは可能です。たとえば、次のようになります。

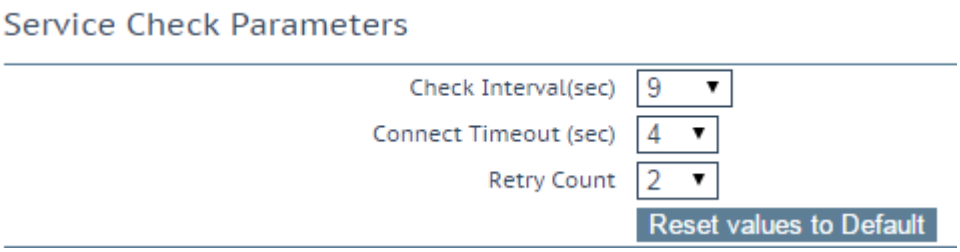
/access/addrule?name=Example&pattern=/¥<img([^¥>¥/]*)¥ssrc¥=¥"([^¥"]*)¥"([^¥>¥/]*)¥/?>/

8.2 パラメータをチェック

パラメータのチェック画面にアクセスするには、LoadMaster WUI のメイン メニューで [ルールとチェック] > [パラメータのチェック] に移動します。 パラメータのチェック画面には、仮想サービスで選択されたスケジューリング方法に応じて、サービス チェック パラメータと、適応パラメータまたは SDN 適応パラメータの 2 つのセクションがあります。 スケジューリング方法がリソースベース (適応型) に設定されている場合、[適応パラメータ] セクションが表示されます。 スケジューリング方法がリソースベース (SDN アダプティブ) に設定されている場合、SDN アダプティブ パラメータ セクションが表示されます。 詳細については、以下の関連セクションを参照してください。

8.2.1 サービス (ヘルス) チェック パラメータ

LoadMaster は、レイヤー 3、レイヤー 4、およびレイヤー 7 のヘルス チェックを利用して、Real Server と仮想サービスの可用性を監視します。



Check Interval(seconds)

このフィールドは、連続するヘルス チェックの試行の間に経過する秒数を指定し、「Health Check Cycle」の長さを定義します。

推奨値およびデフォルト値: 9 秒

有効な値の範囲は、<mininterval> (9) から <maxinterval> (901) までです。

<mininterval> は Retry Count * Connect Timeout (seconds) + 1 です。つまり、デフォルトの

最大値は 9 です。

<maxinterval> は 901 です [60 (最大接続タイムアウト (秒)) * 15 (最大再試行回数) + 1 であるため]。

WUI では、[Check Interval] の値が 120 を超える場合 ([Connect Timeout (秒)] と [Retry Count] の設定によってこの値に強制されるため)、[Check Interval(秒)] ドロップダウン リストを変更しても変更できません。 . これを変更するには、他の 2 つのオプションを構成します。 それ以外の場合、間隔に設定できる最大値は 120 です。

Connect Timeout (seconds)

これは、接続が確立され、ヘルスチェックへの応答が受信されるまでに許容される最大待機時間です。タイムアウトになる前に応答が受信されない場合、再試行回数に達していない限り、接続が再試行されます。 ヘルス チェックに対する HTTP 応答が受信された場合、現在のヘルス チェック サイクルでは再試行は行われません。

デフォルト値:4 秒

有効な値の範囲は 4 ～ 60 です。

Retry Count

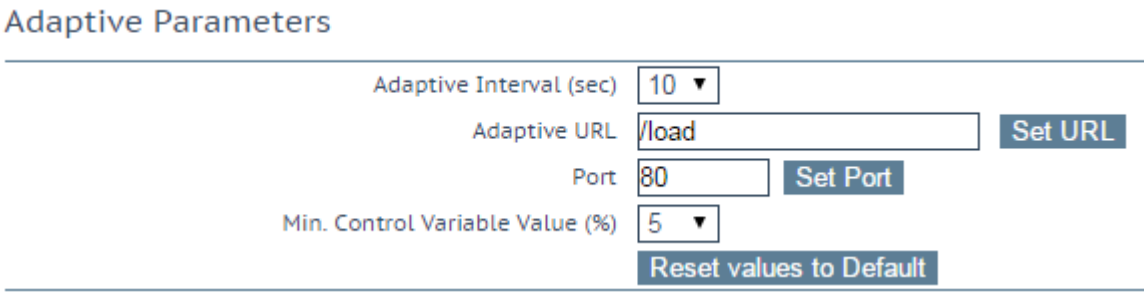
これは、応答を受信する前に上記のタイムアウトに達した場合にヘルスチェックを再試行する回数を指定します。 グローバルな再試行回数の値を上書きするには、ドロップダウン リストから他の値を選択できます。 ヘルスチェックに対して応答があった場合、再試行回数は適用されません。 たとえば、200 または 404 応答を受信した場合、現在のサイクルでは再試行は行われません。

デフォルト値: 2

有効な値の範囲は 2 ～ 15 です。

LoadMaster ファームウェア バージョン 7.2.52 では、各仮想サービスまたはサブ VS でチェック間隔、タイムアウト、および再試行回数の設定を構成できます。 以前は、これらは単なるグローバル設定でした。 詳細については、セクション 実サーバー を参照してください。

8.2.2 適応パラメータ



Adaptive Interval (sec)

これは、LoadMaster がサーバーの負荷をチェックする間隔 (秒単位) です。 低い値は、LoadMaster が負荷に対して非常に敏感であることを意味しますが、LoadMaster 自体に余分な負荷がかかります。 7 秒が適切な開始値です。 この値は、HTTP チェック間隔より小さくてはなりません。

Adaptive URL

Adaptive メソッドは、HTTP 照会を使用してサーバーから負荷情報を取得します。 この URL は、サーバーの負荷情報が保管され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 (Adaptive Agent など) のいずれかです。 標準の場所は /load です。 このファイルの現在の負荷データを ASCII 形式で提供するのは、サーバーの仕事です。 その際、次の点を考慮する必要があります。

最初の行に 0 ～ 100 の範囲の値を含む ASCII ファイル。0 = アイドル、100 = 過負荷。 数が増えると、つまりサーバーの負荷が高くなると、LoadMaster がそのサーバーに渡すトラフィックが少なくなります。 したがって、サーバーの負荷に「適応」します。

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

ファイルはデフォルトで「/load」に設定されています。

ファイルは、HTTP を使用してアクセスできる必要があります。

URL は、適応方式でサポートされるすべてのサーバーで同じでなければなりません。 この機能は、HTTP ベースの仮想サービスだけでなく、すべてのサービスにとって重要です。 HTTP は、実サーバーからアプリケーション固有の負荷情報を抽出するための転送方法としてのみ使用されます。

Port

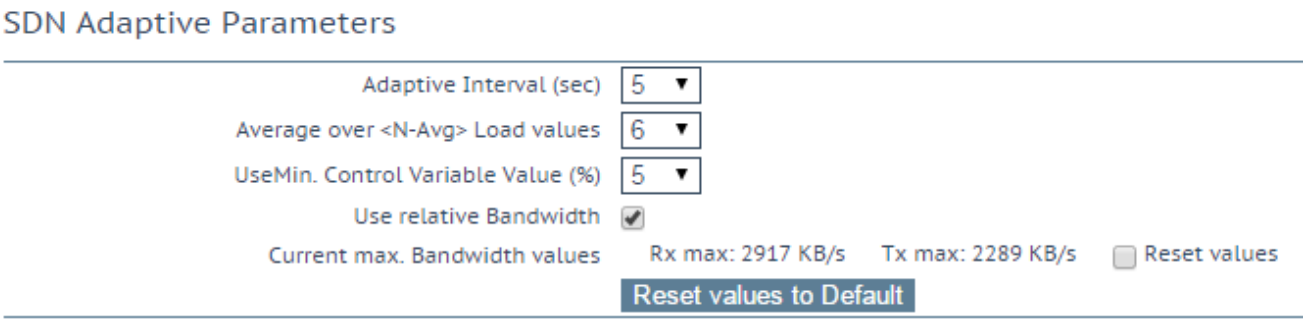
この値は、サーバー上の HTTP デーモンのポート番号を指定します。 デフォルト値は 80 です。

Min. Control Variable Value (%)

この値は、それを下回るとバランサーが静的な重みベースのスケジューリング、つまり通常の加重ラウンド ロビンに切り替えるしきい値を指定します。 値は、最大負荷のパーセンテージ（0 ～ 50）です。 デフォルトは 5 です。

Min. Control Variable Value (%)
この値は、それを下回るとバランサーが静的な重みベースのスケジューリング、つまり通常の加重ラウンド ロビンに切り替えるしきい値を指定します。 値は、最大負荷のパーセンテージ（0 ～ 50）です。 デフォルトは 5 です。

8.2.3 SDN 適応パラメータ



Adaptive Interval (sec)
SDN 適応スケジューリングを使用する場合、SDN コントローラーはポーリングされて、Real Server の負荷値を取得します。 このフィールド値は、これが発生する頻度を指定します。

Average over <N-Avg> Load values
この値を使用して、システムの変動を抑制します。

UseMin. Control Variable Value (%)
ここで設定された値を下回るものはすべてアイドル トラフィックと見なされ、(Real Server 統計画面に表示される) 適応値には影響しません。たとえば、上記のスクリーンショットでは、5% を下回るものはすべてアイドルと見なされます。

Use relative Bandwidth
リンクで観測された最大負荷をリンク帯域幅として使用します。 Progress Kemp は、このオプションを有効にすることを推奨しています。

Current max. Bandwidth values

このセクションには、現在の受信および送信された最大帯域幅の値が表示されます。

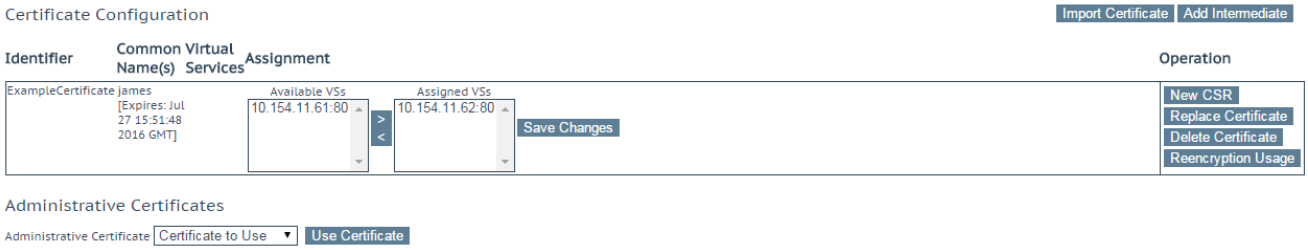
Reset values

このチェックボックスを使用して、現在の最大値をリセットできます。 帯域幅の値。

9 証明書とセキュリティ

以下のセクションでは、LoadMaster WUI の Certificates & Security セクションのさまざまな画面について説明します。

9.1 SSL 証明書



上記は証明書の管理画面です。 この画面のさまざまなオプションの詳細は次のとおりです。

- Import Certificate – 選択したファイル名で証明書をインポートします。
- Add Intermediate - 詳細については、「中間証明書」セクションを参照してください。
- Identifier - 作成時に証明書に付けられた名前です。
- Common Name(s) – サイトの FQDN (完全修飾ドメイン名) です。
- Virtual Service – 証明書が関連付けられている仮想サービス。
- Assignment - 利用可能で割り当てられた仮想サービスのリスト
- Operation –
  - New CSR – 現在の証明書に基づいて、新しい証明書署名要求 (CSR) を生成します。

  証明書にサブジェクト代替名 (SAN) がある場合、この方法で CSR を生成しても SAN は追加されません。 代わりに、CSR を手動で生成してください。 詳細については、「CSR の生成 (証明書署名要求)」セクションを参照してください。
- Replace Certificate - このファイルに保存されている証明書を更新または置き換えます。
- Delete Certificate – 関連する証明書を削除します。

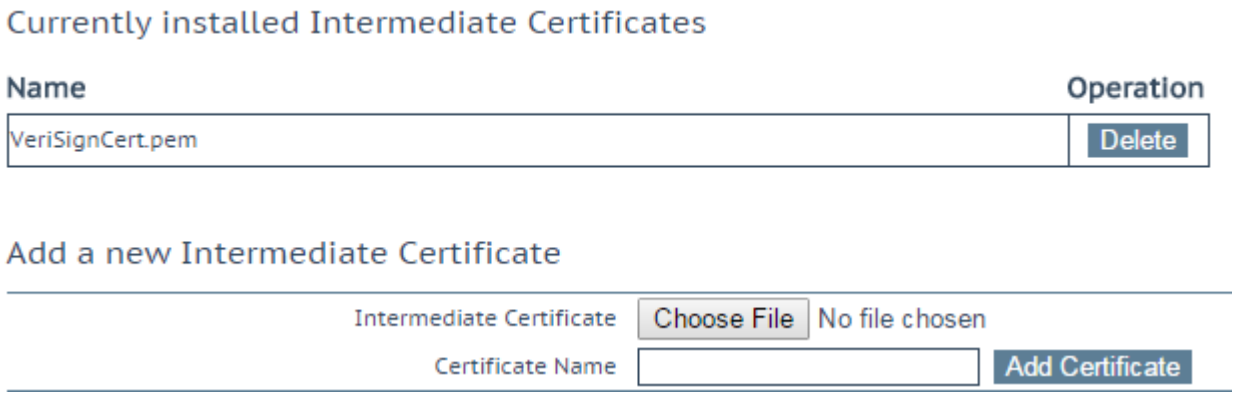
SSL Certificate 画面から Let's Encrypt/DigiCert 証明書を削除または置換することはできません。 Let's Encrypt/DigiCert 証明書は、[Certificate & Security] > [ACME Certificate] からのみ削除または置換できます)。 Let's Encrypt/DigiCert 証明書の [SSL Certificate] 画面で、[Replace Certificate] ボタンと [Delete Certificate] ボタンがグレー表示されます。

- 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仮想サービスを表示します。

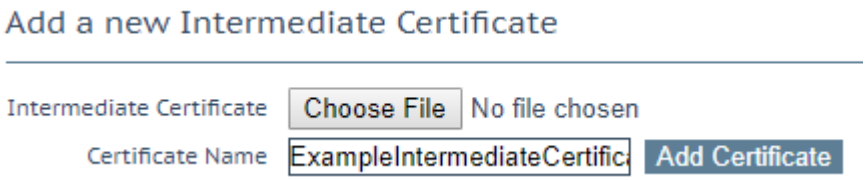
Manage Certificate – 管理インターフェイスに使用する証明書 (存在する場合)。

TPS のパフォーマンスは、キーの長さによって異なります。 キーを大きくすると、パフォーマンスが低下します。

9.2 中間証明書



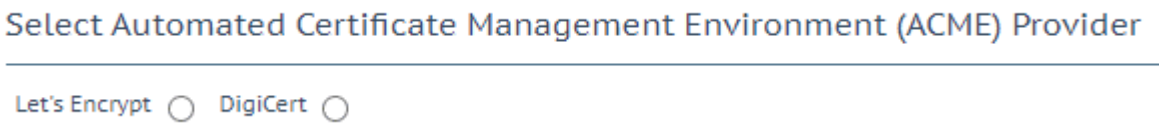
この画面には、インストールされている中間証明書とそれらに割り当てられた名前のリストが表示されます。



すでに証明書を持っている場合、または CSR から証明書を受け取った場合は、[Choose File] ボタンをクリックして証明書をインストールできます。 証明書に移動して選択し、目的の証明書名を入力します。 名前には、最大 32 文字の英字のみを含めることができます。

GoDaddy などの一部の証明書ベンダーが実践しているように、1 つのテキスト内に複数の連続する中間証明書をアップロードすることは許可されています。 アップロードされたファイルは、個々の証明書に分割されます。

9.3 ACME 証明書



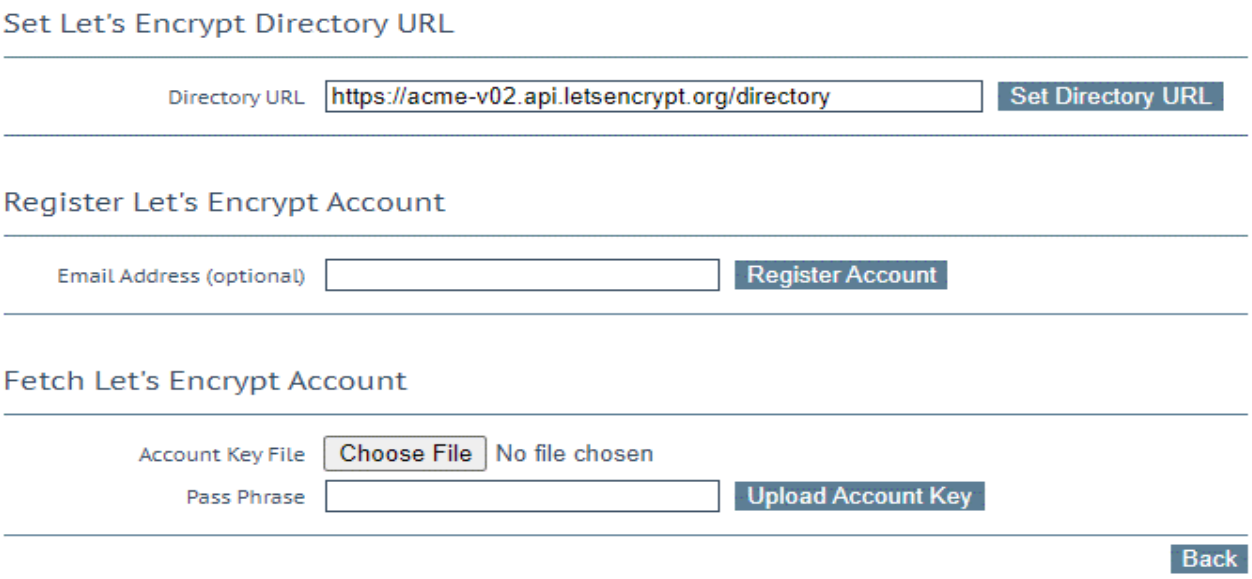
LoadMaster は、2 つの Automated Certificate Management Environment (ACME) プロバイダーのオプションを提供します。

- Let's Encrypt
- DigiCert

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

DigiCert に関する詳細については、Progress Kemp Documentation ページの DigiCert 機能の説明を参照してください。

9.3.1 証明書を暗号化



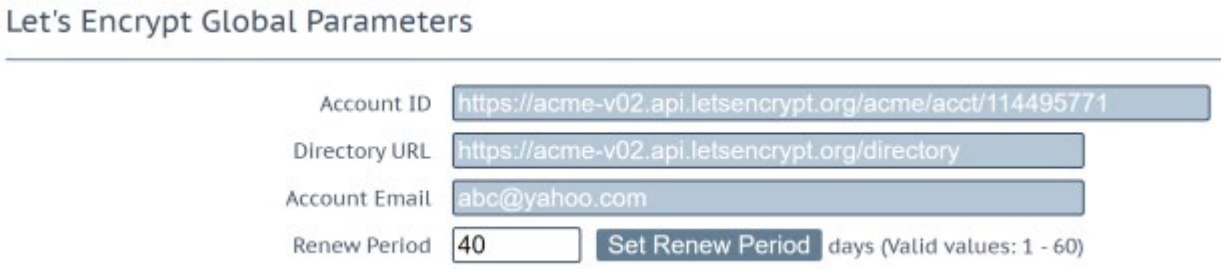
Directory URL: Automated Certificate Management Environment (ACME) サーバーの URL を [Directory URL] フィールドに入力し、[Set Directory URL の設定] をクリックします。デフォルトの URL は、Let's Encrypt の実稼働 ACME サーバー (https://acmev02.api.letsencrypt.org/directory) です。これは必要に応じて変更できます。LoadMaster は、ACME プロトコルの API バージョン 2 をサポートしています。

Email Address (オプション): オプションで電子メール アドレスを入力し、[Register Account] をクリックして、Let's Encrypt アカウントに登録できます。

アカウント キー ファイル: 既存の Let's Encrypt アカウントを既にお持ちの場合は、[Choose Files] ボタンをクリックしてアカウント キー ファイルをアップロードできます。キーファイルに移動して選択します。アカウントを登録した他の ACME クライアント (Certbot など) からアカウント キー ファイルを取得できます。

パスフレーズ: 証明書に関連付けられているパスフレーズを入力し、[Upload Account Key] をクリックして既存のアカウントにリンクします。

既存の Let's Encrypt アカウントへの登録またはリンクが正常に完了すると、[Manage Let's Encrypt Certificate] 画面が表示されます。



Renew Period

Let's Encrypt の証明書は 90 日間有効です。 更新期間の値は、証明書の有効期限が切れる何日前に証明書を更新するかを指定します。 更新期間はアカウント全体の設定です。 現時点では、証明書ごとの更新期間はサポートされていません。 更新期間はデフォルトで 30 日に設定されています。 Let's Encrypt は、有効期限が切れる 30 日前に証明書を更新することをお勧めします。 [更新期間] フィールドの有効な値の範囲は 1 ～ 60 (日) です。 更新が成功すると、古い証明書が置き換えられ、HTTPS 仮想サービスに割り当てられます。 詳細と手順については、Progress Kemp ドキュメントページの Let's Encrypt 機能の説明を参照してください。

Request New Certificate

[Request New Certificate] をクリックして、Let's Encrypt CA から新しい証明書を要求します。 Request a New Certificate 画面のすべてのフィールドは、Certificate Identifier と Common Name を除いてオプションです (また、Common Name フィールドの横にある仮想サービスを選択する必要があります)。 証明書識別子: 一意の識別子を入力します。 証明書識別子の値は、ロードマスター上のすべての証明書に対して一意である必要があります。

Common Name: Web サーバーの FQDN を入力します。 これは大文字と小文字が区別されます。 証明書は、管理している有効なホスティング ドメインに対してのみ発行されます。 このドメインに使用される仮想サービスを選択します。 これは、ドメインの所有権を証明するための検証チャレンジに使用されます。

HTTP/HTTPS レイヤー 7 仮想サービスは、SubVS を追加できるように構成済みである必要があります (そのため、親仮想サービスに実サーバーを追加する必要はありません。ただし、既存の SubVS が存在する場合は、実サーバーを接続できます)。 実サーバーが接続された既存の仮想サービスを、実サーバーが接続された SubVS を含む仮想サービスに変換する方法については、Progress Kemp ドキュメント ページの Let's Encrypt 機能の説明を参照してください。

Let's Encrypt はポート 80 で通信して HTTP-01 チャレンジを実行するため、すべてのポート 80 要求を 443 にリダイレクトするように HTTP リダイレクト仮想サービスを構成する必要があります。 基準を満たすすべての有効な仮想サービスがドロップダウン リストに表示されます。

2 Letter Country Code: オプションで 2 文字の国コードを入力します。有効な国コードのリストについては、SSL 証明書の国コードのページを参照してください。 Let's Encrypt を使用している場合、2 文字の国コードから電子メール アドレスへのフィールドは切り捨てられます。
State/Province: オプションで、証明書に含める都道府県を入力します。フルネームを入力します。たとえば、ニューヨーク (NY ではありません) などです。
City: オプションで、証明書に含める都市を入力します。
Company: オプションで、証明書に含める会社の名前を入力します。
Organization: 必要に応じて、この証明書に関して連絡する必要がある部門または組織単位を入力します。
Email Address: 必要に応じて、この証明書に関して連絡する必要がある個人または組織の電子メール アドレスを入力します。
楕円曲線リクエストの生成: 必要に応じて、このオプションを有効または無効にします。これを有効にすると、RSA リクエストの代わりに楕円曲線リクエストが生成されます。
Key Size: ドロップダウン リストからアルゴリズム サイズを選択します。楕円曲線 (EC) リクエストを生成している場合、[キー サイズ] ドロップダウンはグレー表示されます。 EC 要求には、デフォルト サイズの 256 ビットが使用されます。 RSA 要求を生成している場合は、キー サイズを指定できます。
SAN/UCC Name: サブジェクト代替名 (SAN) を入力します。これは有効なドメインでなければなりません。最大 10 の SAN を指定できます。

すべての SAN について、HTTP/HTTPS レイヤー 7 仮想サービスを選択する必要があります (同じ仮想サービスを使用できます)。 各 SAN について、Let's Encrypt サーバーに対する権限を証明する必要があります。 HTTP/HTTPS 仮想サービスは、SubVS を追加できるように構成済みである必要があります (そのため、親仮想サービスに実サーバーを追加する必要はありません。ただし、既存の SubVS が存在する場合は、実サーバーを接続できます)。 実サーバーが接続された既存の仮想サービスを、実サーバーが接続された SubVS を含む仮想サービスに変換する方法については、Progress

Kemp ドキュメント ページの Let's Encrypt 機能の説明を参照してください。

Request Certificate: 関連するフィールドの設定が完了したら、[Request Certificate] をクリックして、指定したデータを使用して新しい証明書リクエストを作成します。 Let's Encrypt Certs 画面の下部に、発行された証明書と関連する詳細の一覧が表示されます。 [HTTP Challenge VS(s)] 列には、HTTP チャレンジに使用された仮想サービス (またはサービス) が一覧表示されます。 これらは、証明書が割り当てられる仮想サービスではありません。 証明書が正常に発行されると、[Certificates & Security] > [SSL Certificates] に表示されます。 その後、それを任意の HTTPS 仮想サービスに割り当てるか、管理証明書として使用できます。

新しい証明書を初めて仮想サービスに手動で割り当てると、仮想サービスが再起動するため、Progress Kemp は勤務時間外にこれを行うことを推奨しています。

Let's Encrypt 証明書が更新されると、証明書が割り当てられている仮想サービスは、更新された証明書で自動的に更新されます。

証明書の自動更新と更新はシームレスで、仮想サービスのトラフィックには影響しません。

証明書は、各証明書の有効期限の前に、更新期間で指定された日数で自動的に更新されます。[Renew Certificates] をクリックして、証明書を手動で更新できます。

[Delete Certificate] をクリックして、ドメインに関連付けられている証明書を削除することもできます。

証明書が使用されている場合 (たとえば、仮想サービスで割り当てられている場合、または管理証明書として使用されている場合)、[Delete Certificate] ボタンはグレー表示されます。

SSL Certificate 画面から Let's Encrypt 証明書を削除または置換することはできません。 Let's Encrypt 証明書画面からのみ、Let's Encrypt 証明書を削除または置換できます。 Let's Encrypt 証明書の [SSL Certificate] 画面で、[Replace Certificate] ボタンと [Delete Certificate] ボタンがグレー表示されます。

9.4 CSR の生成（証明書署名要求）

証明書をお持ちでない場合は、証明書署名要求（CSR）フォームに入力して、[Create CSR] ボタンをクリックしてください。 LoadMaster によって生成される CSR は SHA256 を使用します。

自己署名証明書の処理が EC 署名付きの EC 証明書に設定されている場合（[証明書とセキュリティ] > [Remote Access] で）、CSR の生成は管理（bal）ユーザーのみに制限されます。 Self-Signed Certificate Handling が別の値に設定されている場合、すべてのユーザーは（権限に関係なく）CSR を生成できます。

2 Letter Country Code（ex. US）

証明書に含める必要がある 2 文字の国コード。たとえば、米国の場合は US を入力する必要があります。

State/Province（Entire Name – New York, not NY）

証明書に含まれる州。 NY ではなく New York など、フルネームをここに入力します。

City

証明書に含める都市の名前。

Company

証明書に含める必要がある会社の名前。

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

証明書に含める部門または組織単位。

Common Name

Web サーバーの完全修飾ドメイン名 (FQDN)。

Email Address

この証明書に関して連絡する必要がある責任者または組織の電子メール アドレス。

SAN/UCC Names

代替名のスペース区切りのリスト。

Generate Elliptical Curve Request

RSA 要求ではなく楕円曲線 (EC) 要求を生成するには、このチェック ボックスをオンにします。

Display Private Key

この新しいオプション (LoadMaster ファームウェア バージョン 7.2.52 および LTS バージョン 7.2.48.3 で導入) は、[Certificate & Security] > [Remote Access] > [Self-Signed Certificate Handling] オプションが [EC certs with an EC signature] に設定されている場合にのみ表示されます。 曲線暗号は、証明書とデジタル署名の両方に使用されます。

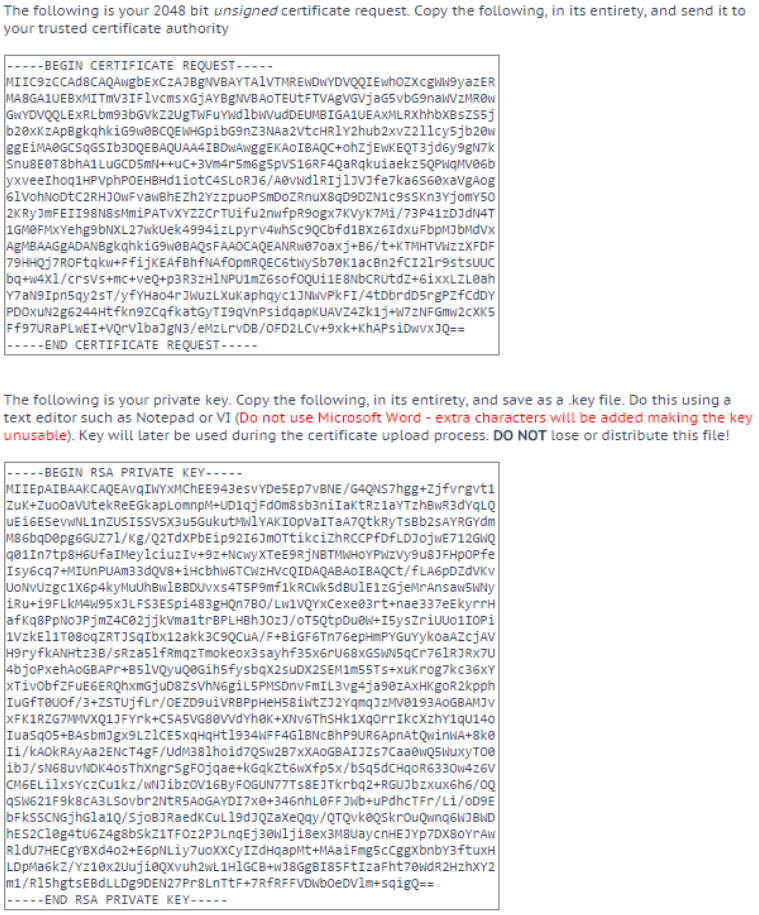
上記のオプションを選択すると、[Certificate & Security] > [Generate CSR] ページに [Display Private Key] チェック ボックスが表示されます。

- [Display Private Key] が無効になっている場合 (デフォルト)、CSR の作成後に秘密キーは WUI に表示されません。 未署名の CSR は、以前のリリースと同様に、ユーザーによってダウンロードされます。 認証局によって署名されたら、ユーザーは署名済み証明書を LoadMaster にアップロードします。以前のリリースとの違いは、ユーザーが秘密鍵をアップロードする必要がないことです。これは、秘密鍵の表示が無効になっている場合、LoadMaster が秘密鍵を内部で保持するためです。 保存された秘密鍵が新しい証明書と一致する場合、証明書は取得されます
  インポートされ、保存された秘密鍵は削除されます。 保存された秘密鍵は暗号化されていませんが、外部からアクセスすることはできず、見ることも表示することもできません。
- Display Private Key が有効になっている場合、LoadMaster は以前のリリースと同様に動作します。秘密鍵はユーザーに表示され、秘密鍵とともに LoadMaster にアップロードする必要があります。

秘密鍵はマシンごとに 1 つだけあり、高可用性 (HA) ペア間では共有されません。 これは、新しく

生成された証明書を、CSR が作成されたマシンにインストールする必要があることを意味します。

で生成されます。 [Create CSR] ボタンをクリックすると、次の画面が表示されます。



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-----
```

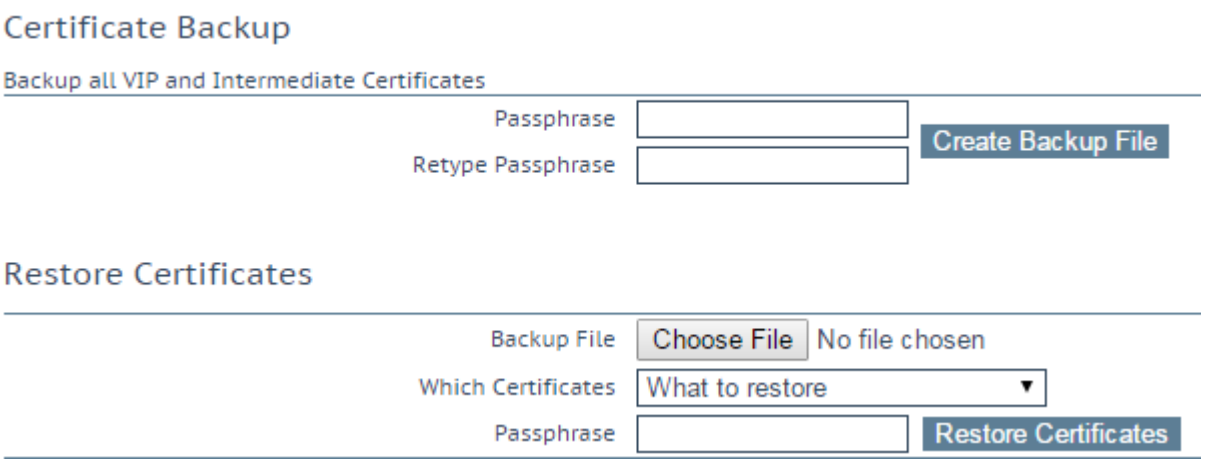
The following is your private key. Copy the following, in its entirety, and save as a .key file. Do this using a text editor such as Notepad or VI (Do not use Microsoft Word - extra characters will be added making the key unusable). Key will later be used during the certificate upload process. **DO NOT**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

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvqIWYxMChEE943esvYDe5Ep7vBNE/G4QNS7hgg+Zjfvrgvt1
ZuK+ZuoOaVUtekReEGkapLomnpM+UD1qjFdOm8sb3niIaKtRz1aYTzhBwR3dVqLQ
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/SjoBJRaedKCuL19dJQZaXeQqy/QTQvk0QSkrOuQwnq6WJBwD
hES2Cl0g4tU6Z4g8bSkZ1TFOz2PJLnqEj30Wlji8ex3M8UaycnHEJYp7DX8oYrAw
RldU7HECgYBXd4o2+E6pNLiy7uoXXCyIZdHqapMt+MAaiFmg5cCggXbnbY3ftuxH
LDpMa6kZ/Yz10x2Uuji0QXvuh2wL1HlGCB+wJ8GgBI85FtIzaFht70WdR2HzhXY2
m1/RlShgtsEBdLLDg9DEN27Pr8LnTtF+7RfRFFVDWbOeDVlm+sqigQ==
-----END RSA PRIVATE KEY-----
```

画面の上部をコピーしてプレーン テキスト ファイルに貼り付け、選択した認証局に送信する必要があります。 彼らは情報を検証し、検証済みの証明書を返します。

画面の下部は秘密鍵であり、安全な場所に保管する必要があります。 このキーは、証明書を使用するために必要になるため、配布しないでください。 秘密鍵をコピーしてプレーン テキスト ファイルに貼り付け (Microsoft Word などのアプリケーションは使用しないでください)、ファイルを安全に保管してください。

9.5 証明書のバックアップ/復元

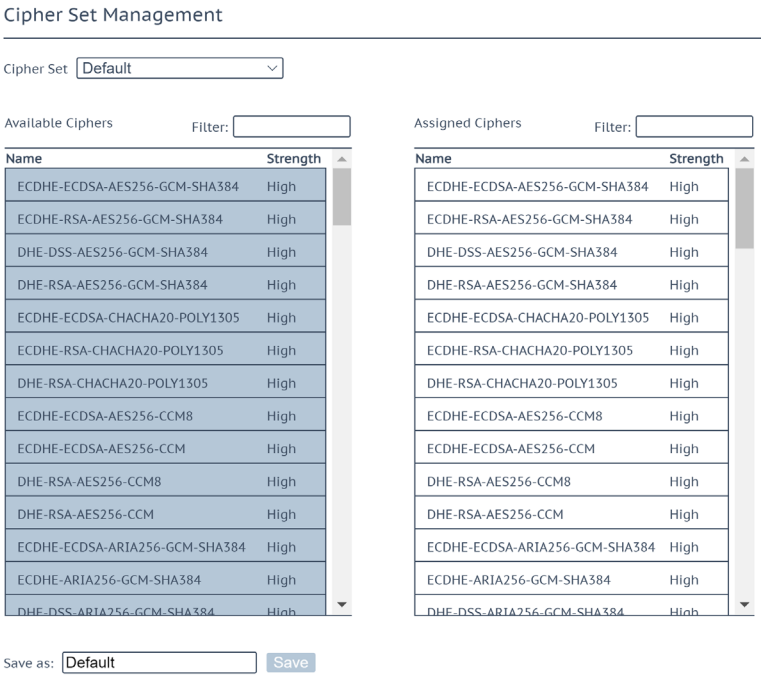


すべての VIP および中間証明書のバックアップ: 証明書をバックアップするとき、必須のパスフレーズ (パスワード) を 2 回入力するように求められます。 パスフレーズのパラメーターは、英数字である必要があり、大文字と小文字が区別され、最大 64 文字です。

注意: このパスフレーズは、証明書を復元するための必須要件です。 パスフレーズがないと、証明書を復元できません。 忘れた場合、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 Certificate: 復元する証明書を選択します。
Pass Phrase: 証明書のバックアップ ファイルに関連付けられているパスフレーズを入力します

9.6 暗号セット



Cipher Set

表示/変更する暗号セットを選択します。

システム定義の暗号セットは次のとおりです。

- Default: 新規インストールの LoadMaster で設定された暗号セット。 この暗号セットは、LoadMaster の以前のリリースとの後方互換性を目的としています。
- Default_NoRc4: 最新のネットワークでは安全でないと見なされている RC4 暗号を含まない、より安全なデフォルト セットのバージョン。
- BestPractices: これは LoadMaster で使用する推奨の暗号セットであり、現在の業界のベスト プラクティスを反映するために随時更新されます。 古いブラウザーやアプリケーションの展開で必要になる可能性のある、古いレガシー暗号セットは含まれません。 BestPractices セットの最後の更新は、LMOS 7.2.52.0 で行われました。 詳細については、LoadMaster のリリース ノートを参照してください。
- Intermediate_compatibility: この暗号セットには、古いブラウザやサービスの実装で必要とされるいくつかの暗号が含まれていますが、これらはまだフィールドで見られます。
- Backward_compatibility: この暗号セットは、Windows XP/IE6 に戻るクライアントに対して最大限の下位互換性を提供しますが、安全性の低い暗号を使用するリスクがあります。

Backward_compatibility 暗号セットは、最後の手段としてのみ使用してください。

- WUI: これは、管理ユーザー インターフェイスで使用されるデフォルトの暗号セットです。 [Certificate & Security] > [Admin WUI Access] の下のコントロールを使用して変更できます。
- FIPS: このセットには、連邦情報処理標準 (FIPS) 140-2 レベル 1 標準に準拠する暗号のみが含まれており、それを必要とする展開でのみ使用する必要があります。
- Legacy: この暗号セットは、レガシー LoadMaster ファームウェア バージョン (v7.0-10 以前) のアップグレード互換性のためにのみ提供されています。 LoadMaster の最新バージョンにアップグレードした後は、より安全な暗号セットを選択することをお勧めします。
- Null_Ciphers: この暗号セットには、「null ciphers」と呼ばれるものが含まれています。これは、暗号化による保護を提供せず、提供するアプリケーションに依存します。一般に、これらの暗号は、アプリケーションで必要とされ、そのアプリケーションが提供する場合にのみ使用してください。独立した暗号保護。
- ECDSA_Default: この暗号セットには、楕円曲線暗号を使用する暗号セットのみが含まれており、EC 暗号を必要とする展開に推奨されます。
- ECSDA_BestPractices: これは ECDSA_Default セットの修正版であり、Common Criteria 標準に準拠する暗号のみが含まれています。

各暗号セットに含まれる暗号を確認するには、[Certificate & Security] > [Cipher Set] に移動します。 関連する暗号セットを選択します。

Progress Kemp は、業界のセキュリティ基準とベスト プラクティスの変更に応じて、これらの暗号セットの内容をいつでも変更する権利を留保します。

Available Ciphers と Assigned Ciphers の 2 つのリストが表示されます。これらのリストは、表示される [フィルター] テキスト ボックスにテキストを入力してフィルター処理できます。フィルタ テキスト ボックスには、暗号名に含まれる有効なテキスト (ECDHE など) のみを入力できます。無効なテキストが入力された場合、テキスト ボックスが赤くなり、無効なテキストが削除されます。暗号は、必要に応じて [Available] および [Assigned] リストにドラッグ アンド ドロップできます。す

でに割り当てられている暗号は、[available Cipher] リストでグレー表示されます。構成済みの暗号セットを変更することはできません。ただし、事前構成済みの暗号セットから開始することもできます。必要に応じて変更を加えてから、暗号セットを新しいカスタム名で保存します。 [名前を付けて保存] 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、さまざまな仮想サービスで使用でき、WUI 暗号セットとして割り当てることができます。構成済みの暗号セットを削除することはできません。ただし、関連するカスタム暗号セットを選択し、[暗号セットの削除] ボタンをクリックすると、カスタム暗号セットを削除できます。

9.7 リモートアクセス

以下のセクションでは、LoadMaster WUI のリモート アクセス画面内のさまざまな領域について説明します。

9.7.1 管理者アクセス

Allow Remote SSH Access

クライアントが LoadMaster の SSH 管理インターフェースに接続できるネットワークを制限できます。

Using

LoadMaster へのリモート管理 SSH アクセスを許可するアドレスを指定します。

「bal」ユーザーのみが、SSH を使用して LoadMaster にアクセスする権限を持っています。

LoadMaster ファームウェア バージョン 7.2.48.4 以降の長期サポート

(LTS) および 7.2.53 では、LoadMaster への SSH アクセスで RSA キーがサポートされなくなりました。 SSH アクセスに RSA キーを使用していて、これらのバージョン (またはそれ以降) のいずれかにアップグレードする場合は、別のキー タイプに移行する必要があります。 RSA キーの代替として使用できるキー タイプは 2 つあります。ecdsa-sha2-nistp384 と ssh-ed25519 です。

Port

SSH プロトコルを使用して LoadMaster にアクセスするために使用するポートを指定します。

SSH Pre-Auth Banner

SSH ログイン時のログインプロンプト前に表示される SSH 事前認証バナーを設定します。 このフィールドは最大 5,000 文字まで入力できます。

Allow Web Administrative Access

このチェックボックスを選択すると、LoadMaster への管理 Web アクセスが許可されます。 このオプションを無効にすると、次回の再起動時にアクセスが停止します。 [Set Administrative Access] をクリックして、このフィールドに変更を適用します。

Web アクセスを無効にすることはお勧めしません。

Using

管理 Web アクセスを許可するアドレスを指定します。 [Set Administrative Access] をクリックして、このフィールドに変更を適用します。 変更が適用された後、新しいアドレスを使用して WUI に再接続する必要があります。

Port

管理 Web インターフェイスへのアクセスに使用するポートを指定します。 [Set Administrative Access] をクリックして、このフィールドに変更を適用します。 変更が適用された後、新しいポートを使用して WUI に再接続する必要があります。

Admin Default Gateway

デフォルト以外のインターフェースから LoadMaster を管理する場合、このオプションを使用すると、ユーザーは管理トラフィックのみに別のデフォルト ゲートウェイを指定できます。 [Set Administrative Access] をクリックして、このフィールドに変更を適用します。

Allow Multi Interface Access

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。 このオプションを有効にすると、[Allow Administrative WUI Access] という新しいオプションが各インター

フェイス画面（[System Configuration] > [eth<n>]）に表示されます。 これらのオプションの両方が有効になっている場合、WUI は、関連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構成されている追加のアドレスからアクセスできます。 [Set Administrative Access] をクリックして、このフィールドに変更を適用します。

WUI 接続を保護するためにデフォルトで使用される証明書は、最初の WUI IP アドレスを指定するため、他のインターフェイスの WUI 接続では機能しません。 複数のインターフェイスで WUI を有効にする場合は、WUI 用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。 証明書の詳細については、SSL Accelerated Services の機能説明を参照してください。 複数のインターフェイスで WUI を有効にすると、システムのパフォーマンスに影響を与える可能性があります。 追跡できる最大 64 のネットワーク インターフェイスがあります。 システムがリッスンする合計アドレスは最大 1024 です。

RADIUS Server

ここで、LoadMaster へのユーザー アクセスを検証するために使用される RADIUS サーバーのアドレスを入力できます。 RADIUS サーバーを使用するには、共有シークレットを指定する必要があります。

共有シークレットは、LoadMaster と RADIUS サーバー間のパスワードとして機能するテキスト文字列です。 再検証間隔は、ユーザーが RADIUS サーバーによって再検証される頻度を指定します。

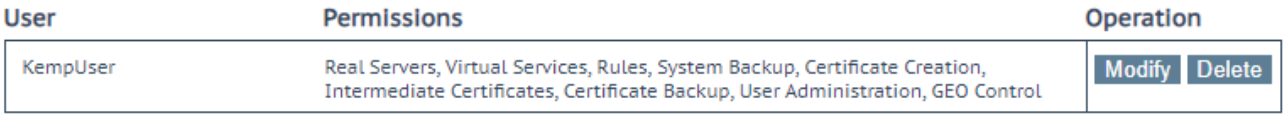
RADIUS Server Configuration

LoadMaster で RADIUS が正しく動作するように構成するには、RADIUS サーバーで認証を構成し、RADIUS 応答メッセージを LoadMaster のアクセス許可にマップする必要があります。 次の表に示すように、Reply-Message の値は LoadMaster のアクセス許可に対応しています。

返信メッセージ	ロードマスター権限
real	Real Server
VS	仮想サービス
rules	Rules
backup	System Backup
certs	中間証明書
certBackup	証明書バックアップ

usres	ユーザー管理
geo	GEO 設定

Reply-Message の値は、図 119 のように WUI のユーザー権限ページにマップする必要があります。ただし、「All Permission」は例外です。



Linux FreeRADIUS サーバーを構成するには、以下のテキストを /etc/freeradius/users ファイル内の指定されたセクションに挿入してください。 以下の例では、ユーザー「LMUSER」の権限を構成しています。

LMUSER Cleartext-Password := "1fourall"Reply-Message = "real,vs,rules,backup,certs,cert3,certbackup,users"

The /etc/freeradius/clients.conf file must also be configured to include the LoadMaster IP address.

This file lists the IP addresses that are allowed to contact RADIUS.

セッション管理が有効になっている場合、この画面で RADIUS サーバー オプションを使用することはできません。 詳細については、WUI の認証と承認のセクションを参照してください。

セッション管理が有効な場合に RADIUS サーバーを構成する方法に関する情報。

Enable API Interface

RESTful アプリケーション プログラム インターフェイス (API) を有効または無効にします。 API インターフェイスへのアクセスに使用するポートを指定することもできます。 ポートが設定されていない場合は、Web インターフェイス ポート経由で API にアクセスできます。

Self-Signed Certificate Handling

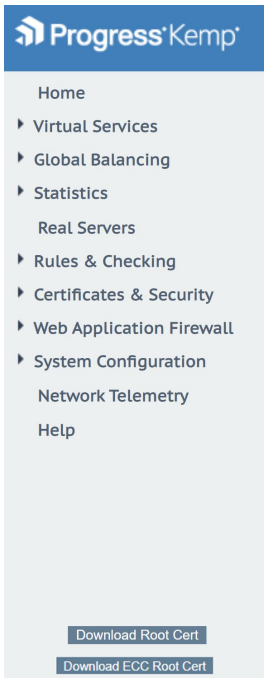
システムが使用する自己署名証明書のタイプを選択します。 オプションは次のとおりです。

- RSA self-signed certs: デフォルトでは、これらは Progress Kemp RSA ルート証明書で署名された RSA 証明書です。
- EC certs with a RSA signature: LoadMaster は、元の RSA Progress Kemp ルート証明書によっても署名された EC 証明書を生成できます。

- EC certs with an EC signature: LoadMaster は、Progress Kemp EC ルート証明書によって署名された EC 証明書を生成できます。 このモードでは、生成されるすべての CSR も EC になります。

自己署名証明書の処理が EC 署名付きの EC 証明書に設定されている場合、CSR の生成は管理 (bal) ユーザーのみに制限されます。 Self-Signed Certificate Handling が別の値に設定されている場合、すべてのユーザーは (権限に関係なく) CSR を生成できます。自己署名証明書の処理が EC モードに設定されていて、乱数生成 (RNG) が失敗した場合 (たとえば、レガシー システムのようにハードウェアがサポートしていない場合)、ホーム画面に「CC モードを開始できませんでした」というメッセージが表示されます -システムが無効になり、WUI が使用できなくなります。これにより、RNG を初期化できない、CC モードが無効になっているという重大なログ メッセージと、RNG の開始に失敗しました、CC モードが開始されていないという authlog も生成されます。このモードを終了するには、(コンソールまたは SSH を使用して) isetup メニューを使用する必要があります。 [Local Admin] > [Web Address] > [Confirm switch out of CC mode] に移動します。このオプションは、LoadMaster がこの状態にある場合にのみ表示されます。これにより、システムは通常どおり動作します (ただし、Common Criteria (CC) モードでは動作しません)。

RSA 自己署名証明書から EC 署名付きの EC 証明書に直接切り替えることはできません。 これを行うと、EC Kemp Certificate Authority (CA) 証明書がないため、接続が失敗します。 これを回避するには、最初に RSA 自己署名証明書から RSA 署名付きの EC 証明書に切り替える必要があります。



次に、ページを更新した後、メイン メニューの下の WUI の右下にある [Download ECC Root Cert] をクリックして、新しい EC Kemp CA 証明書をダウンロードします。 証明書をダウンロードしたら、接続を失うことなく EC 署名付きの EC 証明書に切り替えることができます。

Outbound Connection Cipher Set

アウトバウンド接続 (OCSP、電子メール、LDAP など) で使用する暗号セットを選択します。 これは、すべてのアウトバウンド接続に対してグローバルです。 使用可能な各暗号セットについては、「Cypher Sets」セクションを参照してください。

再暗号化接続は、送信暗号セットの影響を受けません。

Admin Login Method

このオプションは、セッション管理が有効になっている場合にのみ表示されます。 セッション管理の詳細については、「Manage WUI Access」セクションまたは「User Management Feature Description」を参照してください。

LoadMaster WUI にアクセスするためのログイン オプションを指定します。 次のオプションを使用できます。

すべての管理者ログイン方法オプションを使用可能にするには、管理者 WUI アクセス画面の事前認

証クリックスルー バナーを設定する必要があります。

- Password Only Access (デフォルト): このオプションは、ユーザー名とパスワードのみを使用したアクセスを提供します。クライアント証明書を使用したアクセスはありません。
- Password or Client Certificate: ユーザーは、ユーザー名/パスワードまたは有効なクライアント証明書を使用してログインできます。有効なクライアント証明書が存在する場合、ユーザー名とパスワードは必要ありません。クライアントは証明書を要求されます。クライアント証明書が提供されている場合、LoadMaster は一致をチェックします。 LoadMaster は、証明書がローカル証明書の 1 つと一致するかどうか、または証明書のサブジェクト代替名 (SAN) または共通名 (CN) が一致するかどうかを確認します。照合の実行時には、CN よりも優先して SAN が使用されます。一致する場合、ユーザーは LoadMaster へのアクセスを許可されます。これは、API を使用した両方で機能しますおよびユーザー インターフェイス。無効な証明書はアクセスを許可しません。クライアント証明書が提供されない場合、LoadMaster はユーザー名とパスワードが (API 用に) 提供されることを期待するか、標準の WUI ログイン ページを使用してユーザーにパスワードの入力を求めます。
- Client Certificate Required: アクセスは、クライアント証明書を使用する場合にのみ許可されます。 ユーザー名とパスワードを使用してログインすることはできません。 SSH アクセスはこれによる影響を受けません (SSH を使用してログインできるのは bal ユーザーのみです)。
- Client Certificate Required (OCSP 経由で検証): これは [クライアント証明書が必要] オプションと同じですが、クライアント証明書は OCSP サービスを使用して検証されます。これを機能させるには、OCSP サーバー設定を構成する必要があります。 OCSP サーバー設定の詳細については、「暗号セット」セクションを参照してください。

LoadMaster ファームウェア バージョン 7.2.53 以降では、証明書に機関情報アクセス (AIA) 拡張機能がある場合、OCSP サーバー設定を LoadMaster で構成する必要はありません。 LoadMaster は、提供された AIA との接続を試みます。 導入された機能の詳細については、WUI の認証と承認のセクションを参照してください。

クライアント証明書の方法に関する注意点を以下に示します。

- bal ユーザーにはクライアント証明書がありません。 したがって、クライアント証明書が必要な方法を使用して bal として LoadMaster にログインすることはできません。 ただ

し、非 bal ユーザーを作成してすべての権限を付与することはできます。 これにより、bal ユーザーと同じ機能が可能になります。

- クライアント証明書を使用して WUI にログインしているユーザーは、ログアウトすることができないため、ログアウト オプションはありません (ユーザーがログアウトした場合、次のアクセスで自動的に再度ログインします)。 ページが閉じられるか、ブラウザが再起動されると、セッションは終了します。

クライアント証明書の WUI 認証の詳細については、構成方法の段階的な手順を含めて、Progress Kemp ドキュメント ページのユーザー管理、機能の説明を参照してください。

Allow Client Certificate Login Without Locally Installed User Certificate

このオプションを有効にすると、クライアント証明書が LoadMaster から削除されていても、ローカル ユーザーのクライアント証明書ログインが許可されます。 デフォルトでは、このオプションは有効になっています。

Enable Software FIPS 140-2 level 1 Mode

セッション管理が無効になっている場合、FIPS モードを有効にすることはできません。 セッション管理の詳細については、「Manage WUI Access」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 認定モードに切り替えます。 アクティブ化するには、LoadMaster を再起動する必要があります。

FIPS を有効にする前に、いくつかの警告が表示されます。 LoadMaster で FIPS が有効になっている場合、簡単に無効にすることはできません。 FIPS が有効になっており、無効にしたい場合は、Progress Kemp サポートにお問い合わせください。

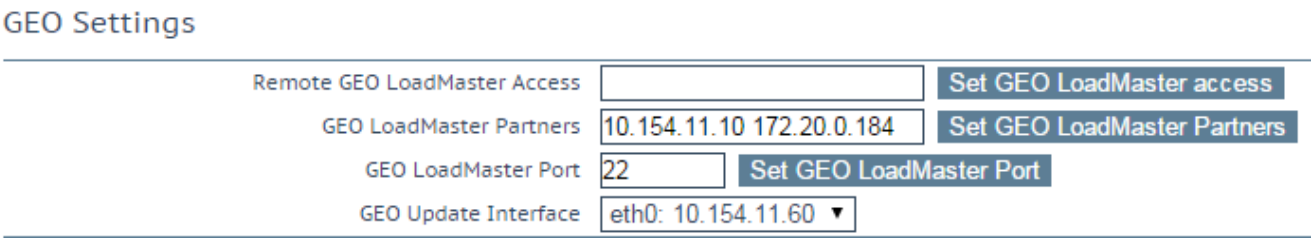
LoadMaster が FIPS レベル 1 モードの場合、LoadMaster WUI の右上に FIPS-1 が表示されます。 FIPS レベル 1 には、非 FIPS LoadMaster とは異なる暗号のセットがあります。 デフォルトの暗号セットがあり、他に選択できるシステム定義の暗号セットはありません。

FIPS が有効になっている場合、RADIUS 認証は使用できません。

Enable Kemp Analytics

統計データと使用状況データを分析のために Progress Kemp に送信できるようにします。 このデータは、厳密には製品の使用状況、有効な機能、および統計に関するものです。 機密性の高いユーザーデータや、あらゆる種類のトラフィックが収集または伝達されることはありません。 詳細については、https://kemp.ax/KempAnalytics をご覧ください。

9.7.2 地域設定



Remote GEO LoadMaster Access

この LoadMaster からサービス ステータス情報を取得できる 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られています。 HA モードの場合、共有アドレスのみを入力する必要があります。

GEO LoadMaster Partners

GEO 機能は GSLB Feature Pack の一部として提供され、LoadMaster に適用されたライセンスに基づいて有効になります。 GSLB 機能パックを入手したい場合は、Kemp に連絡してライセンスをアップグレードしてください。

パートナーの 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られています。 これらの GEO LoadMaster は、DNS 構成を同期させます。

GEO LoadMaster を提携する前に、適切な / 好ましい構成を持つ関連する GEO LoadMaster のバックアップを作成する必要があります。 このバックアップは、元の LoadMaster と提携する他の LoadMaster に復元する必要があります。 詳細および段階的な手順については、GEO、機能の説明を参照してください。 最大 64 の GEO HA パートナー アドレスを追加できます。

GEO LoadMaster Port

GEO LoadMaster がこの LoadMaster ユニットとの通信に使用するポート。

GEO update interface

SSH パートナー トンネルが作成される 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インターフェイスです。

9.7.3 パートナーのステータス

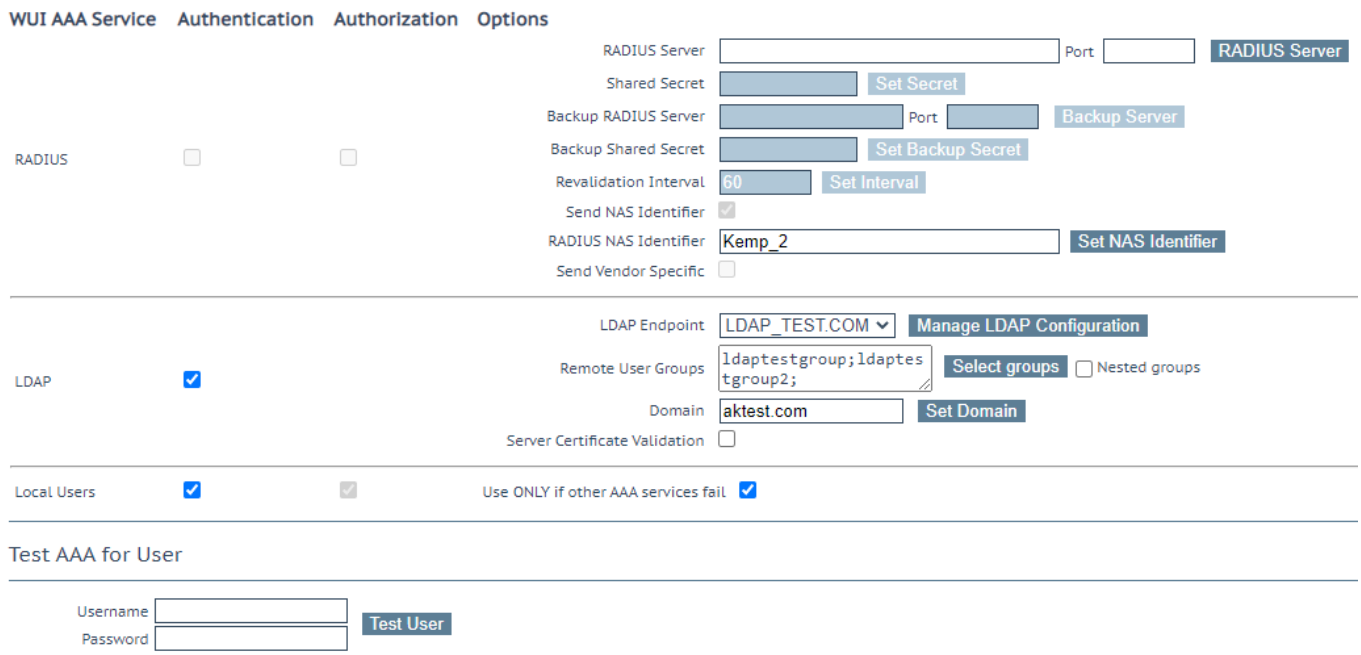
このセクションは、GEO パートナーが設定されている場合にのみ表示されます。

緑の GEO パートナー ステータスは、 2 つのパートナーが相互に認識できることを示します。 赤の GEO パートナー ステータスは、ロードマスターが通信できないことを示します。 この理由には次のようなものがあります (他の可能性の中でも)。 パートナーの 1 つで電源がオフになっている場合、停電が発生しているか、ケーブルが切断されている可能性があります。 GEO パートナーの更新に失敗した場合、パートナーへの GEO 更新が失敗したことを示すエラー メッセージがログに表示されます。 メッセージには、パートナーの IP アドレスが表示されます。

9.7.4 WUI の認証と承認

WUI Authorization Options

[Remote Access] 画面の [WUI Authorization Option] ボタンをクリックして、[WUI Authentication & Authorization] 画面を表示します。 このオプションは、セッション管理が有効になっている場合にのみ使用できます。



WUI の [WUI Authentication & Authorization] 画面では、利用可能な認証 (ログイン) および承認 (許可されたアクセス許可) オプションを管理できます。

Authentication

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

1. RADIUS
2. LDAP
3. Local Users

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

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

Authorization

LoadMaster では、RADIUS、LDAP、またはローカル ユーザー認証を使用してユーザーを認証でき

ます。 ユーザーの権限によって、ユーザーが持つ権限のレベルと、LoadMaster で実行できる機能が決まります。

RADIUS 認証方式を使用するには、[RADIUS Authentication] チェック ボックスをオンにする必要があります。 認証はアクセス用であり (ユーザーが有効なユーザー名とパスワードを持っていることを確認するため)、承認はアクセス許可に使用されます。

すべての認証方法が選択されている場合、LoadMaster は次の順序で認証をチェックします。

1. RADIUS
2. LDAP
3. Local Users

たとえば、RADIUS サーバーが使用できない場合は、LDAP サーバーが使用されます。 LDAP サーバーも使用できない場合は、ローカル ユーザー認証方法が使用されます。 RADIUS と LDAP のどちらの認証/許可方法も選択されていない場合は、デフォルトでローカル ユーザー認証方法が選択されます。 使用している RADIUS/LDAP サーバーを構成して、WUI のユーザー アクセス許可ページに表示されるのと同じユーザー アクセス許可を承認する必要があります ([All Permission] を除く)。 RADIUS サーバーから返された Reply-Message は、許可されている権限を示します。 Linux システムでは、メッセージは次のようになります。

LMUSER Cleartext-Password := "1fourall"Reply-Message = "real,vs,rules,backup,certs,cert3,certbackup,users"

上記の例は、Linux システムにデプロイされた RADIUS サーバー上の RADIUS ユーザー構成です。 LoadMaster は、"Reply-Message" からユーザーのアクセス許可を決定します (アクセス許可は、LoadMaster のローカル WUI ユーザーのものと似ています)。

bal ユーザーは常に、ローカル ユーザー認証および承認方法を使用して認証および承認されます。 ローカル ユーザー認証を無効にしても、bal ユーザーはロックアウトされません。 Bal は管理者/スーパー ユーザーであり、ロードマスターでローカル ユーザー認証が無効になっている場合でも、ロードマスター WUI にログインできます。

RADIUS Server Configuration

RADIUS Server

LoadMaster へのユーザー WUI アクセスを認証するために使用される RADIUS サーバーの IP アドレスとポート。

Shared Secret

この入力フィールドは、RADIUS サーバーの共有シークレット用です。 共有シークレットは、LoadMaster と RADIUS サーバー間のパスワードとして機能するテキスト文字列です。

Backup RADIUS Server

LoadMaster へのユーザー WUI アクセスの認証に使用されるバックアップ RADIUS サーバーの IP アドレスとポート。 このサーバーは、メインの RADIUS サーバーに障害が発生した場合に使用されます。

Backup Shared Secret

このテキスト ボックスは、バックアップ RADIUS サーバーの共有シークレットを入力するためのものです。

Revalidation Interval

ユーザーが RADIUS サーバーによって再検証される頻度を指定します。

Send NAS Identifier

このチェック ボックスが無効になっている場合 (デフォルト)、NAS 識別子は RADIUS サーバーに送信されません。 有効になっている場合、ネットワーク アクセス サーバー（NAS）の識別子文字列が RADIUS サーバーに送信されます。 デフォルトでは、これはホスト名です。 または、値が RADIUS NAS 識別子テキスト ボックスに指定されている場合、この値が NAS 識別子として使用されます。 NAS 識別子を追加できない場合でも、RADIUS アクセス要求は処理されます。 NAS 識別子の送信には、次の 2 つの目的があります。

- 単にホスト IP アドレスを送信するのではなく、リクエストを送信しているデバイス タイプを分類するのに役立ちます。これにより、トラブルシューティングとログの消費が容易になります。
- 識別子に基づいて、カスタマイズされた認証応答をサーバーから送り返すことができます。

Send Vendor Specific

LoadMaster ファームウェア バージョン 7.2.51 以降では、RADIUS サーバーが設定されている場合、ユーザー インターフェース (UI) に Send Vendor Specific というチェック ボックスがあります。 Send Vendor Specific チェックボックスが有効で、ユーザーが Cisco Access Control Server (ACS) または Identity Services Engine (ISE) で RADIUS 認証を使用して LoadMaster UI にログ

インしている場合、LoadMaster は属性値ペア (AVP) をサーバーに送信します。 Kemp のベンダー ID を含むログイン要求の一部として。 サーバーは、受信時にこの AVP を使用して LoadMaster デバイスを識別できます。 この属性の形式と要件は、RFC 2865 のセクション 5.26 にあります。 Kemp ベンダー ID は 12196 です。

RADIUS NAS Identifier

Send NAS Identifier チェックボックスが選択されている場合、RADIUS NAS Identifier フィールドが表示されます。 指定すると、この値が NAS 識別子として使用されます。 それ以外の場合、ホスト名が NAS 識別子として使用されます。 NAS 識別子を追加できない場合でも、RADIUS アクセス要求は処理されます。

LDAP Endpoint

使用する関連する LDAP エンドポイントを選択します。 [Manage LDAP Configuration] ボタンをクリックして、[LDAP Configuration] 画面に移動します。 LDAP エンドポイントの詳細については、「LDAP 構成」セクションを参照してください。 LoadMaster ファームウェア バージョン 7.2.53 では、PIV スマート カード認証のサポートが追加されました。 その結果、[Certificate & Security] > [Remote Access] > [WUI Authorization Option] 画面に、新しい [Select Certification to User Mapping] ドロップダウン リストが追加されました。 このフィールドには次の値があります。

- ユーザープリンシパル名 (デフォルト値)
- 件名
- 発行者とサブジェクト
- 発行者とシリアル番号

構成に関する注意事項を以下に示します。

- [WUI Authorization Option] ボタンを表示するには、セッション管理を有効にする必要があります ([Certificate & Security] > [Administrator WUI])。
- [Certificate & Security] > [Remote Access] の [Admin Login Method] を [Client Certification] に設定して、新しい [Select Certificate to User Mapping] ドロップダウン リストを表示する必要があります。
- [Certificate & Security] > [Remote Access] で [Admin Login Method] としてクライアント証明書方法を選択するには、[Certificate & Security] > [Admin WUI Access] で事前認証クリックスルー バナーを設定する必要があります。
- 証明書が取り消された後、証明書は認証に失敗します。ただし、キャッシュに残っている場

合があるため、すぐに失敗するようにするには、[System Configuration] > [System Administration] > [Log Options] > [Debug Options] で [Flush OCSPD Cache] オプションを使用してください。

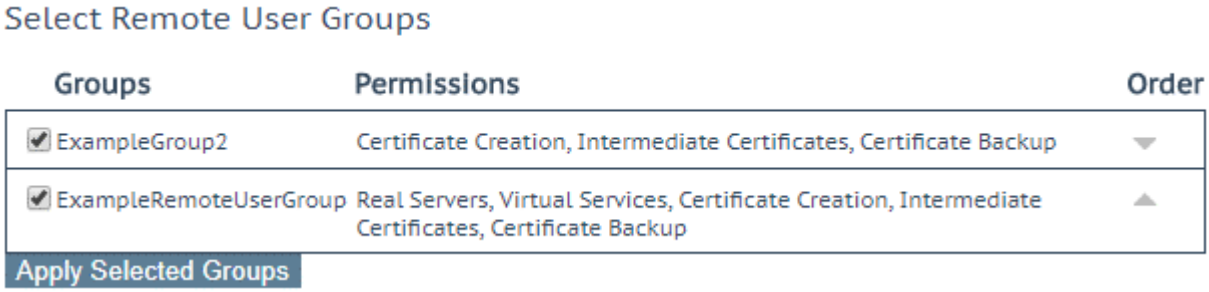
- LDAP クエリが複数の一致を返した場合、ログインは失敗します。
- 証明書に機関情報アクセス (AIA) が存在する場合、LoadMaster は提供された AIA に接続しようとします。これが機能しない場合は、ローカル サーバーへの接続を試みます。
- LoadMaster が証明書 AIA で構成されたサーバーのステータスを取得できない場合、LoadMaster はローカル サーバーにフェールバックしません。
- サーバーが使用できないために証明書を検証できない場合は、[Certificate & Security] > [OCSP Configuration] に、[Allow Access on Server] というオプションがあり、認証に合格するかどうかを決定できます。このチェック ボックスを有効にすると、OCSP サーバー接続の失敗またはタイムアウトが、OCSP サーバーが有効な応答を返したかのように扱われます。つまり、クライアント証明書は有効なものとして扱われます。

クライアント ユーザーがクライアント証明書で認証されている場合、共通名 (CN) は小文字に正規化されます。 したがって、アクセス許可に必要な関連するローカル ユーザー エントリ (パスワードなし) も小文字にする必要があります。

Remote User Groups

選択されたすべてのリモート ユーザー グループがここに表示されます。 グループを選択、クリア、または並べ替えるには、[Select Groups] をクリックします。

グループを選択して適用することが重要です。 グループが選択されていない場合、グループ チェックは実行されず、リモート ユーザーはグループ チェックなしでログインできます。



この画面に表示されるグループは、[System Configuration] > [System Administration] > [User Management] で設定されたリモート ユーザー グループから取得されます。 詳細については、「ユーザー管理」セクションを参照してください。 ユーザーがログインすると、次の条件がすべて満たされている場合、Active Directory 上のユーザー グループのチェックが実行されます。

- LDAP WUI 認証が有効な場合
- グループのリストが定義されている
- ログインしているユーザーがローカルで定義されていないか、ローカル ユーザー オプションが無効になっています

この画面でグループの順序を変更できます。 最初のグループが最初にチェックされます。 最初のグループ一致で、アクセスが有効になり、それ以上のグループはチェックされません。 一致するグループがない場合、ユーザー アクセスは失敗し、適切なログが syslog に報告されます。 ユーザーがグループ チェックを使用してログインすると、一致したグループ権限が付与されます。

Nested Groups

[Nested groups] チェック ボックスを使用して、WUI の [Authentication and Authorization] 画面でユーザーのネストされたグループを有効または無効にできます。

Domain

グループ WUI 認証を使用しているときに、ユーザー名にドメインが指定されていない場合に使用するドメインを指定します。 Windows ログオンがプレフィックス¥ユーザー名の形式で使用されている場合、グループ検索のドメインとして常に使用されます。

ドメイン フィールドは、 1 つまたは複数のグループが割り当てられている場合にのみ表示されます。

Server Certificate Validation

このチェック ボックスは、選択した LDAP エンドポイントの LDAP プロトコルが StartTLS または LDAPS である場合にのみ表示されます。

サーバー証明書の検証が StartTLS で機能しないという既知の問題があります。

サーバー証明書の検証が有効になっている場合、安全な接続を開始するために使用されたホスト名または IP アドレスが、証明書の証明書サブジェクトまたはサブジェクト代替名 (SAN) に存在することが

保証されます。 サーバー証明書の検証はデフォルトで無効になっています。

Local Users Configuration

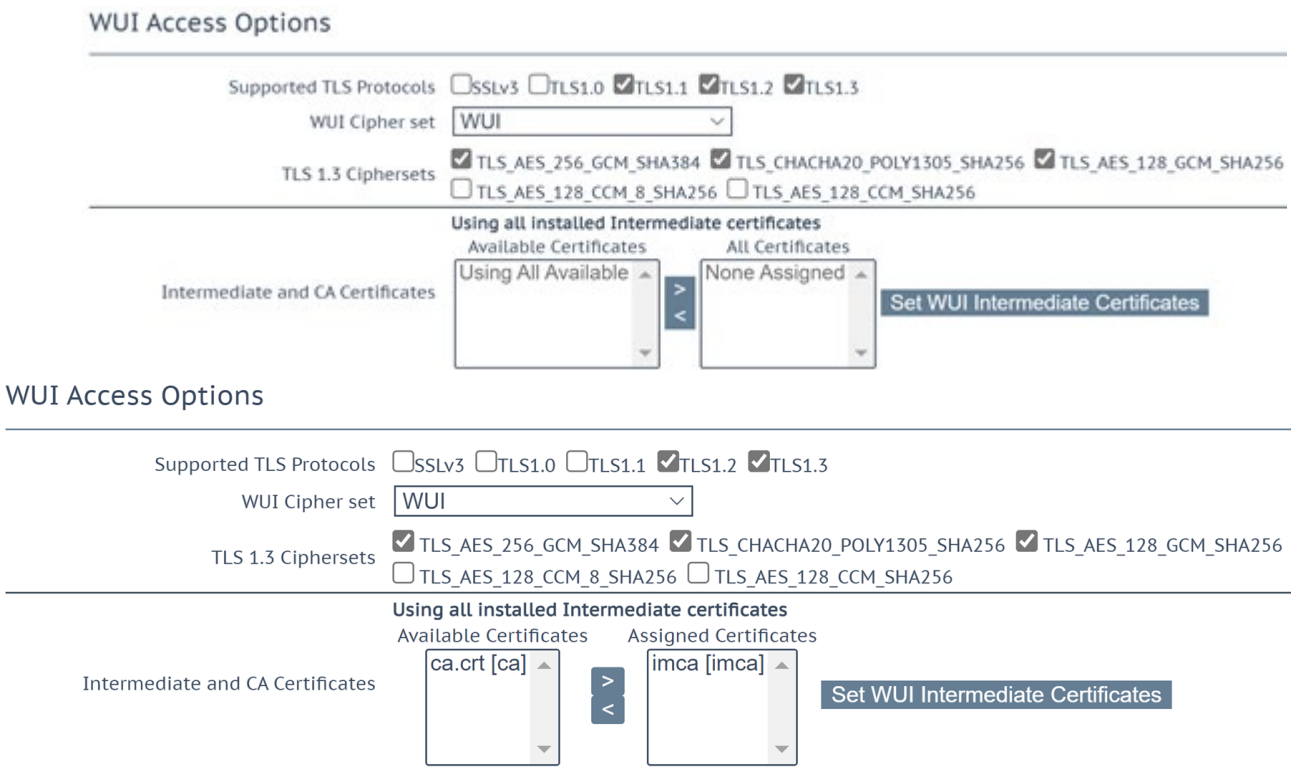
Use ONLY if other AAA services fail

選択すると、RADIUS や LDAP の認証および承認サービスが応答しないかタイムアウトした場合にのみ、ローカル ユーザーの認証および承認方法が使用されます。

Test AAA for User

ユーザーの資格情報をテストするには、[Username] フィールドと [Password] フィールドにユーザー名とパスワードを入力し、[Test User] ボタンをクリックします。 ユーザーが検証されているかどうかを通知するメッセージが表示されます。 これは、ログインまたはログアウトせずにユーザーの資格情報を確認するための便利なユーティリティです。

9.8 管理者 WUI アクセス



Supported TLS Protocols

以下のプロトコルを使用して LoadMaster WUI に接続できるかどうかを指定するために使用できるチェックボックスがここに用意されています。 SSLv3、TLS1.0、TLS1.1、TLS1.2、または TLS1.3。 TLS1.1、TLS1.2、および TLS1.3 はデフォルトで有効になっています。 SSLv3 は一部

の古いブラウザーでしかサポートされていないため、SSLv3 のみを選択することはお勧めしません。Web ブラウザーを使用して WUI に接続する場合、ブラウザーと WUI の両方で相互にサポートされている最高のセキュリティ プロトコルが使用されます。

FIPS モードが有効な場合、使用可能なオプションは TLS1.1 と TLS1.2 のみです。

WUI Cipher set

WUI アクセスに使用する関連する暗号セットを選択します。 使用可能な各暗号セットについては、「暗号セット」セクションを参照してください。

TLS1.3 Cipher sets

管理者 WUI アクセス プロトコルでサポートされている暗号の任意の組み合わせを使用して許可される TLS1.3 プロトコルの暗号セットを選択します。 デフォルトでは、次の 3 つの暗号セットが有効になっています。

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS1.3 暗号セットは、TLS1.3 プロトコルが有効になっている場合にのみ使用可能になります。
３つのデフォルトの暗号セットをすべて無効にすると、LoadMaster への接続が失われる可能性があります。

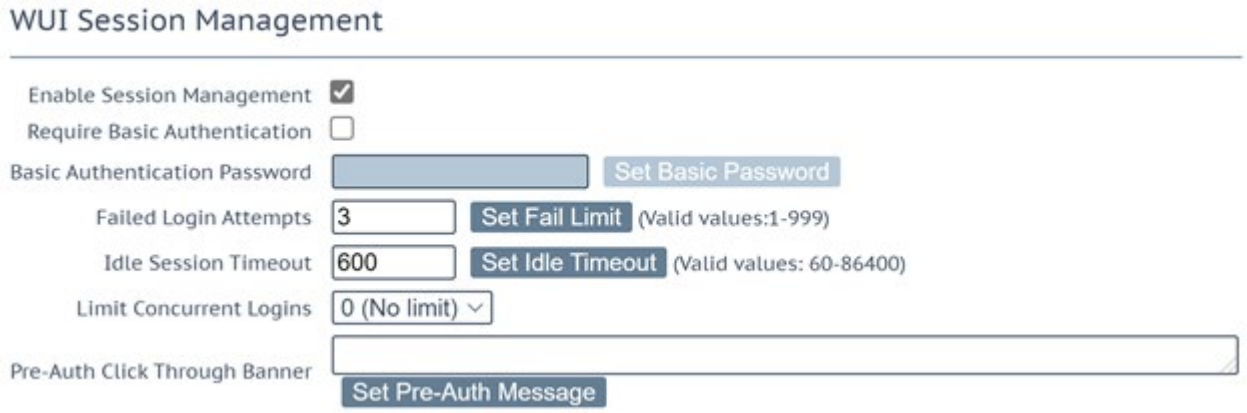
Intermediate and CA Certificates

UI アクセス認証のデフォルトの動作は、信頼された LoadMaster ストア内のいずれかによって検証されたクライアント証明書を受け入れることです。 LoadMaster ファームウェア バージョン 7.2.55 では、ユーザーは特定の中間証明書を指定して、UI アクセス認証用のクライアント証明書を検証するために使用できるようになりました。 使用可能な証明書は、左側の [Available Certificates] 選択リストに表示されます。 証明書を割り当てたり、割り当てを解除したりするには、証明書を選択して右矢印または左矢印ボタンをクリックします。 次に、[Set WUI Intermediate Certificates] をクリックします。 キーボードで Ctrl を押しながら必要な各証明書をクリックすると、複数の証明書を選択できます。

LoadMaster ファームウェア バージョン 7.2.55 では、中間および CA 証明書のサポートが追加さ

れました。 デフォルトでは、すべての中間証明書は、WUI アクセスに使用される [すべての証明書] リストの下に表示されます。 いずれかの証明書が [すべての証明書] リストから [使用可能な証明書] リストに移動されると、[すべての証明書] リストの名前が [割り当てられた証明書] リストに変更されます。 このシナリオでは、割り当てられた証明書リストにリストされている証明書が WUI アクセスに使用されます。

WUI Session Management



セッション管理は、LTS ファームウェア バージョン以降で最初にデプロイされたすべてのロードマスターで、デフォルトで有効になっています。
ユーザー権限のレベルによって、表示および変更できる WUI セッション管理フィールドが決まります。 権限の内訳については、次の表を参照してください。

管理対象	Bal User	すべての権限をもつユーザー	ユーザー管理権限をもつユーザー	その他のユーザー
セッション管理	Modify	View	View	None
基本認証パスワード	Modify	View	View	None
ログイン試行の失敗	Modify	View	View	None
アイドル セッション タイム	Modify	Modify	View	None
同時ログインを	Modify	Modify	View	None

制限する				
事前認証クリックスルー バナー	Modify	Modify	View	None
現在アクティブなユーザー	Modify	Modify	View	None
現在ブロックされているユーザー	Modify	Modify	View	None

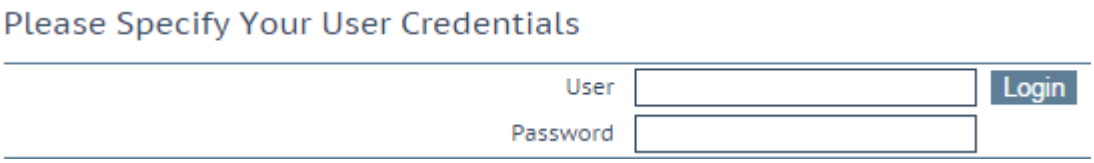
WUI セッション管理を使用する場合、1 段階または 2 段階の認証を使用できます。 [Enable Session Management] チェックボックスがオンになっており、[Require Basic Authentication] が無効になっている場合、ユーザーはローカルのユーザー名とパスワードを使用してログインするだけで済みます。 ユーザーは、bal またはユーザー ログインを使用してログインするように求められません。 [Enable Session Management] チェック ボックスと [Require Basic Authentication] チェック ボックスの両方が選択されている場合、LoadMaster WUI にアクセスするために 2 つのレベルの認証が適用されます。 初期レベルは、システムによって定義されたデフォルトのユーザー名である bal またはユーザー ログインを使用してユーザーがログインする基本認証です。
ユーザー user の目的は、管理者が bal 資格情報を提供する代わりに、ユーザー user の資格情報を人々に提供できるようにすることです。 ユーザー user のパスワードは、[Basic Authentication Password] テキスト ボックスを構成することで設定できます。 基本認証パスワードの設定は、bal ユーザーのみが許可されています。基本認証を使用してログインすると、ユーザーはローカルのユーザー名とパスワードを使用してログインし、セッションを開始する必要があります。

Enable Session Management

[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。 これにより、すべてのユーザーが通常の資格情報を使用してセッションにログインすることが強制されます。 このチェック ボックスをオンにすると、ユーザーは LoadMaster を引き続き使用するためにログインする必要があります。

LDAP ユーザーは、完全なドメイン名を使用してログインする必要があります。 例えば; LDAP ユー

ザー名は、test だけでなく、test@kemp.com にする必要があります。



ユーザーがログインした後、画面の右上隅にある [Logout] ボタン をクリックしてログアウトできます。 WUI セッション管理機能が有効になると、すべての WUI セッション管理オプションが表示されます。

Require Basic Authentication

WUI セッション管理と基本認証の両方が有効になっている場合、LoadMaster WUI にアクセスするために 2 つのレベルの認証が適用されます。 初期レベルは、システムによって定義されたデフォルトのユーザー名である bal またはユーザー ログインを使用してユーザーがログインする基本認証です。基本認証でログインしたら、ユーザーはローカルのユーザー名とパスワードを使用してログインし、セッションを開始する必要があります。

Basic Authentication Password

ユーザー ログインの基本認証パスワードを設定するには、[Basic Authentication Password] テキスト ボックスにパスワードを入力し、[Set Basic Password] ボタンをクリックします。 パスワードは 8 文字以上で、英字と数字を組み合わせてください。 パスワードが弱すぎると思われる場合は、新しいパスワードの入力を求めるメッセージが表示されます。 基本認証パスワードを設定できるのは、bal ユーザーだけです。

Failed Login Attempts

ユーザーがブロックされるまでに正しくログインできなかった回数を、このテキスト ボックスで指定できます。 入力できる有効な値は 1 ～ 999 の数字です。ユーザーがブロックされている場合、bal ユーザーまたはすべての権限が設定されている他のユーザーのみが、ブロックされたユーザーのブロックを解除できます。 bal ユーザーがブロックされている場合、bal ユーザーが再度ログインできるようになるまでに 10 分間の「クールダウン」期間があります。

Idle Session Timeout

ユーザーがアイドル状態 (アクティビティが記録されていない状態) でセッションからログアウトされるまでの時間 (秒単位)。 入力できる有効な値は、60 ～ 86400 (1 分 ～ 24 時間) の数値です。

自動的に更新されるページは、WUI Idle Session Timeout 設定からタイムアウトしません。 たとえば、リアルタイム統計ページ、GSLB 統計ページ、WAF 誤検知分析ページなどです。

Limit Concurrent Logins

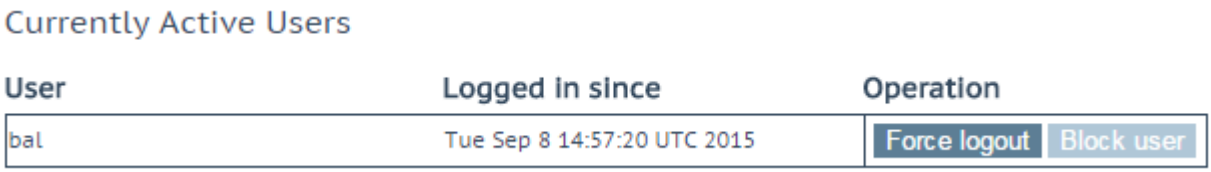
このオプションを使用すると、LoadMaster 管理者は、1 人のユーザーが LoadMaster WUI に同時にログインできる同時ログイン セッションの最大数を制限できます。 選択できる値の範囲は 0 から 9 です。値 0 を指定すると、無制限にログインできます。 入力した値は合計数を表し、すべての bal ユーザー ログインを含みます。

Pre-Auth Click Through Banner

LoadMaster WUI ログイン ページの前に表示される認証前のクリック スルー バナーを設定します。 このフィールドには、プレーン テキストまたは HTML コードを含めることができますが、JavaScript を含めることはできません。 セキュリティ上の理由から、' (一重引用符) および " (二重引用符) 文字は使用できません。 このフィールドは最大 5,000 文字まで入力できます。

Active and Blocked Users

この機能を使用できるのは、bal ユーザーまたは「すべての権限」が設定されているユーザーのみです。 「ユーザー管理」権限が設定されているユーザーは画面を表示できますが、すべてのボタンと入力フィールドがグレー表示されます。 他のすべてのユーザーは、画面のこの部分を表示できません。



Currently Active Users

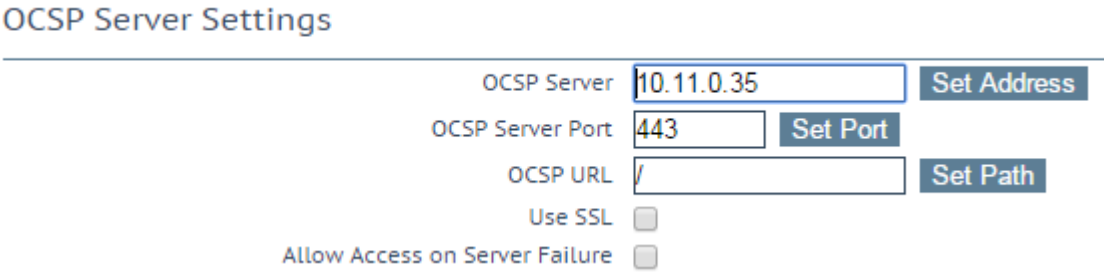
LoadMaster にログインしているすべてのユーザーのユーザー名とログイン時刻が、このセクションに一覧表示されます。 ユーザーをただちにログアウトさせ、強制的にシステムに再度ログインさせるには、[Force logout] ボタンをクリックします。 ユーザーがシステムにログインできないようにブロックするには、[Block user] ボタンをクリックします。 ブロックが解除されるか、LoadMaster が再起動するまで、ユーザーはシステムに再度ログインできません。 [Block user] ボタンをクリックしても、ユーザーは強制的にログオフされません。これを行うには、[Force logout] ボタンをクリックします。 ユーザーがログオフせずにブラウザーを終了すると、タイムアウトに達するまで、そのセッションは現在アクティブなユーザー リストで開いたままになります。 同じユーザーが再度ログインする

と、タイムアウトに達する前に、別のセッション内になります。

Currently Blocked Users

ユーザーがブロックされたときのユーザー名とログイン時刻がこのセクションに表示されます。 ユーザーのブロックを解除してシステムへのログインを許可するには、[Unlock] ボタンをクリックします。

9.9 OCSP 構成



OCSP Server

OCSP サーバーのアドレス。 これは、IP アドレスまたは完全修飾ドメイン名（FQDN）形式のいずれかです。

OCSP Server Port

OCSP サーバーのポート。

OCSP URL

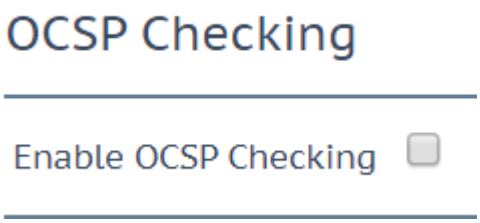
OCSP サーバーでアクセスする URL。

Use SSL

SSL を使用して OCSP サーバーに接続するには、これを選択します。

Allow Access on Server Failure

OCSP サーバー接続の失敗またはタイムアウトを、OCSP サーバーが有効な応答を返したかのように扱います。つまり、クライアント証明書を有効なものとして扱います。

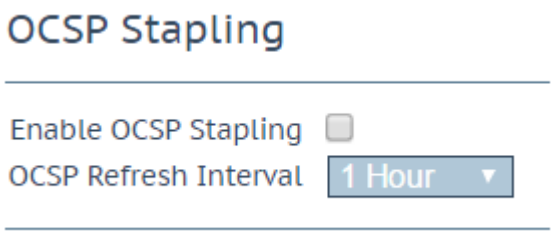


OCSP Checking

証明書認証 (LDAP やリモート ロギングなど) を使用するアウトバウンド管理接続の OCSP チェックを有効にするために必要なのは、[Enable OCSP Checking] UI コントロール (および関連する API) だけです。

- OCSP サーバー/ポート/URL オプションが設定されていない場合、すべての OCSP チェックは、検証される証明書の AIA 情報の OCSP サーバー設定に依存し、この情報はオプションです。 この情報が存在しないか無効な場合、チェックは実行されません。
- OCSP サーバー/ポート/URL オプションが設定されている場合、AIA セクションで OCSP サーバーが設定されていない証明書は、指定された OCSP サーバーの詳細を使用してチェックされます。
- 証明書と OCSP サーバー/ポート/URL の両方に OCSP サーバー アドレスの詳細が設定されている場合、証明書で使用可能な情報のみが証明書の検証に使用されます。証明書で OCSP サーバーに提供された詳細が無効な場合 、OCSP チェックは、証明書を検証するために LoadMaster OCSP サーバー設定に切り替わりません。

OCSP サーバー/ポート/URL 設定に関する上記の動作は、サーバー証明書チェーンの OCSP チェックにも適用されます。 上記の制御では、実サーバー接続の OCSP チェックが有効にならないことにも注意してください。 実サーバーの OCSP 証明書チェックは、Force Real Server Certificate Checking オプションによって有効になります。



Enable OCSP Stapling

LoadMaster が OCSP ステープル要求に応答できるようにするには、このチェック ボックスをオンにします。 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、これが返されます。仮想サービス証明書のみが検証されます。 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 デーモンによって維持されます。 OCSP デーモンがサーバーに要求を送信するとき、証明書で指定された名前を使用します (Authority Information Access フィールド内)。 この名前を解決できない場合は、[OCSP Server] テキスト ボ

ックスで指定されたデフォルトの OCSP サーバーを使用します。

OCSP Refresh Interval

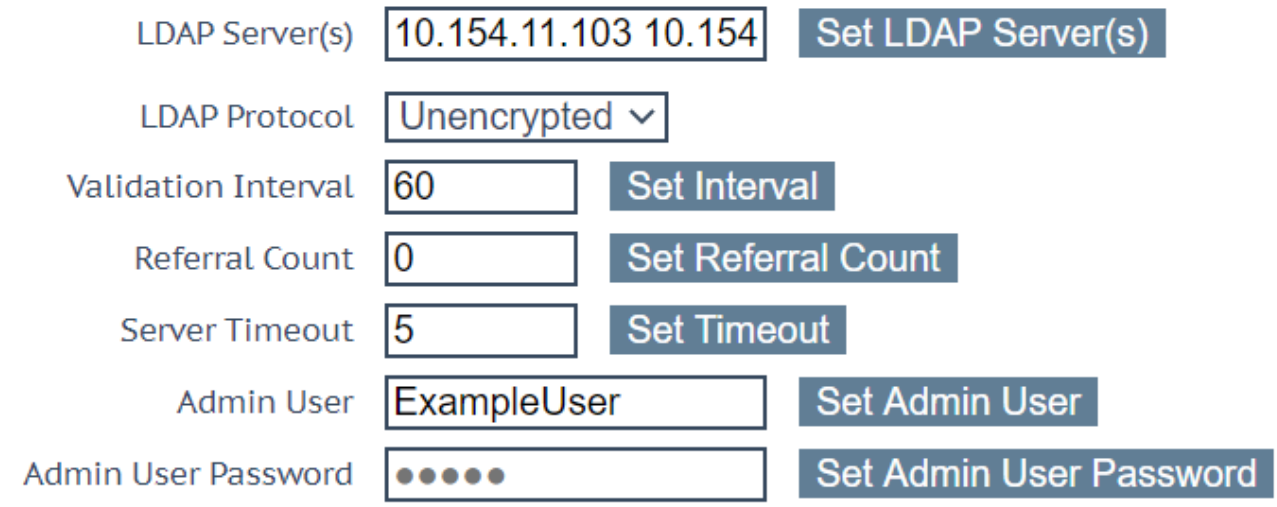
LoadMaster が OCSP ステープル情報を更新する頻度を指定します。 OCSP デーモンは、ここで指定された時間までエントリをキャッシュし、その後更新されます。 有効な値の範囲は、1 時間 (デフォルト) から 24 時間です。

9.10 LDAP 構成

[LDAP 構成] 画面に移動するには、[Certificates & Security] を展開し、[LDAP Configuration] をクリックします。 この画面は、LDAP エンドポイントの管理インターフェースを提供します。 これらの LDAP エンドポイントは、次の 3 つの異なる領域で使用できます。

- ヘルスチェック
- SSO ドメイン
- WUI 認証

既存の LDAP エンドポイントがすべてここに一覧表示され、変更と削除のオプションが表示されます。 LDAP エンドポイントが使用中の場合、削除できません。 新しい LDAP エンドポイントを追加するオプションもあります。 エンドポイントの名前を入力し、[Add] をクリックします。 LDAP エンドポイント名にスペースと特殊文字を使用することはできません。



LDAP Server(s)

使用する LDAP サーバーのスペース区切りのリストを指定します。 Windows アドミン コントローラー (AC)/ドメイン コントローラー (DC) の場合、複数のドメインと許可されたグループのアクセス範囲はユニバーサルに設定されます。 必要に応じて、ポート番号も指定できます。 複数のドメインがあり、許可されたグループを使用している場合、グローバル カタログのポート番号を含める必要がある場合があります。そうしないと、許可されたグループが失敗します。 デフォルトのポートは 3268 です。たとえば、10.110.20.23:3268 です。 LoadMaster は OCSP を使用して、構成された LDAPS サーバーによって提供されるサーバー証明書の有効性を確認します。 これらのチェックに失敗した場合、サーバーへの接続は許可されません。

LDAP Protocol

LDAP サーバーとの通信時に使用するトランスポート プロトコルを選択します。

認証プロトコルを証明書に設定して SSO ドメインを作成する場合は、LDAP プロトコルを LDAPS に設定してください。

LDAP エンドポイントで。

Validation Interval

LDAP サーバーでユーザーを再検証する頻度を指定します。

Referral Count

LoadMaster は、Active Directory ドメイン コントローラーからの LDAP 参照応答をサポートするベータ機能を提供します。 これが 0 に設定されている場合、参照サポートは有効になりません。 このフィールドを 1 ～ 10 の値に設定して、紹介の追跡を有効にします。 指定された数によって、ホップ数が制限されます (紹介が追跡されます)。

複数のホップがあると、認証の待ち時間が長くなる可能性があります。 構成で必要なリフェラルの数と深さに応じて、パフォーマンスに影響があります。 紹介の制限を適切に設定するには、Active Directory の構造をよく理解している必要があります。 すべての検索に同じ資格情報が使用されます。 Active Directory グローバル カタログ (GC) の使用が推奨されます
LDAP リフェラルの追跡を有効にする代わりに、解決の主要な手段として設定を使用します。 LDAP と参照プロセスに依存する代わりに、GC クエリを使用して GC キャッシュをクエリできます。
Active Directory GC を使用すると、LoadMaster のパフォーマンスがほとんどまたはまったく低下しません。 GC を追加/削除する手順については、次の TechNet 記事を参照してください:
https://technet.microsoft.com/en-us/library/cc755257 (v=ws.11).aspx

Server Timeout
LDAP サーバーのタイムアウトを秒単位で指定します。 デフォルト値は 5 です。有効な値の範囲は 5 ～ 60 です。

Admin User
管理者ユーザーのユーザー名を入力します。

Admin User Password
指定した管理者ユーザーのパスワードを入力します。

9.11 侵入検知オプション (IPS/IDS)

SNORT は、侵入防止システム (IPS) および侵入検知システム (IDS) です。 SNORT ルールを LoadMaster にインポートして、HTTP/HTTPS 接続に適用できます。 SNORT 2.8 および 2.9 ルール セットを使用して、独自のルールを作成することもできます。

LoadMaster は、バージョン 2.9 以下の SNORT ルールをサポートしています。

[Virtual Services] > [View/Modify Services] > [Modify] > [Advanced Properties] で [Detect

Malicious Requests] チェック ボックスを選択して、仮想サービスのルールを有効にできます。

Download the SNORT Rules

SNORT ルール セットは、SNORT Web サイトからダウンロードできます。 [Rule] セクションの [Community] で、[community-rules.tar.gz] をクリックしてダウンロードを開始します。

Install the SNORT Rules

LoadMaster に SNORT ルールをインストールするには、次の手順に従います。

1. LoadMaster WUI のメイン メニューで、[証明書とセキュリティ] > [IPS / IDS] に移動します。
2. [Detection Rules] の横にある [Choose Files] をクリックします。
3. 以前にダウンロードしたコミュニティ rules.tar.gz ファイルを参照して選択します。
4. [Install new Rules] をクリックします。
5. 選択した検出レベルを選択します。

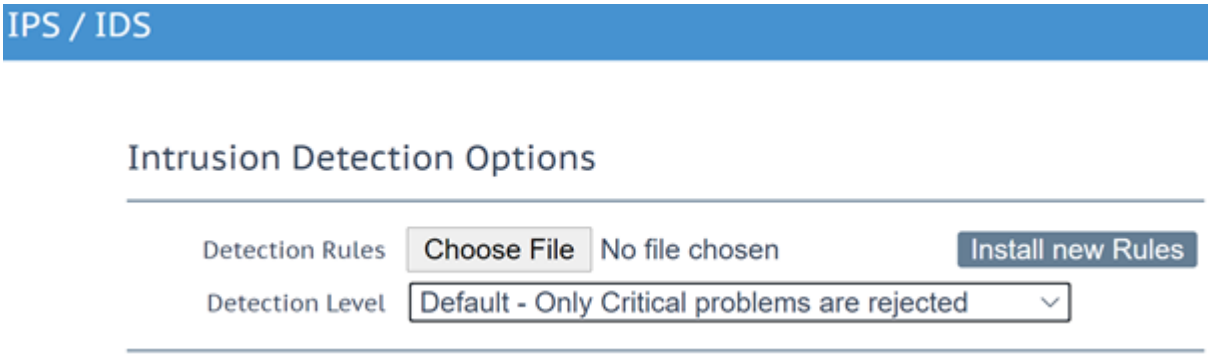
Deactivate/Activate the SNORT Rules

community-rules.tar.gz ファイルは、ルールをコメント アウトまたはコメント アウト解除することで変更できます。 これを行うには、7-Zip などのファイル アーカイブ ツールを使用してファイルをアーカイブとして開きます。

1. 7-Zip を開きます。
2. [File] をクリックし、[Open] を選択します。
3. community-rules.tar.gz ファイルを参照します。
4. ファイルをダブルクリックしてアーカイブを開きます。
5. 次のファイルが表示されるまで、ダブルクリックを続けます。
   - community.rules
   - AUTHORS
   - LICENSE
   - sid-msg.map
   - VRT-License.txt
6. community.rules を右クリックします。
7. [Edit] を選択して、ファイルをテキスト エディターで開きます (編集のショートカット キーは F4 です)。
8. シグニチャー ID (SID) で目的のルールを検索します (例: sid:2067)。

9. ルールを無効にするには、行頭にハッシュ記号（#）を追加してルールをコメントアウトします。
10. ルールを有効にするには、行頭の # を削除してルールのコメントを解除します。
11. 変更が完了したら、[File] > [Exit] をクリックしてテキスト エディタを閉じます。
12. ファイルを保存するように求められたら、[Yes] をクリックします。

詳細については、次のナレッジベースの記事を参照してください: KEMP Loadmaster (IPS+SNORT) で侵入保護を構成する方法。



Detection Rules

関連する検出ルールを選択し、[新しいルールのインストール] ボタンをクリックしてインストールします。 SNORT ルールを実装している場合は、次の点に注意してください。

- 宛先ポートは $HTTP_PORTS でなければなりません
- 「メッセージ」はオプションで設定できます
- フローは「to_server, Established」に設定する必要があります
- 実際のフィルタは「content」または「pcre」のいずれかです
- 追加の「http_」パラメータを設定できます
- クラスタイプは有効な値に設定する必要があります

更新またはカスタマイズされた SNORT ルールを取得するには、SNORT Web サイト (https://www.snort.org/) を参照してください。

Detection Level

問題が発生した場合の対処方法について、次の 4 つのレベルをサポートしています。

- Low – 拒否せずにロギングのみ
- Default – 重大な問題のみ拒否

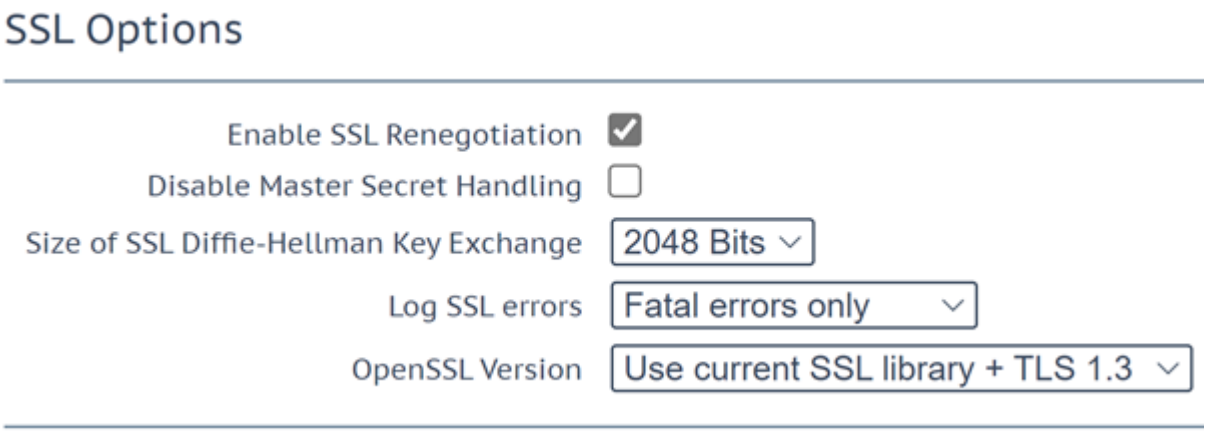
- High – 深刻で重大な問題が拒否されました
- Paranoid – 検出されたすべての問題を拒否

重大度の 4 つのレベルは、SNORT ルール構成ファイルの classtype 値に従って分類されます。 重大度が設定値より小さい場合、診断が生成され、接続がドロップされます。 重大度のレベルは、Low = 1、Default = 2、High = 3 の値に対応しています。SNORT ルールのクラスタイプとそれに対応する値は、次の表で確認できます。

クラスタイプ	値
not-suspicious	3
unknown	3
bad-unknown	3
attempted-recon	2
successful-recon-limited	2
successful-recon-largescale	2
attempted-dos	2
successful-dos	2
attempted-user	1
unsuccessful-user	1
successful-user	1
attempted-admin	1
successful-admin	1
rpc-portmap-decode	2
shellcode-detect	1
string-detect	3
suspicious-filename-detect	2
suspicious-login	2
system-call-detect	2
trojan-activity	1
unusual-client-port-	2

connection	
network-scan	3
denial-of-service	2
non-standard-protocol	2
protocol-command-decode	3
web-application-activity	2
web-application-attack	1
misc-activity	3
misc-attack	2
icmp-event	3
kickass-porn	1
inappropriate-content	1
policy-violation	1
default-login-attempt	2
sdf	2

9.12 SSL オプション



Enable SSL Renegotiation

デフォルトでは、LoadMaster はクライアントが SSL トランザクション中に自動的に再ネゴシエートすることを許可します。 このオプションをオフにすると、クライアントから再ネゴシエーションが要求された場合に SSL 接続が終了します。

Disable Master Secret Handling

LoadMaster ファームウェア バージョン 7.2.52 では、[Disable Master Secret Handling] チェック ボックスが追加されました。 デフォルトでは、LoadMaster はマスター シークレット SSL 拡張を処理します。 これにより、一部のレガシー クライアントで問題が発生する可能性があるため、この処理を無効にすることができます。

Size of SSL Diffie-Hellman Key Exchange

Diffie-Hellman キー交換で使用されるキーの強度を選択します。 この値を変更した場合、新しい値を使用するには再起動が必要です。 デフォルト値は 2048 ビットです。 LoadMaster ファームウェア バージョン 7.2.53 では、SSL Diffie のサイズの値として 4096 を選択できます。
Hellman Key Exchange ドロップダウン リスト。 7.2.53 より前のバージョンからアップグレードした後、4k キーを生成するのに最大 30 分 (小さいモデルの場合) かかる場合があります。 アップグレードの 30 分後にドロップダウン リストに 4096 オプションが表示されない場合は、ログイン プロセスを再起動してみてください。

7.2.53 より前のバージョンからのアップグレード中に、新しい 4096 ビット DHE キーが生成されます。 小規模な LoadMaster では、これにより CPU とメモリが大量に消費され、通常の仮想サービス トラフィックに影響を与える可能性があります。 そのため、Kemp は、この更新をメンテナンス間隔で実行することを強くお勧めします。

4K キーを使用すると、2K キーを使用する場合に比べてパフォーマンスが大幅に低下します。

Log SSL errors

ログの SSL エラー レポートのレベルを設定します。 デフォルトでは、LoadMaster は一般的な SSL アラートを記録しません。 この値を次のいずれかに設定すると、SSL エラー ログの詳細度を上げることができます。

- Fatal errors only - 致命的なエラーのみがログに記録されます
- Include Client errors - この設定は、ロードマスターに報告されたすべてのクライアント エラーをログに記録します。
- All errors – この設定では、LoadMaster で観察されたすべての SSL エラーがログに記録されます。これには、実際の問題を示す場合と示さない場合があるすべての一般的なアラートと警告が含まれます。

OpenSSL Version

デフォルトでは、LoadMaster は最新バージョンの OpenSSL を使用します。 これにより、負荷の高いサイトでパフォーマンスの問題が発生する可能性があります。 OpenSSL バージョン フィールドを使用して、これらの問題の一部を軽減する古いライブラリに戻すことができます。 古いライブラリを使用すると、TLS 1.3 がサポートされなくなります。 そのため、[仮想サービスの変更] 画面の [SSL Properties] チェック ボックスを使用できなくなりました。 [OpenSSL Old version イブラリの使用から現在のライブラリの使用に切り替えると、すべての仮想サービスで TLS1.3 が自動的に再度有効になります。

> This option is not applicable for following LoadMaster/Kemp ECS Connection Manager models:
> - LM-X25
> - LM-X40 Rev 05
> - LM-X40M
> - LM XHC 25G/40G/100G
> - ECS Connection Manager H3 Rev 02
> - ECS Connection Manager H3M
> - ECS Connection Manager H3 25G/40G/100G
>
> For these LoadMaster models, the **OpenSSL Version** field is available but the LoadMaster will continue to use the current

OpenSSL Version フィールドが Use old SSL library - no TLS 1.3 に設定されている場合でも、OpenSSL 実装。 OpenSSL バージョンを切り替えると、切り替え中に SSL が完全に停止します。この操作は、勤務時間中に実行しないでください。

10 ウェブ アプリケーション ファイアウォール(WAF)

WAF を利用すると、LoadMaster の展開のパフォーマンスに大きな影響を与える可能性があります。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。

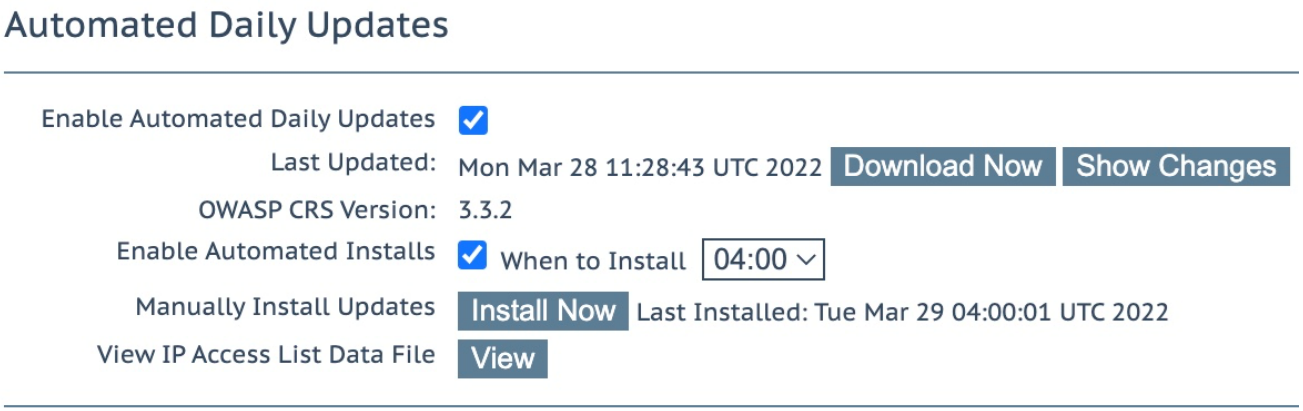
仮想およびベアメタルの LoadMaster インスタンスの場合、WAF の動作には最低 2GB の RAM が割り当てられている必要があります。 LoadMaster オペレーティング システム バージョン 7.1-22 より前の仮想 LoadMaster および LoadMaster ベア メタル インスタンスのデフォルトのメモリ割り当ては、1 GB の RAM です。 このデフォルトの割り当てが変更されていない場合は、WAF 構成

に進む前にメモリ設定を変更します。 WAF を有効にするチェック ボックスがグレー表示されている場合は、LoadMaster に WAF を実行するための十分なメモリがないことを意味している可能性があります。
仮想サービスごとに 64000 の WAF エンジンのオープン接続制限があります。

WAF 接続の制限に達するリスクを軽減するために、リモート ログ サーバーの応答が遅すぎる場合、開いている接続は 20 秒後に閉じられます。 使用中の接続への影響はありません。 レガシー WAF ルールは 2021 年 6 月 29 日に廃止され、それ以上の更新は利用できません。 Progress kemp ザーが構成を新しい WAF サービスに移行することを推奨しています。

10.1 設定

Progress Kemp ライセンス サーバーの IP/FQDN とポートは、ファイアウォールで開いている必要があります。 FQDN と IP アドレスは、licensing.kemp.ax 52.166.52.190 で、ポートは 443 です。 は 52.136.251.129 です。 LoadMaster のバージョンによっては、これらも開く必要がある場合があります。Progress Kemp が提供する毎日の更新は、Enterprise Plus サブスクリプションをお持ちの場合にのみ利用できます。 サブスクリプション層の詳細については、ロードマスター サポート サブスクリプションにアクセスしてください。



Enable Automated Daily Updates

毎日の更新の自動ダウンロードを有効にします。

WAF サポート ライセンスの有効期限が切れている場合、[Download Now] オプションと [Install Now] オプションはグレー表示されます。 この場合は、Progress Kemp に連絡してサブスクリプシ

ョンを更新してください。

OWASP CRS version

LoadMaster で実行されている最新の OWASP Core Rule Set (CRS) バージョンを表示します。OWASP CRS の現在のバージョンを確認するには、リンク https://coreruleset.org を参照してください。

Enable Automated Installs

毎日の更新プログラムの自動インストールを有効にする デフォルトでは、[Enable Automated Install] オプションと [Manually Install Upgrade] オプションはグレー表示になっています。 これらのオプションが使用可能になる前に、ルールを初めてダウンロードする必要があります。

When to install

毎日の更新プログラムを自動的にインストールする時刻 (時刻) を選択します。

毎日の更新を有効にするには、仮想サービスに割り当てる必要があります。

Download Now

毎日の更新をすぐにダウンロードします。ルールが過去 7 日間更新されていない場合、またはルールがまったくダウンロードされていない場合は、警告メッセージが表示されます。

Show Changes

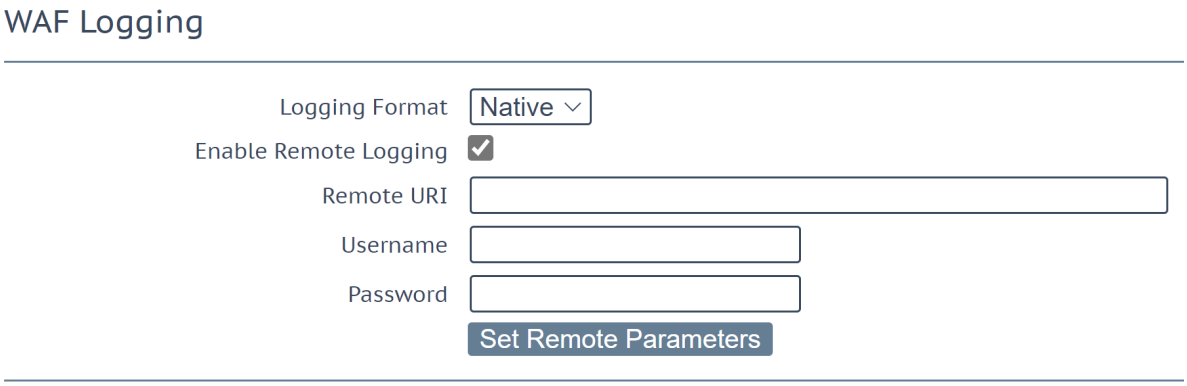
毎日の更新がダウンロードされた後に表示されます。 このボタンをクリックして、Kemp WAF ルール セットに加えられた変更のログを取得します。

Install Now

毎日の更新プログラムを手動でインストールします。

毎日の更新を有効にするには、仮想サービスに割り当てる必要があります。

10.2 ログのエクスポート



Logging Format

監査ログを表示する形式に応じて、ネイティブまたは JSON のいずれかを選択します。

Enable Remote Logging

このチェック ボックスを使用すると、WAF のリモート ログを有効または無効にできます。

Remote URI

リモート ログ サーバーの URI (Uniform Resource Identifier) を指定します。

Username

リモート ログ サーバーのユーザー名を指定します。

Password

リモート ログ サーバーのパスワードを指定します。

10.3 カスタム ルール

サードパーティのルールを LoadMaster にアップロードできます。 アップロード可能な独自のカスタム ルールを作成することもできます。 正しくアップロードするには、これらのルールを ModSecurity ルール形式にする必要があります。 [Customer Rule] 画面では、WAF カスタム ルール (.conf) および関連する WAF カスタム ルール データ (.data または .txt) ファイルをアップロードできます。 ファイル名には、英数字と次の特殊文字を含めることができます: -. _ gzip で圧縮された Tarball ファイル (.tar.gz) をアップロードすることもできます。このファイルには、複数のルールとデータ ファイルが含まれています。

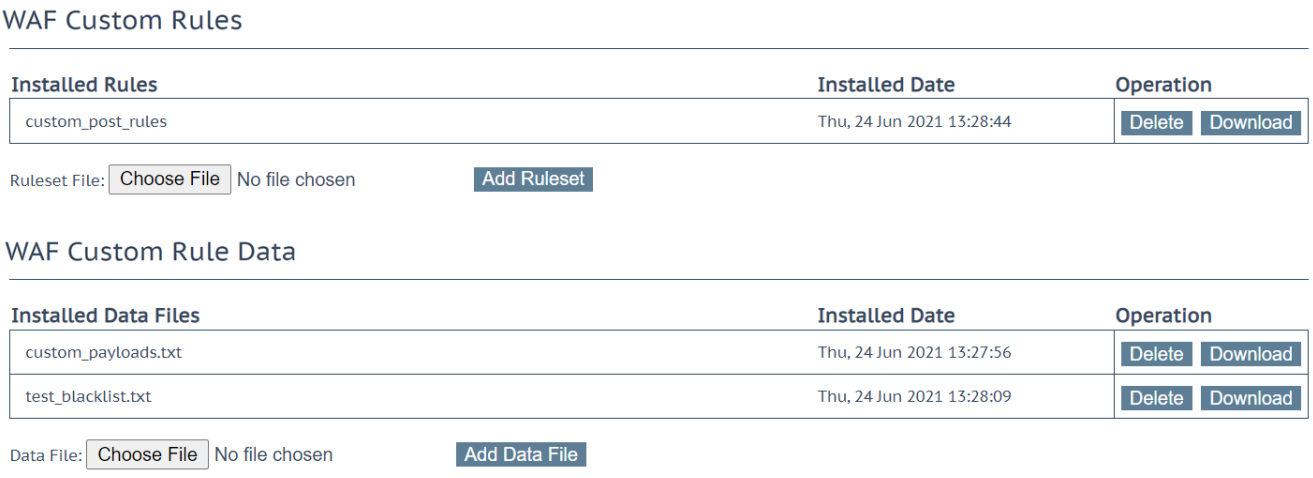
Progress Kemp は、システム パフォーマンスに影響を与えるため、カスタム ルールで WAF ルー

ルの「リダイレクト」アクションを使用することをお勧めしません。 そのためには、代わりにコンテンツ ルールを使用する必要があります。 OWASP が推奨するベスト プラクティスに基づいて、ロードマスター ファームウェア バージョン 7.2.57 で WAF ルール処理の順序が変更されました。7.2.57 以降、カスタム ルールは OWASP CRS ルールの前に処理されます。

ルールが処理される順序を確認するには:

1. [System Configuration] > [Logging Options] > [System Log Files] > [Debug Options] に移動し、[Enable WAF Debug Logging] の横にある [Enable Logging] ボタンをクリックします。
2. WAF デバッグ ログが有効になっている場合、WAF デバッグ ログがある場合、[System Log Files] 画面で [WAF Debug Log Files] オプションが使用可能になります。 [View] をクリックして、WAF デバッグ ログ ファイルを表示します。
3. ルールが処理される順序を確認できます。Invoking rule と書かれている行は、ルールがいつ処理されたかを示します。

WAF デバッグ ログを有効にすると、一般データ保護協定 (EU GDPR) で定義されている個人を特定できる情報が含まれる可能性があるログが生成されることに注意してください。 ログ内のデータの匿名化、削除、暗号化など、組織のベスト プラクティスに従ってこの情報を保護する必要があります。



Installed Rules: Choose File.

個々のカスタム ルールは、.conf ファイルとしてアップロードできます。 または、ルールのパッケー

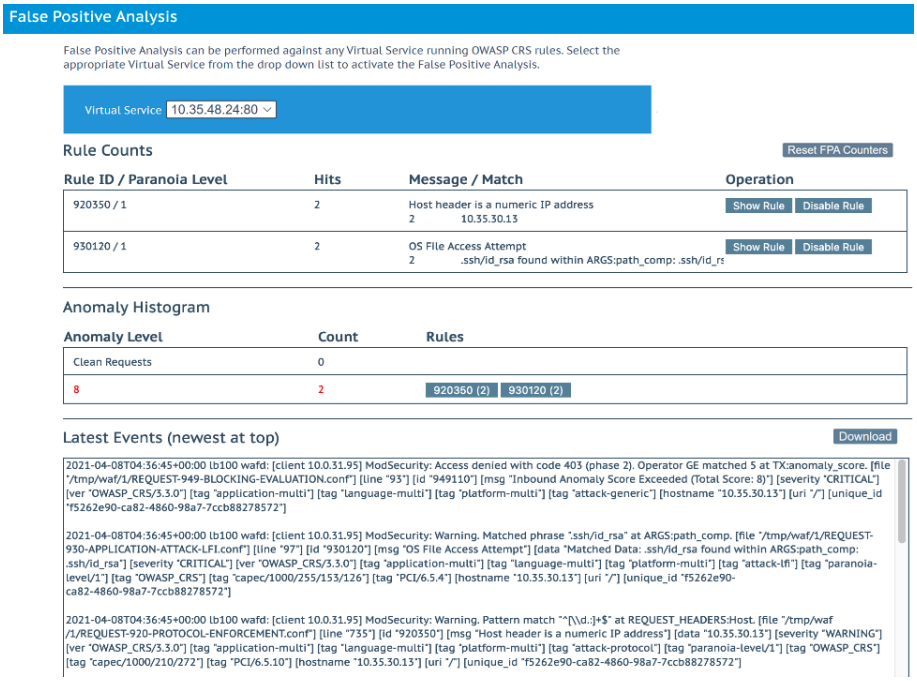
ジを .tar.gz ファイルにロードすることもできます。 アップロードするルール ファイルを選択したら、[Add Rule Set] ボタンをクリックします。

WAF Custom Rule Data : Choose File.
ルールの関連データを含む追加のデータ ファイルをアップロードします。 追加のファイルは、ルールに関連付けられたデータ ファイル用です。 ルールのアップロード時に Tarball をアップロードした場合は、ルールとデータ ファイルを一緒にパッケージ化できます。 アップロードするデータ ファイルを選択したら、[Add Data File] ボタンをクリックします。

カスタム ルールとデータ ファイルは、関連するボタンをクリックして削除またはダウンロードできます。 ルールが仮想サービスに割り当てられている場合、そのルールは削除できません。

10.4 False Positives

誤検知分析を実行するには、少なくとも 1 つの仮想サービスが OWASP ルールと異常スコアリングを使用して WAF を実行している必要があります。 ドロップダウン リストから適切な仮想サービスを選択すると、トリガーされたルールが WAF ログ情報とともに表示されます。



Rule Counts

[Rule Counts] セクションには、リクエストによってトリガーされたすべてのルールに関する情報が表示されます。 ルール ID、ルールが実行されているパラノイア レベル、ルールをトリガーしたリクエストごとのヒット数、およびリクエストのメッセージまたは一致が、トリガーされたルールごとに表示されます。 [Operation] 列の [Show Rule] ボタンをクリックすると、トリガーされたルールに関連付けられているルール ファイルの内容が表示されます。 これは別のタブで開き、URL にはトリガーされたルール ID が含まれます。ルールを無効にするには、[Disable Rule] ボタンをクリックします。

Reset FPA Counter

仮想サービスのすべての誤検知分析カウンター (異常ヒストグラムと最新イベント) をリセットします。 最新のイベントをクリアしても、LoadMaster からログは削除されません。ログは、[System Configuration] > [Logging Options] > [System Log Files] > [WAF Event Log File] で引き続き利用できます。

ファイル。

Anomaly Histogram

[Anomaly Histogram] セクションの最初の行には、ルールをトリガーせずに実行されたリクエストの数が表示されます。 後続の各行には、トリガーされ、異常スコアに影響を与えているルールの詳細が

示されます。 各行には、累積異常スコア、ルールをトリガーしたリクエストの数、およびルールの詳細が表示されます

Latest Events (newest at top)

トリガーされた各ルールのイベントの詳細を表示します。 これらのメッセージは標準の ModSecurity ログ形式であり、異常スコア、警告メッセージ、攻撃状態、パラノイア レベルが含まれています。

Download

[Download] ボタンをクリックして、表示されている WAF イベント ログの詳細をダウンロードします。

11 システム構成

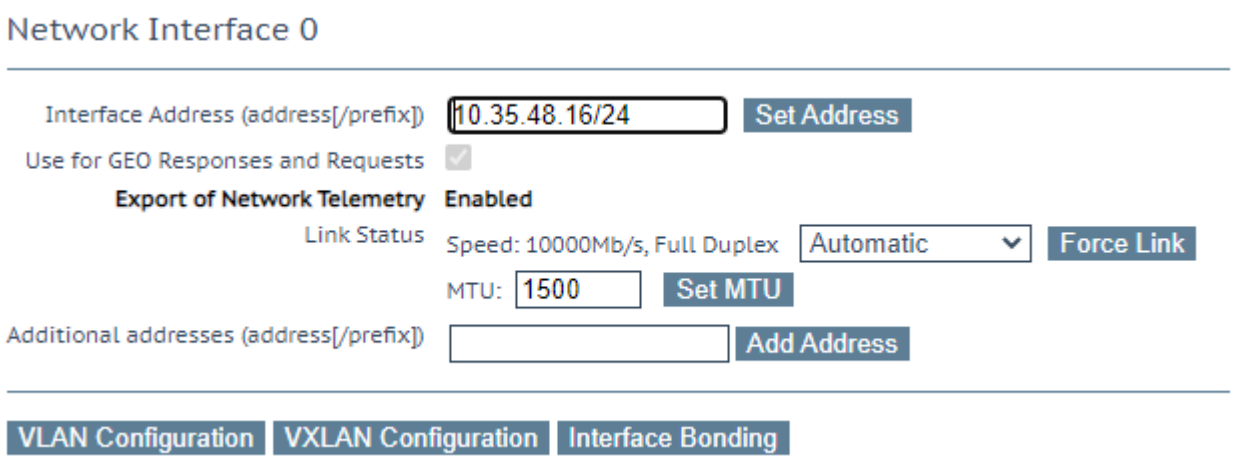
11.1 ネットワークセットアップ

11.1.1 インターフェイス

この画面では、外部ネットワークおよび内部ネットワーク インターフェイスに関連する設定を提供します。 インターフェイスに関する重要な注意事項を以下に示します。

- 仮想サービスは、既知のネットワークまたはサブネットにのみ追加できます。 その範囲内の IP アドレスを持つインターフェイスが存在する場合、そのネットワークまたはサブネットは既知であると見なされます。
- ルーティングの問題が発生する可能性があるため、同じサブネット上に 2 つのインターフェイスを配置することはできません。
- インターフェイスと仮想サービスで同じ IP アドレスを使用しないでください。 このルールには例外が 1 つあります。Azure で LoadMaster を使用する場合です。

画面には、eth0 および eth1 イーサネット ポートに関する同じ情報が表示されます。 以下の例は、非 HA (高可用性) ユニットの eth0 の場合です。



Interface Address

[Interface Address (address[/prefix])] テキスト ボックス内で、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。 [Certificate & Security] > [Remote Access] で [Allow Multi Interface Access] が有効になっている場合、別のインターフェイス (eth0 以外) に IP アドレスを設定すると、「"Would you like to enable admin WUI access for this interface?"(このインターフェイスに対して管理 WUI アクセスを有効にしますか?)」というポップアップが表示されます。 [OK] をクリックして、[Allow Administrative WUI Access] チェック ボックスをオンにします。 [Cancel] をクリックすると、[Allow Administrative WUI Access] チェック ボックスは無効のままになり、そのオプションが有効になるまで、そのインターフェイスでの WUI アクセスは許可されません。

[Allow Multi Interface Access]] オプションが有効になっていて、管理 WUI インターフェイスが変更されている場合、インターフェイスの変更を検出するには、Web アクセスを再起動する必要があります。 Web サーバーを再起動するには、管理コンソール (lsetup) に bal としてログインします。 [Local Admin] > [Web Address] に移動し、[Immediately Stop Web Server Access] オプションを選択して、[OK] をクリックします。 ページが更新されたら、[Immediately Start Web Server Access] オプションを選択します。 終了するには、前のメニューに戻るを選択してから、設定の終了を選択します。

Cluster Shared IP address

クラスターへのアクセスに使用できる共有 IP アドレスを指定します。 これは、サーバー NAT を使用する場合のデフォルトの送信元アドレスとしても使用されます。

クラスタリング オプションは、クラスタリング ライセンスがあり、クラスタリングが設定されている LoadMaster でのみ使用できます。 ライセンスにクラスタリング機能を追加するには、Progress Kemp の担当者にお問い合わせください。 クラスタリングの詳細については、LoadMaster クラスタリング、機能の説明を参照してください。

Use for Cluster checks

このオプションを使用して、ノード間のクラスターのヘルス チェックを有効にします。 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

このオプションを選択すると、このインターフェイスを使用して、クラスター内の他のすべてのノードと構成を同期できます。

Speed

デフォルトでは、リンクの速度は自動的に検出されます。 特定の構成では、この速度は正しくないため、特定の値に強制する必要があります。

AWS Elastic Network Adapter (ENA) インターフェイスでは、インターフェイスから読み取ることができない速度は表示されません。 ENA ドライバー インターフェイスの場合、表示される速度は結合されたインターフェイスと同様に動作します。インターフェイス全体の速度は、そのインターフェイスで定義された個別の論理インターフェイスの数の総計として表示されます。

Use for Default Gateway

[Use for Gateway] チェック ボックスは、[Network Option] 画面で [Enable Alternate GW Support] が選択されている場合にのみ使用できます。 表示されている設定がデフォルト インターフェイス用である場合、このオプションはグレー表示され、選択されています。 別のインターフェイスでこのオプションを有効にするには、左側のメイン メニューでクリックして、別のインターフェイスに移動します。 次に、このオプションを選択できます。 このオプションを選択すると、[Default Gateway] 画面が表示されます。 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 ゲートウェイが変更されたことを知らせる通知が表示されます。

新しいデフォルト ゲートウェイを設定する前に再起動すると、ゲートウェイが設定から削除されます。

Allow Administrative WUI Access

このオプションは、[Certificate & Security] > [Remote Access] で [Allow Multi Interface Access] チェック ボックスが有効になっている場合にのみ使用できます。
これらのオプションの両方を有効にすると、関連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追加のアドレスから WUI にアクセスできます。

これらすべてのアドレスに接続されているインターフェイスは 1 つだけであるため、使用される証明書がワイルドカード証明書でない限り、問題が発生する可能性があります。 証明書の詳細については、SSL Accelerated Services 機能の説明を参照してください。 追跡できる最大 64 個のネットワーク インターフェイスと、システムがリッスンする合計最大 1024 個のアドレスがあります。

Use for GEO Responses and Requests

デフォルトでは、デフォルト ゲートウェイ インターフェイスのみが DNS 要求のリッスンと応答に使用されます。 このフィールドには、追加のインターフェイスでリッスンするオプションがあります。

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、これは eth0 です。

このオプションを有効にすると、GEO はインターフェイスに設定された追加アドレスもリッスンします。

Export of Network Telemetry

これは、このインターフェイスのネットワーク テレメトリ モニタリングが有効か無効かを示します ([ネットワーク テレメトリ] 画面で選択されているインターフェイスによって異なります)。 詳細については、ネットワーク テレメトリのセクションを参照してください。

MTU

MTU フィールド内で、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。 有効な範囲は 512 から 9216 です。

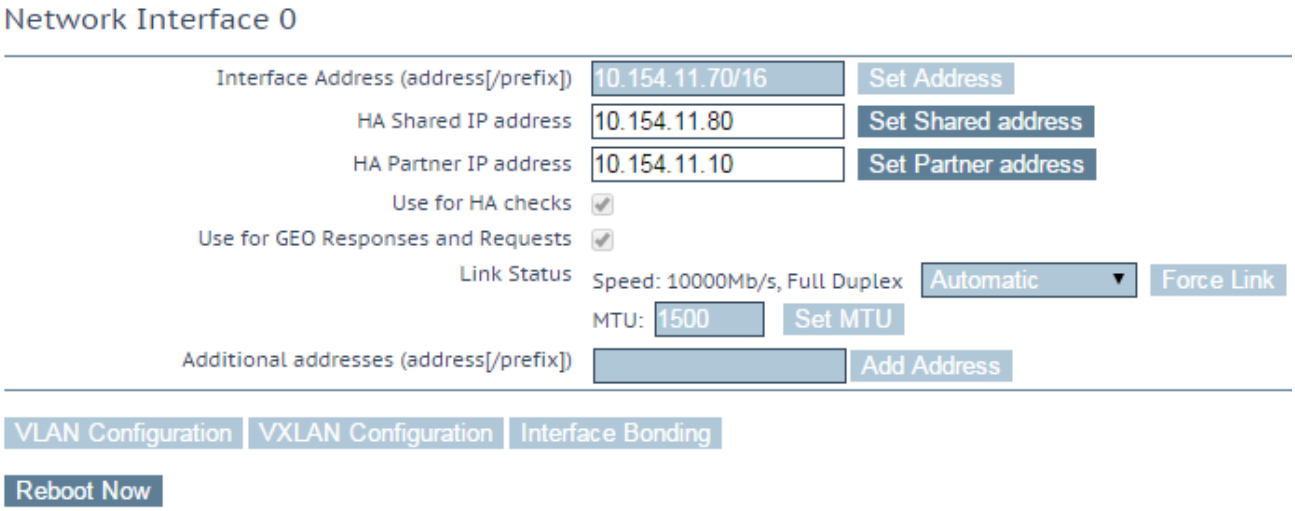
512 ～ 9216 の有効な範囲は、VLM が実行されているハードウェアに依存するため、VLM には適用されない場合があります。 ハードウェアの制限を確認することをお勧めします。

Additional addresses

追加のアドレス フィールドを使用すると、LoadMaster はエイリアスとして各インターフェースに複数のアドレスを与えることができます。 これは、「スティック上のルーター」と呼ばれることもあります。 標準の IP+CIDR 形式で IPv4 と IPv6 の両方のアドレスを使用できるため、これを使用して、同じインターフェイスで IPv4 と IPv6 アドレスの混合モードを実行することもできます。 ここで追加されたサブネットはいずれも、仮想 IP と実サーバー IP の両方で使用できます。

HA

ユニットが HA 構成の一部である場合、インターフェースの 1 つをクリックすると、次の画面が表示されます。



この画面はユーザーに次のことを伝えます。

- これはペアのマスター マシンです (画面の右上)
- この LoadMaster は起動しており、ペアリングされたマシンは停止しています (緑と赤のアイコン)
- この LoadMaster の IP アドレス
- HA 共有 IP アドレス。 これは、ペアを構成するために使用される IP アドレスです。
- ペアリングされたマシンの IP アドレス
- このインターフェースは、HA ヘルスチェックに対して有効になっています
- このインターフェイスは、デフォルト ゲートウェイとして使用されます

- リンクの速度は自動的に検出されます このインターフェイスの代替アドレス
- このインターフェイスの代替アドレス

Creating a Bond/Team

結合インターフェースを作成する前に、次の点に注意してください。

- 親より上位のインターフェースのみを結合できるため、eth1 から開始することを選択した場合、eth2、eth3 以降を結合できますが、eth0 を結合することはできません (eth0 から開始しない限り)。
- VLAN タグが必要な場合はリンクを最初に結合し、結合が構成された後に VLAN を追加します
- ボンディングされたインターフェースにリンクを追加するには、最初に追加するリンクからすべての IP アドレッシングを削除する必要があります
- Active-Backup モードを有効にする場合、通常、スイッチの介入は必要ありません
- eth0 と eth1 のボンディングは重大な問題を引き起こす可能性があるため、許可されていません

[Interface Bonding] をクリックして、結合を要求します。

[Create a bonded interface] をクリックして、結合の作成を確認します。

警告ダイアログを確認します。

Web ユーザー インターフェイス (WUI) を使用して、[System Configuration] > [Interfaces] > [bndx] メニュー オプションを選択します。

bndX インターフェイスが表示されない場合は、ブラウザーを更新してから、結合されたインターフェイスを選択し、[Bonded Devices] ボタンをクリックします。

希望の結合モードを選択します。

この結合に追加のインターフェースを追加します。

結合されたインターフェイスで IP とサブネット マスクを構成します。

Removing a Bond/Team

最初に、結合されたインターフェイス上のすべての VLAN を削除します。 それらを削除しない場合、結合が開始された物理ポートに自動的に割り当てられます。 [System Configuration] > [Interfaces] > [bndx] メニュー オプションを選択します。 bndX インターフェイスが表示されない場合は、ブラウザーを更新してから、結合されたインターフェイスを選択し、[Bonded Devices] ボタンをクリックします。 [Unbind Port] をクリックして各ポートのバインドを解除し、すべてのポートが結合から削除されるまで繰り返します。 すべての子ポートのバインドが解除されたら、

[Unbond this interface] ボタンをクリックして、親ポートのバインドを解除できます。

Adding a VLAN

インターフェイスを選択し、[VLAN Configuration] ボタンを選択します。

VLAN ID 値を追加し、[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、ドロップダウン リストを展開します。

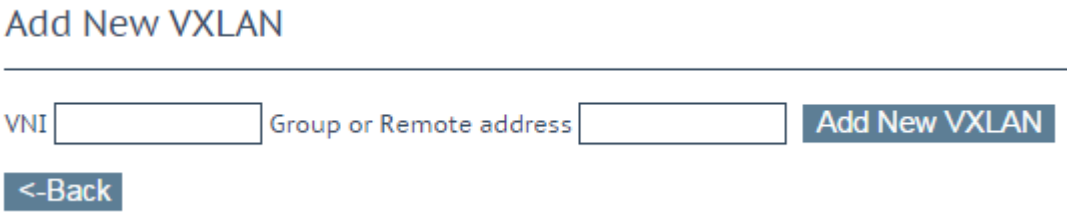
Removing a VLAN

VLAN を削除する前に、インターフェイスが他の目的 (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) に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、ドロップダウン リストから適切な VLAN ID を選択します。 選択したら、IP を削除し、[Set Address] をクリックします。 IP が削除されると、[Delete the VLAN] ボタンをクリックして、VLAN を削除するオプションが表示されます。 必要に応じて繰り返します。 VLAN を表示するには、System Configuration > Interfaces メニュー オプションを選択し、ドロップダウン リストから適切な VLAN ID を選択します。

Adding a VXLAN

関連する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。



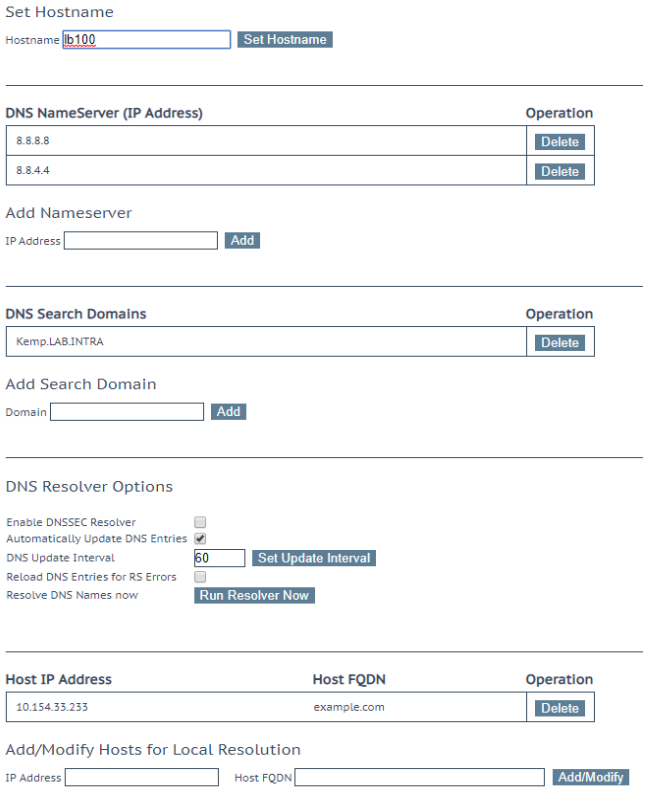
VNI テキスト ボックスに新しい VXLAN ネットワーク識別子 (VNI) を入力します。 [グループまたはリモート アドレス] テキスト ボックスに、マルチキャスト グループまたはリモート アドレスを入

力します。 [新しい VXLAN を追加] をクリックします。 VXLAN を変更するには、[System Configuration] > [Interfaces] に移動し、ドロップダウン リストから 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。 この画面から VXLAN を削除することもできます。 HA が有効になっている場合、VXLAN で HA パラメータを設定できます。

- HA 共有 IP アドレス。 これは、HA ペアの構成に使用される 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 チェックに使用するかどうかを指定します。

11.1.2 ホストと DNS の構成



[Hostname] テキスト ボックスにホスト名を入力し、[Set Hostname] 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。 英数字のみを使用できます。

Add NameServer (IP Address)

ロードマスターで名前をローカルに解決するための DNS サーバーの IP アドレスをこのフィールドに入力し、[Add] をクリックします。 最大 3 つの DNS サーバーが許可されます。

DNSSEC クライアントが有効になっている場合、最後に残った NameServer を削除することはできません。 [Host & DNS Configuration] 画面で DNSSEC クライアントを無効にすることができます。

Add Search Domain

このフィールドで、DNS NameServer への要求の先頭に追加するドメイン名を指定し、[追加] をクリックします。 最大 6 つの検索ドメインが許可されます。

Add/Modify Hosts for Local Resolution

これらのフィールドは、LoadMaster WUI からホスト ファイルを操作する機能を提供します。 エントリの IP アドレスとホスト FQDN を指定します。

Enable DNSSEC Resolver

デデフォルトでは、LoadMaster DNSSEC クライアントは無効になっています。 必要な場合にのみ、このオプションを有効にしてください。 状況によっては、DNSSEC 検証が失敗するまでにかなりの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したように見える場合があります。 このオプションを選択すると、ロードマスターで DNSSEC 機能が有効になります。 DNSSEC を有効にする前に、少なくとも 1 つのネームサーバーを追加する必要があります。 機能を有効化/無効化するには、DNSSEC オプションを変更した後、LoadMaster を再起動する必要があります。 設定を変更すると、ロードマスターを再起動するまで変更できません。

HA を使用する場合 – DNSSEC オプションは、両方のデバイスで個別に構成する必要があります。

DNSSEC は、LoadMaster の次のユーティリティと連携します。

- Vipdump
- Ping and ping6
- Syslog
- SNMP
- Wget

- NTP
- SMTP
- Real Servers

Automatically Update DNS Entries

このオプションを有効にすると、ロードマスターは (DNS 更新間隔に基づいて) 変更された DNS 名を自動的に更新しようとします。

- アドレスが見つからない場合、または以前と同じである場合、何も実行されません (ログエントリが生成される場合を除く)。
- アドレスが異なる場合、可能な場合、Real Server エントリは新しいアドレスで更新されます。
- 新しいアドレスが何らかの理由で無効な場合 (たとえば、それが非ローカル アドレスであり、[Enable Non-Local Real Server] オプションが無効になっている場合)、変更は行われず、ログが生成されます。

DNS Update Interval

DNS エントリの更新間隔を設定します。 有効な値の範囲は 1 ～ 60 (分) です。 デフォルト値は 60 です。

Reload DNS Entries for RS Errors

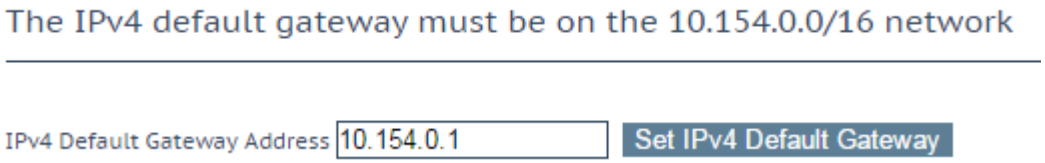
このオプションを有効にすると、ヘルス チェックにエラーがあり、FQDN が実サーバーの IP アドレスに関連付けられている場合に、DNS エントリがリロードされます。

Resolve DNS Names now

[Run Resolver Now] ボタンをクリックすると、DNS 名の新しい解決が強制されます。 動作は、これが手動 (自動ではなく) チェックであることを除いて、[Automatically Update DNS Entries] オプションと同じです。

11.1.3 デフォルトゲートウェイ

デフォルト ゲートウェイを設定する前に、ネットワーク インターフェイス アドレスを設定する必要があります。 LoadMaster には、インターネットと通信できるデフォルト ゲートウェイが必要です。



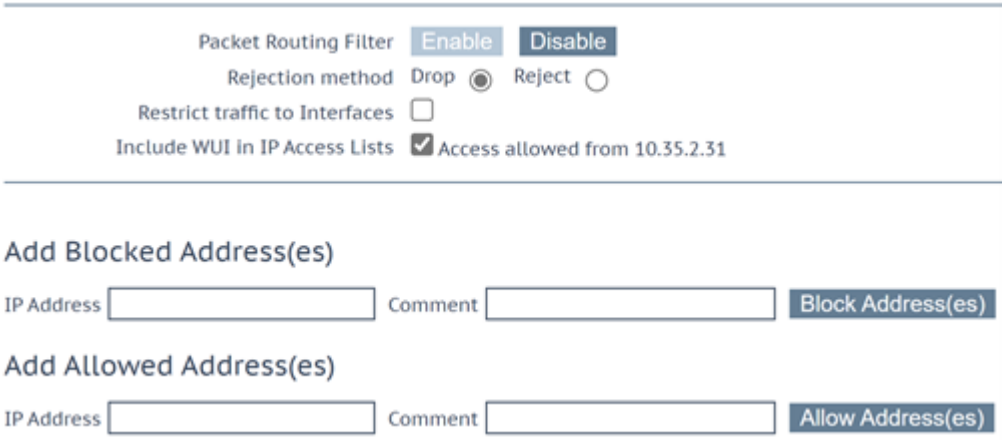
LoadMaster で IPv4 と IPv6 の両方のアドレスが使用されている場合は、IPv4 と IPv6 の両方のデフォルト ゲートウェイ アドレスが必要です。

IPv4 と 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ある必要があります。

11.1.4 追加ルート

さらにルートを追加できます。 これらのルートは静的であり、ゲートウェイは LoadMaster と同じネットワーク上にある必要があります。 トラフィックをセグメント化するために、仮想サービス レベルのデフォルト ゲートウェイを利用することもできます。

11.1.5 パケット ルーティング フィルタ



Packet Routing Filter

パケット ルーティング フィルタがアクティブになると、LoadMaster へのトラフィックが制限されますが、インターフェース アドレス (SSH 22、HTTPS 443、SNMP 161、および DNS 53) で実行されているサービスへのクライアント アクセスは影響を受けません。 SNAT を有効にすると、LoadMaster のデフォルト ゲートウェイ インターフェイスと同じ IP アドレスを持つ仮想サービスへのトラフィックをブロックできなくなります。 これは、Azure または単一の IP アドレスを使用するクラウド プラットフォームに影響を与える可能性があります。 パケット ルーティング フィルタが有効化されていない場合、LoadMaster は単純な IP フォワーダとしても機能します。

パケット ルーティング フィルタが無効になっている場合、[Reject/Drop blocked packets] および [Restrict traffic to Interfaces] フィールドは表示されません。

Reject/Drop blocked packets

アクセス制御リスト (ACL) を使用してブロックされているホストから IP パケットを受信すると、通常、その要求は無視 (ドロップ) されます。 LoadMaster は ICMP 拒否パケットを返すように設定できますが、セキュリティ上の理由から、ブロックされたパケットを黙ってドロップすることをお勧めします。

Restrict traffic to Interfaces

この設定により、接続されたサブネット間のルーティングに制限が適用されます。 Progress Kemp では、このオプションがデフォルトで無効になっています。

Include WUI in IP Access lists

このオプションを有効にすると、WUI へのアクセスもパケット フィルタによって制御されます。 [Include WUI in IP Access lists] オプションを有効にしているクライアントの IP アドレスは、パケット フィルターに引き続きアクセスできます (内部で許可リストに登録されます) - チェック ボックスの横に、Access
[allowed from <IP Address>] というメッセージが表示されます。 これにより、WUI からロックアウトされるのを防ぐことができます。 [IP アクセス リストに WUI を含める] オプションは、1 つの IP アドレスでのみ動作するように設計されています。 [Include WUI in IP Access lists] オプションを有効にしても、仮想サービスの接続には影響しません。 Add Allowed Address(es) フィールドを使用して IP アドレスを追加すると、他のすべての IP アドレスの接続が仮想サービスに対してブロックされます。 [Include WUI in IP Access lists] オプションを無効にすると、WUI へのアクセスはパケット フィルターの影響を受けません。

Add Blocked Address(es)

LoadMaster は、アクセス制御リスト (ACL) システムをサポートしています。 ACL に入力されたホストまたはネットワークは、ロードマスターが提供するサービスへのアクセスをブロックされます。ACL は、パケット フィルタが有効になっている場合にのみ有効になります。許可リストは、特定の IP アドレスまたはアドレス範囲のアクセスを許可します。アドレスまたは範囲がブロック リスト内のより大きな範囲の一部である場合、許可リストは指定されたアドレスに対して優先されます。ユーザーがブロック リストにリストされているアドレスを持たず、許可リストにリストされているアドレスのみを持っている場合、許可リストにリストされているアドレスからの接続のみが許可され、他のすべてのアドレスからの接続はブロックされます。このオプションを使用すると、ユーザーはホストまたはネットワーク IP アドレスをアクセス制御リストに追加または削除できます。 IPv4 アドレスに加えて、システムが IPv6 アドレス ファミリで構成されている場合、IPv6 アドレスがリストで許可されます。ネットワーク指定子を使用して、ネットワークを指定します。たとえば、ブロック リストでアドレス 192.168.200.0/24 を指定すると、192.168.200 ネットワーク上のすべてのホストがブロックされます。

特定のトラフィックをブロックするように定義されたアクセス リストを持つ静的ポート仮想サービスは、同じ IP アドレスにワイルドカード仮想サービスもある場合、正しく機能しません。 静的ポート仮想サービスがトラフィックを拒否した後、ワイルドカード仮想サービスはトラフィックを受け入れます。 この場合、この相互作用による予期しない動作を回避するために、別の IP アドレスを使用することをお勧めします。

11.1.6 VPN 管理

VPN 管理リンク/画面は、LoadMaster が IPsec トンネリングのライセンスを取得している場合にのみ使用できます。 このドキュメントは、最新の LoadMaster Long Term Support (LTS) リリースで利用可能なポリシーベースの VPN 機能をカバーしています。 LoadMaster ファームウェア バージョン 7.2.53 以降、VPN 管理メニュー オプションがポリシー ベース VPN に変更され、ルートベース VPN のサポートが追加されました。

IPsec トンネリングの詳細については、設定方法の段階的な手順を含めて、IPSec トンネリング機能の説明を参照してください。

Connection Name

接続を識別する一意の名前を指定します。

Create

指定された名前で一意に識別可能な接続を作成します。

View/Modify

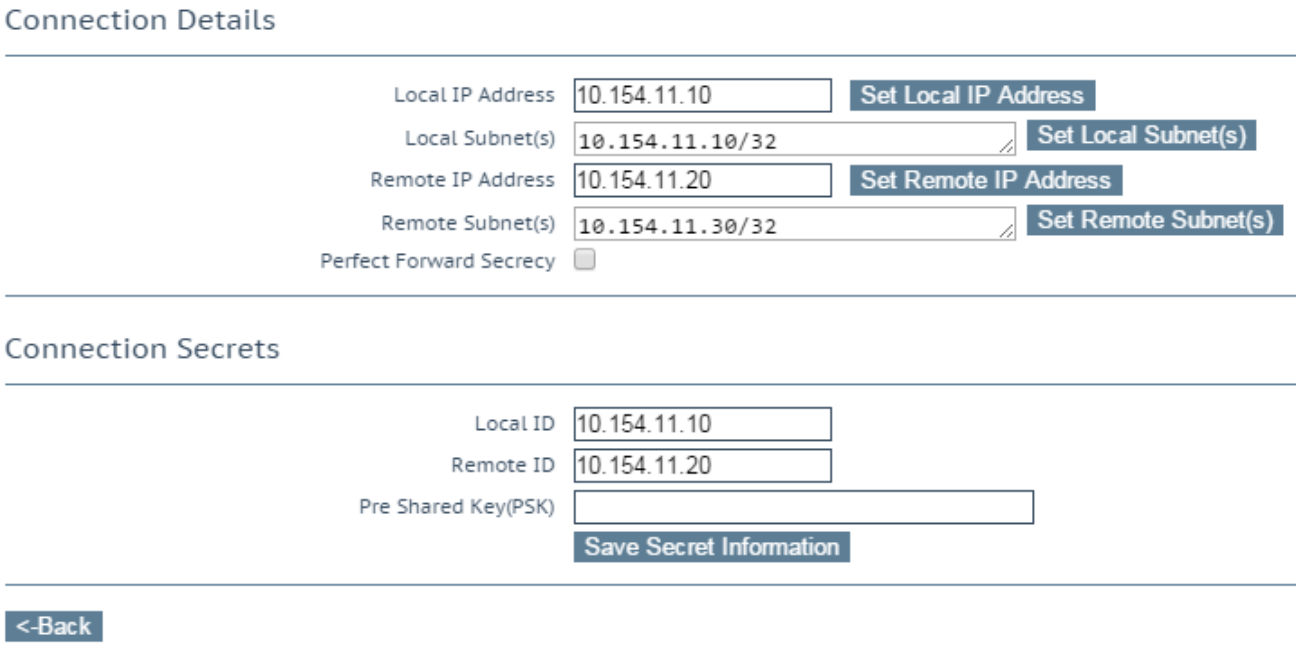
この接続の構成パラメータを表示または変更します。

Delete

この接続を削除します。

関連するすべての構成が完全に削除されます。 接続は、実行中であってもいつでも削除できます。

11.1.6.1 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

接続のローカル側の IP アドレスを設定します。 非 HA モードでは、ローカル IP アドレスは LoadMaster の IP アドレス、つまりデフォルト ゲートウェイ インターフェイスの IP アドレスである必要があります。HA モードでは、ローカル IP アドレスは共有 IP アドレスである必要があります。 HA がすでに構成されている場合、これは自動的に設定されます。 HA 構成でのトンネリングのセットアップの詳細については、次のセクションを参照してください。

Local Subnet Address

ローカル IP アドレスを設定すると、ローカル サブネット アドレス テキスト ボックスが自動的に入力されます。 /32 CIDR を指定すると、該当する場合はローカル IP が唯一の参加者になる可能性があります。 ローカル サブネット アドレスを確認し、必要に応じて更新します。 アドレスが変更されているかどうかに関係なく、Set Local Subnet Address をクリックして設定を適用してください。 カンマ区切りのリストを使用して、複数のローカル サブネットを指定できます。 最大 10 個の IP アドレスを指定できます。

Remote IP Address

接続のリモート側の IP アドレスを設定します。 Azure エンドポイントのコンテキストでは、この IP アドレスは、仮想プライベート ネットワーク (VPN) ゲートウェイ デバイスの公開 IP アドレスであると想定されます。

Remote Subnet Address

接続のリモート側のサブネットを設定します。 カンマ区切りのリストを使用して、複数のリモート サブネットを指定できます。 最大 10 個の IP アドレスを指定できます。

Perfect Forward Secrecy

Perfect Forward Secrecy オプションを有効または無効にします。

使用されているクラウド プラットフォームによって、Perfect Forward Secrecy オプションの設定値が決まります。 一部のプラットフォームでは Perfect Forward Secrecy が必要ですが、他のプラットフォームではサポートされていません。 お使いのクラウド プラットフォームで何が機能するかを確認するには、ドキュメントを参照してください。

Local ID

接続のローカル側の識別。 これは、ローカル IP アドレスの場合があります。 LoadMaster が HA モードでない場合、このフィールドにはローカル IP アドレスと同じアドレスが自動的に入力されます。LoadMaster が HA モードの場合、Local ID フィールドは自動的に %any に設定されます。LoadMaster が HA モードの場合、この値は更新できません。

Remote ID
接続のリモート側の識別。 これは、リモート IP アドレスの場合があります。

Pre Shared Key (PSK)
事前共有キー文字列を入力します。

Save Secret Information

接続 ID とシークレット情報を生成して保存します。

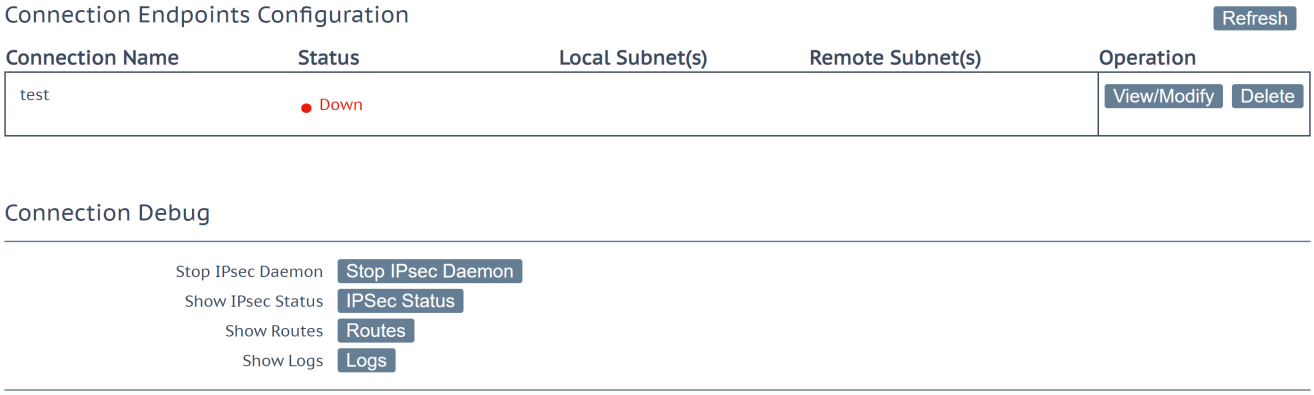
11.1.7 ルートベース VPN

LoadMaster ファームウェア バージョン 7.2.53 より前は、LoadMaster はポリシーベースの仮想プライベート ネットワーク (VPN) のみをサポートしていました。 LoadMaster バージョン 7.2.53 以降、ルートベースの VPN サポートが導入されました。 ルートベースの VPN 機能は、Progress Kemp サポート サイトからダウンロードできるアドオン パックとして利用できます。 アドオン ファイルを入手したら、[システム構成] > [System Configuration] > [Update Software] でインストールします。 アドオンをインストールした後、LoadMaster を再起動して有効にします ([System Configuration] > [System Administration] > [System Reboot])。

ルートベースの VPN アドオンは、ファームウェア バージョン 7.2.53 以降でのみサポートされます。 LoadMaster のルートベースの VPN 機能は、strongSwan IPsec VPN ソリューションに基づいています。 strongSwan ドキュメントの詳細については、strongSwan Web サイト リンク https://www.strongswan.org/ を参照してください。

アドオンをインストールして LoadMaster を再起動すると、新しいメイン メニュー オプションが利用可能になります: System Configuration > Network Setup > Route Based VPN。 接続を識別する一意の名前を指定し、[Create] をクリックします。 VPN 接続の詳細を設定すると、接続のデバッグ オプションも表示されます。

- LoadMaster で IPsec デーモンを停止してから開始します。
- 接続状態を表示します。
- ルートを表示します。
- ログを表示します。



Connection Name

接続を識別する一意の名前を指定します。

Create

指定された名前で一意に識別可能な接続を作成します。

View/Modify

この接続の構成パラメータを表示または変更します。

Delete

この接続を削除します。

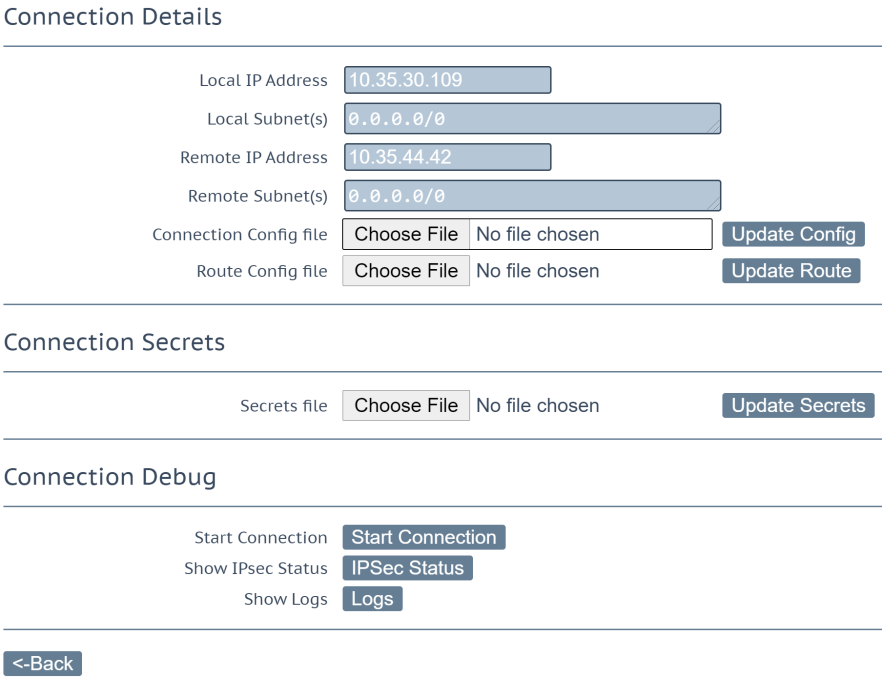
接続名が、アップロードする ipsec.conf ファイル内の接続名と同じであることを確認してください。接続名の長さは 3 文字以上、最大 20 文字である必要があります。 有効な文字は、a ～ z、A ～ Z、0 ～ 9、_、および - です。

最初に接続を作成した後、strongSwan 標準形式に基づいて、接続構成、ルート構成、およびシークレット ファイルをアップロードする必要があります。 これらのファイルは、ユーザーが strongswan IPsec を構成するために使用できる複数の構成オプションをサポートします。

ipsec.conf ファイルの左側の IP アドレスを LoadMaster の IP アドレス (eth0) に設定してください。

ファイルがアップロードされて検証されると、接続の詳細が [View/Modify VPN Connection] 画面のフィールドに表示されます。

11.1.7.1 VPN 接続の表示/変更



Local IP Address

接続のローカル側の IP アドレスを表示します。 非 HA モードでは、ローカル IP アドレスは LoadMaster の IP アドレス、つまりデフォルト ゲートウェイ インターフェイスの IP アドレスである必要があります。 HA モードでは、ローカル IP アドレスは共有 IP アドレスである必要があります。 HA がすでに構成されている場合、これは自動的に設定されます。 HA 構成でのトンネリングのセットアップの詳細については、次のセクションを参照してください。

Local Subnet(s)

接続のローカル側のローカル サブネットを表示します。

Remote IP Address

接続のリモート側の IP アドレスを表示します。 Azure エンドポイントのコンテキストでは、この

IP アドレスは、仮想プライベート ネットワーク (VPN) ゲートウェイ デバイスの公開 IP アドレスであると想定されます。

Remote Subnet(s)

接続のリモート側のサブネットを表示します。

Connection Config file

[Choose File] をクリックし、ファイルを参照して選択し、[Update Config] をクリックします。 構成ファイルには、構成されたすべての IPsec 接続のデフォルト値 conn %default が含まれています。 この構成は、strongswan IPsec エンジンに直接与えられます。 接続構成ファイルの形式には、次のパラメーターが含まれます。

```
conn %default
dpddelay=30
dpdtimeout=120
dpdaction=restart
ikelifetime=28800s
#keylife=20m
keylife=1d
rekeymargin=3m
keyingtries=1
authby=secret
keyexchange=ikev2
mobike=yes
ike=aes256-sha384-ecp384
esp=aes256-sha384-ecp384,aes256gcm16
conn routevpn
left=10.35.45.170
leftsubnet=10.35.99.170/32
right=65.51.241.146
rightsubnet=10.0.70.1/32
leftid=78.56.45.56
rightid=%any
mark=1
auto=start
ikelifetime=1h
```

lifetime = 1h
margintime = 9m
rekeyfuzz = 100%
ike=aes256gcm16-sha384-modp2048
esp=aes256gcm16-sha384-modp2048

Route Config file

[Choose File] をクリックし、ファイルを参照して選択し、[Update Route] をクリックします。
Route Config ファイルには、作成された IPsec トンネルを使用して特定のリモート ネットワークにパケットをルーティングするためのルーティング情報が含まれています。 Route Config ファイルの形式には、次のパラメータが含まれます。
<LEFT IP> <RIGHT IP> <REMOTE NETWORK> <SOURCE IP>

Secrets file

[Choose File] をクリックし、ファイルを参照して選択し、[Update Secrets] をクリックします。
Secrets ファイルには、リモート エンドポイントとローカル エンドポイントのアドレス、およびリモート エンドポイントと通信するためのシークレットが含まれています。 シークレット ファイルの形式の例: 10.35.45.170 65.51.241.146 %any: PSK "fE31$I#%w&"

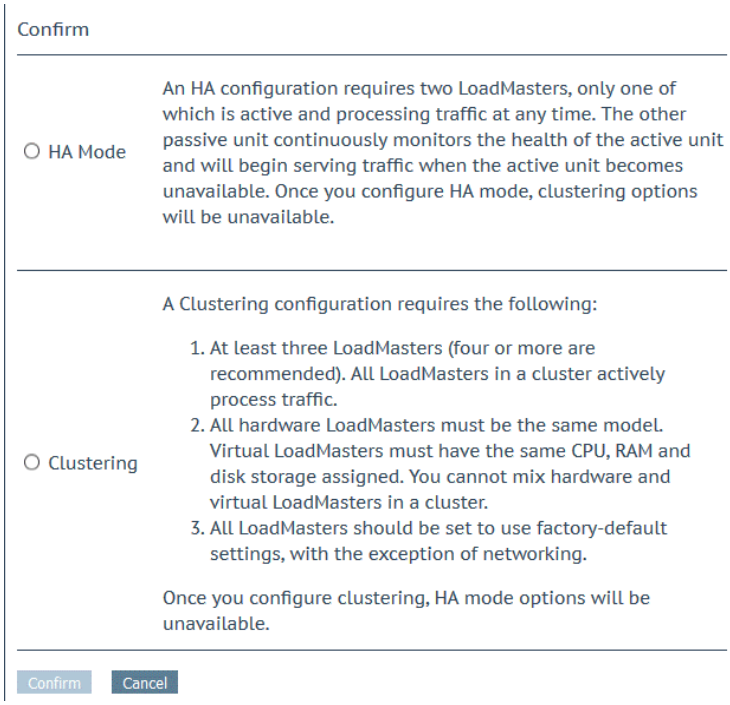
Show IPsec Status

[IPSec Status] をクリックすると、接続ステータスを表示できます。

Show Logs

[Log] をクリックすると、接続ログを表示できます。

11.2 HA とクラスタリング



WUI のこのセクションは、クラスタリングが有効になっている LoadMaster ライセンスを持っている場合にのみ、HA およびクラスタリングと呼ばれます。 クラスタリングがない場合、このセクションは HA パラメータと呼ばれ、上記の画面は表示されません。 クラスタリングが構成されている場合、このセクションは Cluster Control と呼ばれます。 この画面では、HA モードとクラスタリングの両方について説明します。 関連するオプションを選択し、[Confirm] をクリックします
続ける。

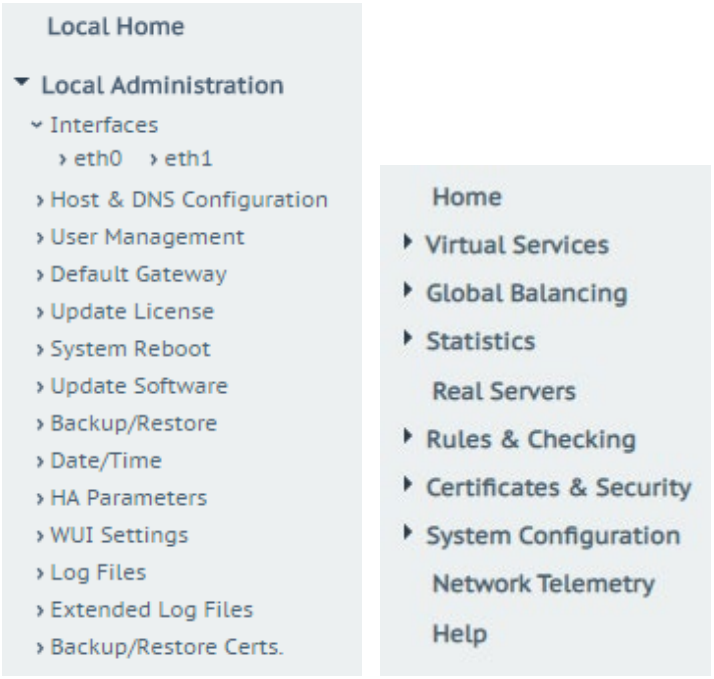
クラスタリングが構成されると、HA モード オプションは使用できなくなります

11.2.1 HA モード

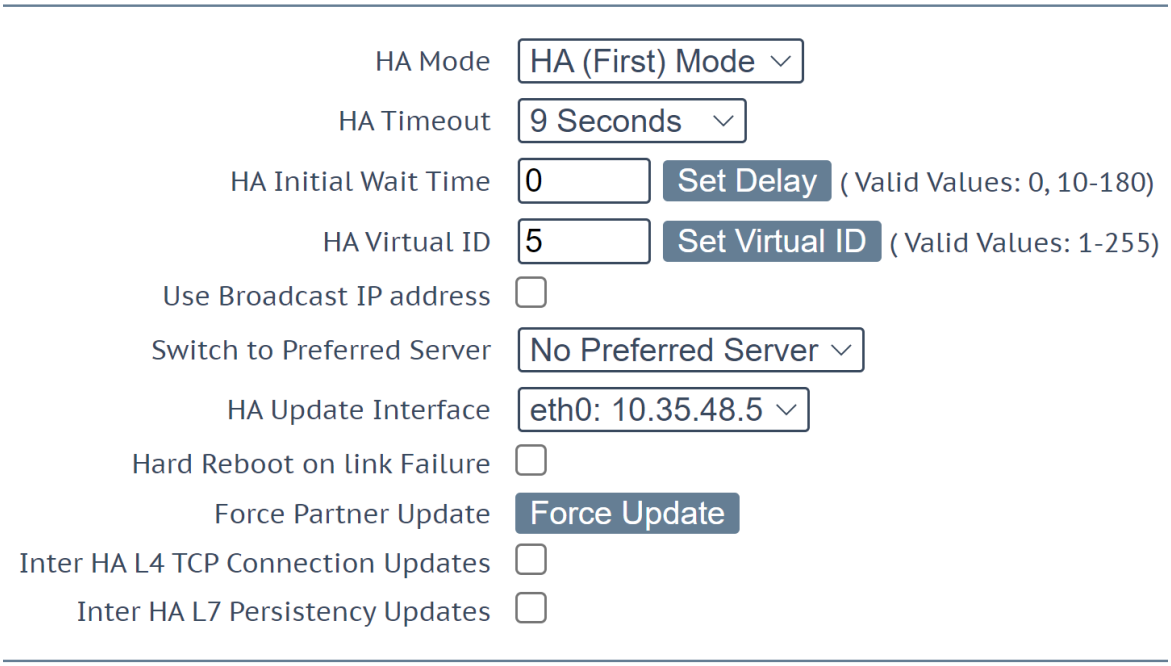
LoadMaster をクラウド環境で使用している場合は、Azure HA パラメータまたは AWS HA パラメータのセクションを参照してください。 LoadMaster for AWS 製品を使用している場合は、AWS HA パラメータを参照してください。

アプライアンスの役割は、HA モードを設定することで変更できます。 HA モードとして HA (第 1) モードまたは HA (第 2) モードが選択されている場合、共有 IP を追加するよう促すプロンプトが表

示されます。 HA モードを変更すると再起動が必要になるため、詳細設定後、表示された [Reboot] ボタンをクリックします。 LoadMaster が再起動すると、役割が「非 HA モード」でない場合、システム構成セクションで HA メニュー オプションが使用可能になります。 両方のマシンが同じに指定されている場合、HA は機能しません。 HA クラスターにログインしたら、共有 IP アドレスを使用してペアの全機能を表示および設定します。 いずれかのデバイスの直接 IP アドレスにログインすると、メニュー オプションはまったく異なります (以下のメニューを参照)。 LoadMaster の 1 つに直接ログインすることは、通常、メンテナンスのために予約されています。

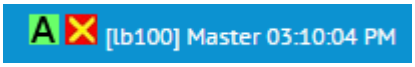


LoadMaster が HA モードの場合、HA パラメータ メニュー オプションを選択すると、次の画面が表示されます。



HA Status

画面上部の時刻の横にアイコンが表示され、クラスタ内の LoadMaster ユニットのリアルタイム ステータスが示されます。 クラスタ内の各ユニットのアイコンがあります。 関連するステータス アイコンをクリックすると、１つ目または ２つ目の HA ユニットの WUI を開くことができます。



可能なアイコンは次のとおりです。

緑（「A」付き）		ユニットはオンラインで動作しており、HA ユニットは正しくペアリングされています。 正方形の中央にある A は、これがアクティブなユニットであることを示します。
緑（「A」なし）		ユニットはオンラインで動作しており、HA ユニットは正しくペアリングされています。 正方形の中央に「A」がない場合は、これがスタンバイ ユニットではないことを示します。
赤/黄		ユニットは動作していません。 オフラインであるか、正しく構成されていない可能性があります。 ユニットは引き継ぐ準備ができていません。 オフラインである

		か、正しくペアリングされていない可能性があります。
青		ユニットが 5 分間に 3 回以上再起動すると、鎮静状態に移行します。 この状態では、マシンは (共有 WUI ではなく) 直接のマシン WUI を使用してのみアクセスでき、どの HA アクティビティにも参加していません。つまり、アクティブなユニットからの変更は受信されず、引き継がれません。 アクティブ ユニットが失敗します。 ユニットを pacified 状態から削除するには、SSH またはコンソールを介して pacified LoadMaster にログインし、再起動します。
グレー		マシンは不確定な状態にあり、操作に戻るには再起動が必要になる場合があります。 場合によっては、これは両方のマシンがアクティブであること、つまり両方がアクティブに設定されていて、何か重大な問題が発生したことを意味する場合があります。 再起動しても問題が解決しない場合は、Progress Kemp サポートに連絡してこの問題の支援を受けてください。
HA アイコンなし		HA ステータスの正方形が WUI に表示されない場合は、HA が有効になっていない可能性があります。 システム管理に移動し、HA オプションを選択します。 HA モードが First または Second に設定されていることを確認します。

HA モードでは、各 LoadMaster に独自の IP アドレスがあり、ユニット上で直接診断目的でのみ使用されます。 HA ペアには、WUI を使用してペアを単一のエンティティとして構成および管理する共有 IP アドレスがあります。

HA1 と HA2 の両方が、同じデフォルト ゲートウェイを持つ同じサブネット上にあり、同じ物理サイトにある必要があります。 サイト内リンクでそれらを分離してはならず、同じゲートウェイを使用してトラフィックを返す必要があります。

HA Mode

単一の LoadMaster を使用している場合は、非 HA モードを選択します。 HA モードを設定する場

合、一方の LoadMaster を HA (First) に設定し、もう一方を HA (Second) に設定する必要があります。 両方が同じオプションに設定されている場合、HA は動作しません。

HA Timeout

スイッチオーバーが発生する前に、アクティブなマシンが使用できなくなる必要がある時間。 このオプションを使用すると、HA クラスターが障害を検出するのにかかる時間を 3 秒から 15 秒まで 3 秒単位で調整できます。 デフォルト値は 9 秒です。 値が小さいほど障害が早く検出され、値が大きいほど DOS 攻撃に対する保護が強化されます。

HA Initial Wait Time

LoadMaster の初回起動後、マシンがアクティブになる必要があると判断するまでの時間。 パートナー マシンが実行中の場合、この値は無視されます。 この値を変更して、一部のインテリジェント スイッチが LoadMaster の起動を検出し、リンクを確立するのにかかる時間を軽減できます。

HA Virtual ID

同じネットワーク上で複数の HA LoadMaster クラスターを使用する場合、この値は各クラスターを一意に識別するため、望ましくない相互作用が発生する可能性はありません。

HA ペアに構成されている、または構成される予定のネットワーク上のすべての LoadMaster には、一意の HA 仮想 ID 番号を割り当てる必要があります。

7.2.36 リリース以降、LoadMaster は最初に構成されたインターフェースの共有 IP アドレス (最後の 8 ビット) に基づいて仮想 ID を選択します。 共有アドレスとパートナー アドレスの両方が設定されると、選択されて表示されます。 値を任意 (1 ～ 255 の範囲) に変更することも、既に選択されている値のままにすることもできます。 仮想 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。

Use Broadcast IP address

デフォルトでは、LoadMaster は CARP パケットの送信時に IP マルチキャスト アドレスを使用します。 このオプションを有効にすると、代わりに IP ブロードキャスト アドレスが強制的に使用されます。

Switch to Preferred Server

デフォルトでは、HA クラスター内のどちらのパートナーも優先されません。 そのため、スイッチオーバー後にマシンが再起動すると、マシンはスタンバイになり、強制的にアクティブになるまでその状

態にとどまります。 優先ホストを指定すると、このマシンの再起動時に常にアクティブになろうとし、パートナーはスタンバイ モードに戻ります。 優先サーバーが指定されている場合、アクティブ ユニットに障害が発生すると、スタンバイ ユニットがアクティブとして引き継ぎ、優先ユニットが復旧すると、アクティブとして引き継ぎます。これにより、二重のフェールオーバー イベントが発生します。

HA Update Interface

HA クラスター内で HA 情報を同期するために使用されるインターフェース。

Hard Reboot on link Failure

LoadMaster ファームウェア バージョン 7.2.53 では、新しいオプションであるリンク障害時のハード リブートが導入されました。 [Hard Reboot on link Failure] チェック ボックスが有効になっている場合、HA で構成された LoadMaster は、構成されたインターフェースがネットワークとの接続を失った場合 (つまり、リンク障害が発生した場合) に再起動します。 LoadMaster の HA ステータス (プライマリまたはスタンバイ) に関係なく、再起動が行われます。 次の両方が該当する場合、[System Configuration] > [HA Parameters] 画面で [Hard Reboot on link Failure] チェック ボックスを使用できます。

- 高可用性 (HA) が構成されている
- [Switch to Preferred Server] オプションが [No Preferred Server] に設定されている。

[Switch to Preferred Server] ドロップダウン リストから優先サーバーを選択すると、[Hard Reboot on link Failure] チェック ボックスは使用できなくなります。

リンク障害時のハード リブートが有効になっている場合、優先サーバーを設定することはできません。設定した場合、アクティブなロードマスター ユニットとスタンバイ ロードマスター ユニットの間で循環スワッピングが発生する可能性があります。

Force Partner Update

通常の更新を待たずに、アクティブ ユニットからスタンバイ ユニットへの設定をただちに強制します。

Inter HA L4 TCP Connection Updates

L4 サービスを使用している場合、更新を有効にすると、接続テーブルを共有することにより、HA ス

イッチオーバー全体で L4 接続を維持できます。 このオプションは、L7 サービスでは無視されます。

Inter HA L7 Persistence Updates

L7 サービスを使用する場合、このオプションを有効にすると、永続性情報を HA パートナー間で共有できます。 HA フェイルオーバーが発生した場合、永続性情報は失われません。 このオプションを有効にすると、パフォーマンスに大きな影響を与える可能性があります。

HA Multicast Interface

Inter-HA Updates が有効な場合にレイヤ 4 およびレイヤ 7 トラフィックを同期するために使用されるマルチキャスト トラフィックに使用されるネットワーク インターフェイス。

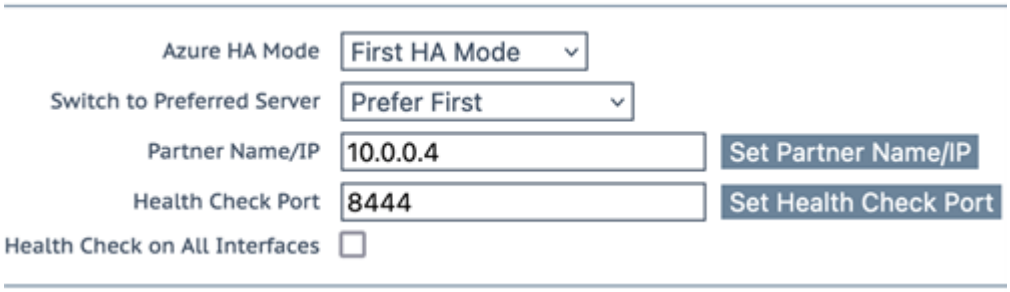
Use Virtual MAC Addresses

このオプションを有効にすると、スイッチオーバー中に MAC アドレスが強制的に HA ペア間で切り替わります。これは、gratuitous ARP (HA IP アドレスの変更をスイッチに伝達する際に使用される) が許可されていない場合に役立ちます。

このオプションは、ハードウェア LoadMaster でのみ使用できます

11.2.1.1 Azure HA パラメータ

この画面は、LoadMaster for Azure 製品でのみ使用できます。



Azure HA Mode

このユニットに必要な HA モードを選択します。 次の 3 つのオプションがあります。

- First HA Mode
- Second HA Mode
- Non HA Mode

LoadMaster を 1 台だけ使用している場合は、Non HA Mode を選択します。 HA モードを使用す

る場合、1 台のマシンを 1 台目 (アクティブ) として指定し、2 台目のマシンを 2 台目 (スタンバイ) として指定する必要があります。

両方のユニットで Azure HA モードに同じ値が選択されている場合、HA は機能しません。 仮想サービス設定の同期は、アクティブからスタンバイに対してのみ発生します。 アクティブに加えられた変更は、スタンバイに複製されます。 ただし、スタンバイ ユニットに加えられた変更がアクティブ ユニットに複製されることはありません。 アクティブ ユニットに障害が発生した場合、接続はスタンバイ ユニットに転送されます。 アクティブ ユニットはアクティブであり、障害が発生してもスタンバイになることはありません。 同様に、スタンバイ ユニットがアクティブ ユニットになることはありません。 アクティブ ユニットが復旧すると、接続は自動的にアクティブ ユニットに再び向けられます。

LoadMaster の上部バーのモードを確認することで、どのユニットがアクティブで、どのユニットがスタンバイであるかが一目でわかります。

Switch to Preferred Server

選択できる値は 2 つあります。

- No Preferred Host: 他のユニットに障害が発生すると、各ユニットが引き継ぎます。 パートナーの再始動時にスイッチオーバーは実行されません。
- Preferred First: HA1 (アクティブ) ユニットが常に引き継ぎます。 これはデフォルトのオプションです。

Partner Name/IP

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

ヘルスチェックを実行するポートを設定します。 HA が正しく機能するには、アクティブ ユニットとスタンバイ ユニットの両方でポートが同じである必要があります。

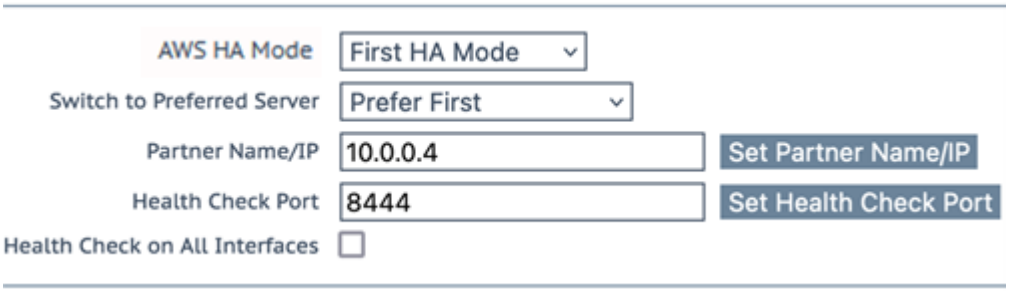
Health Check on All Interfaces

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イスでリッスンします。 これは、マルチアーム構成を使用する場合に必要です。 これが無効になっている場合、ヘルスチェックはプライマリ eth0 アドレスでリッスンします (これがデフォルトの動作です)。

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のみに制限されます。 ユニットがアクティブまたはチェックされていない状態の場合、完全な WUI アクセスが利用可能です。

11.2.1.2 AWS HA パラメータ

この画面は、LoadMaster for Amazon Web Services (AWS) 製品でのみ使用できます。



AWS HA Mode

このユニットに必要な HA モードを選択します。 次の 3 つのオプションがあります。

- First HA Mode
- Standby HA Mode
- Non HA Mode

LoadMaster を 1 台だけ使用している場合は、Non HA Mode を選択します。 HA モードを使用す

る場合、1 台のマシンを 1 台目 (アクティブ) として指定し、2 台目のマシンを 2 台目 (スタンバイ) として指定する必要があります。

両方のユニットで同じ値が選択されている場合、HA は機能しません。
AWS HA モード。 仮想サービス設定の同期は、アクティブ ユニットからスタンバイ ユニットにのみ発生します。 アクティブ ユニットに加えられた変更は、スタンバイ ユニットに複製されます。 ただし、スタンバイ ユニットに加えられた変更がアクティブ ユニットに複製されることはありません。 アクティブ ユニットに障害が発生した場合、接続はスタンバイ ユニットに転送されます。 アクティブ ユニットはアクティブであり、障害が発生してもスタンバイになることはありません。 同様に、スタンバイ ユニットがアクティブ ユニットになることはありません。 アクティブ ユニットが復旧すると、接続は自動的にアクティブ ユニットに再び向けられます。

LoadMaster の上部バーのモードを確認することで、どのユニットがアクティブで、どのユニットがスタンバイであるかが一目でわかります。

Switch to Preferred Server

選択できる値は 2 つあります。

- No Preferred Host: 他のユニットに障害が発生すると、各ユニットが引き継ぎます。 パートナーの再始動時にスイッチオーバーは実行されません。
- Preferred Host: HA1 (アクティブ) ユニットが常に引き継ぎます。 これはデフォルトのオプションです。

Partner Name/IP

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

ヘルスチェックを実行するポートを設定します。 HA が正しく機能するには、アクティブ ユニットとスタンバイ ユニットの両方でポートが同じである必要があります。

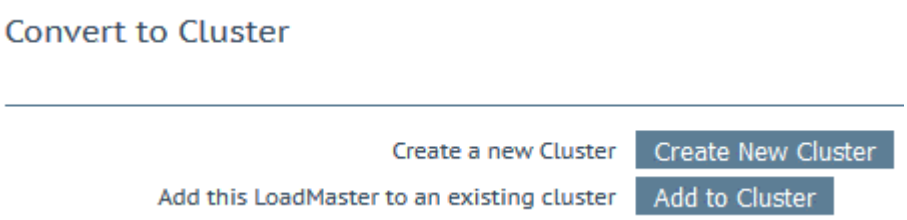
Health Check on All Interfaces

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イスでリッスンします。 これは、マルチアーム構成を使用する場合に必要です。 これが無効になっている場合、ヘルスチェックはプライマリ eth0 アドレスでリッスンします (これがデフォルトの動作です)。

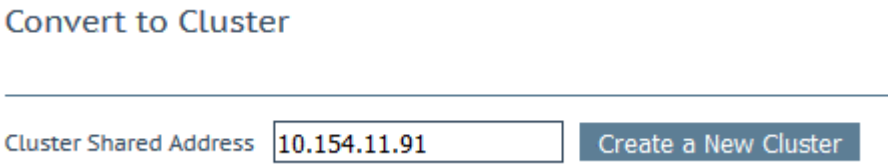
ユニットがスタンバイ モードの場合、WUI アクセスはローカル管理のみに制限されます。 ユニットがアクティブまたはチェックされていない状態の場合、完全な WUI アクセスが利用可能です。

11.2.2 クラスター制御

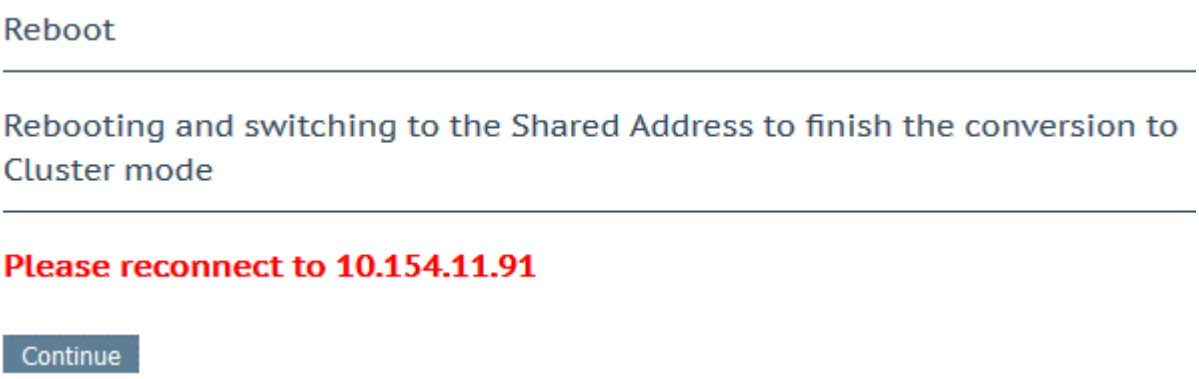
Cluster Control オプションは、クラスタリング ライセンスを持つ LoadMaster でのみ使用できます。 ライセンスにクラスタリング機能を追加するには、Progress Kemp の担当者にお問い合わせください。 クラスタリングの詳細については、LoadMaster クラスタリング機能の説明を参照してください。



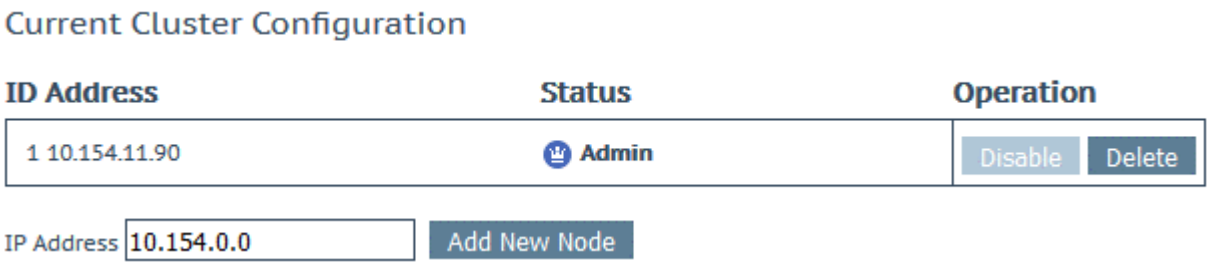
Create New Cluster: 新しいクラスターを設定する場合は、このボタンをクリックします。
Add to Cluster: この LoadMaster を既存のクラスターに追加します。



[Create New Cluster] ボタンをクリックすると、上記の画面が表示され、クラスターの共有 IP アドレスを設定するよう求められます。 共有 IP アドレスは、クラスターの管理に使用されるアドレスです。

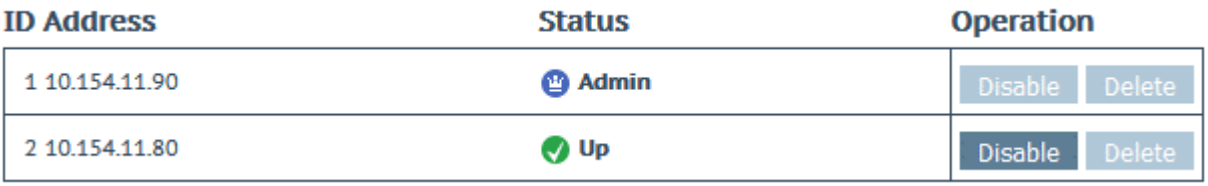


Create a New Cluster ボタンをクリックすると、LoadMaster が再起動します。 設定した共有 IP アドレスへの再接続を求めるメッセージが表示されます。



クラスタを作成した後、共有 IP アドレスの WUI の Cluster Control 画面で、LoadMaster ノードをクラスタに追加できます。

LoadMaster は、クラスターが使用可能であり、LoadMaster がクラスターへの参加を待機している場合にのみ、クラスターに追加できます。 詳細と手順については、LoadMaster クラスタリング機能の説明を参照してください。



共有 IP アドレス WUI の Cluster Control 画面には、クラスタ内の各ノードの詳細が表示されます。 オプションの表示: [オプションの表示] 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、クラスターの仮想 ID とノードのドレイン時間を設定するために使用できる 2 つの追加フィールドが含まれています。 詳細については、Progress Kemp ドキュメント ページの LoadMaster クラスタリング機能の説明を参照してください。

ID: クラスター ID。

アドレス: LoadMaster ノードの IP アドレス。 最初の IP アドレスの後に 2 番目の IP アドレスが括弧内に表示される場合、2 番目の IP アドレスはインターフェイス ポートの IP アドレスです。

ステータスに応じてアイコンが表示されます。

アイコン	ステータス	説明
	Admin	ノードはプライマリ コントロール ノードです。
	Disable	ノードは無効です - 接続はそのノードに送信されません。
	Starting	ノードは起動中 (有効化中) です。
	Up	ノードが起動しています。
	Down	ノードがダウンしています。
	Draining	ノードが無効になり、接続が正常にシャットダウンされています。 デフォルトでは、ドレン停止は 10 秒間続きます。 これは、Cluster Control 画面で Node Drain Time の値を変更することで更新できます。 詳細については、LoadMaster クラスタリング機能の説明を参照してください。

Operation: ノートに関連して実行できるさまざまな操作:

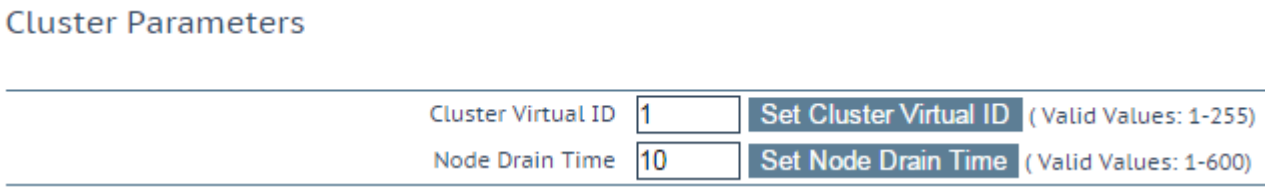
- Disable: ノードを無効化します。 無効になっているノードは、最初にドレーン停止を行います。 ドレン停止時間中は、接続が整然とシャットダウンされます。 排出後、ノードは無

効になり、トラフィックはそのノードに送られなくなります。

- Enable: ノードを有効にします。 ノードが起動しても、すぐにローテーションされるわけではありません。 起動してから 30 秒後にのみオンラインになります。
- Delete: クラスターからノードを削除します。 ノードが削除されると、通常の単一の LoadMaster インスタンスになります。 後で LoadMaster がクラスターに追加された場合、共有 IP アドレスで行われた構成の変更はノード LoadMaster に伝達されます。
- Reboot: クラスター全体のファームウェア更新を実行する場合、ファームウェア更新パッチのアップロード後に、この画面に [再起動] ボタンが表示されます。 クラスタ全体のファームウェア アップデートを実行する手順については、ロードマスター クラスタリング機能の説明を参照してください。

Add New Node: 指定した IP アドレスを持つ新しいノードをクラスターに追加します。

11.2.2.1 クラスタ パラメータ



[Show Options] ボタンをクリックすると、[Cluster Parameters] セクションが表示されます。 このセクションには、クラスターの仮想 ID とノードのドレイン時間という 2 つの追加の WUI オプションが含まれています。

Cluster Virtual ID

同じネットワーク上で複数のクラスターまたは LoadMaster HA システムを使用する場合、仮想 ID は各クラスターを識別し、望ましくない相互作用が発生する可能性を防ぎます。 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、必要に応じて変更できます。 有効な ID の範囲は 1 ～ 255 です。管理ロードマスターに加えられた変更は、クラスター内のすべてのノードに反映されます。

Node Drain Time

ノードが無効になっている場合、そのノードによって引き続きサービスが提供されている接続は、[Node Drain Time] テキスト ボックスで指定された秒数の間継続できます。 この間、ノードは新しい接続を処理しません。 Node Drain Time はデフォルトで 10 秒に設定されていますが、必要に応

じて変更できます。 有効な値の範囲は 1 ～ 600 (秒) です。 排出時間中は、指定された排出時間が経過するまでステータスが「排出中」に変わります。 ドレーン時間が経過すると、ステータスが無効に変わります。

11.3 QoS/制限

11.3.1 グローバル制限

グローバル制限セクションでは、次のオプションを構成できます。

- Maximum Concurrent Connections: LoadMaster に許可される同時接続の最大数 (TCP 接続と UDP 接続の合計) を制限します。 制限を 0 に設定すると、このオプションが無効になります。 有効な値は 0 ～ 100000000 です。

最大値は、使用中のハードウェアまたは Virtual LoadMaster に基づいており、モデルによって異なる場合があります。

- Global Connections/s Limit: 接続試行の最大数 (1 秒あたり) を制限します。 制限を 0 に設定すると、このオプションが無効になります。 有効な値は 0 ～ 1000000 です。
- Global HTTP Requests/s Limit: HTTP リクエストの最大試行回数 (1 秒あたり) を制限します。 これは、HTTP 以外のトラフィックには影響しません。 制限を 0 に設定すると、このオプションが無効になります。 有効な値は 0 ～ 1000000 です。

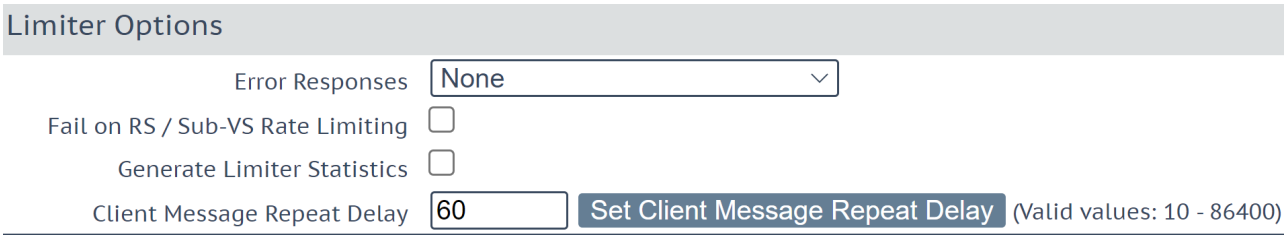
グローバル制限は、構成されている他の制限よりも優先されます。 たとえば、クライアント同時接続制限を 5000 に設定し、グローバル最大同時接続制限が 50 に設定されている場合、50 が適用される制限になります。 すべてのクライアントからの接続の合計数がグローバル制限を超えると、それらはドロップされます。

Global Bandwidth Limit: グローバル帯域幅制限。 制限を 0 に設定すると、帯域幅制限が無効になります。 単位はキロビット/秒です。 最小値は 16 キロビット/秒 (2 キロバイト/秒) です。 最大値は 99999999 です (これは 100 Gbit をわずかに下回ります) が、ほとんどの LoadMasters ECS

Connection Manager ではライセンスに帯域幅制限が設定されており、グローバル帯域幅制限フィールドで指定された値がそれより大きい場合、ライセンスの帯域幅制限が適用されます。 帯域幅を計算する場合、両方向のデータが追跡され、計算に使用されます。

仮想サービスごとの帯域幅制限を構成することもできます。
詳細については、Progress Kemp ドキュメント ページのレート制限機能の説明を参照してください。 可能な 3 つの制限 (グローバル、クライアント、および仮想サービス) のうち、最初に到達した最も低い制限が適用されます。 グローバル制限はすべての仮想サービスに対するものであり、仮想サービス制限は複数のクライアントを持つ現在の仮想サービスに対するものであり、クライアント制限は単一のクライアントに対するものであることに注意してください。

11.3.2 リミッターのオプション



[Limiter Options] セクションでは、次のオプションを構成できます。

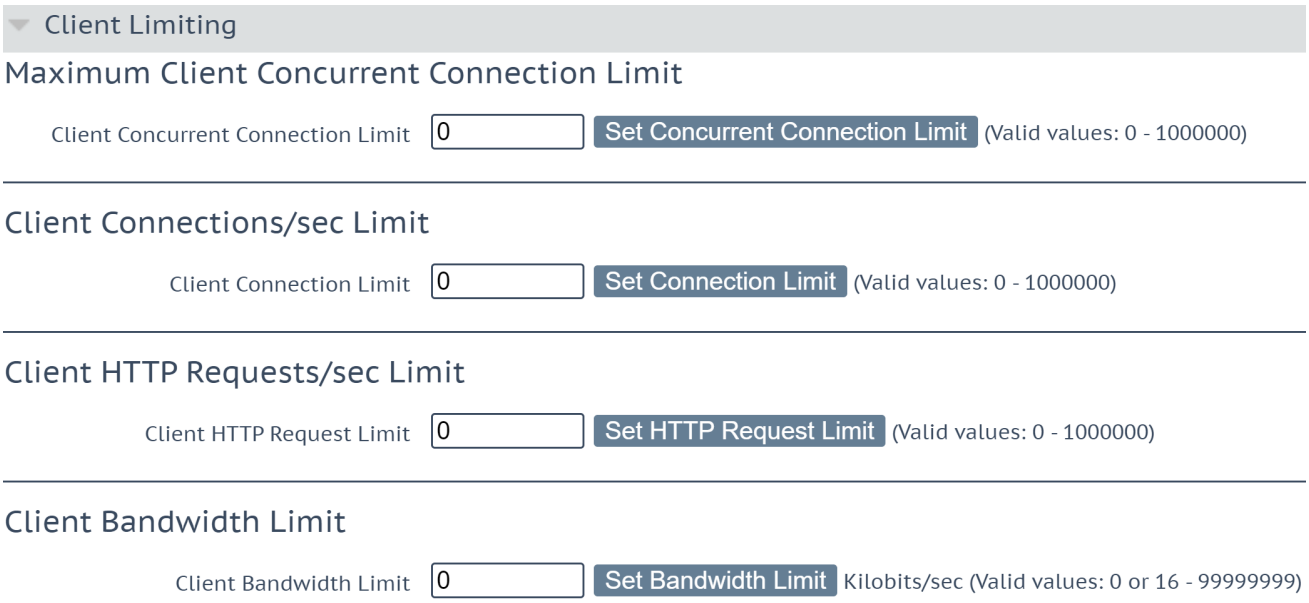
- Error Response: デフォルトでは、ロードマスターは RPS 制限に達すると、すべての接続を単純にドロップします。 このドロップダウン リストで適切なオプションを選択すると、システムは代わりに 429 または 503 HTTP エラー応答を送信できます (クローズが続きます)。
- Fail on RS/Sub-VS Rate Limiting: 実サーバー (RS) または SubVS に対してレート制限が有効になっている場合、LoadMaster は通常、接続に使用する別の RS/SubVS を選択しようとします。 このチェック ボックスを有効にすると、選択された RS が (たとえば永続性によって) レート制限されている場合、要求は強制的に失敗します。 [エラー応答] ドロップダウン リストでエラー応答が選択されている場合は、エラー応答が返されます。
- Generate Limiter Statistics: このオプションを有効にすると、制限 QoS サブシステムの現在の状態を含むグローバル サマリー syslog メッセージが 5 秒ごとに生成されます。

このオプションはデフォルトで無効になっています。 クライアント制限の構成によっては、リソース

を大量に消費する可能性がある多くのログ メッセージが生成される可能性があります。

- Client Message Repeat Delay: クライアントの制限が解除されてから新しいメッセージが生成されるまでの最小時間を設定します。 クライアントがメッセージを生成し、継続的に制限に達したために引き続きブロックされる場合、新しいメッセージは生成されません。 クライアントが遅延期間中静かになった場合にのみ、新しいメッセージが生成されます。 有効な値の範囲は 10 ～ 86400 秒です。 デフォルト値は 60 秒です。

11.3.3 クライアント制限



Maximum Client Concurrent Connection Limit

このセクションでは、特定のアドレスまたはネットワークの同時接続制限を構成するオプションを取得する前に、グローバル クライアント同時接続制限を構成する必要があります。 クライアント同時接続制限は、特定のホストからの同時接続試行のデフォルトの最大数 (1 秒あたり) を制限します。 制限を 0 に設定すると、このオプションが無効になります。 有効な値の範囲は 0 ～ 1000000 です。

Client Connections/sec Limit

このセクションでは、特定のアドレスまたはネットワークの CPS 制限を構成するオプションを取得する前に、グローバル クライアント接続制限を構成する必要があります。 クライアント接続制限は、特定のホストからのデフォルトの最大接続試行回数 (1 秒あたり) を制限します。 制限を 0 に設定すると、このオプションが無効になります。 有効な値の範囲は 0 ～ 1000000 です。

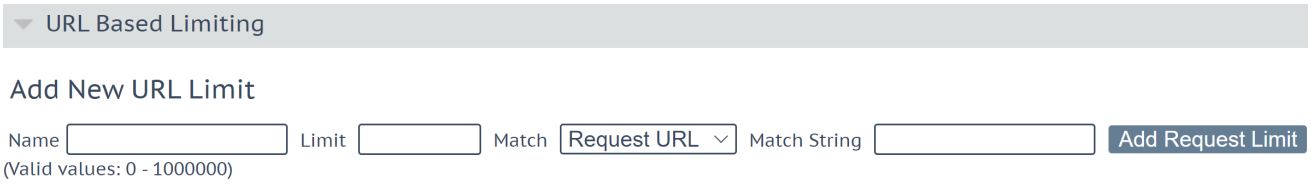
Client HTTP Requests/sec Limit

このセクションでは、特定のアドレスまたはネットワークの RPS 制限を構成するオプションを取得する前に、グローバル クライアント HTTP 要求制限を構成する必要があります。 クライアント HTTP 要求制限は、特定のホストからのデフォルトの HTTP 要求試行（1 秒あたり）の最大数を制限します。 これは、HTTP 以外のトラフィックには影響しません。 制限を 0 に設定すると、このオプションが無効になります。 有効な値の範囲は 0 ～ 1000000 です。

Client Bandwidth Limit

このセクションでは、特定のアドレスまたはネットワークの帯域幅制限を構成するオプションを取得する前に、グローバル クライアント帯域幅制限を構成する必要があります。 クライアント帯域幅は、特定のホストからのデフォルトの最大帯域幅試行回数（1 秒あたり）を制限します。 制限を 0 に設定すると、このオプションが無効になります。 単位はキロビット/秒です。 最小値は 16 キロビット/秒（2 キロバイト/秒）です。 最大値は、グローバル帯域幅制限で構成された値です。 帯域幅を計算する場合、双方向のデータが追跡され、使用されます。 これは、クライアント側とサーバー側の両方のデータが追跡され、計算の一部として使用されることを意味します。 詳細と手順については、Progress Kemp ドキュメント ページのレート制限機能の説明を参照してください。

11.3.4 URL ベースの制限



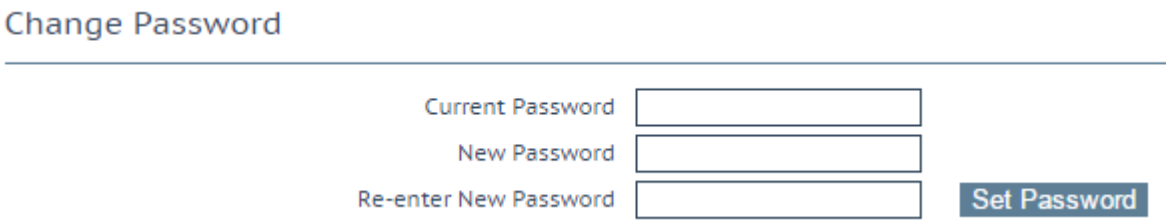
URL ベースの制限は、HTTP 要求のオプションに基づいています。 リクエストは、URL、メソッド、およびリクエスト ヘッダーで構成されます。 Host と User-Agent はリクエスト ヘッダーです。 LoadMaster の URL ベースの制限ルールは、[Match] ドロップダウン リストで選択された内容（リクエスト URL、ホスト、ユーザー エージェント、メソッド、!リクエスト URL、!ホスト、!ユーザー エージェント、または !メソッド）に基づいて検査します。 LoadMaster をヒットすると、応答コードが送信されます（[Limiter Options] セクションの [Error Responses] ドロップダウン リストで設定）。詳細と手順については、レート制限機能の説明を参照してください。

11.4 システム管理

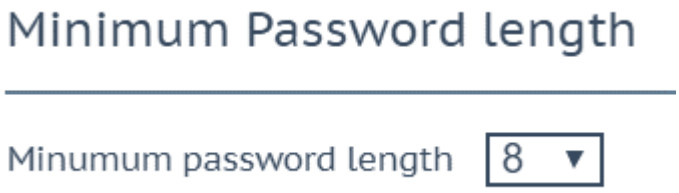
これらのオプションは、LoadMaster の基本レベルの操作を制御します。 HA ペアでこれらのパラメータに変更を適用するには、フローティング管理 IP を使用して行う必要があることを知っておくことが重要です。 これらのオプションの多くは、システムの再起動が必要です。 これらのパラメータを設定すると、ペアのアクティブ システムのみが影響を受けます。

11.4.1 ユーザー管理

以下のコンテンツでは、さまざまなユーザー管理 WUI フィールドについて説明します。 ユーザー管理と WUI 認証の詳細については、ユーザー管理機能の説明を参照してください。

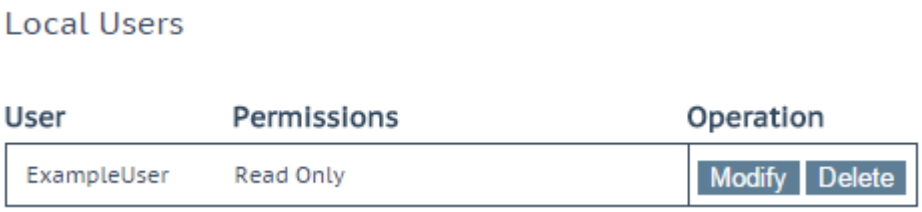


[Change Password] セクションを使用して、アプライアンスのパスワードを変更できます。 これはローカルの変更のみであり、HA 展開のパートナー アプライアンスのパスワードには影響しません。



Minimum Password length

すべてのローカル ユーザー パスワードの最小パスワード長を設定します。 このフィールドに別の値を選択した後、新しい値を適用するには、ページを更新する必要があります。



[Local User] セクションには、既存のローカル ユーザーが一覧表示されます。 既存のユーザーは、

次の 2 つのオプションを利用できます。

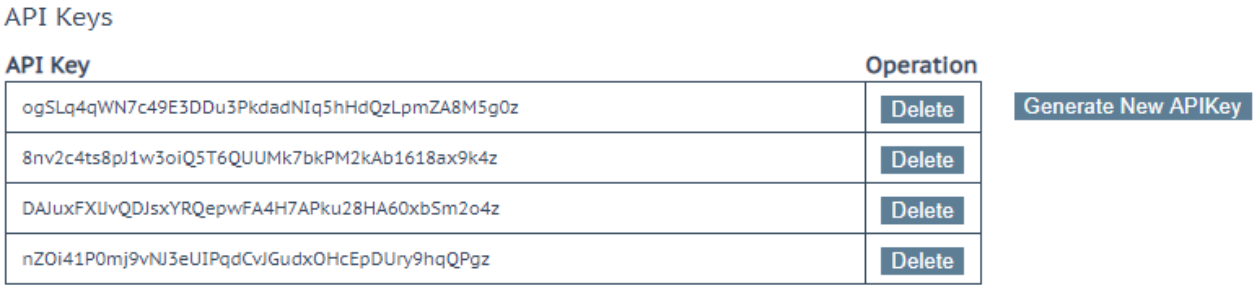
- Modify: 権限やパスワードなど、既存のローカル ユーザーの詳細を変更します。 詳細については、「Modify User」セクションを参照してください。
- Delete: 該当するユーザーを削除します。

新しいユーザーは、[Add User] セクションで追加できます。 ユーザー名の長さは最大 64 文字です。 ユーザー名は数字で始めることができ、次の特殊文字に加えて、英数字を含めることができます: =~^._+#@/-
パスワードの最小長は、[Minimum password length] フィールドに設定されている内容によって定義されます。 すべての文字が許可されます。 Use RADIUS Server オプションでは、ユーザーが LoadMaster にログインするときに RADIUS サーバー認証を使用する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 サーバーの詳細を設定する必要があります。 RADIUS 認証が使用されている場合、LoadMaster はユーザーの詳細を RADIUS サーバーに渡し、RADIUS サーバーはユーザーが認証されているかどうかを LoadMaster に通知します。 RADIUS サーバーの詳細を構成する方法の詳細については、WUI の認証と承認の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、この画面で [RADIUS サーバーを使用する] オプションは使用できません。 セッション管理が有効な場合に RADIUS サーバーを構成する方法の詳細については、WUI の認証と承認のセクションを参照してください。

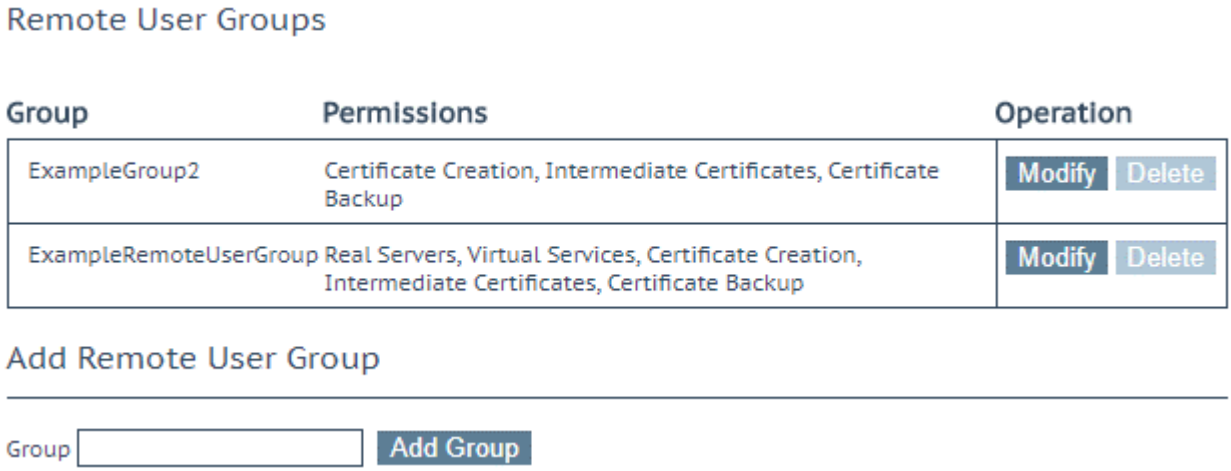
セッション管理を有効にすると、[Add User] セクションに [No Local Password] というチェックボックスが表示されます。 ユーザーが LoadMaster にアクセスするときにクライアント証明書認証を使用してこのユーザーを認証する場合、このオプションを有効にできます。 クライアント証明書認証を有効にするには、リモート アクセス画面で管理者ログイン方法を設定します。 詳細については、リモート アクセスのセクションまたはユーザー管理機能の説明を参照してください。

証明書ベースの認証は、将来のある時点で廃止される予定です。



API コマンドを実行するときは、API キーを使用して認証できます。 API キーは、ユーザーの認証に使用される一意の識別子です。

[User Management] 画面の [API キー] セクションには、ログインしているユーザーに対して現在生成されている API キーが表示されます。 ユーザーごとに最大 16 個の API キーを使用できます。それ以上作成しようとすると、最も古いものがサイレントに削除されます。 最も古い API キーが一番上に表示されます。 特定のユーザーの API キーを生成するには、その特定のユーザーの変更画面に移動します。



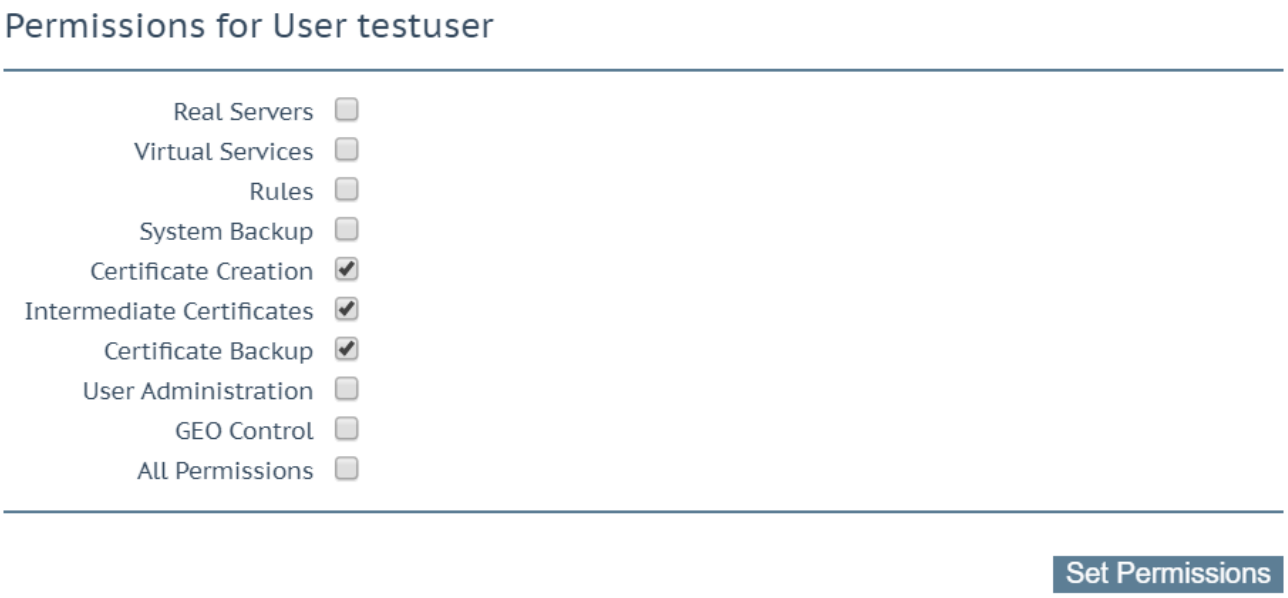
[リモート ユーザー グループ] セクションには、作成されたリモート ユーザー グループが表示されます。 グループ名と関連する権限が表示されます。 これらのグループは、次の場所で LDAP WUI 認証用に選択できます: [Certificate & Security] > [Remote Access] > [WUI Authorization Option]。 詳細については、WUI の認証と承認のセクションを参照してください。

グループを選択して適用することが重要です。 グループが選択されていない場合、グループ チェックは実行されず、リモート ユーザーはグループ チェックなしでログインできます。

名前を入力して [Add Group] をクリックすると、新しいリモート ユーザー グループを追加できます。

グループ名には次の文字を使用できます: 英数字、スペース、または次の特殊記号: =~^._+#,@/-.

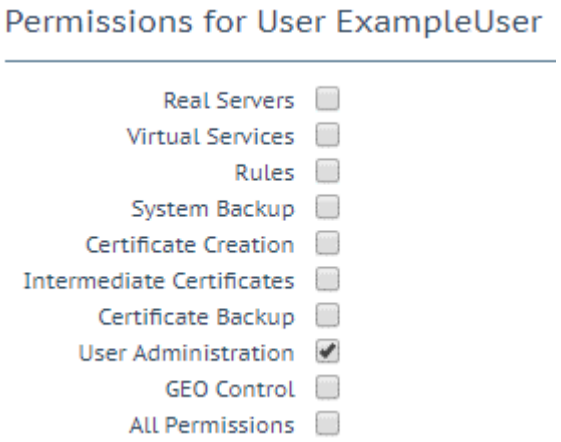
[Modify] をクリックして、グループの権限を編集します。



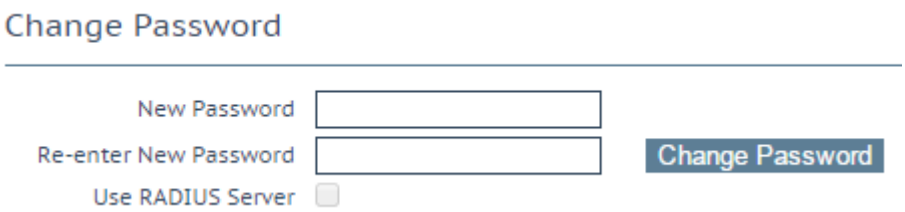
グループ権限の詳細については、ユーザー管理機能の説明を参照してください。

[Allow Extended Permissions] オプションを有効にすると、[Add Virtual Service] という追加のアクセス許可がユーザー アクセス許可画面に表示されます。 詳細については、ユーザー管理機能の説明を参照してください。

11.4.1.1 ユーザーの変更



この画面では、ユーザー権限のレベルを設定できます。 これにより、ユーザーが実行できる構成変更が決定されます。 プライマリ ユーザー (bal) には、常に完全なアクセス許可があります。 セカンダリ ユーザーは、特定の機能に制限される場合があります。 ユーザー権限の詳細については、ユーザー管理機能の説明を参照してください。



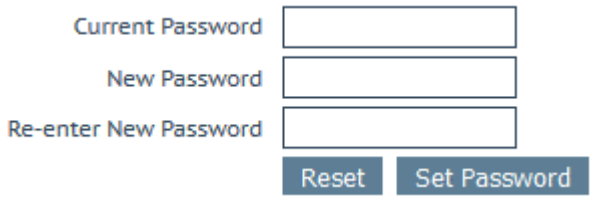
[Change Password] セクションを使用して、ユーザーのパスワードを変更できます。 ユーザーの RADUIS サーバー認証を有効または無効にすることもできます。

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場合に RADIUS サーバーを構成する方法の詳細については、WUI の認証と承認の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] というチェック ボックスが表示されます。 ユーザーが LoadMaster にアクセスするときにクライアント証明書認証を使用してこのユーザーを認証する場合、このオプションを有効にできます。 クライアント証明書認証を有効にするには、リモート アクセス画面で管理者ログイン方法を設定します。 詳細については、Progress Kemp ドキュメント ページのリモート アクセスまたはユーザー管理機能の

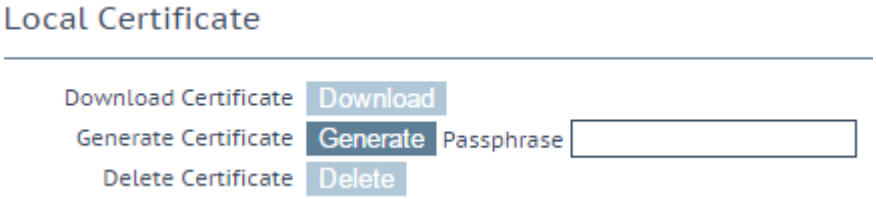
説明を参照してください。

名前付きユーザーは、ユーザー管理権限を持たないユーザーでも、自分のパスワードを変更できます。指定ユーザーが [System Configuration] > [User Management] メニュー オプションをクリックすると、[Change Password] 画面が表示されます。



この画面から、ユーザーは自分のパスワードを変更できます。 パスワードの最小長は、[パスワードの最小長] フィールドに設定されている内容によって定義されます。 ¥"`' を除くすべての文字を使用できます。 変更すると、確認画面が表示された後、ユーザーは新しいパスワードを使用して LoadMaster に再度ログインするように求められます。

API コマンドを実行するときは、API キーを使用して認証できます。 API キーは、ユーザーの認証に使用される一意の識別子です。 [Modify] 画面の [API Key] セクションには、その特定のユーザーに対して現在生成されている API キーが表示されます。 ユーザーごとに最大 16 個の API キーを使用できます。それ以上作成しようとすると、最も古いものがサイレントに削除されます。 最も古い API キーが一番上に表示されます。 特定のユーザーの API キーを生成するには、[Generate New APIKey] をクリックします。



[Local Certificate] セクションで、ユーザーの証明書を生成できます。 秘密鍵の暗号化に使用するパスフレーズをオプションで設定できます。 証明書がダウンロードされると、それをクライアント証明書として使用して、LoadMaster API へのパスワードなしのアクセスを許可できます。 「User Administration」権限を持つユーザーは、自分自身と他のユーザーのローカル証明書を管理できま

す。LoadMaster へのクライアント証明書認証を有効にするには、[Remote Access] 画面で [Admin Login Method] を設定します。 詳細については、Progress Kemp ドキュメント ページのリモート アクセス セクションまたはユーザー管理機能の説明を参照してください。

11.4.2 ライセンス管理

LoadMaster ファームウェア バージョン 7.2.53 では、[License/Owner] ボタンを使用して LoadMaster ライセンスを更新し、LoadMaster ライセンスの所有権を変更します。 詳細については、ライセンス機能の説明を参照してください。

この画面には、現在のライセンスの有効化日と有効期限が表示されます。 ライセンスが変更された場合は、ライセンス管理機能を使用します。たとえば、次の場合です。

- サポートを更新
- ライセンスを更新
- ライセンスの種類を変更

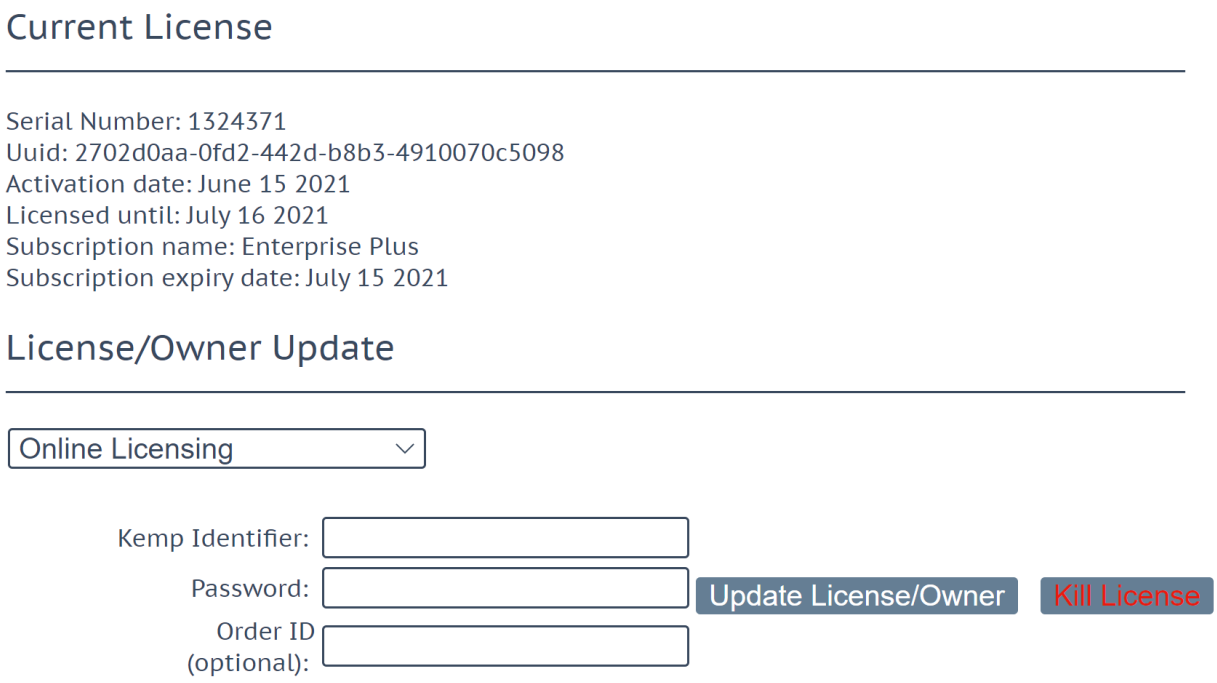
LoadMaster でライセンスを更新する前に、Progress Kemp の担当者に連絡するか、UI のホームページに表示されるアップグレード オプションを使用する必要があります。 Progress Kemp に連絡するか、アップグレード オプションを使用した後、ライセンスを更新するには、オンラインの方法とオフラインの方法の 2 つの方法があります。 それぞれの画面の詳細については、以下のセクションを参照してください。詳細と手順については、ライセンス機能の説明を参照してください。

[License Management] 画面に [Kill License] ボタンが表示される場合があります。

- LoadMaster ライセンスが、Kemp Licensing Server (オンラインまたはオフライン) から取得した永久 (PERM)、一時 (TEMP)、またはサービス プロバイダー ライセンス契約 (SPLA) のいずれかのライセンスである場合、[Kill License] ボタンをクリックするとライセンスが無効になります。 Kemp ライセンス サーバーと、LoadMaster のライセンスに使用された Kemp ID のインベントリにあるライセンス。
- LoadMaster ライセンスが、構成内のローカル Progress Kemp 360 Central インスタンスから取得された Service Provider License Agreement (SPLA) または Metered Licensing Agreement (MELA) ライセンスである場合、[Kill License] ボタンをクリックすると、LoadMaster ライセンスが使用可能な状態に戻ります。 Kemp 360 Central のライセンス プールを解放すると、LoadMaster はライセンスのない状態に戻ります。

Progress Kemp サポートからの指示がない限り、[Kill License] をクリックしないでください。

11.4.2.1 オンライン方式

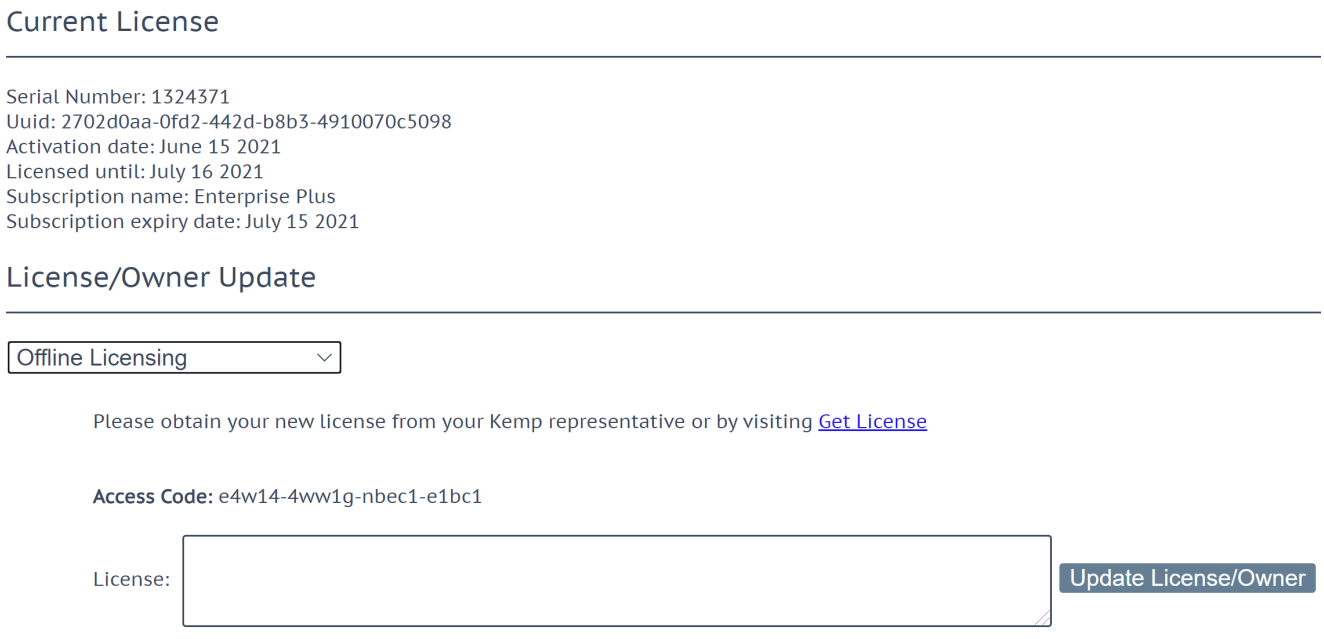


オンライン方式でライセンスをアップグレードするには、LoadMaster がインターネットに接続されている必要があります。 オンライン方式を使用してライセンスを取得するには、Kemp ID とパスワードを入力する必要があります。

ライセンスを更新した後は、再起動することをお勧めします。

Progress Kemp サポートからの指示がない限り、[Kill License] をクリックしないでください。

14.4.2.2 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、ロードマスターにライセンス テキストを入力する必要があります。 これは、Progress Kemp から入手するか、Get License リンクを使用して入手できます。 詳細と手順については、ライセンス機能の説明を参照してください。 ライセンスを更新した後は、再起動することをお勧めします。 ESP ライセンスにアップグレードする場合は、更新後に再起動が必要です。

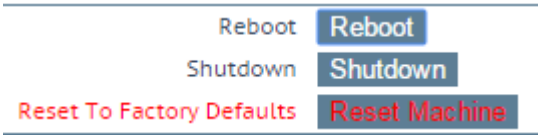
11.4.2.3 デバッグ チェック

ライセンスを取得しようとして問題がある場合は、いくつかのチェックが自動的に実行され、結果と関連するエラー メッセージが表示されます。

これらのチェックは、次のタスクを実行します。

- Ping Default Gateway
- Ping DNS Servers
- Ping Licensing Server

14.4.2.4 システムの再起動

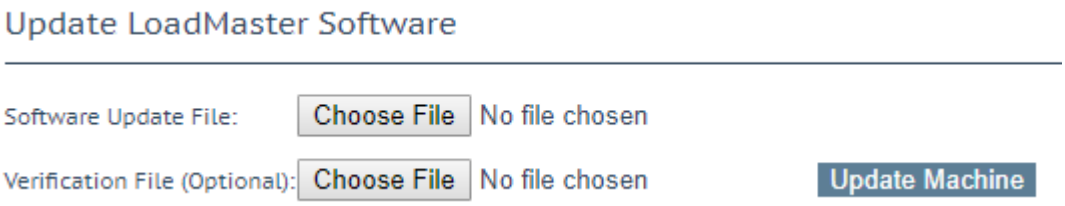


Reboot
アプライアンスを再起動します。

Shutdown
このボタンをクリックすると、LoadMaster の電源をオフにしようとします。 何らかの理由で電源切断に失敗した場合、少なくとも CPU が停止します。

Reset Machine
ライセンス、ユーザー名、およびパスワード情報を除いて、アプライアンスの構成をリセットします。これは、HA ペアのアクティブなアプライアンスにのみ適用されます。

11.4.4 ソフトウェアの更新



Progress Kemp Downloads ページからファームウェア パッチをダウンロードできます。[Verification File] フィールドは、[System Configuration] > [Miscellaneous Options] > [WUI Settings] で [Update Verification Options] フィールドが [Required] または [Optional] に設定されている場合に表示されます (デフォルトでは [Required] に設定されています)。 デフォルトでは、パッチまたはアドオンの整合性はインストール時に検証されます。 これは、セカンダリ XML 検証ファイルを使用せずに行われます。 更新検証オプションを必須またはオプションに設定すると、パッチまたはアドオンをアップロードすると同時に、セカンダリ XML 検証ファイルを使用してアップ

ロードできます。これにより、更新ファイルの署名に使用されたデジタル署名を検証できます。 記録。 XML ファイルに対してパッチを検証できない場合、パッチ/アドオンはインストールされません。

LoadMaster をバージョン 7.2.51 以降にアップグレードし、検証が必要に設定されている場合は、このリリースで提供される 2 つの XML 検証ファイルのいずれかを提供する必要があります。

- 7.2.<リリース/ビルド番号>.RELEASE.PATCH-64-MULTICORE-preV7.2.51.0.checksum.xml: LMOS 7.2.51 より前のリリースを実行している LoadMaster にアップグレードするときに、このファイルを使用します。
- 7.2.<リリース/ビルド番号>.RELEASE.PATCH-64 MULTICORE.checksum.xml: すでに 7.2.51.0 以降を実行している LoadMaster へのアップグレードを繰り返し、アップグレード プロセスを繰り返したい場合は、このファイルを使用します。

Update Verification Options ドロップダウン リストが Required に設定されている場合、LoadMaster ファームウェア 7.2.51 以降にアップグレードすることはできません。 また、7.2.51 からそれ以前のバージョンにダウングレードすることもできません。 これを回避するには、指定したバージョン間でダウングレードまたはアップグレードする前に、[Update Verification Options] フィールドを [Optional] または [No Verification File - deprecated] に設定します。 マシンの更新 ファームウェアをダウンロードしたら、ファイルを参照してファームウェアをロードマスターに直接アップロードできます。 ファームウェアが展開され、LoadMaster で検証されます。 パッチが正常に検証されると、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、アプライアンスを再起動する必要があります。 この再起動は、必要に応じて延期できます。

Update Machine

ファームウェアをダウンロードしたら、ファイルを参照してファームウェアをロードマスターに直接アップロードできます。 ファームウェアが展開され、LoadMaster で検証されます。 パッチが正常に検証されると、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、アプライアンスを再起動する必要があります。 この再起動は、必要に応じて延期できます。

Update Cluster

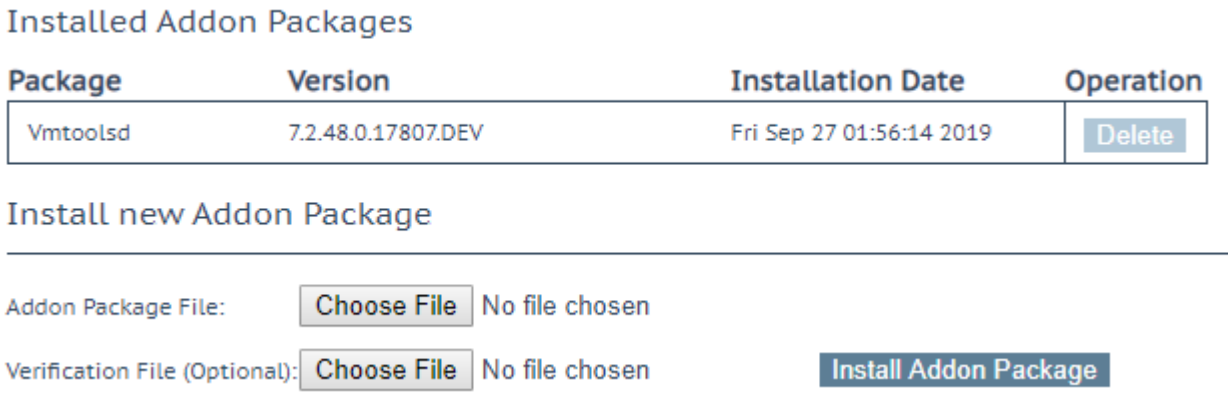
Update Cluster オプションは、クラスタリング ライセンスを持つ LoadMaster でのみ使用できます。 ライセンスにクラスタリング機能を追加するには、Progress Kemp の担当者にお問い合わせください。 クラスタリングの詳細については、LoadMaster クラスタリング機能の説明を参照してください。

クラスター内のすべてのロードマスターのファームウェアは、[Update Cluster] ボタンをクリックすることで、共有 IP アドレスを使用して更新できます。 クラスター全体のソフトウェア更新を実行する手順については、LoadMaster クラスタリング機能の説明を参照してください。

Restore Software

LoadMaster ファームウェアの更新が完了している場合は、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



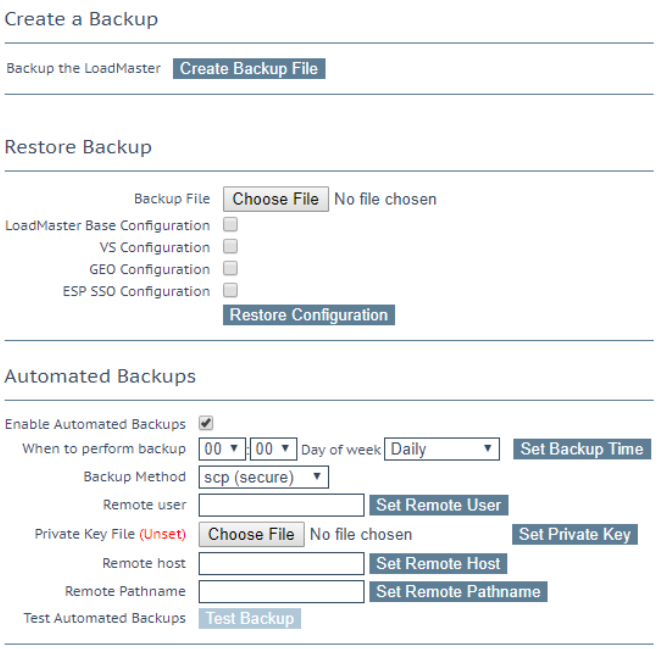
アドオン パッケージは Kemp LoadMaster にインストールできます。 アドオン パッケージは、LoadMaster に既に含まれている機能に追加される機能を提供します。 今後、Progress Kemp は追加のアドオン パッケージを作成する予定です。 アドオン パッケージは、Kemp の Web サイト (www.kemptechnologies.com) からダウンロードできます。

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、ファイルを参照して選択し、[Install Addon Package] をクリックします。 アドオン パッケージを完全にインストールするには、再起動が必要です。 同名のアドオンパッケージがアップロードされた場合、既存のものは上書き/更新されます。

[System Configuration] > [Miscellaneous Options] > [WUI Settings] で [Display Verify Update Option] が選択されている場合、[Verification File] フィールドが表示されます (これはデフォルトで有効になっています)。 デフォルトでは、パッチまたはアドオンの整合性はインストール時に検証されます。 これは、セカンダリ XML 検証ファイルを使用せずに行われます。 Display Verify Update Option を有効にすると、セカンダリ XML 検証ファイルをオプションで同時にアップロード

できます。 XML ファイルに対してパッチを検証できない場合、パッチ/アドオンはインストールされません。 インストールされたアドオン パッケージを開始できない場合、テキストは赤で表示され、ホバー テキストはパッケージを開始できなかったことを示します。

11.4.5 バックアップ/リストア



Create Backup File

仮想サービス構成、ローカル アプライアンス情報、および統計データ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。 識別しやすいように、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 は取得したバックアップに Netstat 出力を含めます。 これが含まれていると、バックアップの完了に時間がかかります。 [Troubleshooting] 画面 ([System Configuration] > [Troubleshooting]) で [バックアップに Netstat を含める] オプションを無効にすることで、Netstat 出力が含まれないようにすることができます。

Restore Backup

(リモート マシンから) 復元を実行する場合、ユーザーは復元する情報を選択できます。

- VS Configuration
- LoadMaster Base Configuration
- GEO Configuration

- ESP SSO 構成 (これにより、SSO ドメイン、LDAP エンドポイント、および SSO カスタム イメージ セットが復元されます。これにより、仮想サービスの設定は復元されません。それらを復元するには、VS 構成オプションを使用します。)
- オプションの組み合わせ

単一のマシン構成を HA マシンに復元したり、HA 構成を単一のマシンに復元したりすることはできません。ESP が有効になっていないマシンに、ESP が有効な仮想サービスの構成を復元することはできません。 WAF 構成は、WAF ライセンスを持つ LoadMaster にのみ復元できます。

Automated Backups

[Enable Automated Backups] チェック ボックスが選択されている場合は、自動バックアップを毎日または毎週実行するようにシステムを構成できます。 識別しやすいように、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。 自動バックアップが正しい時間に実行されていない場合は、NTP 設定が正しく構成されていることを確認してください。 詳細については、日付/時刻セクションを参照してください。

When to perform backup

バックアップの時刻 (24 時間制) を指定します。 また、毎日バックアップするか、特定の曜日にバックアップするかを選択します。 準備ができたら、[Set Backup Time] ボタンをクリックします。

状況によっては、誤ったエラー メッセージが表示されることがあります。
次のようなシステム ログに記録されます。
12 月 8 日 12:27:01 Kemp_1 /usr/sbin/cron[2065]: (システム) リロード (/etc/crontab)
12 月 8 日 12:27:01 Kemp_1 /usr/sbin/cron[2065]: (CRON) 悪い時間 (/etc/crontab)
これらは安全に無視でき、自動バックアップは正常に完了する可能性があります。

Backup Method

自動バックアップのファイル転送方法を選択します。

- Ftp (insecure)
- scp (secure)
- sftp (secure)

scp または sftp を使用する場合は、秘密鍵 (Private Key)ファイルを指定する必要があります

Remote user

リモート ホストへのアクセスに必要なユーザー名を設定します。

Private Key File

scp をバックアップ方法として使用する場合は、秘密鍵ファイルを提供する必要があります。 これは、リモート scp サーバーで ssh-keygen を使用して生成された SSH 秘密鍵です。

Remote password

リモート パスワードは、バックアップ方法が Ftp (安全でない) に設定されている場合に使用されます。 リモートホストへのアクセスに必要なパスワードを設定します。 このフィールドは、英数字と英数字以外のほとんどの文字を受け入れます。 使用できない文字は次のとおりです。

- 制御文字
- ' (アポストロフィ)
- ` (墓)
- 削除文字

Remote host

バックアップ アーカイブを送信するリモート ホストの IP アドレスまたはホスト名を設定します。オプションでコロンとポート番号を続けます。 ポートが指定されていない場合は、選択したプロトコルのデフォルト ポートが使用されます。

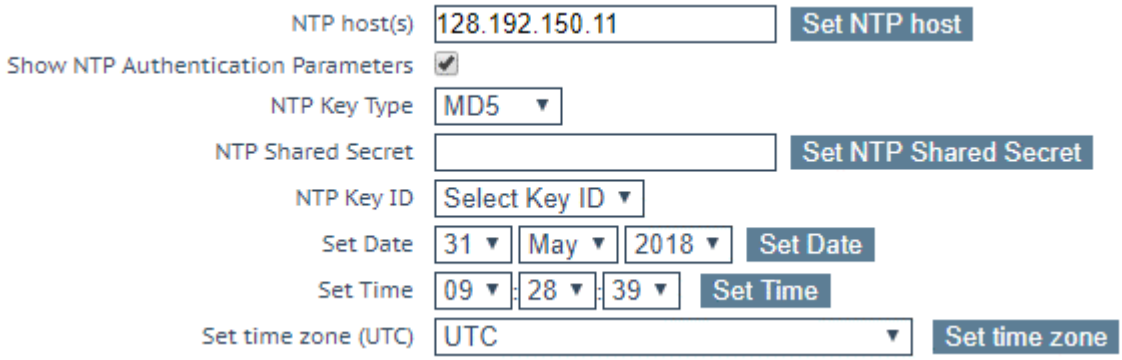
Remote Pathname

ファイルを保存するリモート ホスト上の場所を設定します。

Test Automated Backups

[Test Backup] ボタンをクリックすると、自動バックアップ構成が正しく機能しているかどうかを確認するための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 ファイル内で表示できます。

11.4.6 日付時刻



LoadMaster の日付と時刻を手動で設定するか、NTP サーバーを利用することができます。

NTP host(s)

NTP サーバーとして使用するホストを指定します。 HA クラスターでは、NTP が強く推奨されるオプションです。 単体の場合は、ユーザーの裁量に任されています。 [Set NTP Host] ボタンをクリックすると、構成された詳細に基づいて時刻が更新されます。 ローカル NTP サーバーがない場合は、www.pool.ntp.org で、使用できるパブリック NTP サーバー プールのリスト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

LoadMaster は、暗号署名を使用して安全な NTP サーバーに問い合わせる NTPv4 をサポートしています。 これは、共有シークレットとキーを使用してサーバーからの応答が実際に有効であることを検証する単純な承認スキームを使用します。 [Show NTP Authentication Parameters] チェック ボックスをオンにして、NTP 認証要求をサポートするために必要なパラメーターを表示します。
[Disable NTP Authentication] チェックボックスをオンにしていずれかのパラメータを変更すると、チェック ボックスの名前が Disable NTP Authentication [] に変わります。

NTPv4 機能が動作するには、ファイルが
サーバー (/etc/ntp.keys) の形式は次のとおりです。
<keyid> M <秘密の文字列>
...
<keyid> M <秘密の文字列>

キーの使用を有効にするには、/etc/ntp.conf の trustedkey 行にキー ID を指定します。たとえば、キー ID が 5 の場合、「trustedkey5」を指定する必要があります。 trustedkey 値は、trustedkey 1 2 3 4 5 9 10 など、複数の値を取ることができます。

NTP Key Type

[Show NTP Authentication Parameters] チェック ボックスをオンにして、[NTP Key Type] ドロップダウン リストを表示します。 MD5、SHA-1、または従来の SHA NTP キー タイプのいずれかを選択します。 MD5 がデフォルト値です。

NTP Shared Secret

NTP 共有秘密文字列。 NTP シークレットは、最大 20 文字の ASCII 文字または 40 文字の 16 進文字にすることができます。

NTP Key ID

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

Set Date

LoadMaster で日付を設定します。

Set Time

LoadMaster で時刻を設定します。

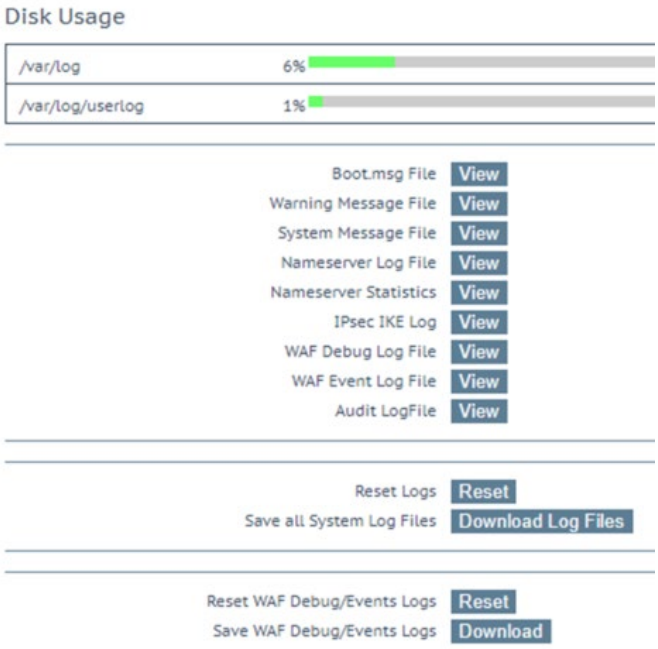
Set time zone

LoadMaster が設置されている場所のタイム ゾーンを設定します。

11.5 ロギング オプション

LoadMaster イベントのログは、プッシュすることも、アプライアンスからプルすることもできます。 LoadMaster のログ ファイルは履歴ではないことに注意してください。アプライアンスを再起動すると、ログはリセットされます。 リモート施設の LoadMaster で生成されたイベントの記録を保持することが重要です。

11.5.1 システム ログ ファイル



Disk Usage - このセクションは、ログ パーティションの使用率/空き率を示します。 色分けは、さまざまな使用レベルを強調するために使用されます。

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

Boot.msg File - LoadMaster の初回起動時の現在のバージョンなどの情報が含まれています。

Warning Message file - LoadMaster の操作中にログに記録された警告が含まれています。

System Message File - LoadMaster の操作中に記録されたシステム イベントが含まれます。 これには、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含まれます。

Nameserver Log File - DNS ネーム サーバーのログを表示します。

Nameserver Statistics - 最新のネームサーバー統計を表示します。

IPsec IKE Log - IPsec IKE ログを表示します。

VPN 管理の場合、[IPsec IKE Log] ボタンは表示されません。

[System Configuration] > [Network Setup] > [Manage VPN] で構成されていません。

WAF Debug Log File - WAF の問題のデバッグに役立つデバッグ トレースが含まれています。 Kemp テクニカル サポートから要求された場合にのみ、このオプションを有効にしてください。

WAF デバッグ ログがない場合、[WAF Debug Log File] ボタンは表示されません。

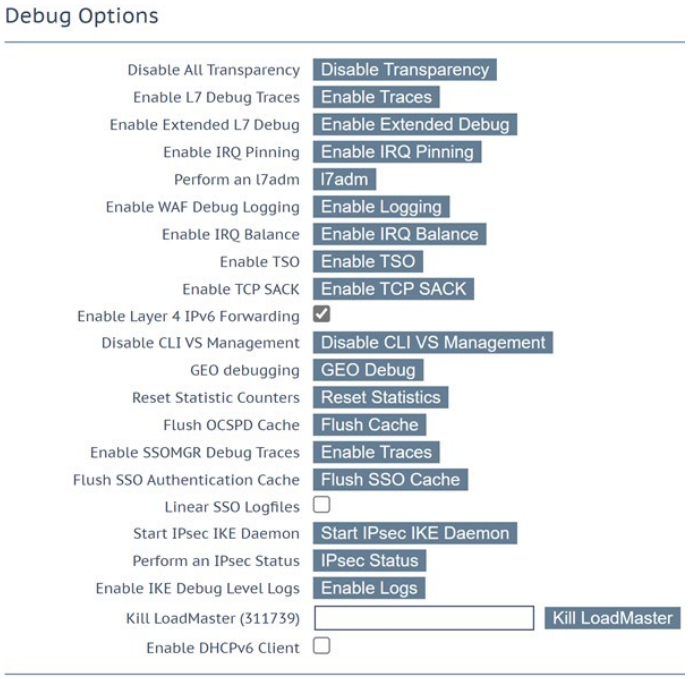
WAF Event Log File - 最近トリガーされた WAF ルールのログが含まれます。

WAF イベント ログがない場合、[WAF Event Log File] ボタンは表示されません。

Audit LogFile - ユーザーが実行した各アクションのログが含まれます。 API または WUI を使用します。 これは、セッション管理が有効になっている場合にのみ機能します。 セッション管理の詳細については、「Manage WUI Access」セクションを参照してください。
Clear Logs - 警告とシステム メッセージのログファイルをクリアします。 [Clear All] をクリックしてすべてのシステム ログ ファイルをクリアするか、矢印をクリックして特定のログ ファイルを選択してクリアすることができます。
Save Logs - サポート作業の一環として Kemp サポートにログを送信する必要がある場合は、このオプションを使用できます。 [Save All] をクリックして、すべてのシステム ログ ファイルをコンピュータに保存し、Kemp サポートに転送します。 矢印をクリックして、保存する特定のログ ファイルを選択します。
logrotate については、https://linux.die.net/man/8/logrotate を参照してください。 または、Linux マシンで man logrotate を実行します。 LoadMaster の logrotate 構成と照合するには、/etc/logrotate.d/ の構成ファイル、特に syslog と userlogs を調べます。

11.5.1.1 デバッグ オプション

LoadMaster には、ユーザーと Kemp サポート スタッフが接続の問題を診断するのに役立つさまざまな機能があります。 [Debug Options] をクリックすると、次の画面が表示されます。



警告 – Kemp は、通常の操作中にデバッグ コマンドを使用することをお勧めしません。 理想的には、Kemp サポート技術者の推奨事項と組み合わせてのみ使用する必要があります。
注: デバッグ コマンドは LoadMaster のパフォーマンスに影響を与え、実行中にシステムを追加のセキュリティ脆弱性にさらす可能性があります。

Disable All Transparency

すべての仮想サービスで透過性を無効にし、強制的にレイヤー 7 を使用します。注意して使用してください。

このオプションはデバッグ専用であり、仮想サービスごとに透過性を有効または無効にする通常のコントロールを置き換えるものではありません。 このオプションを使用して透過性を無効にすると、透過性を無効にする前に構成ファイルのコピーが保存されます。 いつ
透過性がオンに戻ると (変更前にすべての仮想サービスで透過性がオンになっているわけではありません)、元の構成が復元されます。 したがって、この期間中の構成への変更はすべて失われます。 これには、新しい仮想サービスの作成が含まれます。

Enable L7 Debug Traces

このオプションは、すべてのレイヤー 7 (L7) 接続でのデバッグを有効にします。 メッセージ ファイルでログ トラフィックを生成します。 多数のファイルがログに記録されるため、L7 処理が遅くなり

ます。

このオプションを有効にすると、より多くのリソースが消費される可能性があり、一部の認証パラメーターが公開される可能性があります。 Kemp サポートが推奨する場合にのみ、このオプションを有効にしてください。

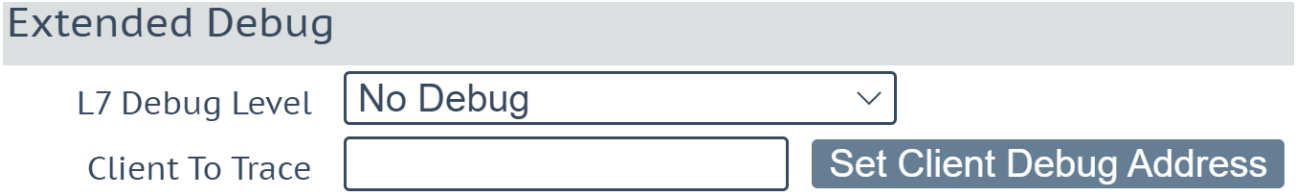
Enable Extended L7 Debug

[Enable Extended Debug] をクリックして、L7 拡張デバッグ オプションを有効にします。 LoadMaster ファームウェア バージョン 7.2.53 では、[Enable Extended L7 Debug] オプションが強化されました。 広範なテストを実行する場合は、このオプションを有効にする必要がある場合があります。 Enable Extended L7 Debug オプションを有効にすると、Process Debug ボタンが表示されます。 [Process Debug] をクリックすると、プロセスのリストとデバッグ レベルが表示されます。

ユーザーは、ログを外部に提供する前にサニタイズする必要があります。 ログは、デバッグ目的でのみ有効 (デバッグ レベルを 1 に設定) にし、その直後に無効 (デバッグ レベルを 0 に設定) にする必要があります。 デバッグが完了したら、できるだけ早く LoadMaster からログを削除する必要があります。

拡張 L7 デバッグ オプションを有効にすると、より多くのリソースを消費する可能性があり、一部の認証パラメーターが公開される可能性があります。 Progress Kemp サポートが推奨する場合にのみ、このオプションを有効にしてください。

拡張デバッグを有効にすると、すべての VS の仮想サービス変更画面 ([Virtual Service] > [View/Modify Service] > [MOdify]) で追加の拡張デバッグ構成セクションが使用可能になります。 Sub-Virtual Services (SubVS) を使用する場合、Extended Debug 設定も SubVS に継承されるため、 1 つの呼び出しを完全にログに記録できます。 必要に応じて、単一の SubVS でデバッグを有効にすることもできます。さらに、クライアント IP アドレスを指定してログを制限するオプションもあります。 この機能に関連するすべてのログは、システム メッセージ ファイル messages.txt に記録されます。



このセクションで設定できるフィールドは 2 つあります。

- L7 Debug Level: この仮想サービスの Layer7 デバッグのレベルを設定します。 可能な値は次のとおりです。
  - No Debug
  - Call Tracing
  - Full Debug
  - Full Debug + HTTP Headers

  Call Tracing は、最も関連性の高い操作を表示する基本レベルのログであり、Full Debug は、使用可能なすべてのデバッグ ログを表示します。これは、Enable L7 Debug Traces のグローバル設定と同じですが、VS ごとのレベルです。

デフォルトでは、L7 Debug Level は、すべての仮想サービスとサブ VS に対して [No Debug] に設定されています。 のログを有効にするには

特定の仮想サービスまたはサブ VS を変更するには、[Virtual Service or SubVS Modify] 画面の [Extended Debug] セクションで、L7 デバッグ レベルを [Call Tracing] または [Full Debug] に設定する必要があります。 L7 デバッグ レベルを Full Debug + HTTP ヘッダーに設定すると、機密情報が公開される可能性があります。

- トレースするクライアント: クライアントの IP アドレスを指定することで、デバッグ情報をさらに制限することもできます (IPv4 または IPv6 アドレスを指定できます)。 アドレスが指定されている場合、その特定のクライアント IP からの接続のみが記録/トレースされます。 これにより、単一アドレスからのデバッグ機能が可能になります。

Enable IRQ Pinning

ボタンをクリックして、割り込み要求ライン (IRQ) ピンニングを有効にします。 これはデフォルトで無効になっています。

このオプションは、Kemp サポートと相談してのみ有効にしてください。 IRQ ピンニング オプションをオフからオンに変更すると、IP アドレスが割り当てられているすべてのネットワーク インターフェイスで IRQ ピンニングが有効になります。 IRQ ピニングが有効で、IP アドレスを未構成のインターフェースに追加すると、IRQ ピニングをオフにして再度オンに切り替えるか、システムを再起動するまで、そのインターフェースでは IRQ ピニングが有効になりません。

Perform an l7adm

L7 サブシステムに関する生の統計を表示します。

Enable WAF Debug Logging

ロギングを有効にして、ウェブ アプリケーション ファイアウォールによって分析されるトラフィックに関する詳細情報を取得できます。 ログに含まれる情報には、LoadMaster WAF が LoadMaster リソースからリクエストを受信した時刻、リクエストに関する詳細情報、および各リクエストが一致したルールのアクションが含まれます。
WAF デバッグ トレースを有効にします。

このオプションを有効にすると、一般データ保護協定 (EU GDPR) で定義されているように、個人を特定できる情報を含む可能性があるログが生成されることに注意してください。 ログ内のデータの匿名化、削除、暗号化など、組織のベスト プラクティスに従ってこの情報を保護する必要があります。
これにより、大量のログ トラフィックが生成されます。 また、WAF 処理も遅くなります。
Progress Kemp テクニカル サポートから要求された場合にのみ、このオプションを有効にしてください。 Progress Kemp は、実稼働環境でこのオプションを有効にすることをお勧めしません。

WAF デバッグ ログは閉じられず、大きくなりすぎるとローテーションされます。 デバッグ ログを再度有効にするには、WAF が有効なすべての仮想サービス設定で 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、仮想サービスに関連するルールを使用して、ルールの更新を実行します。

Enable IRQ Balance

このオプションは、Kemp のサポート スタッフに相談した後にのみ有効にしてください。

Enable TSO

TCP セグメンテーション オフロード (TSO) を有効にします。

このオプションは、Kemp テクニカル サポートに相談した後にのみ変更してください。 このオプションへの変更は、再起動後にのみ有効になります。

Enable TCP SACK

このボタンをクリックして、TCP SACK (Selective ACKnowledgement) 処理を有効にします。 これは、すべてのレイヤー 7 仮想サービスに影響するグローバル設定です。 仮想サービス クライアントと LoadMaster で TCP SACK が有効になっている場合にのみ機能します。

Enable Layer 4 IPv6 Forwarding

このオプションを有効にすると (デフォルト)、LoadMaster オペレーティング システム (LMOS) 7.2.50 より前のバージョンの LoadMaster でサポートされている IPv6 転送動作がサポートされます。 このオプションを無効にすると、IPv6 標準で必要な IPv6 転送動作がサポートされます。 展開で IPv6 標準に準拠した IPv6 転送動作が必要な場合は、このオプションを無効にする必要があります。

Enable/Disable CLI VS Management

コマンド ライン インターフェイス (CLI) サービス管理機能を有効または無効にします。

GEO Debugging

GEO Debug をクリックすると、GEO Debug ページが表示されます。 GEO デバッグ ページには、GEO 構成関連の情報とさまざまな GEO デバッグ オプションが表示されます。 GEO デバッグの詳細については、「GEO Debug」セクションを参照してください。

Display RAID Information

[RAID 情報を表示] および [Display RAID Disk] ボタンは、ロードマスターに RAID コントローラがインストールされている場合にのみ表示されます。

Redundant Array of Independent Disks (RAID) コントローラの詳細を表示します。 いくつかの例の情報を以下に示します。

```
Controller details
------------------------------------------------------------------
- Chip ID.....: 10
- Parent Controller Index: 255
```

- OS Physical Name.....: /dev/sda
- Serial Number.....: 427491329
- AES Power on State.....: 0
- Sata Ports.....: 2

Raid Port 0 details

- Raid Model Name.....: H/W RAID1
- Raid Serial Number.....: OUEYEXCXTQ53GE1BSOSN
- EZBackup Disk Support.....: 0
- Port Multiplier port.....: 0
- Raid Capacity.....: 953 (29 GB)
- Raid Capacity low word.....: 0
- Raid State.....: 1 (Active)
- Raid Status.....: 3 (Normal)
- Raid Level.....: 1 (Raid 1 (mirror))
- Mark Type.....: 0
- Active Member.....: 15
- Active Level.....: 0
- Rebuild Priority.....: 3
- Standby Timer.....: 0
- Total members in the RAID....: 2

Member disk 0

- Ready.....: 1
- Lba 48 Bit Support.....: 1
- SATA Page.....: 0
- SATA Port.....: 0
- SATA Base.....: 0
- SATA Size.....: 953

Member disk 1

- Ready.....: 1
- Lba 48 Bit Support.....: 1
- SATA Page.....: 0
- SATA Port.....: 1
- SATA Base.....: 0
- SATA Size.....: 953

Display RAID Disks Information

RAID ディスクに関する詳細を表示します。 いくつかの例の情報を以下に示します。

Sata Port 0 details

- Disk Model Name.....: 32GB SATA Flash Drive
- Disk Serial Number.....: C0122916B01000000074
- Disk Firmware Version.....: SFDC001D
- EZBackup Disk Support.....: 1
- Port Multiplier port.....: 15
- Disk Capacity.....: 954 (29 GB)
- Port Type.....: 2 (RAID)
- Port Speed.....: 2 (GB)
- Page 0 State.....: 2
- Page 0 Raid Index.....: 0
- Page 0 Member Index.....: 0
- Page 0 Raid Name.....:
- Page 0 Raid Serial Number....:
- Page 0 Raid Segment Base.....: 0
- Page 0 Raid Size.....: 953
- Page 0 Raid EZ Backup Support: 0
- Page 1 State.....: 0
- Page 1 Raid Index.....: 0
- Page 1 MemberIndex.....: 0

- Page 1 Raid Name.....:
- Page 1 Raid Serial Number....:
- Page 1 Raid Segment Base.....: 0
- Page 1 Raid Size.....: 0
- Page 1 Raid EZ Backup Support: 0
- PortErrorStatus.....: 0

Sata Port 1 details

- Disk Model Name.....: 32GB SATA Flash Drive
- Disk Serial Number.....: E011321290100000005A
- Disk Firmware Version.....: SFDC001D
- EZBackup Disk Support.....: 1
- Port Multiplier port.....: 15
- Disk Capacity.....: 954 (29 GB)
- Port Type.....: 2 (RAID)
- Port Speed.....: 2 (GB)
- Page 0 State.....: 2
- Page 0 Raid Index.....: 0
- Page 0 Member Index.....: 1
- Page 0 Raid Name.....:
- Page 0 Raid Serial Number....:
- Page 0 Raid Segment Base.....: 0
- Page 0 Raid Size.....: 953
- Page 0 Raid EZ Backup Support: 0
- Page 1 State.....: 0
- Page 1 Raid Index.....: 0
- Page 1 MemberIndex.....: 0
- Page 1 Raid Name.....:
- Page 1 Raid Serial Number....:
- Page 1 Raid Segment Base.....: 0

- Page 1 Raid Size.....: 0
- Page 1 Raid EZ Backup Support: 0
- PortErrorStatus.....: 0

Reset Statistic Counters

すべての統計カウンターをゼロにリセットし、古いグラフを削除します。 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、これらのファイルは必要に応じて自動的に再作成されます。

Flush OCSPD Cache

OCSP を使用してクライアント証明書を検証する場合、OCSPD は OCSP サーバーから取得した応答をキャッシュします。 このキャッシュは、このボタンを押すことでフラッシュできます。 OCSPD キャッシュのフラッシュは、テスト時、または証明書失効リスト (CRL) が更新されたときに役立ちます。

Stop IPsec IKE Daemon

LoadMaster で 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ダウンします。

Perform an IPsec Status

生の IPsec ステータス出力を表示します。

Enable IKE Debug Level Logs

IPsec IKE ログ レベルを制御します。

Flush SSO Authentication Cache

[Flush SSO Cache] ボタンをクリックすると、すべてのシングル サインオン (SSO) レコードがフラッシュされ、すべての認証サーバー ステータスがリセットされ、KCD ドメインがリセットされ (該当する場合)、構成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 に接続す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 サーバーのタイムアウト値を秒単位で設定します (デフォルト値は 5 秒です)。

Linear SSO Logfiles

デフォルトでは、ファイルシステムがいっぱいにならないように、古いログ ファイルが削除されて新しいログ ファイル用のスペースが確保されます。 Linear SSO Logfiles チェックボックスを選択すると、古いファイルが削除されなくなります。

リニア SSO ロギングを使用している場合、ログ ファイルが定期的に削除されず、ファイル システムがいっぱいになると、ESP 対応の仮想サービスへのアクセスがブロックされ、仮想サービスへのログなしのアクセスが防止されます。 非 ESP 対応の仮想サービスへのアクセスは、リニア SSO ログファイル機能の影響を受けません。

Kill LoadMaster

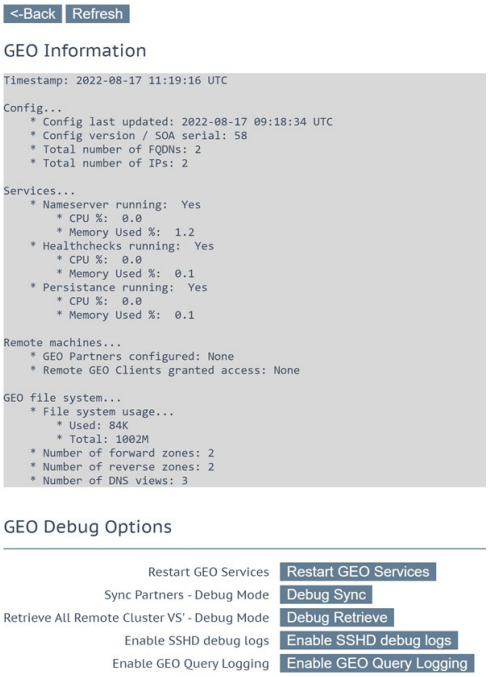
LoadMaster のすべての機能を永久に無効にします。 LoadMaster は、ライセンスを再取得することで再度有効にすることができます。

Progress Kemp テクニカル サポートに相談せずに LoadMaster を強制終了しないでください。 Kill LoadMaster オプションは、Kemp マルチテナント LoadMaster のテナントである LoadMaster では使用できません。

Enable DHCPv6 Client

このオプションを有効にすると、DHCPv6 クライアントがプライマリ インターフェイスで実行されます。 これにより、起動時に IPv6 アドレスを取得する機能が提供されます。 ブートごとに DHCPv6 を実行する場合は、このオプションを有効のままにします。 ただし、これは長時間実行されるプロセスであり、有効にするとバックグラウンドで実行され続けるため、IPv6 アドレスのみを割り当てる必要があり、IPv6 アドレスを更新して解放する必要がない場合は、IPv6 の後でこのオプションを無効にする必要があります。 アドレスが割り当てられます。

11.5.1.2 GEO デバッグ



GEO Information

このセクションには、次のような GEO システムの状態に関する情報が表示されます。

- Config: 最終更新日 (YYYY-MM-DD 形式) と時刻、バージョン、および FQDN と IP アドレスの総数を表示します。
- Service: ネームサーバー、ヘルスチェック、永続性の詳細を表示します
- Remote Machine: 構成された GEO パートナーとリモート GEO クライアントに関する詳細を表示します。
- GEO File System: 順方向ゾーンの数、逆方向ゾーンの数、および DNS ビューの詳細の数を含む、GEO ファイル システムに関する詳細を表示します。

[Refresh] ボタンをクリックすると、[GEO Information] セクションに表示されるデータが更新されます。

GEO Debug Options

Restart GEO Services

[Restart GEO Service] をクリックすると、ネームサーバー、ヘルス チェック、スティッキネス サービスが再起動します。

Sync Partners - Debug Mode

[Debug Sync] をクリックすると、GEO 構成が構成済みのパートナーにプッシュされ、接続のデバッグ情報がメッセージ ログに記録されます。

Retrieve All Remote Cluster VS' - Debug Mode

[Debug Retrieve] をクリックすると、設定されたすべての LoadMaster クラスタからリモート仮想サービス データが取得され、接続のデバッグ情報がメッセージ ログに記録されます。

Enable SSHD debug logs

[Enable SSHD Debug Log] をクリックすると、SSHD デバッグ ログがリモート マシンからの着信接続をデバッグできるようになります。

Enable GEO Query Logging

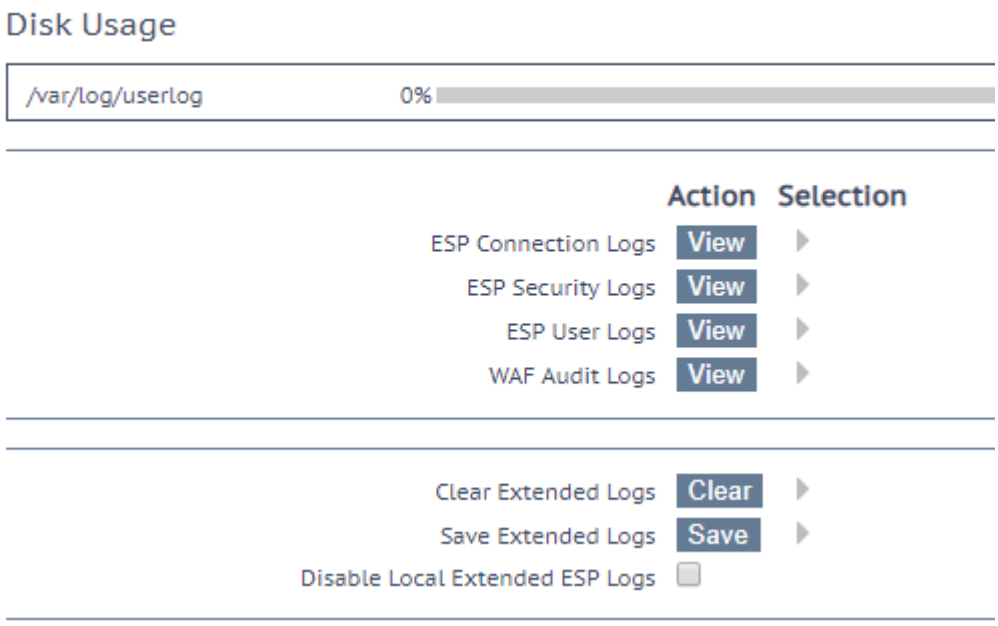
GEO のバインド デバッグ トレース ログを有効にします。

GEO Query Logging 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にのみ有効にする必要があります。

11.5.2 拡張ログ ファイル

[Extended Log Files] 画面には、ESP および WAF 機能に関連するログのオプションが表示されます。 拡張ログ ファイル画面にアクセスするには、LoadMaster WUI で、[System Configuration] > [Logging Options] > [Extended Log File] に移動します。

WAF ログはリアルタイムで生成されません。WAF エンジンが実際に処理しているものより最大 2 分遅れることがあります。



Disk Usage - このセクションは、ログ パーティションの使用率/空き率を示します。 色分けは、さまざまな使用レベルを強調するために使用されます。

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

LoadMaster には、ESP に関連する複数のログ ファイルが保存されています。 これらは、[Disk Usage] セクションの下に一覧表示されます。 これらのログは、LoadMaster の再起動後も保持されます。 [View] ボタンまたは [Save Action] ボタンの 1 つをデフォルトのフィルター オプションで選択して、さまざまなログ ファイル (接続ログ、セキュリティ ログなど) にアクションを適用できます。 [Clear] ボタンの場合、最初に [選択] コントロールを使用してクリアするログを選択する必要があります。 選択コントロールにアクセスするには、ボタンの右側にある右キャレット アイコンのいずれかをクリックします。 たとえば、[Clear] ボタンと [Save] ボタンの右側にあるアイコンをクリックすると、これらのコントロールが表示されます。

from コントロールと to コントロールを使用してログをフィルター処理し、日付でクリアまたは保存できます。また、右側の複数選択リストからログ ファイルのサブセットを選択することもできます。

- ESP Connection Log: 各接続を記録するログ。
- ESP Security Log: すべてのセキュリティ アラートを記録するログ。
- ESP User Log: すべてのユーザー ログインを記録するログ。

LoadMaster ファームウェア バージョン 7.2.51 では、ESP ユーザー ログが拡張され、大規模なログ インフラストラクチャを持つ企業のお客様にとってより便利で適切なものになりました。ユーザー認証、承認、およびアカウンティング (AAA) 情報は、要求の時間、ユーザー名、ドメイン、AAA サーバー、AAA プロトコル タイプ、AAA 結果、エラー メッセージなど、ログに含まれます。詳細については、Kemp ドキュメント ページの ESP ログ テクニカル ノートを参照してください。

LoadMaster ファームウェア バージョン 7.2.53 では、ESP クライアント セッションのログ記録がさらに強化されました。 LoadMaster のログ:

  - 最初に作成された ESP セッション
  - LoadMaster がセッションをキャッシュからクリアした時刻。キャッシュ全体がクリアされた場合、クリア時に 1 つのログ メッセージが記録されます。これは、その時点で存在していたすべてのセッションがキャッシュからクリアされたことを示しています。
  - ESP セッションが削除された場合 (ユーザーがアプリケーションからログアウトしたとき、セッションが期限切れになったとき、またはユーザーが無効な資格情報を入力したとき)。 LoadMaster がセッションをクリアした時刻も記録されます。
- WAF Audit Log: 仮想サービスの変更画面の [WAF Option] セクションの [Audit Mode] ドロップダウン リストで選択された内容に基づいて、WAF ログを記録します。 各ログ エントリに表示される番号は、仮想サービスの ID に対応しています。 仮想サービス ID を取得するには、まず API インターフェイスが有効になっていることを確認します ([証明書とセキュリティ] > [リモート アクセス] > [API インターフェイスを有効にする])。次に、Web ブラウザのアドレス バーに

https://<LoadMasterIPAddress>/access/listvs と入力します。 仮想サービスのインデックスを確認してください。 これは、監査ログ エントリの番号に対応する番号です。

ログを表示するには、関連するオプションを選択し、関連する [View] ボタンをクリックしてください。

一部のログは、さまざまな方法でフィルタリングできます。 ログ メッセージを日付でフィルタリングするには、開始フィールドと終了フィールドで関連する日付を選択し、[View] ボタンをクリックします。 ESP ログの日付を選択するときは、リストに次の日付を含めて、目的の日付のすべてのレコードを含めます (翌日のファイルには前の日付のログが含まれている可能性があるため)。

ファイル名のリストから関連するファイルを選択し、[View] をクリックすると、 1 つまたは複数のアーカイブ ログ ファイルを表示できます。 フィルター フィールドに単語または正規表現を入力して [表示] をクリックすると、ログ ファイルをフィルター処理できます。

LoadMaster WUI の正規表現で引用符を使用する場合、制限があります。 詳細については、「Limitations of Using Regular Expressions in the LoadMaster WUI」セクションを参照してください。

Clear Extended Logs

[クリア] をクリックすると、すべての拡張ログを削除できます。 特定の日付範囲でフィルタリングするか、ログ ファイル リストで 1 つ以上の個々のログ ファイルを選択するか、ログ ファイル リストで特定のログ タイプ (接続、セキュリティ、ユーザーなど) を選択して [Clear] をクリックすることにより、特定のログ ファイルを削除できます。 ボタン。 警告メッセージが表示されたら、[OK] をクリックします。

Save Extended Logs

矢印をクリックしてオプションを展開します。 ファイルの種類 (接続など) を選択するか、日付範囲を入力します。 [Save] をクリックすると、すべての拡張ログをファイルに保存できます。 これにより、ファイルがマシンに保存されます。 特定の日付範囲でフィルタリングするか、ログ ファイル リストで 1 つ以上の個別のログ ファイルを選択するか、ログ ファイル リストで特定のログ タイプ (接続、セキュリティ、ユーザーなど) を選択して [Save] をクリックすることにより、特定のログ ファイルを保存できます。

Disable Local Extended ESP Logs

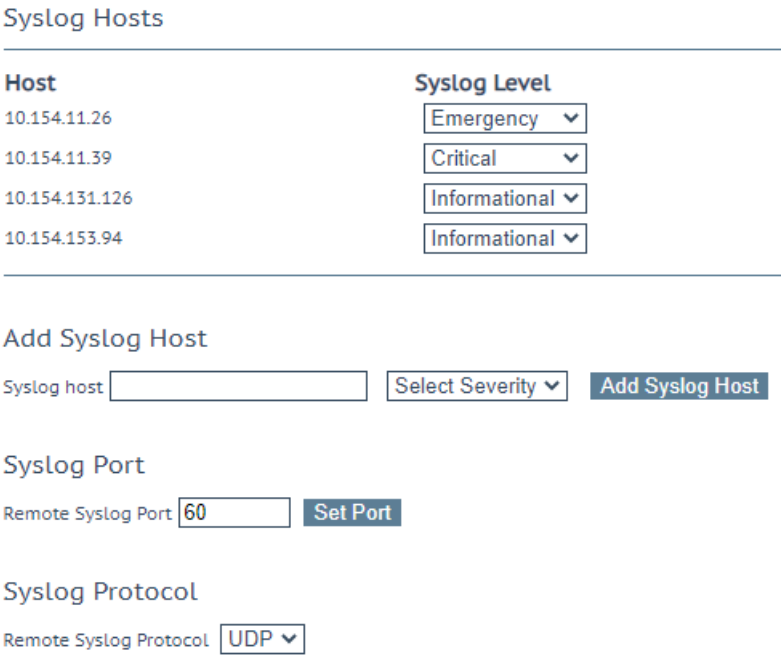
[Disable Local Extended ESP Logs] が無効になっている場合 (デフォルト オプション)、メッセー

ジは適切に拡張 ESP ログに書き込まれ、定義されているリモート syslog サーバーには送信されません。 [Disable Local Extended ESP Logs] が有効になっている場合、メッセージは拡張 ESP ログに書き込まれず、メッセージはリモート ロガー (定義されている場合) にのみ送信されます。 リモート ロガーが定義されていない場合、ログは記録されません。 以前のリリースのように、ローカルの拡張 ESP ログにデータを入力し、同じメッセージをリモート syslog サーバーに送信するようにシステムを構成することはできなくなりました。

Clear Temporary WAF Remote Log Data
一時的な WAF リモート ログ データをクリアします。
一時的な WAF リモート ログ データの保存
一時的な WAF リモートログデータを保存します。

11.5.3. シスログ オプション

LoadMaster は、syslog プロトコルを使用して、さまざまな警告およびエラー メッセージを生成できます。 Syslog メッセージには、すべてのメッセージに完全なタイムスタンプと LoadMaster ホスト名が含まれます。 syslog メッセージは RFC5424 に準拠しています。 これらのメッセージは通常、ローカルに保存されます。



また、[Syslog Host] テキスト ボックスに関連する IP アドレスを入力し、重大度を選択して [Add Syslog Host] をクリックすることにより、これらのエラー メッセージをリモート Syslog サーバー

に送信するように LoadMaster を構成することもできます。 Syslog メッセージは、TLS を使用してリモート サーバーに安全に送信されます。 LoadMaster は OCSP を使用して、構成された syslog サーバーによって提供されるサーバー証明書の有効性を確認します。 これらのチェックに失敗した場合、サーバーへの接続は許可されません。 ホスト エントリを削除するには、重大度レベルを [なし] に設定します。 6 つの異なるエラー メッセージ レベルが定義されており、各メッセージ レベルは異なるサーバーに送信される場合があります。 通知メッセージは情報提供のみを目的として送信されます。 緊急メッセージは、通常、即時のユーザー アクションを必要とします。

最大 10 個の個別の IP アドレスを指定できます。 以前の LoadMaster バージョンで 10 を超えるホストが構成されていた場合、アップグレード後、すべてのエントリが表示されますが、それ以上追加することはできません。

表示される可能性のあるメッセージのタイプの例を以下に示します。

- Emergency: カーネルクリティカルエラーメッセージ
- Critical: ユニット 1 に障害が発生し、ユニット 2 がアクティブとして引き継がれています (HA セットアップで)
- Error: 192.168.1.1 からの root の認証に失敗しました
- Warn: インターフェイスがアップ/ダウンしています
- Notice: 時刻が同期されました
- Information: ローカルの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されている場合、メッセージ ファイルには WARN より上のすべてのレベルからのメッセージが含まれますが、それより下のレベルのメッセージは含まれません。

同じホスト アドレスを再度入力すると、同じホストの古いエントリが置き換えられます。 1 つのエントリが、定義されている syslog レベルと、より優先度の高い他のすべてのレベルをカバーするため、同じホストに対して複数のエントリを持つ必要はありません。 そのため、必要な最低レベルの優先度を持つエントリを 1 つだけ含める必要があります。 [Remote Syslog Port] テキスト ボックスに入力し、[Set Port] をクリックして、syslog 転送用の非標準ポートを指定することもできます。

- Remote Syslog Port が構成されていない場合、ログはポート 514 の UDP で行われます。
- Remote Syslog Port が 601 として構成されている場合、ロギングはポート 601 の TCP で行われます。
- Remote Syslog Port が 601 以外のポートとして構成されている場合、ロギングはセキュアな TCP、つまり構成されたポートの SSL で行われます。

リモート Linux サーバーの syslog プロセスが LoadMaster から syslog メッセージを受信できるようにするには、syslog を「-r」フラグで開始する必要があります。 [Remote Syslog Protocol] ドロップダウン リストで適切なオプションを選択することにより、リモート syslog サーバーに接続するときに使用するプロトコルを指定できます。

Server Certificate Validation

このチェック ボックスは、TLS が Remote Syslog Protocol として選択されている場合にのみ表示されます。 サーバー証明書の検証が有効になっている場合、安全な接続を開始するために使用されたホスト名または IP アドレスが、証明書の証明書サブジェクトまたはサブジェクト代替名 (SAN) に存在することが保証されます。

サーバー証明書の検証はデフォルトで無効になっています。

11.5.4 SNMP オプション

[SNMP Option] 画面のフィールドは、SNMP V3 を有効にするかどうかによって異なります。 構成に応じたフィールドの詳細については、以下の関連セクションを参照してください。

11.5.4.1 SNMP オプション

このメニューでは、SNMP 構成を変更できます。

Enable SNMP

このチェック ボックスは、SNMP を有効または無効にします。 このオプションにより、LoadMaster は SNMP 要求に応答できます。 デフォルトでは、SNMP は無効になっています。

注意：SNMP を有効にすると、パフォーマンスが大幅に低下します。

この機能を有効にすると、次のトラップが生成されます。

- ColdStart: 汎用 (SNMP サブシステムの開始/停止)
- VsStateChange: (仮想サービスの状態変更)
- RsStateChange: (実サーバーの状態変化)
- HaStateChange: (HA 構成のみ: LoadMaster フェイルオーバー)

テンプレートを使用して作成された ESP 対応の仮想サービスの SNMP 監視を使用する場合は、マスター サービスに依存するのではなく、各 SubVS を直接監視するようにしてください。 これは、Authentication Proxy サブサービスが常にアップとマークされ、その結果、マスター サービスもアップとマークされるためです。

MIB file	Related Data
IPVS-MIB.txt	仮想サーバー統計
B100-MIB.txt	L7 LoadMaster の構成とステータス情報
ONE4NET-MIB.txt	エンタープライズ ID
CERTS-MIB.txt	SSL 証明書情報

これらの MIB (Kemp のドキュメント ページ - http://kemptechnologies.com/documentation にあります) を SNMP マネージャ マシンにインストールして、SNMP を使用して LoadMaster のパフォーマンス/構成データを要求できるようにする必要があります。 カウンタの説明は、LoadMaster MIB (記述節) から取得できます。 Linux では、MIB を読み取るだけでなく、次のコマンドを使用してこれを行うことができます。

snmptranslate -Td -OS <oid>
where <oid> is the object identifier in question.
For legacy reasons the Kemp object identifier is specified as **one4net**.
Example: <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
SYNTAXCounter32
MAX-ACCESSread-only

STATUScurrent
DESCRIPTION"この RS の合計接続数"
::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12) ipvsRSTable(2) rsEntry(1) 12 }

LoadMaster MIBS で定義されているデータ オブジェクトは、WUI によって表示されるカウンターのスーパーセットです。

LoadMaster のデータ オブジェクトは書き込み可能ではないため、GET 要求 (GET、GET-NEXT、GET-BULK など) のみを使用する必要があります。

CERTS-MIB.txt ファイルを使用して、ファイル名、証明書のサブジェクト名、証明書のシリアル番号、証明書の開始日、証明書の終了日、証明書の発行者情報などの SSL 証明書情報を取得できます。 SNMP は、この情報を最大 256 まで表示できます。
SSL 証明書。 SNMP を使用して、ディスク容量の使用状況の詳細を取得することもできます。

/var/log および /var/log/userlog パーティション情報が利用可能です。 データ パーティションに関しては、これらは Kemp OID の下ではなく、標準 OID の下にあります。 詳細は次のとおりです。

- ディスクがマウントされているパス: .1.3.6.1.4.1.2021.9.1.2.1
- パーティションのデバイスのパス: .1.3.6.1.4.1.2021.9.1.3.1
- ディスク/パーティションの合計サイズ (キロバイト): .1.3.6.1.4.1.2021.9.1.6.1
- ディスクの空き容量: .1.3.6.1.4.1.2021.9.1.7.1
- ディスクの使用容量: .1.3.6.1.4.1.2021.9.1.8.1
- ディスクで使用されている容量の割合: .1.3.6.1.4.1.2021.9.1.9.1
- ディスクで使用されている inode の割合: .1.3.6.1.4.1.2021.9.1.10.1

SNMP Clients

このオプションを使用すると、ロードマスターが応答する SNMP 管理ホストを指定できます。

クライアントが指定されていない場合、LoadMaster は任意のホストからの SNMP 管理要求に応答します。

[Enable SNMP V3] オプションが有効になっている場合、このオプションは使用できません。

SNMP Community String

このオプションを使用すると、SNMP コミュニティ ストリングを変更できます。 デフォルト値は「Public」です。 コミュニティ ストリングで使用できる文字は、a ～ z、A ～ Z、0 ～ 9、_.-@()?#%^+~! です。 [Enable SNMP V3] オプションが有効になっている場合、このオプションは使用できません。

Contact

このオプションを使用すると、SNMP 連絡先文字列を変更できます。 たとえば、これは LoadMaster の管理者の電子メール アドレスである可能性があります。

SNMP Location

このオプションを使用すると、SNMP ロケーション文字列を変更できます。

このフィールドは次の文字を受け入れます。

a-z A-Z 0-9 _ . - ; , = : { } @ ( ) ? # % ^ + ~ !

Location の最初の文字としてハッシュタグ記号 (#) を入力しないでください。

SNMP traps

[Enable SNMP Traps] を選択し、SNMP トラップ シンク テキスト ボックスに IP アドレスを指定すると、ロードマスター、仮想サービス、またはリアル サーバーに重要なイベントが発生したときにトラップが生成されます。 これらは SNMP トラップ シンクに送信されます。 変更が行われると、LoadMaster はすべての変更が完了するのを待ってから、それを読み取る前に 5 秒間待機します。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。 5 秒の待機中に状態の変化があった場合、状態の変化が処理され、待機が再開されます。

Enable/Disable SNMP Traps
このトグル オプションは、SNMP トラップの送信を有効または無効にします。
SNMP トラップはデフォルトで無効になっています。

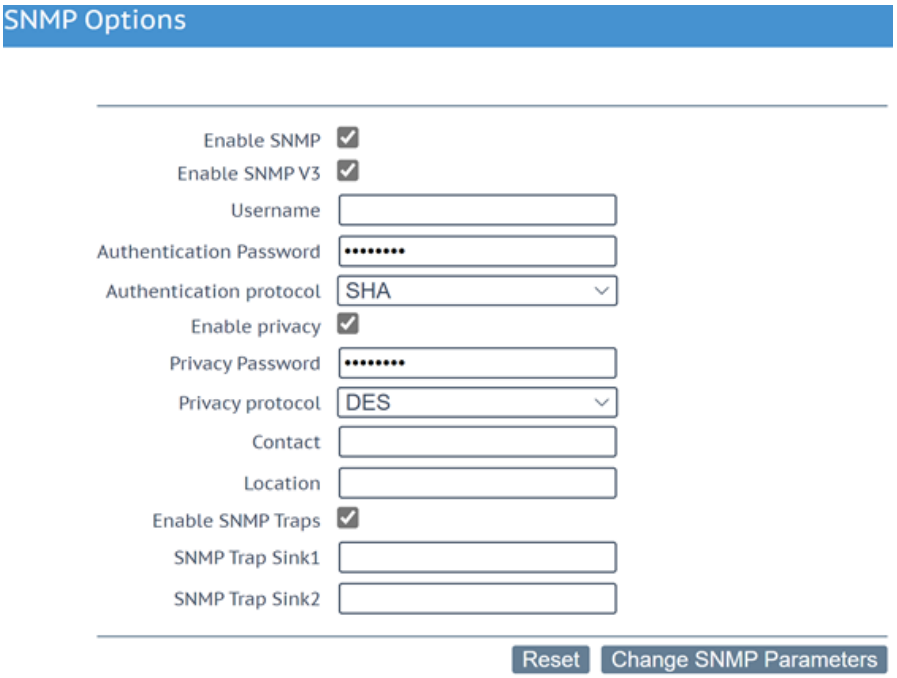
Send SNMP traps from the shared address
このチェック ボックスは、LoadMaster が HA モードの場合にのみ表示されます。
デフォルトでは、SNMP トラップは、アクティブな HA ユニットの IP アドレスを送信元 IP アドレスとして使用して送信されます。 このオプションを有効にすると、共有 IP アドレスを使用してアクティブな HA ユニットから SNMP トラップが送信されます。

SNMP Trap Sink1
このオプションを使用すると、ユーザーは、トラップが生成されたときに SNMPv1 トラップが送信されるホストのリストを指定できます。

SNMP Trap Sink2
このオプションを使用すると、ユーザーは、トラップが生成されたときに SNMPv2 トラップが送信されるホストのリストを指定できます。

11.5.4.2 SNMP V3 オプション

このメニューでは、SNMP V3 構成を変更できます。



Enable SNMP V3

このチェック ボックスは、SNMPv3 を有効にします。 SNMPv3 は主に、セキュリティとリモート構成の機能強化を SNMP に追加します。

このオプションを有効にすると、次の追加フィールドが使用可能になります。

- ユーザー名
- 認証パスワード
- 認証プロトコル
- プライバシーチェックボックスを有効にする

SNMPv3 を機能させるには、ユーザー名と認証パスワードを設定する必要がありますが、プライベート パスワード フィールドはオプションです。 パスワードは 8 文字以上にする必要があります。

Authentication protocol

関連する認証プロトコル (MD5 または SHA) を選択します。 MD5 は安全ではなく非推奨であるため、SHA をお勧めします。

Enable Privacy

このチェックボックスを使用して、SNMPv3 のプライバシー パスワードとプライバシー プロトコルを設定できます。

Privacy protocol

関連するプライバシー プロトコル (AES または DES) を選択します。 DES は推奨されていないため、AES をお勧めします。

Contact

このオプションを使用すると、SNMP 連絡先文字列を変更できます。 たとえば、これは LoadMaster の管理者の電子メール アドレスである可能性があります。

SNMP Location

このオプションを使用すると、SNMP ロケーション文字列を変更できます。 このフィールドは次の文字を受け入れます。

a-z A-Z 0-9 _ . - ; , = : { } @ ( ) ? # % ^ + ~ !

Location の最初の文字としてハッシュタグ記号 (#) を入力しないでください。

SNMP traps

[SNMP トラップを有効にする] を選択し、SNMP トラップ シンク テキスト ボックスに IP アドレスを指定すると、ロードマスター、仮想サービス、またはリアル サーバーに重要なイベントが発生したときにトラップが生成されます。 これらは SNMP トラップ シンクに送信されます。 変更が行われると、LoadMaster はすべての変更が完了するのを待ってから、それを読み取る前に 5 秒間待機します。 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。 5 秒の待機中に状態の変化があった場合、状態の変化が処理され、待機が再開されます。

Enable/Disable SNMP Traps

このトグル オプションは、SNMP トラップの送信を有効または無効にします。
SNMP トラップはデフォルトで無効になっています。

Send SNMP traps from the shared address

このチェック ボックスは、LoadMaster が HA モードの場合にのみ表示されます。
デフォルトでは、SNMP トラップは、アクティブな HA ユニットの IP アドレスを送信元 IP アドレスとして使用して送信されます。 このオプションを有効にすると、共有 IP アドレスを使用してアクティブな HA ユニットから SNMP トラップが送信されます。

SNMP Trap Sink1

このオプションを使用すると、ユーザーは、トラップが生成されたときに SNMPv1 トラップが送信されるホストのリストを指定できます。

SNMP Trap Sink2

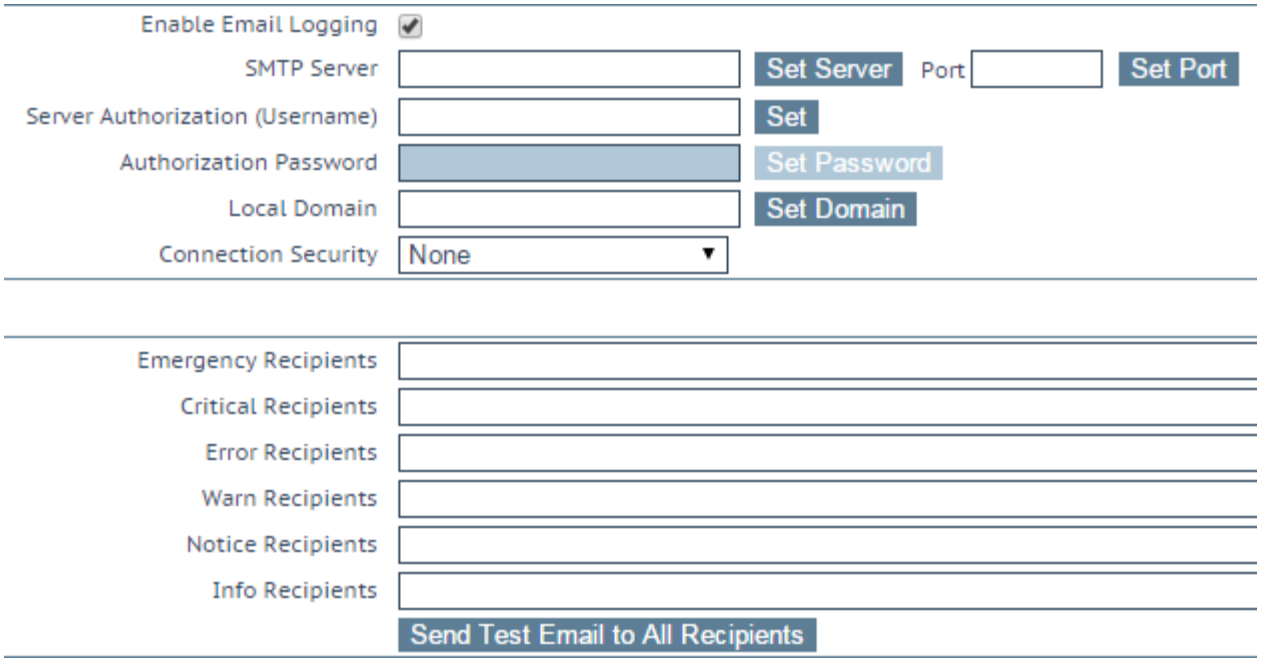
このオプションを使用すると、ユーザーは、トラップが生成されたときに SNMPv2 トラップが送信さ

れるホストのリストを指定できます。

11.5.5 メールオプション

この画面では、LoadMaster イベントの電子メール アラートを設定できます。 電子メール通知は、事前定義された 6 つの情報レベルで配信できます。 各レベルは個別の電子メール アドレスを持つことができ、各レベルは複数の電子メール受信者をサポートします。 電子メール アラートはメール サーバーに依存し、オープン リレー メール サーバーと安全なメール サーバーの両方がサポートされます。

サンプルの電子メール アラートは上にあります。 これは Info レベルからのものです。 syslog 電子メールには、1 行以上の syslog が含まれます (可能であればグループ化されます)。



SMTP Server

メール サーバーの FQDN または IP アドレスを入力します。 FQDN を使用している場合は、DNS サーバーを設定してください。

Port

電子メール イベントを処理する SMTP サーバーのポートを指定します。

Server Authorization (Username)

電子メール ヘッダーの「差出人」アドレスとして使用する電子メール アドレスを入力します。

Authorization Password

メール サーバーがメール配信の承認を必要とする場合は、パスワードを入力します。 メールサーバーが承認を必要としない場合、これは必須ではありません。

Local Domain

メール サーバーがドメインの一部である場合は、トップ レベル ドメインを入力します。 これは必須パラメーターではありません。

Connection Security

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

さまざまな [受信者] テキスト ボックスに、希望する通知レベルに対応する電子メール アドレスを入力します。 重大度のレベルに加えて、より重大度の高いものについて通知が送信されるため、複数のテキスト ボックスに電子メール アドレスを入力する必要はありません。これにより、通知が重複して送信される可能性があります。 たとえば、[重要な受信者] テキスト ボックスに入力された電子メール アドレスには重要な電子メールだけでなく、緊急の電子メールも送信されます。 複数の電子メール アドレスは、次のようなカンマ区切りのリストでサポートされています。

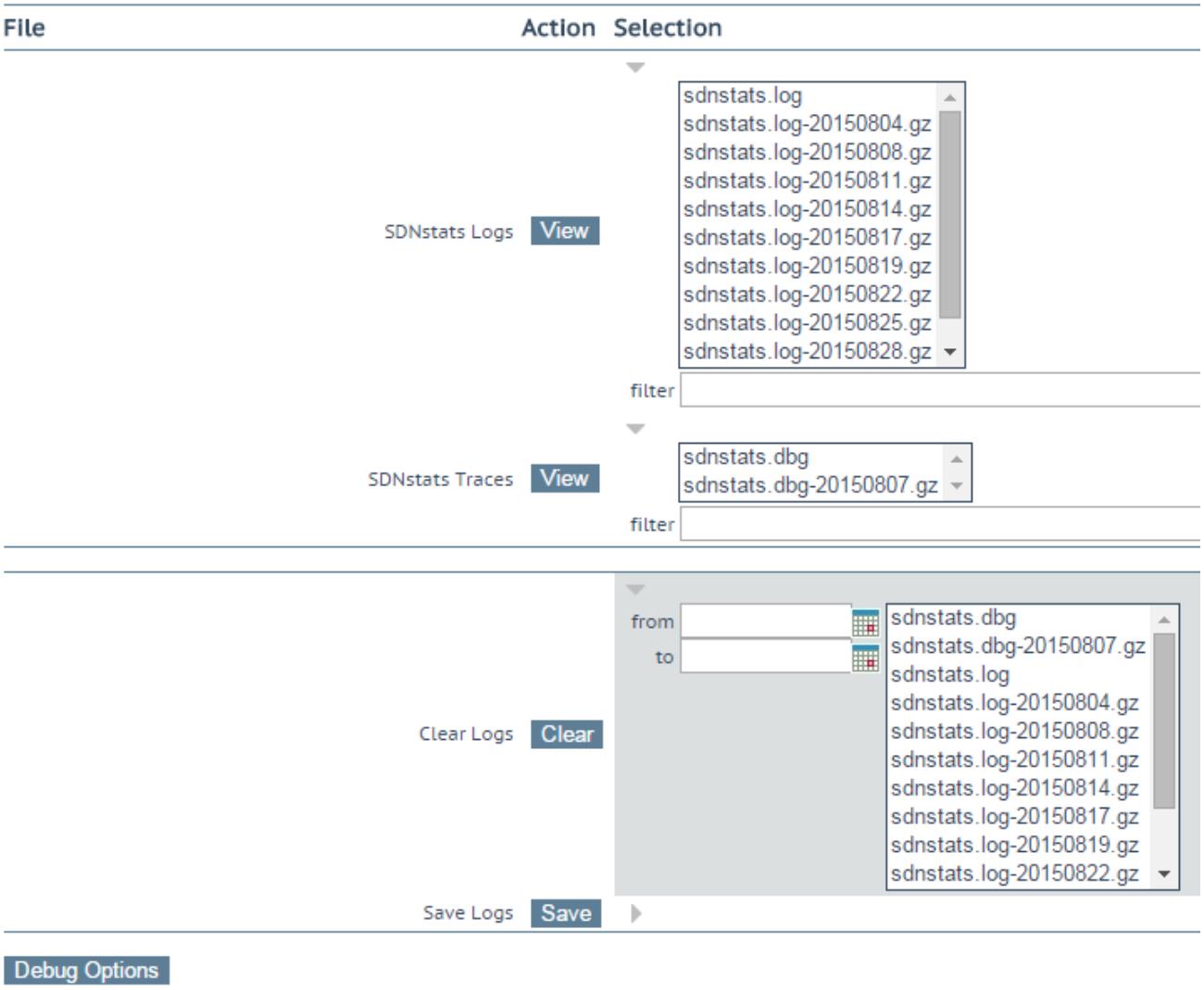
情報受信者: info@kemptechnologies.com, sales@kemptechnologies.com

エラー受信者: support@kemptechnologies.com

テスト電子メールをすべての受信者に送信ボタンをクリックすると、リストされているすべての電子メール受信者にテスト電子メールが送信されます。

電子メール アラートの例を上に示します。 電子メールの件名には、関連する最高の警告レベルが含まれています。 1 通の電子メールに複数のアラートが含まれる場合があります。受信トレイがいっぱいになるのを避けるために、アラートは 30 秒間まとめて照合されます。

11.5.6 SDN ログ ファイル



SDN ログ ファイル画面には、SDN 機能に関連するログのオプションが表示されます。 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 ログを表示するには、関連するログ ファイルを選択し、[View] をクリックしてください。 sdnstats.log ファイルはメインのローリング ログ ファイルです。 .gz ファイルは、特定の日のログのバックアップです。 ファイル名のリストから関連するファイルを選択し、[View] ボタンをクリックすると、１つまたは複数のアーカイブ ログ ファイルを表示できます。 フィルタ フィールドに単語または正規表現を入力し、[View] ボタンをクリックすると、ログ ファイルをフィルタリングできます。

View SDNstats Traces

このオプションは、SDNstats デバッグ ログが有効になっている場合にのみ使用できます ([System Configuration] > [Log Options] > [SDN Log Files] > [Debug Options] > [Enable Debug Log])。 SDNstats ログを表示するには、関連するログ ファイルを選択し、[View] をクリックしてください。 ファイル名のリストから関連するファイルを選択し、[View] をクリックすると、 1 つまたは複数のアーカイブ ログ ファイルを表示できます。 ログ ファイルは、フィルター フィールドに単語または正規表現を入力し、[View] をクリックしてフィルター処理できます。

```
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
```

トレースはプローブ結果を示します。これは、LoadMaster が SDN コントローラーと正常に通信できるかどうかを示します。

Clear Logs

[クリア] ボタンをクリックすると、すべての SDN ログを削除できます。 from フィールドと to フィールドを使用して日付範囲を指定することにより、特定の範囲のログ ファイルをフィルタリングできます。 日付範囲を指定すると、右側のボックスに適用される関連ログ ファイルが選択されます。 個々のログ ファイルは、必要に応じて右側で選択/選択解除できます。

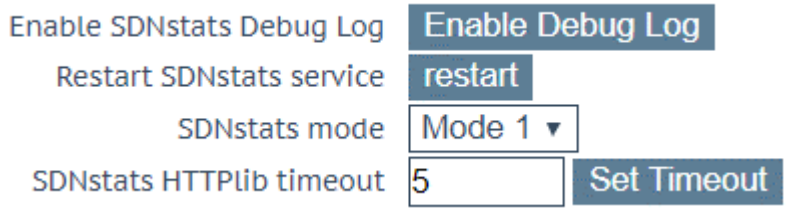
重要: sdnstats.log ファイルが選択されている場合、日付範囲フィールドで選択されている日付に関係なく、そのファイル内のすべてのログが消去されます。

Save Extended Logs

[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。 特定のログ ファイルを保存するには、特定の日付範囲でフィルタリングするか、ログ ファイル リストのログ ファイル リストで 1 つ以上の個々のログ ファイルを選択し、[Save] ボタンをクリックします。

11.5.6.1 デバッグ オプション

SDN Debug Options 画面を表示するには、SDN Log Files 画面の Debug Options ボタンをクリックします。



Enable Debug Log

SDNstats デバッグ ログを有効にします。

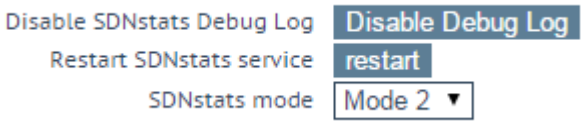
SDN 統計ログを表示するには、[System Configuration] > [Log Options] > [SDN Log Files] を開き、表示するログ ファイルを選択して [View] ボタンをクリックします。 デバッグ ログは、LoadMaster のパフォーマンスに影響を与えるため、トラブルシューティング時にのみ有効にする必要があります。

Restart SDNstats service

SDN に関する問題のトラブルシューティングを行う場合、SDN サービス全体を再起動できます。 接続を再起動しても、トラフィック接続には影響しません。ロードマスターと SDN コントローラー間の接続が再起動されるだけです。 成功した場合、プロセス ID は新しい ID に変更されます。 プロセス ID 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て確認できます。 これにより、接続されているすべての SDN コントローラーへの接続が再開されます。

SDNstats mode

SDN 統計の収集に使用できるモードは 2 つあります。



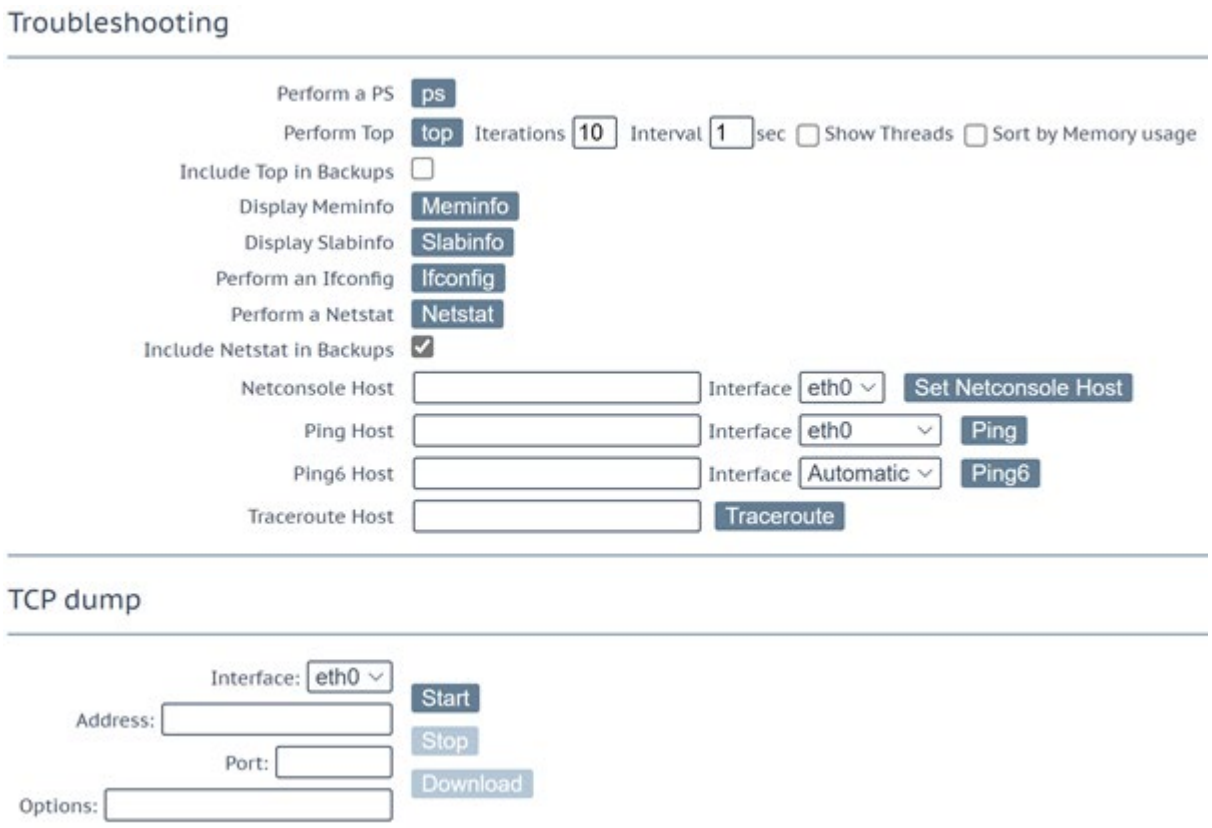
このモードを設定するには、[System Configuration] > [Log Options] > [SDN Log Files] > [Debug Options] に移動し、SDNstats モードを設定します。 モードについて以下に説明します。

- Mode 1: モード 1 に設定すると、サーバーに接続されているスイッチ ポートから統計が取得され、統計が LoadMaster に中継されます。
- Mode 2: モード 2 に設定すると、パスに沿ったすべてのスイッチ ポートから情報が取得されます。

SDNstats HTTPlib timeout

このフィールドを使用すると、SDN コントローラーの応答を待機する時間を増やすことができます。これにより、環境内の遅延によって発生するタイムアウトの可能性を減らすことができます。 このフィールドの有効な値の範囲は 5 ～ 60 です。

11.6 トラブルシューティング



Perform a PS

システムで ps を実行します。

Perform a Top

top コマンドを実行すると、LoadMaster のメモリ、CPU、および I/O の使用状況が表示されます。サンプル数とサンプル間の間隔を指定できます (デフォルトは 10 サンプルで 1 秒間隔です)。 適切なチェック ボックスをオンにすることで、スレッドを表示したり、メモリ使用量で並べ替えたりすることもできます。 デフォルトでは、結果は CPU 使用率でソートされます。

Include Top in Backups

デフォルトでは、LoadMaster はトップ出力をバックアップに含めません。 これは、このチェックボックスをオンにすることで有効にできます。 バックアップに含まれる場合、top は (WUI での構成に関係なく) デフォルトのパラメーターを使用して実行され、メモリ使用量によって並べ替えられます。

Display Meminfo

ロウメモリ統計を表示します。

Display Slabinfo

生のスラブ統計を表示します。

Perform an Ifconfig

ロウ Ifconfig 出力を表示します。

Perform a Netstat

Netstat 出力を表示します

Include Netstat in Backups

デフォルトでは、LoadMaster は取得したバックアップに Netstat 出力を含めます。 これが含まれていると、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 出力が含まれないようにすることができます。

Netconsole Host

Kemp サポート エンジニアの指示があれば、この機能を使用して、LoadMaster の障害またはクラッシュが発生した場合に重要なカーネル ログを syslog サーバーに送信できます。 Netconsole ホストとして構成された syslog サーバーは、重要なカーネル メッセージをすべて受信します。 [インターフェース] ドロップダウンを使用して、ネットコンソール ホストを設定するインターフェースを選択できます。 指定したネットコンソール ホスト IP 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、エラーが発生する可能性があります。

Netconsole Host パラメーターは、IPv4 または IPv6 アドレスのいずれかに設定できます。唯一の制限は、Netconsole IP アドレスが、選択したインターフェースの LoadMaster の IP アドレスと同じアドレス ファミリーに属している必要があることです。 つまり、選択したインターフェースの LoadMaster の IP アドレスが IPv4 アドレスの場合、ネットコンソール ホストの IP アドレスも IPv4 アドレスでなければなりません。 Netconsole ホストに IPv6 アドレスを使用する場合は、ロードマスターが IPv6 アドレスを持つインターフェイスを選択する必要があります。 Netconsole

は、結合されたインターフェイスでは構成できません。

Ping Host
指定されたホストで ping を実行します。 ping を送信するインターフェイスは、[Interface] ドロップダウン リストで指定できます。 自動オプションは、特定のネットワーク上のアドレスを ping するための正しいインターフェイスを選択します。 インターフェイスは、ping を実行するアドレスが IPv4 または IPv6 アドレスであるかどうかを判断しようとし、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、これは簡単ですが、数値以外のアドレスでは不可能なため、常に IPv4 アドレスとして扱われます。

Ping6 Host
特定の IPv6 ホストの ping6 を実行します。

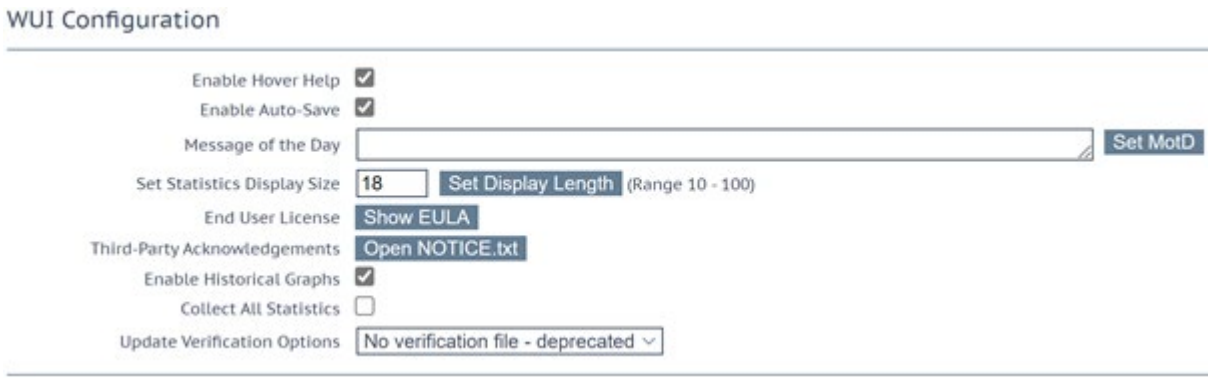
Traceroute Host
特定のホストの traceroute を実行します。

TCP dump
TCP ダンプは、1 つまたはすべてのイーサネット ポートでキャプチャできます。 アドレスとポートのパラメーター、およびオプションのパラメーターを指定できます。 で許可される最大文字数 オプション テキスト ボックスは 255 です。ダンプを停止および開始できます。 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 アナライザ ツールで分析できます。 詳細については、パケット トレース ガイドのテクニカル ノートを参照してください。

11.7 その他のオプション

11.7.1 WUI 設定

この機能を使用できるのは、bal ユーザーまたは「All Permission」が設定されているユーザーのみです。 異なる権限を持つユーザーは画面を表示できますが、すべてのボタンと入力フィールドがグレー表示されます。

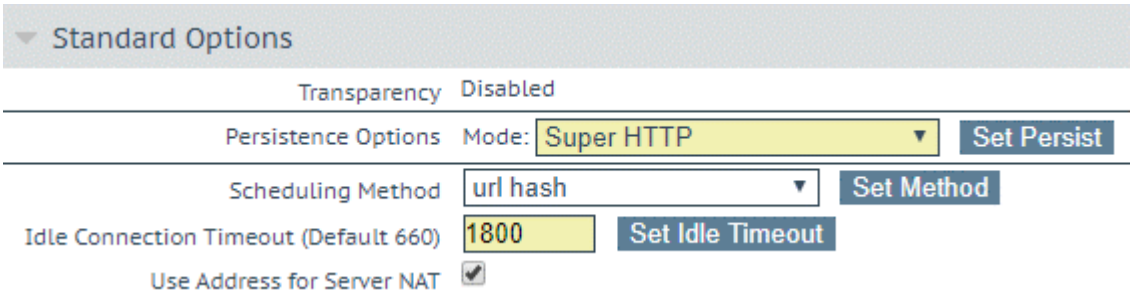


Enable Hover Help

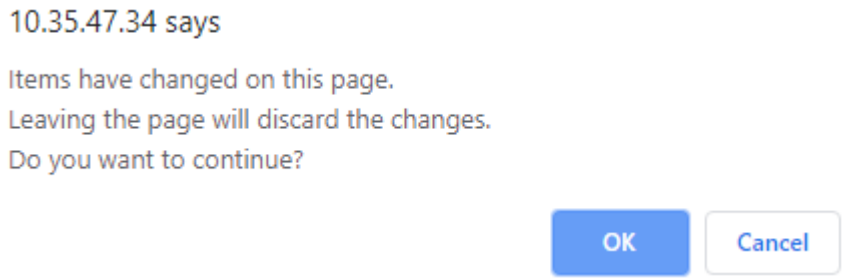
ポインターをフィールド上に置いたときに表示される青いホバー ノートを有効にします。

Enable Auto-Save

自動保存はデフォルトで有効になっています。 自動保存が有効になっている場合、LoadMaster UI で行った変更は即座に適用されます。 たとえば、ドロップダウン リストでオプションを選択すると、変更が即座に適用されます。 自動保存が無効になっている場合、いくつかのデフォルトの UI 動作が変更されます。 たとえば、以下のスナップショットのように、永続オプションの保存されていない変更は、背景色の変更によって示されます。



関連するボタンをクリックして、ドロップダウンの選択を確認する必要があります (自動保存が有効になっている場合、一部のフィールドにはボタンがありません。選択すると、変更が自動的に適用されます)。



変更が保存されていないページから移動しようとすると、警告が表示されます。 自動保存の無効化は、現在ベータ機能です。

自動保存が無効になっている場合、LoadMaster ファームウェアを 7.2.49 より古いバージョンにダウングレードすると、チェック ボックスが使用できなくなるため、自動保存機能を有効にすることはできません。 Kemp のドキュメントは、自動保存を有効にして書かれています。

Message of the Day (MOTD)

フィールドにテキストを入力し、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 セッション管理が有効になっている場合、MOTD はホーム画面ではなくログイン画面に表示されます。 メッセージの最大許容長は 5,000 文字です。 HTML はサポートされていますが、必須ではありません。 単一引用符 (') と二重引用符 (") は使用できませんが、同等の HTML 文字コードを使用できます。 たとえば、&#34it&#39s allowed&#34 と入力すると、MOTD は「it's allowed」になります。

Set Statistics Display Size

これにより、統計ページに表示できる最大行数が設定されます。 許容範囲は、ページに表示される 10 ～ 100 行です。

End User License

[View EULA] ボタンをクリックして、ロードマスター エンド ユーザー ライセンス契約を表示します。

Third-Party Acknowledgements

[Open NOTICE.txt] をクリックすると、実行中の LoadMaster リリースに適用されるサードパーティの承認ファイルを表示できます。 テキスト ファイルが新しいタブで開きます。

Enable Historical Graphs

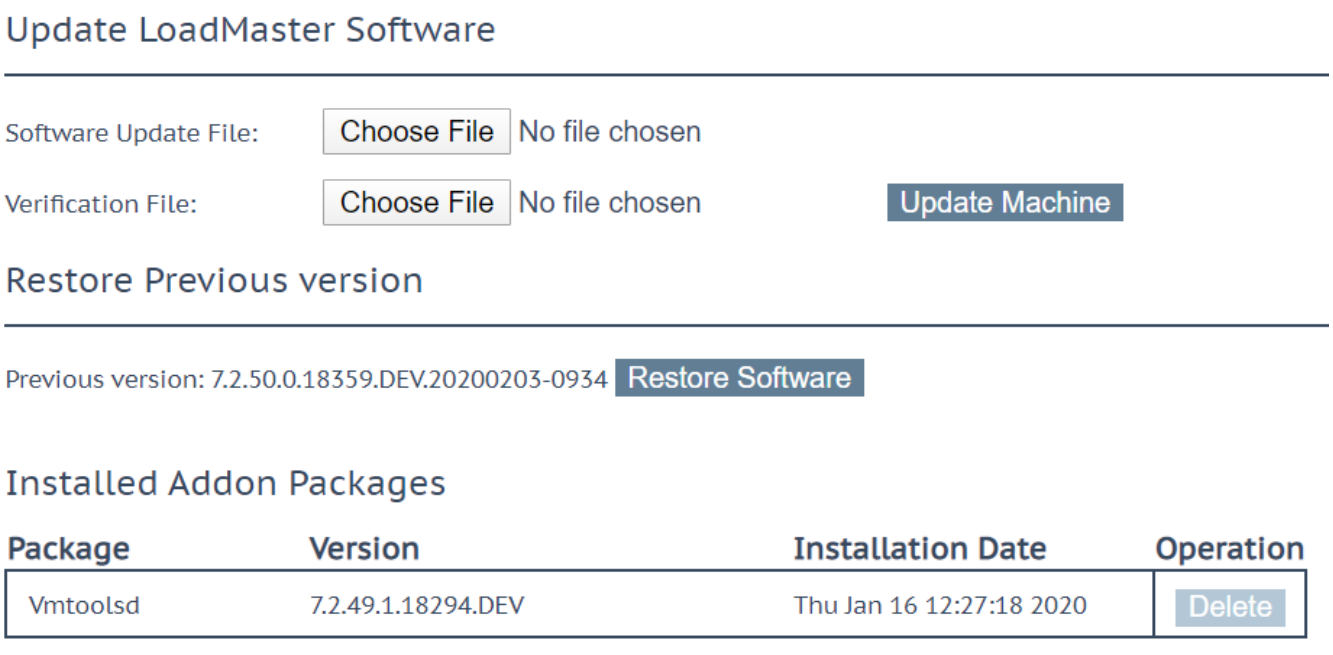
仮想サービスと実サーバーの履歴統計の収集を有効にします。

Collect All Statistics

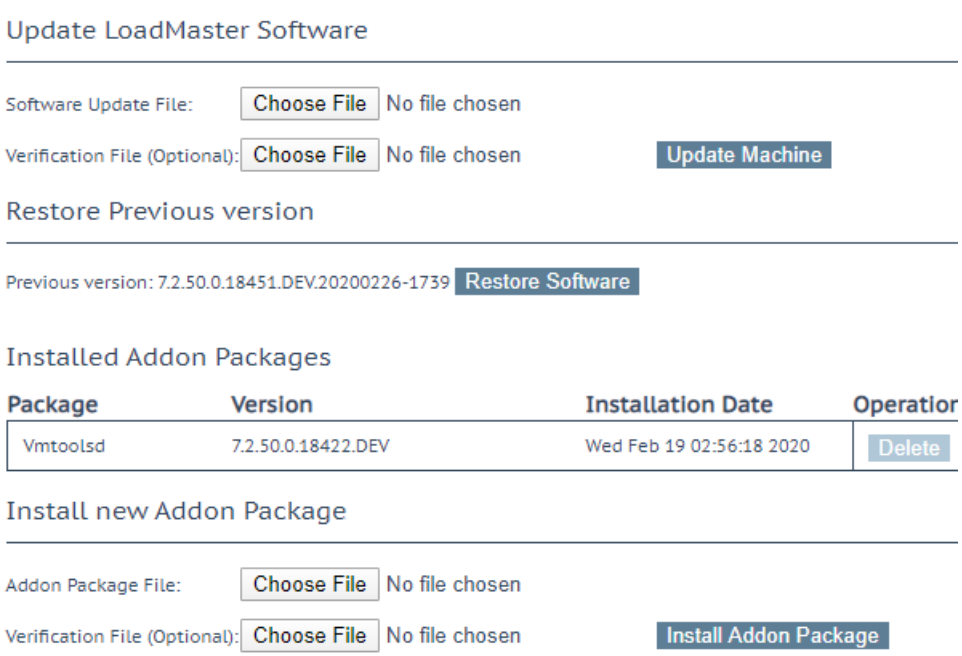
デフォルトでは、このオプションは無効になっています。 これは、ホームページに表示されるように構成されている仮想サービスと実サーバーの統計のみが収集されることを意味します。 このオプションを有効にすると、LoadMaster はすべての仮想サービスと実サーバーの統計を収集します。 多数の仮想サービスと実サーバーがある場合、このオプションにより CPU 使用率が非常に高くなる可能性があります。

Update Verification Options

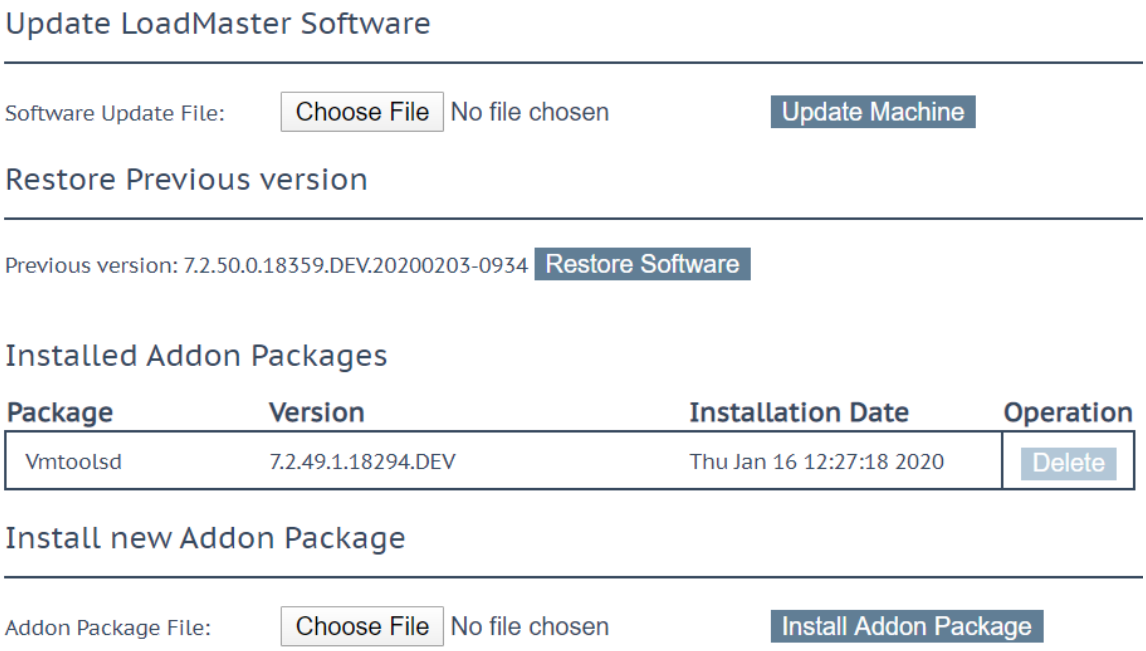
このフィールドは、デフォルトで [Required] に設定されています。 その他のオプションは、オプションおよび検証ファイルなし - 非推奨です。 さまざまなオプションについて以下に説明します。



Required: LoadMaster ソフトウェアを更新し、アドオン パッケージをインストールするための [Software Update] 画面に、[Verification File] オプションが表示されます。 この場合、検証ファイルは必須であり、検証ファイルを提供しないと LoadMaster ソフトウェアを更新したり、アドオンをインストールしたりすることはできません。



Option: LoadMaster ソフトウェアを更新し、アドオン パッケージをインストールするための [Software Update] 画面に、[Verification File] オプションが表示されます。 この場合、検証ファイルはオプションであり、検証ファイルを提供しなくても LoadMaster ソフトウェアを更新したり、アドオンをインストールしたりできます。

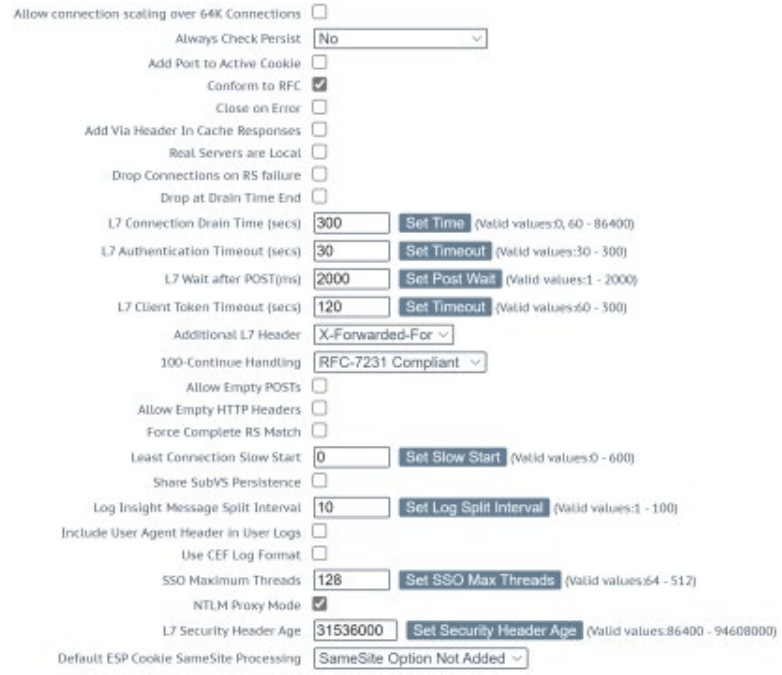


No Verification File - deprecated: [Software Update] 画面に [Verification File] オプションが表

示されません。 この場合、検証ファイルを提供しなくても、LoadMaster ソフトウェアを更新したり、アドオンをインストールしたりできます。 このオプションは、レガシー リリースとの互換性のためにのみ提供されており、非推奨です。

検証ファイル オプションは、パッチまたはアドオンのアップロードと同時にセカンダリ XML 検証ファイルをアップロードできるようにすることで、更新イメージとアドオン イメージに対して常に実行される整合性チェックよりも高いレベルの検証を提供します。 . この XML ファイルは、更新プログラムまたはアドオンに関連付けられたデジタル署名を検証するために使用されます。更新プログラムまたはアドオンは、アップロードされた XML ファイルに対してパッチを検証できない場合はインストールされません。 FIPS マシンの場合 - パッチまたはアドオンをアップロードする場合、セカンダリ XML 検証ファイルのアップロードが必須であるため、[Update Verification Options] フィールドは表示されません。

11.7.2 L7 構成



Allow Connection Scaling over 64K Connections

負荷が非常に高い状況では、ポートの枯渇が発生する可能性があります。 このオプションを有効にすると、使用可能なローカル ポートの数を拡張するために使用できる代替ソース アドレスの設定が可能になります。

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] 入力フィールドで仮想サービス IP を代替アドレスとして設定します。 これにより、各仮想サービスはソース ポートの独自のプールを持つことができます。 透過仮想サービスの同時接続数は 64K に制限されています。 この制限は、仮想サービスごとに適用されます。このオプションを選択した後に代替送信元アドレスを設定すると、[Allow connection scaling over 64K Connections] オプションを選択解除できなくなります。

Always Check Persist

デフォルトでは、L7 モジュールは HTTP/1.1 接続の最初のリクエストでのみ持続をチェックします。 このオプションで [Yes] を選択すると、要求ごとに持続性がチェックされます。 [Yes – Accept Changes] を選択すると、接続の途中であっても、すべての持続性の変更が保存されます。

Add Port to Active Cookie

アクティブ Cookie を使用する場合、LoadMaster は (とりわけ) クライアントの IP アドレスから Cookie を作成します。 ただし、多くのクライアントがプロキシ サーバーの背後にある場合、それらのクライアントはすべて同じ IP アドレスから来ます。 これをオンにすると、クライアントの送信元ポートも文字列に追加され、ビットがよりランダムになります。

Conform to RFC

このオプションは、RFC 1738 に準拠した HTTP リクエストのヘッダーの解析に対処します。リクエストは GET /pathname HTTP/1.1 の 3 つの部分で構成され、「conform」がオンの場合、LoadMaster はスペースが見つかるまでパス名をスキャンします。 次に、次は HTTP/1.x であると想定します。 パス名にスペースが含まれていて、ブラウザが RFC に準拠している場合、パス名にはスペースは「%20」にエスケープされるため、スペースのスキャンは正しく機能します。 ただし、一部の非準拠ブラウザでは、スペースがエスケープされず、間違ったパス名が処理されます。 システムは HTTP/1.x を見つけることができないため、LoadMaster はリクエストを拒否します。 この機能をオフにすると、LoadMaster は、パス名が行の最後のスペースまで続くと想定します。 次に続くのは HTTP/1.x であると想定されます。 そのため、スペースを含むパス名を使用できるようにしますが、RFC 1738 には準拠していません。

Close on Error

LoadMaster が失敗レポートをクライアントに送り返す必要がある場合 (たとえば、ファイルがキャッシュ内で新しい場合)。 これにより、LoadMaster は応答の送信後に強制的に接続を閉じま

す。 障害レポートを送信した後も引き続き接続を使用できますが、一部のシステムが混乱する可能性があります。 このオプションは、続行する代わりに強制的に終了します。

Add Via Header In Cache Responses

関連する HTTP RFC では、プロキシは Via ヘッダーを追加して、何かがキャッシュから来たことを示す必要があると述べています。 残念ながら、古いバージョンの LoadMaster ではこれができませんでした。 このチェック ボックスは、古いバージョンとの下位互換性を有効にするために使用されます (必要な場合)。

Real Servers are Local

LoadMaster には、Transparency (選択的透過性) を目的として、ローカル/非ローカル クライアントの自動検出機能があります。 これはほとんどの場合うまく機能しますが、クライアントが実際にリアル サーバーの場合はうまく機能しません。 このオプションをオンにすると、実サーバーが実際にローカルであることをロードマスターが判断できるようになるため、選択的な Transparency が機能します。 このオプションが 2 アーム環境 (2 番目のインターフェイスにクライアントと Real Server がある) で有効になっている場合、実サーバーはクライアントに対してローカルであるかのように扱われます。つまり、Transparent ではありません。 実サーバーが完全に異なるネットワーク上にある場合、ローカルにすることはできず、常に非ローカルとして扱われます。 ローカルは、同じネットワーク上にあると定義されます。 このオプションを有効にするには、慎重なネットワーク トポロジの計画が必要であり、Kemp サポート チームに連絡する前に試みるべきではありません。

Drop Connections on RS Failure

これは、実サーバーの障害が検出されるとすぐに接続を閉じるため、Microsoft Outlook ユーザーにとって便利です。 Exchange ユーザーは常にこのオプションを選択する必要があります。 Idle Connection Timeout オプションも同時に 86400 に設定されます。 詳細については、『Microsoft Exchange 2010 導入ガイド』を参照してください。

Drop at Drain Time End

有効にすると、無効な実サーバーへのすべての開いている接続は、実サーバーのドレイン停止時間の終わりに、または実サーバーに関連付けられた持続エントリがない場合はすぐにドロップされます。

L7 Authentication Timeout (secs)

このオプションは、SMS や電話による確認などの二次プロセスを持つ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、SSO フォームが認証検証の完了をタイムアウトするまで待機する時間 (秒単位) を決定します。

L7 Client Token Timeout (secs)

認証プロセスの進行中にクライアント トークンを待機する時間 (秒単位) (RSA SecurID および RADIUS 認証に使用)。 有効な値の範囲は 60 ～ 300 です。デフォルト値は 120 です。

L7 Wait after POST(ms)

LoadMaster ファームウェア バージョン 7.2.51 では、Kerberos Constrained Delegation (KCD) バックエンド認証を実行するときに適用できる新しいオプションが導入されました。 このフィールドは、L7 Wait after POST と呼ばれます。 このオプションは、LoadMaster ユーザー インターフェイス (UI) で設定できます。 L7 Wait after POST オプションを使用すると、POST 本文の残りを送信する前に、POST からの 401 応答を待機する時間の長さを変更できます。 待機期間の有効な値は、1 ～ 2000 ミリ秒 (ms) です。 デフォルト値は 2000 です。KCD が使用されていない場合、このオプションは効果がありません。

L7 Connection Drain Time (secs)

L7 Connection Drain Time は、新しい接続のみに影響します。 [Drop at Drain Time End] チェックボックスが選択されていない限り、既存の接続は、その接続が終了するまで、アプリケーション データを無効なサーバーにリレーし続けます。 L7 Connection Drain Time (secs) を 0 に設定すると、Real Server が無効になったときにすべての接続が即座にドロップされます。サービスがレイヤ 4 で動作している場合、ドレイン ストップは適用されません。この場合、持続性レコードは破棄され、有効で正常なサーバーへの接続がスケジュールされ、新しい持続性レコードが作成されます。リアルサーバーを無効にしても、すべての接続がすぐに閉じられるわけではなく、穏やかに閉じられます。有効な持続性レコードがない限り、新しい接続はドレイン時間中に実サーバーに送られません。 [Drop at Drain Time End] が選択されている場合、ドレーン時間が経過すると、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、接続は開いたままになります。 Drop at Drain Time End が有効になっていない限り、ドレイン停止タイマーは既存の接続に影響を与えません。ドレーン停止タイマーは、既存の接続には影響しません。

Additional L7 Header

これにより、HTTP/HTTPS 仮想サービスのレイヤー 7 ヘッダー インジェクションが有効になります。 ヘッダー インジェクションは、X-ClientSide (Kemp LoadMaster 固有)、X-Forwarded-For、または None に設定できます。 デフォルト値は XForwarded-For です。

100-Continue Handling

100-Continue Handling メッセージの処理方法を決定します。 利用可能なオプションは次の

とおりです。

- RFC-2616 準拠: RFC-2616 で概説されている動作に準拠
- Require 100-Continue: LoadMaster が 100-Continue メッセージを待つように強制します。
- RFC-7231 準拠: LoadMaster が 100-Continue メッセージを待機しないようにします。これがデフォルト値。

システムによる 100 Continue メッセージの処理方法を変更するには、上記の RFC で説明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、Progress Kemp テクニカル サポート エンジニアに相談することをお勧めします。

Allow Empty POSTs

デフォルトでは、LoadMaster は Content-Length または Transfer-Encoding ヘッダーを含まない POST をブロックして、リクエスト ペイロードの長さを示します。 Allow Empty POSTs オプションが有効になっている場合、そのようなリクエストはペイロード データを持たないと見なされるため、拒否されません。

バージョン 7.1-24 以降のリリースでは、サポートされる Content-Length の制限が (2GB から) 2TB に増えました。

Force Complete RS Match

デフォルトでは、LoadMaster がコンテンツ スイッチングで使用する実サーバーを見つけようとするとき、ポートが同じでなくても、現在選択されているものと同じ実サーバーを使用しようとします。このオプションを有効にすると、ポートも強制的に比較されます。

Least Connection Slow Start

Least Connection または Weighted Least Connection スケジューリング方法を使用する場合、[Least Connection Slow Start] フィールドを使用して期間をグローバルに指定できます。その間、新しい接続の数が調整され、オンラインになって実サーバーに戻った実サーバーに徐々に増加します。スケジューリングプロセス。実サーバーがサービスを再開し、Least Connection Slow Start がゼロ以外の値に設定されている場合、LoadMaster は実サーバーへの新しいトラフィックを抑制し、突然のトラフィック ストリームによって圧倒されないようにします。テスト中、観察された 1 秒あたりの接続数 (CPS) レート制限は、実サーバーの接続容量が完全に許可されるまで、指定され

た期間にわたってゆっくりと増加することが観察されました。実サーバーがスケジューリング プロセスから削除された理由 (たとえば、手動で無効にした、レート制限など) に関係なく、スロー スタートが適用されます。このスロー スタート期間の値は、0 (無効 - これが既定値) から 600 秒の間です。 Least Connection Slow Start 機能は、LoadMaster ファームウェア バージョン 7.2.51 で導入された Connection Rate Limit 機能と組み合わせて使用できます。

Share SubVS Persistence

デフォルトでは、仮想サービスの各 SubVS には独立した持続性テーブルがあります。 このオプションを有効にすると、SubVS がこの情報を共有できるようになります。 これが機能するには、その仮想サービス内のすべての SubVS で持続性モードが同じである必要があります。 このオプションを有効にするには、再起動が必要です。 共有できない永続モードは、SSL セッション ID だけです。

共有 SubVS 永続性を設定する場合、この機能を完全に機能させるにはいくつかの要件があります。

- SubVS 内のすべての実サーバーは同じである必要があります
- 永続モードは、すべての SubVS で同じである必要があります
- タイムアウトは同じタイムアウト値で設定する必要があります

上記の要件が正しくない場合、永続性は SubVS 内または SubVS 間で正しく機能しない可能性があります。

Log Insight Message Split Interval

Log Insight の分割間隔の値は、次のサーバーに移動する前に、プール内の各サーバーに送信する syslog メッセージの数を制御します。 たとえば、3 つの Log Insight ノードがあり、Log Insight のメッセージ分割間隔が 1 に設定されている場合、1 つのメッセージがサーバー A に送信され、次にサーバー B に送信され、次にサーバー C に送信されてから、サーバー A にメッセージが再度配信されます。

Include User Agent Header in User Logs

有効にすると、ユーザー エージェント ヘッダー フィールドがユーザー ログに追加されます。

Use CEF Log Format

有効にすると、ESP ログは Common Event Format (CEF) で生成されます。 CEF ログ形式は、Splunk、SolarWinds、LogRhythm、AlienVault などのセキュリティ情報およびイベント管理 (SIEM) ツールで簡単に使用できます。

NTLM Proxy Mode

LoadMaster ファームウェア バージョン 7.2.48.4 Long Term Support (LTS) および 7.2.53 では、NTLM Proxy Mode オプションが LoadMaster に追加されました。 古いバージョンの LoadMaster ファームウェアからこれらのバージョン (またはそれ以降) のいずれかにアップグレードする場合、NTLM プロキシ モード オプションはデフォルトでは有効になっていません。 そのため、アップグレード後に NTLM プロキシ モードを手動で有効にする必要があります。 7.2.48.4 LTS または 7.2.53 以降のロードマスターのすべての新規導入では、デフォルトで NTLM プロキシ モードが有効になっています。 NTLM プロキシ モードが有効になっている場合、NTLM 認証は実サーバーに対して機能します。 NTLM プロキシ モードが無効になっている場合は、古い安全でない NTLM 処理が実行されます。 Kemp は、NTLM プロキシ モードが有効になっていることを確認することを強くお勧めします。 NTLM プロキシ モードがグローバルに有効になっている場合、仮想サービスのクライアント認証モードは NTLM-Proxy と呼ばれます。 NTLM プロキシ モードがグローバルに無効になっている場合、仮想サービスのクライアント認証モードは NTLM と呼ばれます。

L7 Security Header Age

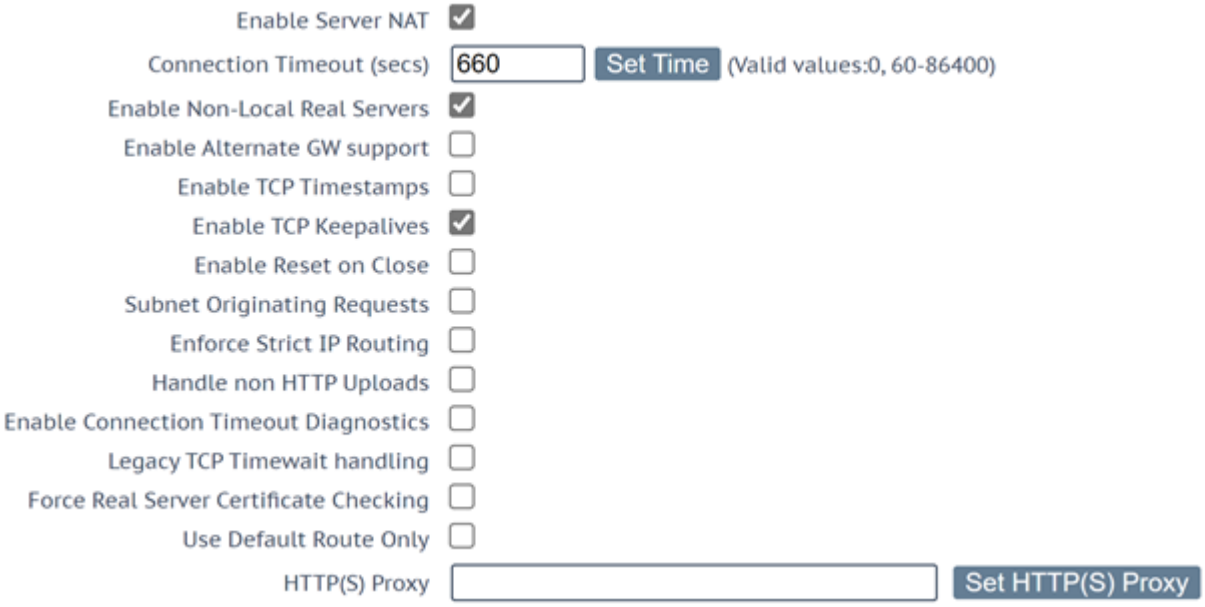
このオプションを使用すると、LoadMaster が送信するセキュリティ ヘッダー (STS) の有効期間 (秒) を決定するカスタム タイムアウト値を設定できます。 有効な値の範囲は 86400 ～ 94608000 です。デフォルト値は 31536000 です。

Default ESP Cookie SameSite Processing

このオプションを使用すると、ESP 処理中に LoadMaster によって送信される Cookie の SameSite オプションのデフォルト値を設定できます。 SameSite 属性は、ファースト パーティまたはサード パーティの状況で、いつ、どのように Cookie を処理するかをブラウザーに伝えます。 SameSite は、Cookie へのアクセスを許可するかどうかを識別するために、さまざまなブラウザーで使用されます。 SameSite オプションは次のとおりです。

- SameSite オプションが追加されていません
- SameSite=None: Cookie データをサードパーティ/外部サイト (広告、埋め込みコンテンツなど) と共有できることを示します。
- SameSite=LAX: Cookie がファースト パーティ Cookie として使用される可能性があることを示しますが、ユーザーがクリックしたリンクを介して外部サイトからサイトにアクセスするときにも使用される可能性があります。
- SameSite=Strict: これは lax のサブセットであり、Cookie をファースト パーティ コンテキストでのみ使用できるようにし、外部サイトからの着信リンクを介してアクセスする場合はその使用を除外します。

11.7.3 ネットワーク オプション



Enable Server NAT

このオプションは、サーバー ネットワーク アドレス変換 (SNAT) を有効にします。これを無効にすると、接続時に実サーバーの IP アドレスが使用されます。

これを有効にすると、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) のアドレスが「プライマリ アドレス」に NAT 変換されます。仮想サービスで [Use Address for Server NAT] が有効になっている場合、仮想サービス アドレスが使用されます。 Use Address for Server NAT オプションの詳細については、「Standard Options」セクションを参照してください。送信元アドレスがプライマリ アドレスと同じファミリにない場合、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 されます。たとえば、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 アドレスの場合、IPv6 アドレスはそのアドレスに SNAT されます。プライマリ アドレスが IPv4 アドレスの場合、IPv6 アドレスは、IPv6 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 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 アドレスの場合、IPv4 アドレスはそのアドレスに SNAT されます。プライマリ アドレスが IPv6 アドレスの場合、IPv4 アドレスは、IPv4 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 されます。

Connection Timeout (secs)

接続が閉じられるまでのアイドル状態の時間 (秒単位)。 この値は、Persistence Timeout 値とは無関係です。 値を 0 に設定すると、値がデフォルト設定の 660 秒にリセットされます。

Enable Non-Local Real Servers

非ローカル実サーバーを仮想サービスに割り当てることを許可します。 これは、LoadMaster が 1 つのインターフェースしか持つことができず、実サーバーがそのインターフェースとは異なるネットワーク上にある場合に必要になることがあります。 このオプションはデフォルトで有効になっています。

Enable Alternate GW support

複数のインターフェイスが有効になっている場合、このオプションを使用すると、デフォルト ゲートウェイを別のインターフェイスに移動できます。 このオプションを有効にすると、別のオプションが [Interfaces] 画面に追加されます – Use for Default Gateway.

GEO のみの LoadMaster では、代替 GW サポートを有効にするオプションが別の画面に表示されます。 代替デフォルト ゲートウェイのサポートは、クラウド環境では許可されていません。

Enable TCP Timestamps

LoadMaster は、クライアントからの接続とリアル サーバーへの接続の両方で、SYN にタイムスタンプを含めることができます。

これは、NAT された接続に影響を与える可能性があるため、Progress Kemp カスタマー サポートに相談してのみ有効にする必要があることに注意してください。

Enable TCP Keepalives

デフォルトでは、TCP キープアライブが有効になっており、存続期間の長い TCP 接続 (SSH セッション) の信頼性が向上します。 キープアライブは通常、通常の HTTP/HTTPS サービスでは必要ありませんが、たとえば FTP サービスでは必要になる場合があります。 キープアライブ メッセージは、ロードマスターからリアル サーバーとクライアントに送信されます。 したがって、クライアントがモバイル ネットワーク上にある場合は、追加のデータ トラフィックに問題がある可能性があります。

Enable Reset on Close

この設定が無効 (デフォルト) の場合、クライアント側とサーバー側の両方でロードマスターへの非暗号化および暗号化された TCP 接続は、FIN および ACK パケットの標準 TCP 交換を使用して閉じら

れます。 仮想サービスの受信接続負荷が高い状況では、[Enable Reset on Close] をオンにすることで、仮想サービスへの新しい接続を確立する機能を向上させることができます。 これにより、ロードマスターは、通常の TCP クロージング交換ではなく、単一の TCP RST (リセット) パケットで TCP 接続を閉じるように指示されます。

Subnet Originating Requests

このオプションを有効にすると、非透過的なリクエストの送信元 IP アドレスは、関連するサブネット (つまり、Real Server が配置されているサブネット、または Real Server にルーティングできるゲートウェイのサブネット) 上の LoadMaster のアドレスから取得されます (実サーバーが非ローカルで、静的ルートを使用するように構成されている場合)。スタティック ルートの設定の詳細については、次の Kemp ナレッジ ベース記事を参照してください: スタティック ルートの作成。これはグローバル オプション/設定です。 Subnet Originating Requests オプションを仮想サービスごとに有効にすることをお勧めします。グローバル オプションが無効になっている場合は、仮想サービス サブネットごとの発信要求オプションが優先されます。つまり、仮想サービスごとに有効または無効にすることができます。これは、[Virtual Service Property] 画面の [Standard Options] セクションで設定できます (透過性が無効になっている場合)。仮想サービスごとのオプションの詳細については、「Standard Option」セクションを参照してください。 SSL 再暗号化が有効になっている仮想サービスに対してこのオプションをオンにすると、接続を処理するプロセスを強制終了して再起動する必要があるため、仮想サービスを現在使用しているすべての接続が終了します。

Enable Strict IP Routing

このオプションを選択すると、送信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着するパケットのみが受け入れられます。 Use Default Route Only オプションは、これを達成するためのより良い方法かもしれません。

Handle non HTTP Uploads

このオプションを有効にすると、非 HTTP アップロード (FTP アップロードなど) が正しく機能することが保証されます。

Enable Connection Timeout Diagnostics

デフォルトでは、接続タイムアウト ログは有効になっていません。 これは、不要なログが多すぎる可能性があるためです。 接続タイムアウトに関連するログを生成する場合は、[Enable Connection Timeout] チェック ボックスをオンにします。

Legacy TCP Timewait Handling

TCP timewait 接続を再利用する従来のモードに戻すには、このオプションを有効にします。
Kemp サポートに相談した後にのみ、Legacy TCP Timewait Handling オプションを有効にしてください。

Force Real Server Certificate Checking

デフォルトでは、トラフィックを再暗号化するとき、LoadMaster はリアル サーバーから提供された証明書をチェックしません。 このオプションは、Real Server の証明書が有効であること、つまり、認証局と有効期限に問題がないことを LoadMaster に確認させます。 これには、すべての中間証明書が含まれます。

Use Default Route Only

デフォルト ルート エントリが設定されている仮想サービスからのトラフィックを、仮想サービスのデフォルト ルートが配置されているインターフェイスにのみルーティングするように強制します。 この設定により、隣接するインターフェースを使用してトラフィックを直接返すことなく、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、同じネットワーク内のすべての仮想サービスに影響します。

HTTP(S) Proxy

このオプションにより、クライアントは、ロードマスターがインターネットへのアクセスに使用する HTTP(S) プロキシ サーバーとポートを指定できます。

11.7.4 SDN Configuration

Add New

新しい SDN コントローラー接続を追加します。

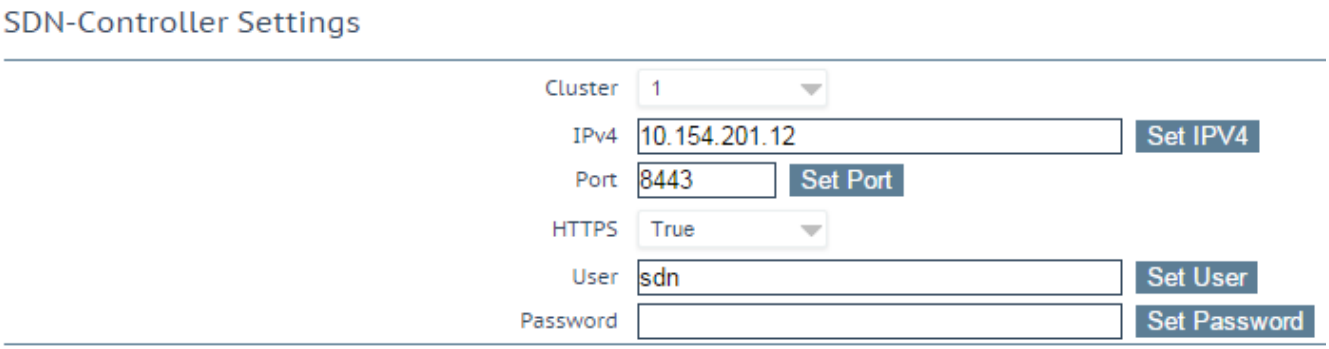
Modify

既存の SDN コントローラー接続を変更します。

Delete

既存の SDN コントローラー接続を削除します。

11.7.4.1 SDN Controller Settings



新しい SDN コントローラー接続を追加すると、最初にクラスター、IPv4 アドレス、およびポートを求める画面が表示されます。 SDN コントローラ接続が追加された後、[SDN Statistics] 画面で [Modify] をクリックして設定を更新できます。

Cluster

SDN コントローラーがメンバーになるクラスター。

Cluster フィールドはデフォルト値のままにします。

IPv4

SDN コントローラーの IPv4 アドレス。

Port

SDN コントローラー WUI のポート。

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

HTTP/HTTPS を使用して SDN コントローラーにアクセスします。

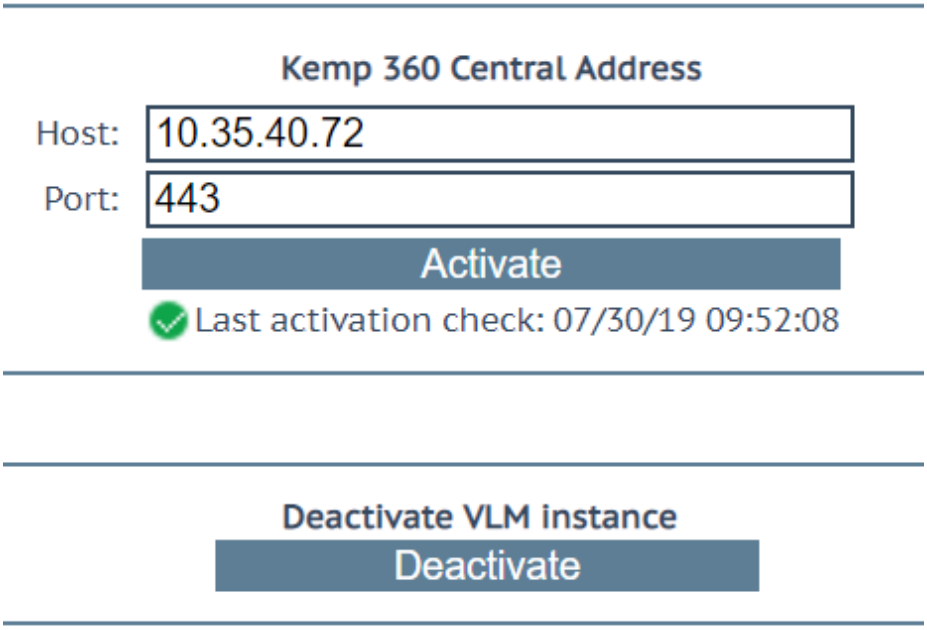
User

SDN コントローラーへのアクセスに使用するユーザー名。

Password

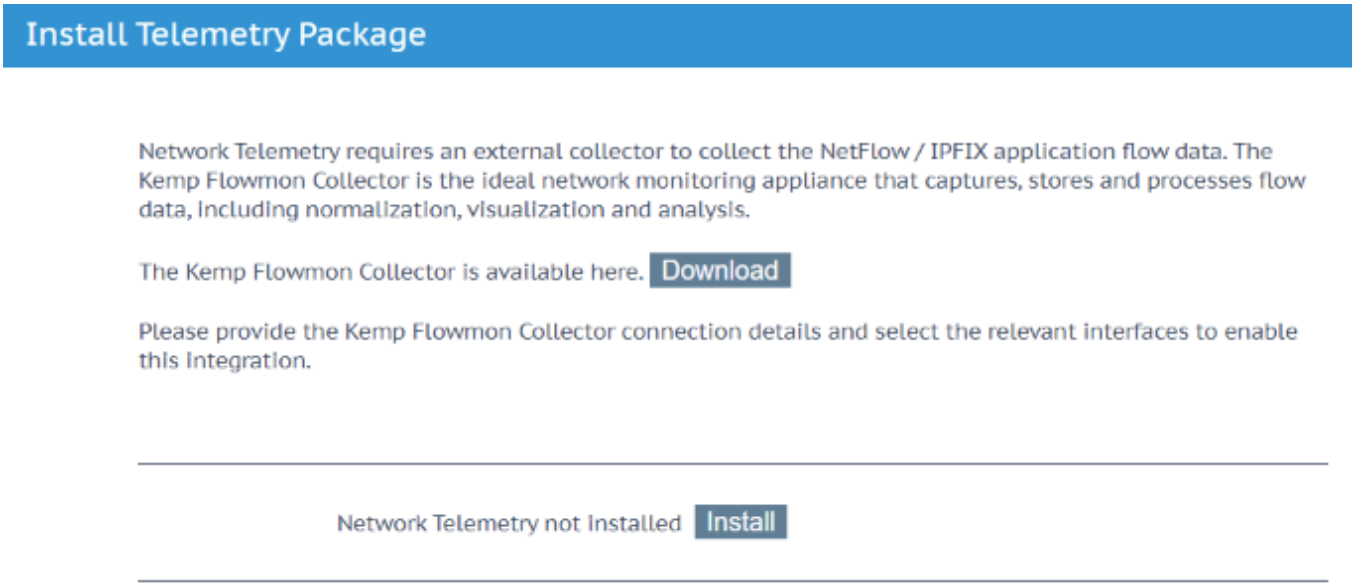
SDN コントローラーへのアクセスに使用するユーザーのパスワード。

11.7.5 Kemp 360 セントラル アクティベーション設定

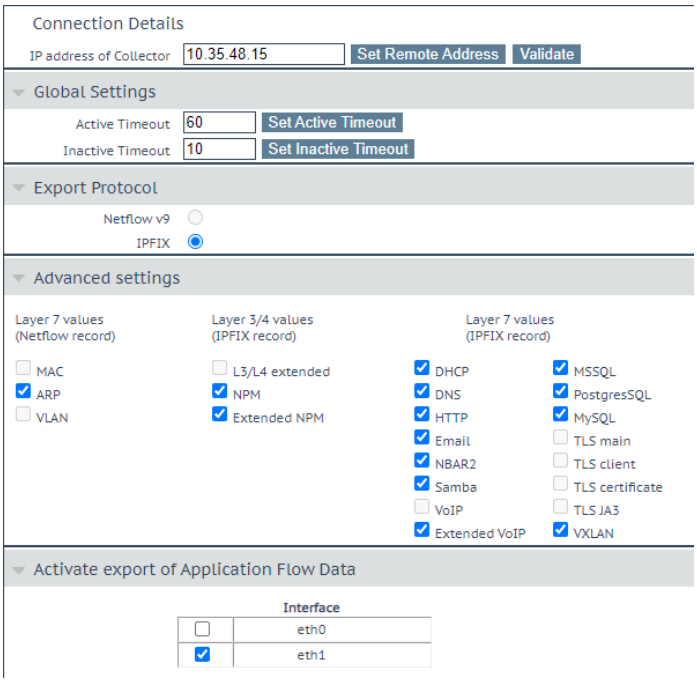


Kemp 360 Central Activation Settings を表示するには、[System Configuration] > [Miscellaneous Options] > [Kemp 360 Central Activation Settings] をクリックします。 LoadMaster がすでに Kemp 360 Central からライセンスされている場合、Kemp 360 Central の IP アドレスとポートがここに表示されます。 空白の場合、このページのコントロールを使用して、ライセンスを要求する Progress Kemp 360 Central 展開の IP アドレスとポートを提供できます。 ここで LoadMaster をアクティブ化すると、自動的に Kemp 360 Central に追加され、システムはすぐに統計の取得を開始できます。 Deactivation ボタンは LoadMaster から現在のライセンスを削除し、LoadMaster をライセンスなしの状態にします。 これにより、LoadMaster へのアクティブなトラフィックが停止するため、細心の注意を払って呼び出す必要があります。 詳細については、Kemp 360 Central 機能の説明を参照してください。

12 ネットワーク テレメトリ



ネットワーク テレメトリには、NetFlow/IPFIX アプリケーション フロー データを収集するための外部コレクタが必要です。 Progress Kemp Flowmon Collector は、ネットワークをキャプチャ、保存、および監視する理想的なネットワーク監視アプライアンスです。
正規化、視覚化、分析などのフロー データを処理します。 Progress Kemp Flowmon Collector をダウンロードするには、[Network Telemetry] 画面で [Download Flowmon Collector] をクリックします。
ネットワーク テレメトリは、ファームウェア バージョン 7.2.53 以降のすべての新しい LoadMaster デプロイメントでデフォルトで利用できます。 Network Telemetry を有効にすると、パフォーマンスのスループットに影響を与える可能性があります。 長期サポート (LTS) の LoadMaster バージョン、または新しいバージョンにパッチが適用された古いバージョンの LoadMaster では、ネットワーク テレメトリ機能を有効にする必要がある場合があります。 ネットワーク テレメトリ機能を有効にするには、LoadMaster WUI のメイン メニューで Network Telemetry [] をクリックし、[Install] をクリックします。



LoadMaster にネットワーク テレメトリを正常にインストールすると、[Network Telemetry] 画面に設定するフィールドがいくつか表示されます。 これらの各オプションの詳細は次のとおりです。

- IP Address of Collector: IPFIX コレクタの宛先 IP アドレスまたは完全修飾ドメイン名 (FQDN) とポート番号を定義します (たとえば、1.1.1.1:2055 または collector.local:3000)。 IPFIX エクスポートは UDP プロトコル上で実行されるため、LoadMaster からネットワーク経由でコレクタに到達できることを確認する必要があります。 コレクタの IP アドレスまたは FQDN を構成したら、[コレクタ] をクリックして [OK] をクリックすることにより、ネットワーク接続を検証できます。 検証はプレーンな ICMP ping メッセージに基づいており、(ポートではなく) IP または FQDN を検証します。 ネットワーク テレメトリは暗号化されていないため、安全なネットワーク経由でのみエクスポートする必要があります。 これは LoadMaster の制限ではありません。これは、IPFIX がプレーン テキストの UDP パケット ストリームであるためです。
- Active Timeout: グローバル アクティブ タイムアウト値を設定します。 デフォルト値は 300 です。
- Inactive Timeout: グローバルな非アクティブ タイムアウト値を設定します。 デフォルト値は 30 です。
- Export Protocol: エクスポート プロトコル (現在、選択可能なプロトコルは IPFIX のみです)。
- Advanced Settings: 収集する値に応じて、ここのチェック ボックスを有効/無効にしま

す。 [Advanced Settings] セクションには、現在変更できないチェック ボックスがいくつかあります。 これらは、将来のリリースで構成可能になります。

- Activate export of Application Flow Data: データを収集する関連するインターフェイス (複数可) を選択します。

ネットワーク インターフェース画面 (たとえば、[System Configuration] > [Network Setup] > [Interface] > [eth0]) は、そのインターフェースに対してネットワーク テレメトリ モニタリングが有効か無効かを示します ([ネットワーク テレメトリ] 画面で選択されているインターフェースによって異なります)。 インターフェイスでネットワーク テレメトリを有効にするには、インターフェイスに IP アドレスが必要です。 仮想 LAN で構成されたインターフェイスでは、IP アドレスが割り当てられていない限り、ネットワーク テレメトリを有効にすることはできません。 2 つの LoadMaster が HA ペアとして動作している場合、ネットワーク テレメトリ トラフィックは、共有アドレスではなく、LoadMaster の物理アドレスから提示されます。 Progress Kemp Flowmon Collector の HA ペアの両方の LoadMaster のプロファイルを作成する必要があります。 ネットワーク テレメトリの詳細については、Progress Kemp ドキュメント ページのネットワーク テレメトリ機能の説明を参照してください。