



ウェブユーザー
インターフェイス
(WUI)
設定ガイド

バージョン : 9.0
更新 : 2016年5月

著作権

Copyright © 2002–2016 KEMP Technologies, Inc. 著作権はKEMP Technologies Inc. が保有しています。 KEMP TechnologiesおよびKEMP Technologiesのロゴは、KEMP Technologies Inc. の登録商標です。

KEMP Technologies Inc. は、ソフトウェアおよびドキュメントを含むロードマスター製品ラインのすべての所有権を保有します。ロードマスターExchangeアプライアンスの使用は、ライセンス契約に従うものとします。このガイドの情報は、事前の予告なしに変更されることがあります。

Microsoft WindowsはMicrosoft Corporationの米国およびその他の国における登録商標です。その他すべての商標とサービスマークはそれぞれの所有者の財産です。

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

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

このソフトウェアの一部（2004年に発行 2006年に修正）は、Frank Denisが著作権を保有しています。2002年の著作権は、Michael Shalayeffがすべての権利を保有し、2003年の著作権は、Ryan McBrideがすべての権利を保有しています。

この部分に関して、ソースおよびバイナリ形式での再配布および使用は、改変の有無にかかわらず、次の条件が満たされていることにより許可されます。

1. ソースコードの再配布は、上記の著作権表示、および本条件と下記免責条項を保持しなければなりません。
2. バイナリ形式で再配布する場合は、上記の著作権表示、本条件、およびドキュメント、または配布時に提供される他の資料に、以下の免責事項を複製して提示する必要があります。

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

本ソフトウェアは、上記の著作権保持者によって“現状有姿”で提供され、明示または黙示の保証を含み、それに限定されない特定の目的に適合するような黙示的な保証は放棄されています。いかなる場合においても、上記の著作権保持者、または貢献者は、損害の可能性について知らされているものも含めて、このソフトウェアの停止によるいかなる直接的、間接的、偶発的、特殊、懲戒的、間接的損害（代替製品やサービスの調達費用、または、これらに限定されない使用不能損失、データ、または利益の損失、または事業の中断による損失）、またはいかなる原因およびその理論による債務、いかなる契約、厳格責任、または不法行為（不注意、またはその他を含む）による損害に対して、何ら責任を負わないものとします。

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

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

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

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

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

（参考訳）

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

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

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

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

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

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

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

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

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

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

いように、その旨を明示しなければなりません。

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

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

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

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

(参考訳)

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

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

目次

1	はじめに.....	10
1.1	ドキュメントの目的.....	10
1.2	対象読者.....	10
2	ホーム.....	11
2.1	一般情報.....	11
2.2	仮想サービスと実サーバーの状態.....	12
2.3	WAFステータス.....	12
2.4	システムメトリックス.....	13
2.5	ライセンス情報.....	13
2.6	その他のリンク.....	14
3	Virtual Services (仮想サービス)	15
3.1	新規追加.....	15
3.2	表示/変更 (既存のHTTPサービス)	15
3.3	Basic Properties.....	18
3.4	Standard Options (標準的なオプション)	19
3.5	SSL Properties (SSLのプロパティ) 画面.....	30
3.6	Advanced Properties (高度なプロパティ)	34
3.7	ウェブアプリケーションファイアウォール (WAF) のオプション.....	42
3.8	エッジセキュリティパック (ESP) のオプション.....	44
3.8.1	SMTP Virtual Services and ESP (SMTPの仮想サービスとESP)	56
3.9	サブ仮想サービス.....	57
3.10	表示/変更 (リモート端末サービス)	60
3.11	Real Servers (実サーバーのアサイン)	61
3.11.1	HTTPまたはHTTPSプロトコルによるヘルスチェック.....	64
3.11.2	バイナリデータによるヘルスチェック.....	68



3.11.3	Add a Real Server (実サーバーの追加)	69
3.11.4	Modify a Real Server (実サーバーの設定変更)	72
3.12	Manage Templates (テンプレートの管理)	73
3.13	Manage SSO Domains (SSOドメインの管理)	74
3.13.1	Single Sign On Domains (SSOドメイン)	75
3.13.2	Single Sign On Image Sets (SSOの画像設定)	84
3.14	WAFの設定	85
4	グローバル負荷分散	88
4.1	Enable/Disable GSLB (GSLBの有効化/無効化)	88
4.2	FQDNの管理	88
4.2.1	Add a FQDN (FQDNの追加)	88
4.2.2	Add/Modify an FQDN (FQDNの追加/変更)	89
4.3	クラスタの管理	94
4.3.1	Add a Cluster (クラスタの追加)	94
4.3.2	Modify a Cluster (クラスタの変更)	95
4.3.3	Delete a Cluster (クラスタの削除)	96
4.3.4	GE0クラスタのアップグレード	96
4.4	その他のパラメータ	97
4.4.1	Source of Authority (権限ソース)	97
4.4.2	リソースチェックのパラメータ	98
4.4.3	Stickiness (持続性)	100
4.4.4	Location Data Update (位置データ更新)	100
4.5	IP範囲の選択条件	100
5	Statistics (統計情報)	103
5.1	実サーバーの統計情報	103
5.1.1	Global (システム統計)	103
5.1.2	実サーバー	105



5.1.3	仮想サービス.....	107
5.1.4	WAF.....	109
5.2	履歴グラフ.....	110
6	SDN統計情報.....	113
6.1.1	デバイス情報.....	114
6.1.2	パス情報.....	116
7	実サーバー.....	119
8	Rules & Checking (ルールとチェック)	120
8.1	コンテンツルール.....	120
8.1.1	Content Matching Rules (コンテンツマッチング用ルール)	120
8.1.2	Content Matching (コンテンツマッチング)	121
8.1.3	Add Header (ヘッダーの追加)	123
8.1.4	Delete Header (ヘッダーの削除)	123
8.1.5	Replace Header (ヘッダーの置換)	124
8.1.6	Modify URL (URLの変更)	125
8.1.7	Header Modification (ヘッダーの変更)	126
8.2	Check Parameters (チェック用パラメータ)	126
8.2.1	Service (Health) Check Parameters (サービス (ヘルス) チェック用パラメータ)	126
8.2.2	アダプティブ負荷分散方式用パラメータ.....	127
8.2.3	SDNのアダプティブ負荷分散方式パラメーター.....	128
9	証明書とセキュリティ.....	130
9.1	SSL Certificates (SSL 証明書)	130
9.1.1	HSMが有効でない場合.....	130
9.1.2	HSMが有効な場合.....	131
9.2	Intermediate Certificates (インターミディエート証明書)	132
9.3	Generate CSR (Certificate Signing Request) (CSR (証明書署名要求) の作成)	132



9.4	Backup/Restore Certificates (証明書のバックアップ/復元)	136
9.4.1	HSMが有効でない場合	136
9.4.2	HSMが有効な場合	137
9.5	Cipher Set (暗号セット)	138
9.6	Remote Access (リモートアクセス)	140
9.6.1	管理者アクセス	140
9.6.2	Geoの設定	146
9.6.3	Geoパートナーのステータス	147
9.6.4	WUI Authentication and Authorization (WUIによる認証と権限設定)	148
9.7	管理用WUIへのアクセス	151
9.8	OCSPの設定	157
9.9	HSMの設定	158
10	System Configuration (システム用設定)	160
10.1	ネットワークの設定	160
10.1.1	Interfaces (インターフェイス)	160
10.1.2	ホストとDNSの設定	167
10.1.3	デフォルト・ゲートウェイ	169
10.1.4	追加ルート	169
10.1.5	Packet Routing Filter (パケット・ルーティング・フィルター)	170
10.1.6	VPN管理	171
10.2	Cluster Control (クラスターの制御)	175
10.2.1	Cluster Parameters (クラスターのパラメーター)	178
10.3	System Administration (システム管理)	179
10.3.1	ユーザの管理	179
10.3.2	Update License (ライセンスの更新)	183
10.3.3	System Reboot (システムリブート)	185
10.3.4	Update Software (ファームウェア更新)	186



10.3.5	Backup/Restore (設定バックアップ／リストア)	188
10.3.6	Date/Time (日付／時間)	190
10.4	Logging Options (ログオプション)	192
10.4.1	System Log Files (システムのログファイル)	193
10.4.2	Extended Log Files (拡張ログファイル)	200
10.4.3	Syslog Options (シスログ・オプション)	203
10.4.4	SNMP Options (SNMP オプション)	204
10.4.5	Email Options (E-Mail オプション)	209
10.4.6	SDN Log Files (SDNログファイル)	212
10.5	Miscellaneous Options (その他のオプション)	215
10.5.1	WUI Settings (WUIの設定)	215
10.5.2	レイヤ7設定	217
10.5.3	Network Options (ネットワーク関連オプション設定) ネットワークオプション	223
10.5.4	AFE Configuration (アプリケーション・フロント・エンド機能設定) OCSPの設定	227
10.5.5	HAのパラメータ	229
10.5.6	AzureのHAパラメータ	234
10.5.7	AWSのHAパラメーター	235
10.5.8	SDNの設定	237
参考ドキュメント		239
Document History		242



1 はじめに

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

1.1 ドキュメントの目的

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

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

1.2 対象読者

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

2 ホーム

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

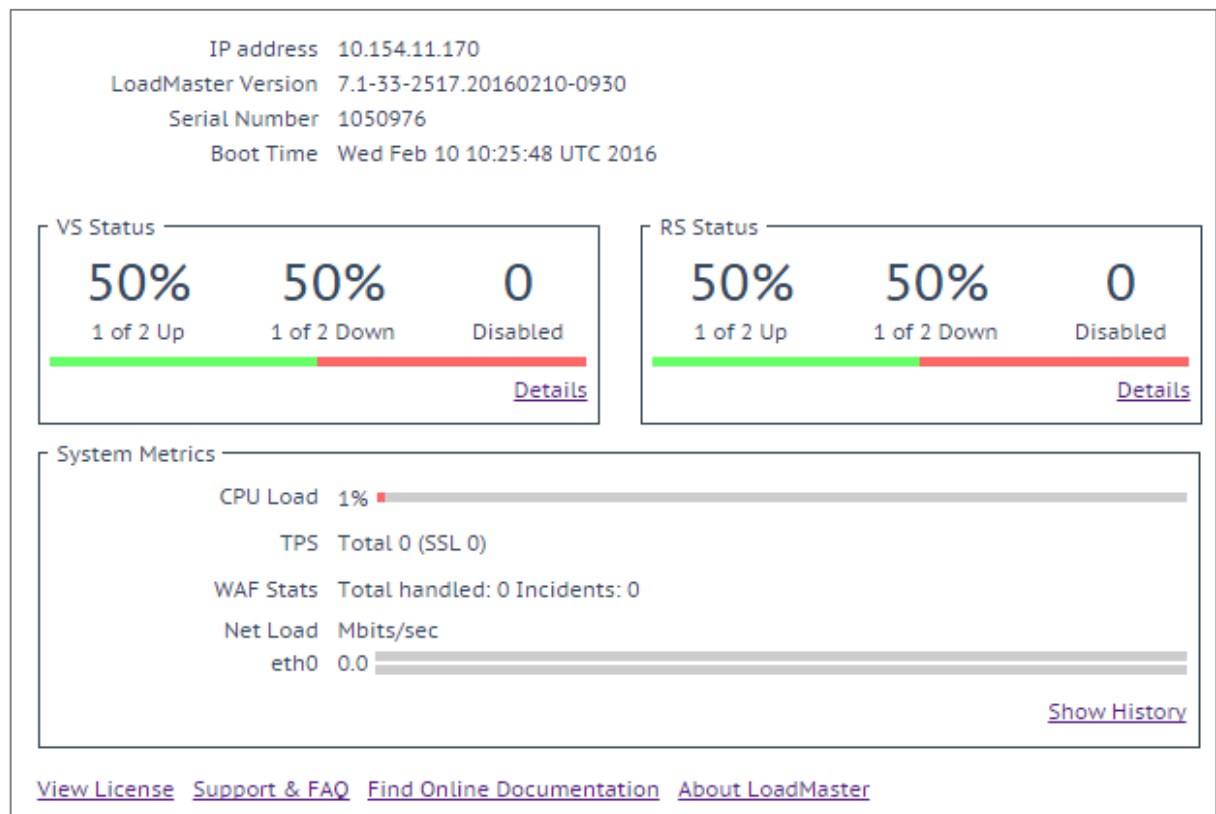


図2-1: ロードマスターのホーム画面

2.1 一般情報

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

IP address (IPアドレス) : ロードマスターのIPアドレス

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

LoadMaster

System Status

New LoadMaster v7.1-24b is now available.For more information and downloads link visit the KEMP Support Center.

図 2-2:新しいソフトウェアが利用可能

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

Serial Number（シリアル番号）：ロードマスターのシリアル番号

Boot Time（ブート時刻）：サーバーを最後にリブートした時刻

2.2仮想サービスと実サーバーの状態

VS Status（VSステータス）

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

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

RS Status（RSステータス）

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

2.3WAFステータス

WAF Status

41

Total Requests
Handled

41

Total Events

41

Events this Hour

41

Events Today

0

Events over
Limit Today

図 2-3:WAFステータス



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

- WAFにより処理されたトータルの要求数（ブロックされたかどうかにかかわらず、すべての要求が表示されます）。各接続につき2つの要求が記録されます（1つは受信要求、1つは送信要求）。
- WAFにより処理されたトータルのイベント数（ブロックされた要求）
- 現在の時間内（xx. 00. 00以降）に発生したイベントの数
- 真夜中（ローカル時刻）以降に発生したイベントの数
- 1日のうちに、設定された警報しきい値をイベントカウンターが越えた回数例えば、しきい値が10に設定されており、20個のイベントが発生した場合、このカウンターは2に設定されます。警報しきい値は、仮想サービス編集画面の“WAF Options”にある“Hourly Alert Notification Threshold”フィールドに入力することで、仮想サービスごとに設定できます。詳細はセクション3.7を参照してください。

2.4 システムメトリックス

CPU Load (CPU負荷)： ロードマスター機器のCPU負荷率

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

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

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

CPU負荷とネット負荷のデータは5秒ごとに更新されます。

2.5 ライセンス情報

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

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

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



2.6 その他のリンク

ホームページの下部に、その他のリンクが用意されています。

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



3 Virtual Services (仮想サービス)

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

3.1 新規追加

Please Specify the Parameters for the Virtual Service.

Virtual Address

10.11.0.194

Port

443

Service Name (Optional)

Exchange 2013 HTTPS

Protocol

tcp ▾

図 3-1: 仮想サービスの新規追加画面

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

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

テンプレートの詳細については、

仮想サービスとテンプレート機能説明ドキュメントを参照してください。

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

3.2 表示/変更 (既存のHTTPサービス)

Add New							
Virtual IP Address	Prot	Name	Layer	Certificate Installed	Status	Real Servers	Operation
10.154.201.8:80	tcp		L7		● Up	10.154.201.2 10.154.201.3 10.154.201.4 10.154.201.5	Modify Delete

図 3-2: 仮想サービスの画面



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

注意

削除すると元に戻すことはできません。注意して使用してください。

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

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

仮想サービスのステータスは、次のいずれかになります。

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



ータスがWAF Misconfiguredに変わり、赤の表示になります。仮想サービスがこの状態にあるとき、すべてのトラフィックがブロックされます。トラブルシューティングの際は、必要に応じてその仮想サービスのAFPを無効にし、トラフィックがブロックされないようにすることが可能です。

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

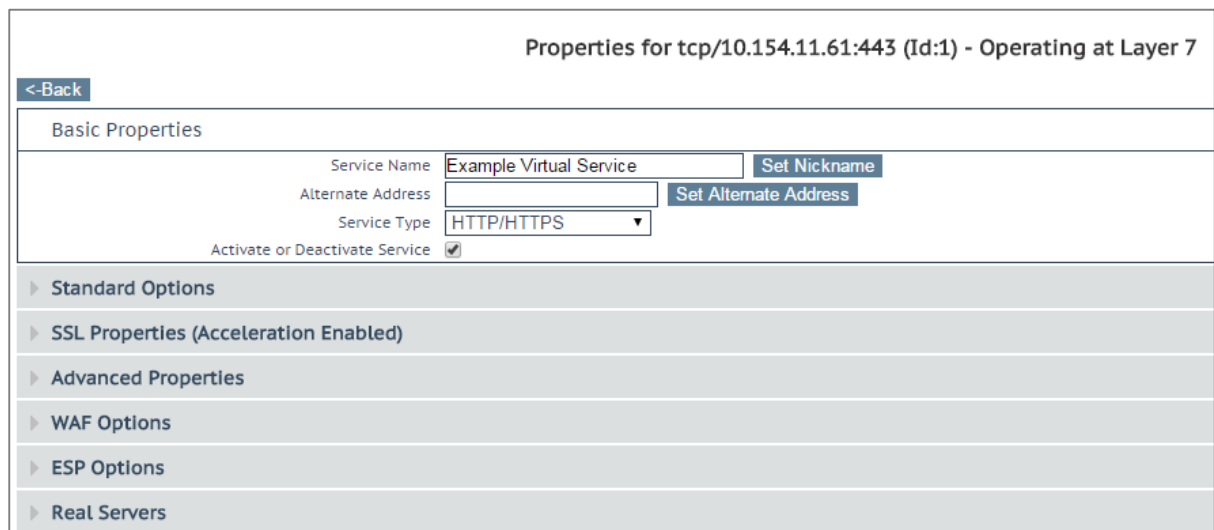


図 3-3: 仮想サービスのプロパティの画面

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

特定のフィールドとオプションは、サービスタイプ、および機能の有効化または無効化に応じてWUIでの非表示/表示が切り替わります。

す。したがって、このドキュメントのスクリーンショットは、すべての構成を網羅していない可能性があります。

3.3 Basic Properties

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

Duplicate VIP (VIPのコピー)

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

Change Address (アドレスの変更)

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

Export Template (テンプレートのエクスポート)

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

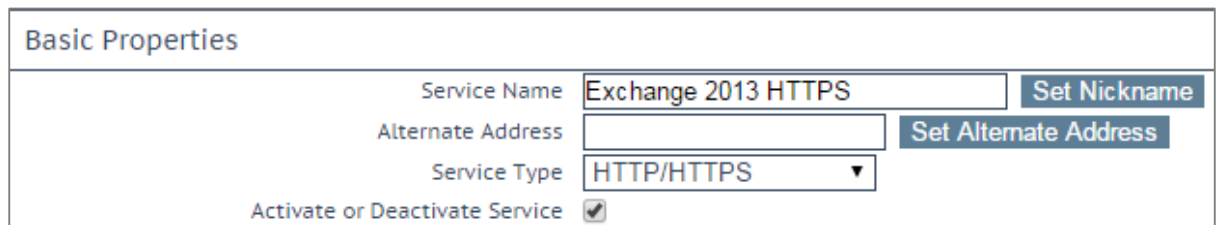


図 3-4: Basic Propertiesセクション

Service Name

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

サービス名には、通常の英数字のほかに、以下の「特殊」文字が使用できます。

. @ - _



ただし、特殊文字の前に1つ以上の英数字がなければなりません。

Alternate Address

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

Service Type (サービスタイプ)

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

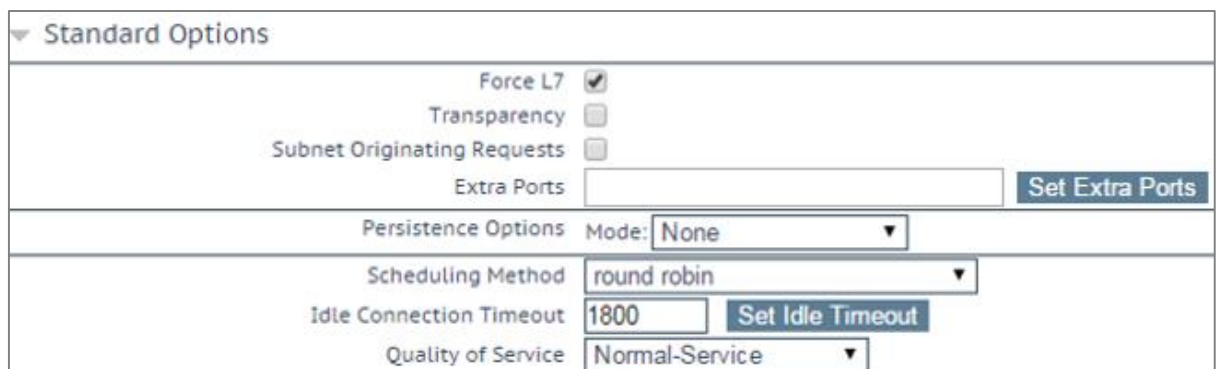
WebSocket仮想サービスは“Generic”サービスタイプに設定する必要があります。

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

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

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

3.4 Standard Options (標準的なオプション)



▼ Standard Options	
Force L7	☒
Transparency	☐
Subnet Originating Requests	☐
Extra Ports	<button>Set Extra Ports</button>
Persistence Options	Mode: None
Scheduling Method	round robin
Idle Connection Timeout	1800 <button>Set Idle Timeout</button>
Quality of Service	Normal-Service

図 3-5: Standard Optionsセクション

Force L7 (L7を強制)

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



L7 Transparency (レイヤ7透過モード)

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

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

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

このオプションは“Transparency”が無効のときのみ利用できます。

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

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

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

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

グローバルオプションが無効の場合、仮想サービスごとに制御できます。

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



Extra Ports (追加のポート)

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

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

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

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

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

以下のプロトコルの選択が可能です。

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

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

Persistence Options (パーシステンスオプション)

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



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

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

- **Source IP Address (ソースIPアドレス・パーシステンス)**

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

- **Super HTTP (スーパーHTTP)**

ロードマスターを使用してHTTPおよびHTTPSのパーシステンスを実現する手法として、スーパーHTTPを推奨します。これは、クライアントブラウザの一意のフィンガープリントを作成し、そのフィンガープリントを使用して適切な実サーバーとの接続を維持します。このフィンガープリントは、“User-Agent” フィールドの値（および利用可能であれば“Authorization” ヘッダーの値）を組み合わせで作成されます。同じヘッダーの組み合わせを持つ接続では、同じ実サーバーにデータが返送されます。

- **Server Cookie (サーバー・クッキー)**

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

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

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

- **Active Cookie (アクティブクッキー)**

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



別することができます。この手法には、サーバーがクッキーの管理または生成を行う必要がなく、サーバー設定の負担が軽くなるというメリットがあります。クライアント接続ごとにより効果的に負荷を分散させるには、“L7 Configuration”の“Add Port to Active Cookie”を有効にします。このオプションについての詳細は、セクション10.5.2を参照してください。

アクティブクッキーパーシステンスを使用すると、そのクッキーは、セッションが継続している間またはパーシステンスがタイムアウトするまで有効になります。例えば、パーシステンスタイムアウトが10分に設定されたアクティブクッキーパーシステンスを使用しており、クライアントが午後2時に接続したとすると、午後2時5分に切断と再接続が行われます。このとき、パーシステンスタイムアウト値がリセットされます。パーシステンスがタイムアウトした後にクライアントが仮想サービスへの接続を試みた場合、そのクライアントには古いクッキーが提示されます。ロードマスターはパーシステンステーブルをチェックし、有効なエントリが含まれていないことを確認します。すると、ロードマスターは、そのクライアント用に新しいクッキーを生成し、パーシステンステーブルを更新します。

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

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

- **Hash All Cookies (ハッシュ全クッキー)**

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

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

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

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

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



- **URL Hash (URLハッシュ)**

同じURLへのリクエストは、同じサーバーへと転送します。

- **HTTP Host Header (HTTPホストヘッダー)**

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

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

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

- **Selected Header (指定ヘッダー)**

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

- **SSL Session ID (SSLセッションID)**

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

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

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

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

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

- **UDP Session Initiation Protocol (SIP) (UDPセッション開始プロトコル (SIP))**



このパーシステンスモードは、“Force L7”が有効になっているときにUDP仮想サービスでのみ利用可能です。SIPは、HTTPと同様のリクエスト/レスポンスランザクションを使用します。最初のINVITEリクエストが送信されますが、このリクエストにはヘッダーフィールドの数が含まれています。このヘッダーフィールドはパーシステンスで使用可能です。

Timeout (タイムアウト)

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

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

Note: Persistence
Timeout is set to 10 minutes in this example

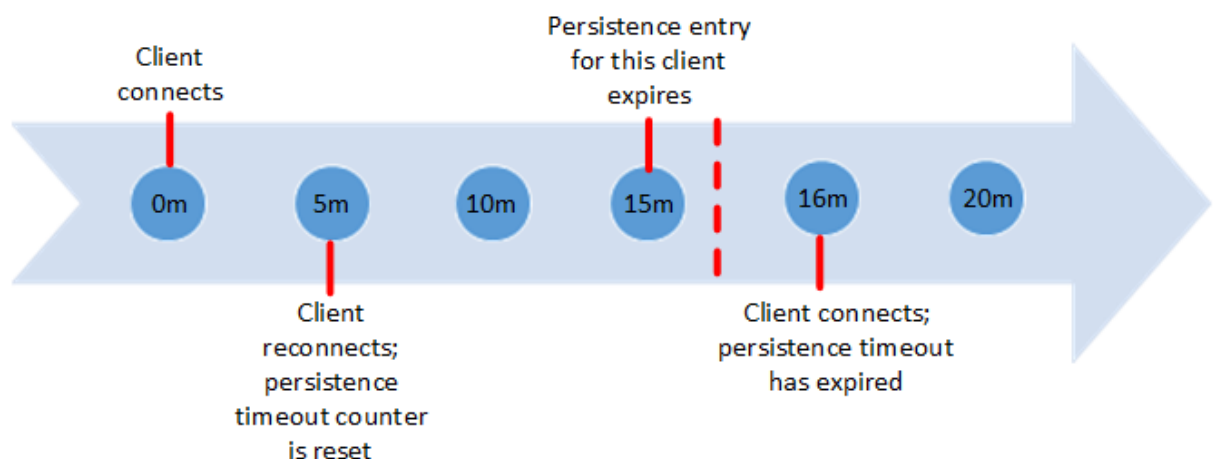


図 3-6: パーシステンスタイムアウトの例

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

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

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

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

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

Header field name (ヘッダーフィールド名)

LoadMasterにおいて、パーシステンスモードとして“UDP Session Initiation Protocol”が選択されている場合、“Header field name”というテキストボックスが表示されます。パーシステンス情報のもととなるヘッダーフィールドをここで入力してください。

Scheduling Methods (負荷分散方式)

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

- Round Robin (ラウンドロビン)

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



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

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

- **Least Connection (最小接続)**

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

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

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

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

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

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

アダプティブスケジューリング方式を使用している仮想サービスは、(SDNを使用しているかどうかにかかわらず) 制御システムとして見えます。これは、実サーバー間で負荷を均等に配分し、コントローラーがそれをもとに誤差を計算するようにするためです(この値は、目的とする負荷均等配分からのずれを表します)。またコントローラーは、誤差が小さくなるようにシステムにフィードバックされる一連の制御値(実サーバーの重み)も計算します。

- **Fixed Weighting (固定重み)**

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

- **Weighted Response Time (加重応答時間)**

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

- **Source IP Hash (ソースIPハッシュ)**



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

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

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

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

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

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

Quality of Service（サービス品質）

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

各オプションについて、以下で説明します。

- **Normal-Service（通常サービス）**：特別な優先順位をトラフィックに割り当てない。



- **Minimize-Cost (コスト最小化)** : 低コストのリンクでデータを転送する必要がある場合に使用。
- **Maximize-Reliability (信頼性最大化)** : 信頼性のあるリンクでデータを宛先に転送して、再転送がほとんど発生しないようにする場合に使用。
- **Maximize-Throughput (スループット最大化)** : リンクの遅延が大きい場合でも、インターバル中に転送されるデータ量が重視される場合に使用。
- **Minimize-Delay (遅延最小化)** : パケットが宛先に到達するまでの所要時間 (遅延) を抑制する必要がある場合に使用。このオプションは、“Quality of Service”の各オプションで、最も待ち時間が短くなります。

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

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

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

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

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

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



3.5 SSL Properties (SSLのプロパティ) 画面

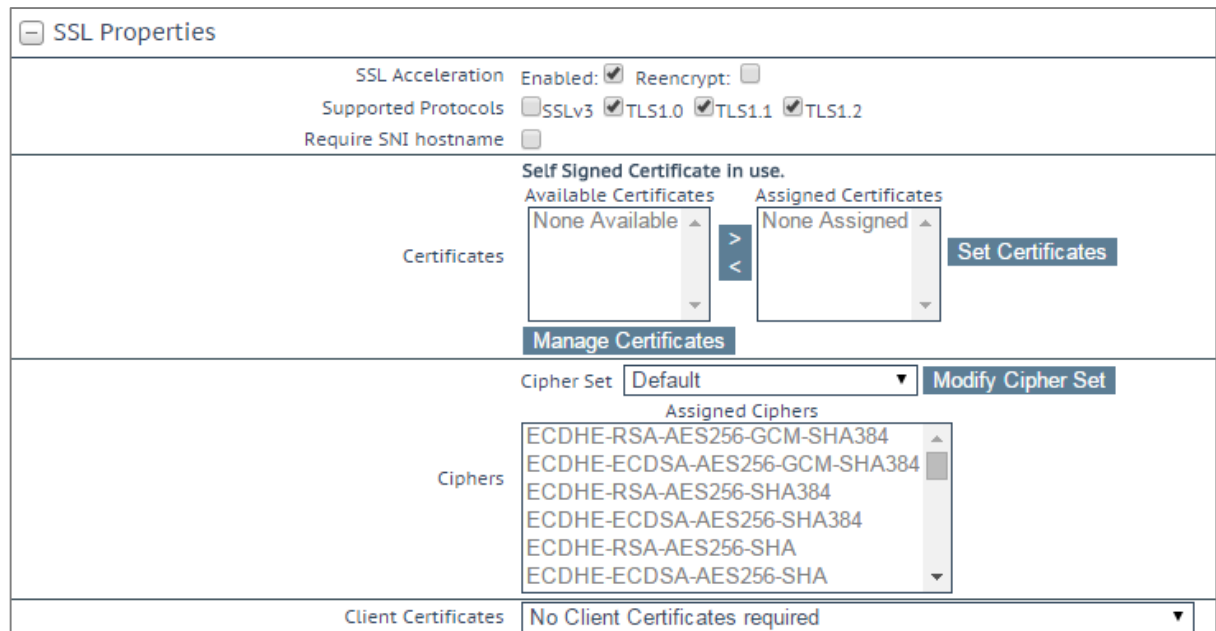


図 3-7: SSLプロパティのセクション

SSL Acceleration (SSLアクセラレーション)

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

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

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

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

Supported Protocols (サポートするプロトコル)



“Supported Protocols” (サポートするプロトコル) セクションにあるチェックボックスを使用すると、仮想サービスでサポートされるプロトコルを指定することができます。デフォルトでは、3つのTLSプロトコルが有効になっており、SSLv3が無効になっています。

Require SNI hostname (SNIホスト名必要)

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

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

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

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

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

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

Certificates (証明書)

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



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

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

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

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

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

このフィールドはSSLの再暗号化が有効な場合のみ表示されます。

Cipher Set (暗号セット)

暗号化方式とは、暗号化/復号化を行うアルゴリズムのことです。

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

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

Ciphers

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



Client Certificates (クライアント証明書)

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

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

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

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

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



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

このオプションはESPが有効な場合のみ表示されます。

3.6 Advanced Properties (高度なプロパティ)

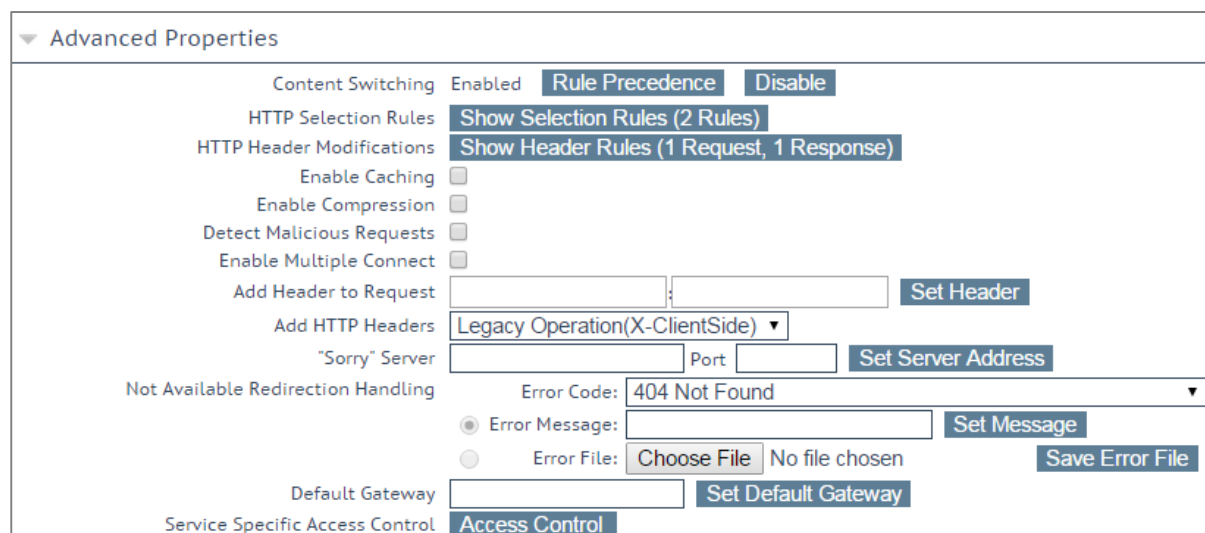


図 3-8: Advanced Properties セクション

Content Switching (コンテンツスイッチ)

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

Rules Precedence (ルールの優先順位)

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

<Back

Rules assigned to Virtual Service tcp/10.154.11.61:443 (Id:1)

Operation Name	Match Type	Options	Header	Pattern
KEMPTest1	RegEx		Test	Test
Promote KEMPTest2	RegEx		Testing	Testing

図 3-9: 要求ルール

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

HTTP Selection Rules (HTTP選択ルール)

仮想サービスに割り当てられている選択ルールを表示します。

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

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

<Back

Modification Rules assigned to tcp/10.154.11.61:443 (Id:1)

Request Rules

Name	Rule Type	Options	Header	Pattern	Replacement	Operation
KEMPHeader1	Add Header		Test		Test	Delete
KEMPHeader3	Replace Header		Testing	Testing	Tested	Promote Delete

Add Rule

Rule:

Delete Header: KEMPHeader2

Add

Response Rules

Name	Rule Type	Options	Header	Pattern	Replacement	Operation
KEMPHeader1	Add Header		Test		Test	Delete

Add Rule

Rule:

Replace Header: KEMPHeader3

Add

図 3-10: 変更ルール

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



ロードマスターシリーズ リリースノート (Ver 7.1.34.1)

Copyright © 2002 – 2016 KEMP Technologies, Inc. All Rights Reserved.

35

Enable Caching (キャッシング有効化)

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

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

Maximum Cache Usage (最大使用キャッシュ)

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

Enable Compression (圧縮の有効化)

ロードマスターから送られたファイルはGzipで圧縮されます。

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

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

サイズが100MB以上のファイルは圧縮しないようにしてください。



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

Detect Malicious Requests (IDS機能の追加)

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

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

“Detect Malicious Requests”チェックボックスをオンにすると、HTTPおよびオフロードされたHTTPS仮想サービスごとにIPSが有効になります。“SNORT” ルールにマッチしたリクエストの扱いには、2つのオプションがあります。すなわち、“Drop Connection” (一致するルールによりHTTPレスポンスは生成されない)、または“Send Reject” (一致するルールによりクライアントへのHTTP 400 “Invalid Request” 応答が生成される) のいずれかを選択できます。どちらのオプションを選択した場合も、リクエストは実サーバーに到達しません。

Enable Multiple Connect (複数の接続を有効にする)

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

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

Port Following (ポートフォローイング)



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

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

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

サブVS上ではポートフォローウィングは利用できません。

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

Add Header to Request (リクエストにヘッダーを追加)

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

この機能を使用するには、“Set Header” ボタンをクリックします。

Add HTTP Headers (HTTPヘッダーの追加)

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

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

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



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

Sorry Server (Sorryサーバー)

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

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

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

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

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

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

- **Error Code (エラーコード)** : 実サーバーが利用できない場合、ロードマスターはHTTPエラーコードに従って接続を終端できます。適切なエラーコードを選択してください。
- **Redirect URL (リダイレクトするURL)** : 実サーバーが利用できず、クライアントにエラーレスポンスを返す必要がある場合、リダイレクトするURLを指定できます。このテキストボックスに文字列を入力する場合、http://またはhttps://を含めないでください。or https://この文字列は現在の場所からの相対位置として扱われます。そのため、リダイレクト時にホスト名がこの文字列に追加されま



す。このフィールドでは、要求されたホスト名を表す“%h”や、ユニフォームリソースアイデンティファイヤー (URI) を表す“%s”などのワイルドカードも使用できます。

- **Error Message (エラーメッセージ)** : 実サーバーが利用できない場合に、エラーレスポンスをクライアントに返すとき、指定したエラーメッセージがそのレスポンスに追加されます。

セキュリティ上の理由から、“Document has moved”の文字だけを含むHTMLページが返送されます（要求に含まれる情報は返送されません）。要求により提供された情報は返されません。

- **Error File (エラーファイル)** : 実サーバーが利用できない場合に、エラーレスポンスをクライアントに返すとき、指定したファイルがそのレスポンスに追加されます。これにより、指定したエラーに対するレスポンスとして、簡単なエラー情報を含むHTMLページを送信できます。

エラーページの最大サイズは16KBです。

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

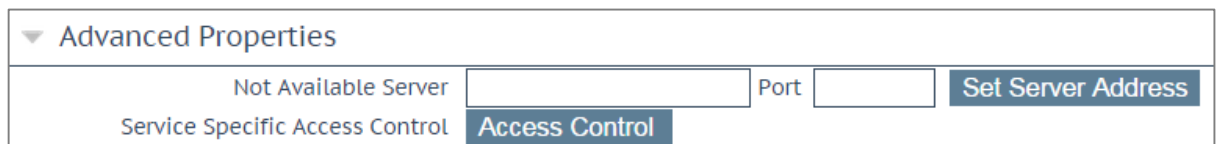


図 3-11: Not Available Server (利用不可時のサーバー)

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

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

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

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

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



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

Default Gateway (デフォルト・ゲートウェイ)

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

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

“System Configuration > Miscellaneous Options > Network Options”にてグローバルの“Use Default Route Only”（デフォルトルートのみ使用）オプションが設定されている場合、“Default Gateway”（デフォルトゲートウェイ）が設定されている仮想サービスからのトラフィックのみ、仮想サービスのデフォルトルートが設定されているインターフェイスに転送されます。これにより、隣接するインターフェイスを使用してトラフィックを直接返送することなく、ロードマスターをクライアントネットワークに直接接続できます。

Alternate Source Addresses (代替ソースアドレス)

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

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

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

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



仮想サービス固有のアクセス・コントロール・リストを変更できます。

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

3.7ウェブアプリケーションファイアウォール (WAF) のオプション

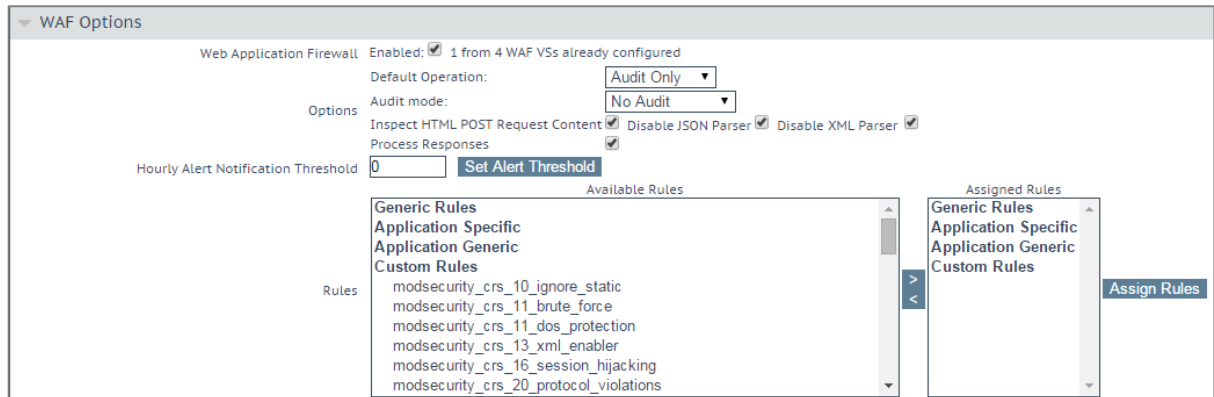


図 3-12:WAFのオプション

これらのオプションを設定する前に、WAF機能を有効にする必要があります。

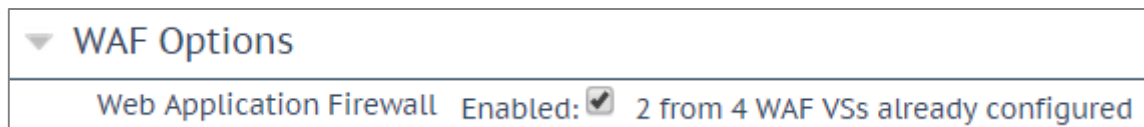


図 3-13:WAFの有効化

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

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

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

は1GBとなっています。このデフォルトの割り当てを変更していない場合は、AFPの設定を行う前に、メモリの設定を変更してください。

Default Operation (デフォルト動作)

WAFのデフォルト動作を選択します。

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

Audit mode (監査モード)

どのログを記録するかを選択します。

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

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

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

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

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

Disable JSON Parser (JSONパーサーを無効にする)

JavaScriptオブジェクト表記法 (JSON) リクエストの処理を無効にします。



Disable XML Parser (XMLパーサーを無効にする)

XMLリクエストの処理を無効にします。

Process Responses (応答を処理する)

このオプションを有効にすると、実サーバーからの応答が検証されます。

このオプションはCPUとメモリを著しく消費します。

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

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

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

Rules (ルール)

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

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

3.8 エッジセキュリティパック (ESP) のオプション

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



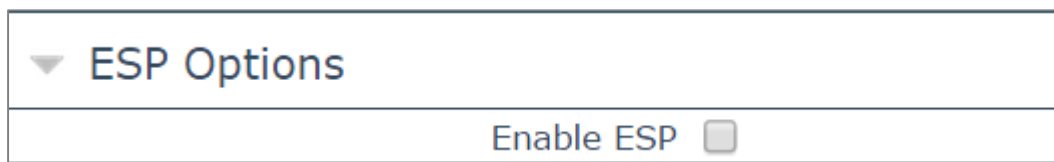


図 3-14:SPオプションの選択

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

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

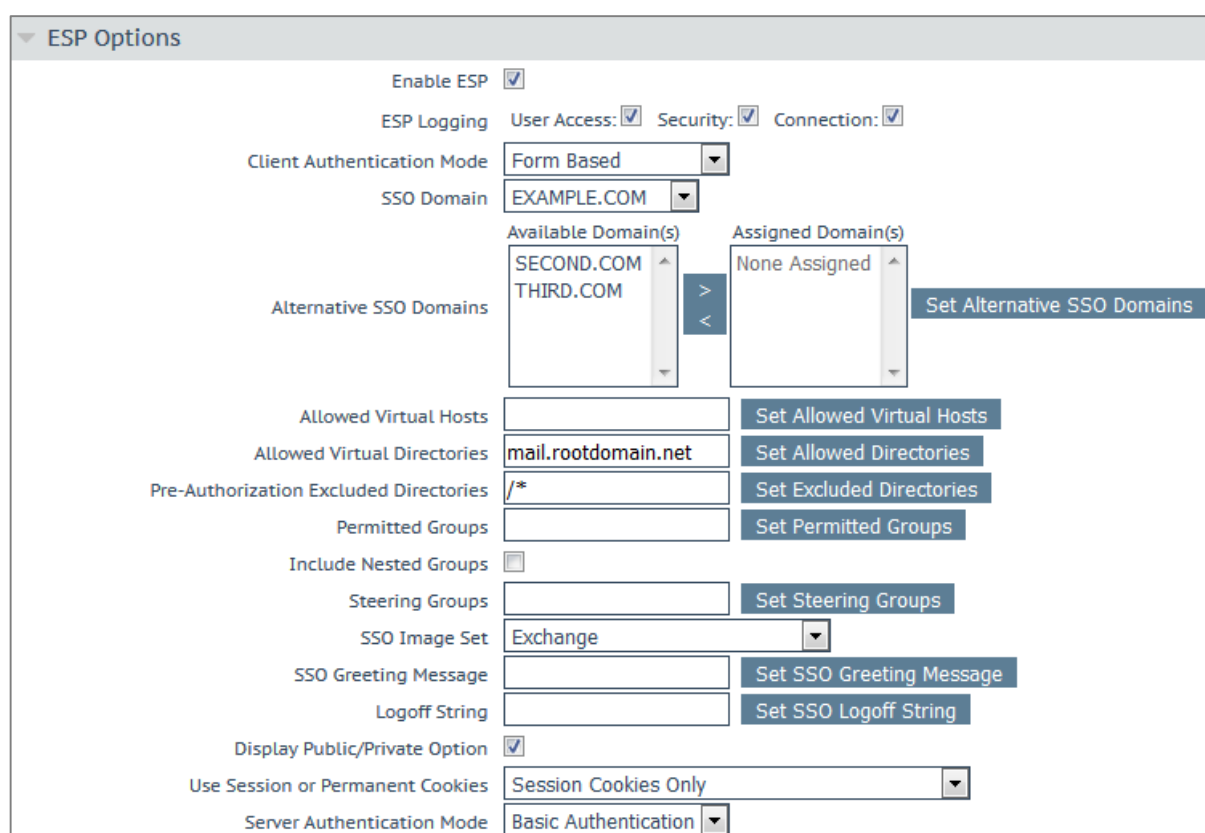


図 3-15:ESPオプション

Enable ESP (ESPの有効化)

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

ESP Logging (ESPのログ作成)



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

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

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

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

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

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

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

SSO Domain (SSOドメイン)

仮想サービスが属するシングルサインオン (SSO) ドメインを選択します。

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

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



Alternative SSO Domains (代替SSOドメイン)

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

このオプションは、複数のドメインが設定されている場合のみ表示されます。

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

現在、このオプションは、“Authentication Protocols” (認証プロトコル) が以下のプロトコルに設定されているドメインで利用できます。

- LDAP
- RSA-SecurID
- Certificates (証明書)

▼ SSL Properties	
SSL Acceleration	Enabled: ☒ Reencrypt: ☒
Supported Protocols	☐ SSLv3 ☒ TLS1.0 ☒ TLS1.1 ☒ TLS1.2
Require SNI hostname	☐

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

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

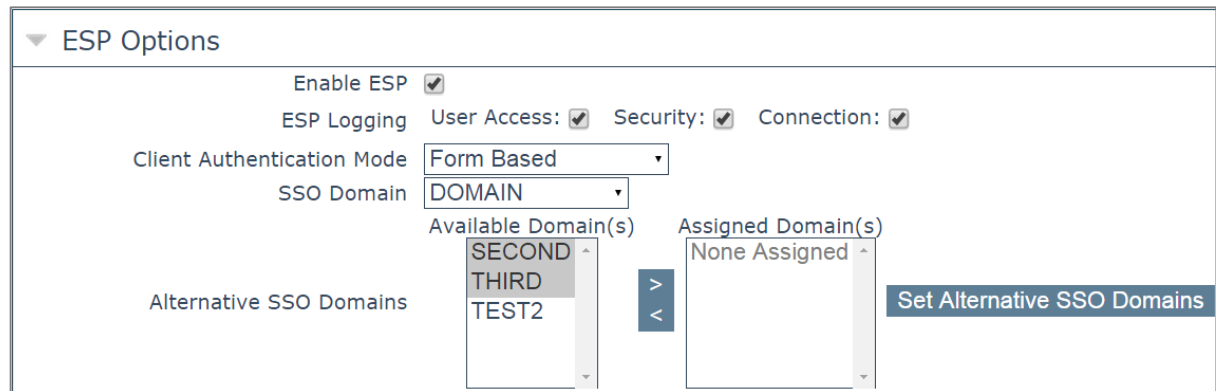


図 3-17: 利用可能なドメイン

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

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

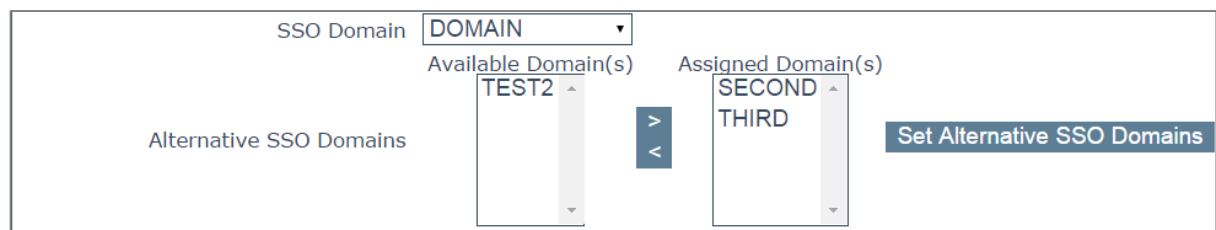


図 3-18: 仮想サービスに割り当てられた代替ドメイン (2次および3次ドメイン)

代替ドメインを割り当てるには以下のようにします。

1. 割り当てたいドメインを反転表示させ、“>”ボタンをクリックします。

割り当てられたドメインは、特定の仮想サービスを使用して認証できます。

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

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

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

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

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

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

Allowed Virtual Hosts (許可された仮想ホスト)

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

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

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

このフィールドでは正規表現を使用できます。

このフィールドが空欄の場合、仮想サービスはブロックされます。

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

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

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

このフィールドでは正規表現を使用できます。



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

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

Permitted Groups (許可グループ)

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

このフィールドに関するガイドラインを以下に示します。

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

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

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

Include Nested Groups (ネストされたグループを含める)

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



SSO Image Set (SSOの画像設定)

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

- Exchange フォーム

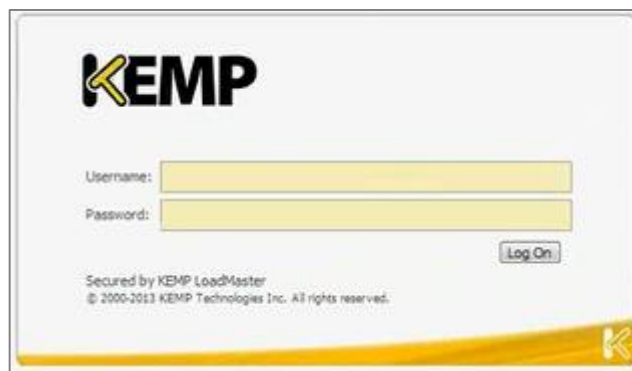


図 3-19: Exchange フォーム

“Exchange Form” にはKEMPのロゴが表示されます。

- ブランクフォーム



図 3-20: ブランクフォーム

“Blank Form” にはKEMPのロゴは表示されません。

- 2要素認証



The image shows a screenshot of the KEMP WUI login interface. At the top is the KEMP logo. Below it is the text "Welcome to DFA ESP Testing!". There are two radio buttons: the first is unselected and labeled "This is a public or shared computer", the second is selected and labeled "This is a private computer". Under the heading "Remote Credentials", there are input fields for "Username:" and "Passcode:". Under the heading "Internal Credentials", there are input fields for "Internal Username:" and "Internal Password:". A "Log On" button is located to the right of the "Internal Password" field. At the bottom, it says "Secured by KEMP LoadMaster" and "© 2000-2015 KEMP Technologies Inc. All rights reserved.". A small KEMP logo is in the bottom right corner of the form area.

図 3-21:2要素認証フォーム

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

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

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

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

SSO Greeting Message (SSOのあいさつメッセージ)



ロードマスターシリーズ リリースノート (Ver 7.1.34.1)

Copyright © 2002 - 2016 KEMP Technologies, Inc. All Rights Reserved.

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

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

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

Logoff String (ログオフ文字列)

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

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

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





The screenshot shows the KEMP login interface. At the top is the KEMP logo. Below it, the text "Please enter your Exchange credentials." is displayed. There are two radio buttons: "This is a public or shared computer" (selected) and "This is a private computer". Below these are two text input fields labeled "Username:" and "Password:". A "Log On" button is located to the right of the password field. At the bottom, it says "Secured by KEMP LoadMaster" and "© 2000-2014 KEMP Technologies Inc. All rights reserved." There is a small KEMP logo in the bottom right corner of the form area.

図 3-22:パブリック/プライベートオプション

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

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

このフィールドでは3つのオプションを選択できます。

- **Session Cookies Only (セッションクッキーのみ使用)** :これはデフォルトの設定です。最も安全なオプションです。
- **Permanent Cookies only on Private Computers (プライベートコンピューターでのみパーマネントクッキーを使用)** :パブリックコンピューターにセッションクッキーを送信します。
- **Permanent Cookies Always (常にパーマネントクッキーを使用)** :すべての状況においてパーマネントクッキーを送信します。

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



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

Server Authentication Mode (サーバー認証モード)

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

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

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

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

Server Side configuration (サーバー側設定)

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

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

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

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





図 3-23:ESPオプション

Enable ESP (ESPの有効化)

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

Connection Logging (接続ログ)

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

Permitted Domains (許可ドメイン)

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

3.9サブ仮想サービス

仮想サービス内に“サブ仮想サービス”（サブVS）を作成できます。サブVSは、親仮想サービスにリンクされ、親仮想サービスのIPアドレスを使用します。サブVSには、その親の仮想サービスや別のサブVSと異なる設定（ヘルスチェック方式やコンテンツルールなど）を保持できます。これにより、関連性のある仮想サービスを、同じIPアドレスでグループ化することが可能となります。これは、ExchangeやLyncのように、多くの仮想サービスからなる構成で有効です。

仮想サービスの権限を持つユーザーは、サブVSを追加できます。

実サーバーの権限を持つユーザーは、サブVSを追加できません。

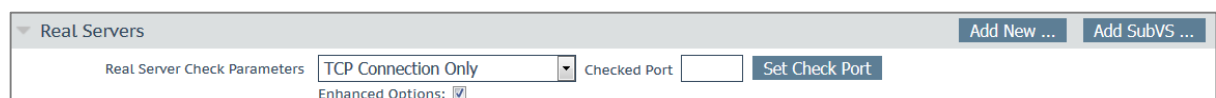


図 3-24:実サーバーのセクション



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

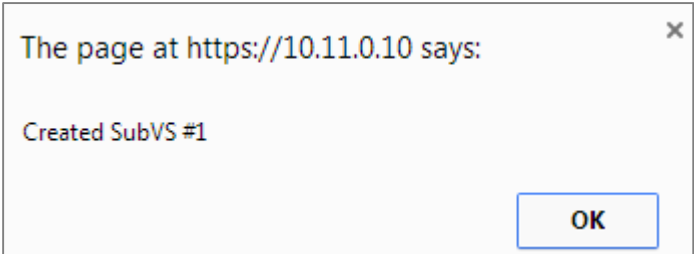


図 3-25:SubVSの作成

すると、サブVSが作成されたことを示すメッセージが表示されます。

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

▼ SubVSs						Add New ...		
Id	Name	Weight	Limit	Critical	Status	Operation		
1		1	1	☐	Enabled	Disable	Modify	Delete
2		1000	0	☐	Enabled	Disable	Modify	Delete

図 3-26:SubVSセクション

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

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

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

Basic Properties	
SubVS Name	Set Nickname
SubVS Type	HTTP/HTTPS v
SubVS Weight	1000 Set Weight
SubVS Limit	0 Set Limit
▼ Standard Options	
Transparency	☒
Persistence Options	Mode: None v
Scheduling Method	round robin v
Idle Connection Timeout (Default 660)	Set Idle Timeout
Quality of Service	Normal-Service v
▼ Advanced Properties	
Content Switching	Disabled
HTTP Selection Rules	Show Selection Rules
HTTP Header Modifications	Show Header Rules
Enable Multiple Connect	☐
Add Header to Request	Set Header
Add HTTP Headers	Legacy Operation(X-ClientSide) v
"Sorry" Server	Port Set Server Address
Not Available Redirection Handling	Error Code: v
	Redirect URL: Set Redirect URL
▼ WAF Options	
Web Application Firewall	Enabled: ☐
▼ ESP Options	
Enable ESP	☐
▼ Real Servers	
Real Server Check Parameters	HTTP Protocol v Checked Port Set Check Port
URL:	Set URL
Use HTTP/1.1:	☐
HTTP Method:	HEAD v
Custom Headers:	Show Headers

図 3-27: SubVS編集画面のセクション

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

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

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

3.10 表示/変更 (リモート端末サービス)

このセクションは、ロードマスターExchangeでは関係ありません。

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

Persistence (パーシステンス)

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

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

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

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

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

“ICMP”、“TCP”、“RDP”の3つのオプションのみ利用できます。リモート端末プロトコル (RDP) は、実サーバーのサービスポート (ポート3389) に対してTCP接続を開きます。ロードマスターは、サーバーにコード1110 (接続要求) を送信します。サーバーからコード1110 (接続確認) が送信されると、ロードマスターは、接続を閉じてそのサーバーがアクティブであるとしてマーキングします。設定された回数だけ接続を要求しても、



設定された応答時間内にサーバーから応答が返されなかった場合、または、他のステータスコードが返された場合、そのサーバーは動作していないとみなされます。

3.11 Real Servers (実サーバーのアサイン)

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

Real Server Check Parameters (実サーバー・チェック用パラメータ)

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

Real Servers

Add New ...

Real Server Check Parameters

TCP Connection Only

Checked Port

Set Check Port

Enhanced Options: ☒ Minimum number of RS required for VS to be considered up

2

Id	IP Address	Port	Forwarding method	Weight	Limit	Critical	Status	Operation
1	10.154.11.18	80	nat	1000	0	☐	Enabled	Disable Modify Delete
2	10.154.11.19	80	nat	1000	1000	☐	Enabled	Disable Modify Delete

図 3-28:実サーバー

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

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

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

方式	アクション
ICMP Ping:	Pingを実サーバーへ送信します
HTTP	HTTP GET/HEADリクエストを送信します



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

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

方式	アクション
ICMP Ping:	Pingを実サーバーへ送信します
TCP	TCP接続を試みます
Remote Terminal Protocol (リモートターミナルプロトコル)	実サーバーにRDPのルーティングトークンが渡されます。 このヘルスチェックでは、ネットワークレベルの認証が可能です。
None (なし)	ヘルスチェックを行いません



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

Enhanced Options (拡張オプション)

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

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

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

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

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

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

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

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

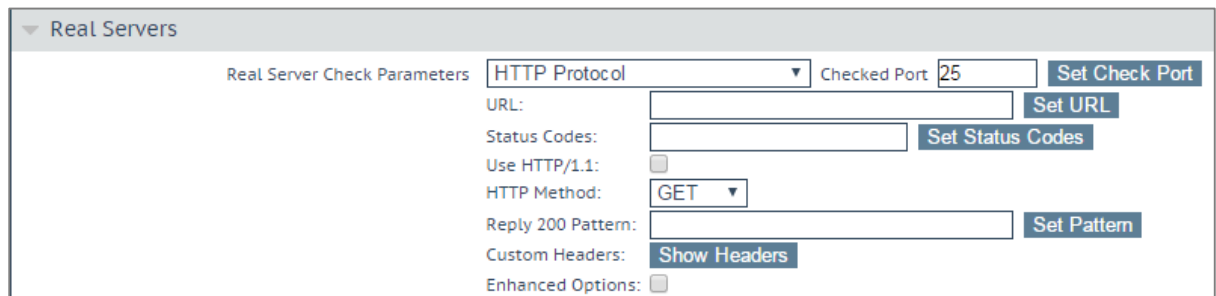


サブVSにてコンテキストルールを使用する場合、必要な実サーバーの最小数が持つ意味は少し異なります。ルールが割り当てられている利用可能な実サーバーの数が下限値以上の場合のみ、そのルールが利用可能とみなされて照合することができます。利用可能な実サーバーの数が下限を下回ると、そのルールは照合されません。そのサブVSは停止中とマークされ、その旨がログに記録されます。

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

3.11.1 HTTPまたはHTTPSプロトコルによるヘルスチェック

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



The screenshot shows the 'Real Servers' configuration section. Under 'Real Server Check Parameters', there is a dropdown menu for 'HTTP Protocol' and a 'Checked Port' field set to '25'. Below these are fields for 'URL:', 'Status Codes:', 'Use HTTP/1.1:' (with a checkbox), 'HTTP Method:' (set to 'GET'), 'Reply 200 Pattern:', and 'Custom Headers:'. Each of these fields has a corresponding 'Set' button. There is also an 'Enhanced Options:' checkbox. The 'Show Headers' button is also visible.

図 3-29: 実サーバーのセクション

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

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

URL

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

Status Codes (ステータスコード)



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

- 200-299
- 301
- 302
- 401

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

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

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

Use HTTP/1.1 (HTTP/1.1を使う)



デフォルトでは、ロードマスターはHTTP/1.0を使用します。ただし、より処理効率が高いHTTP/1.1を使用できます。HTTP/1.1を使用する場合、ヘルスチェックは1つの接続にマルチプレックスされます。これは、1つの接続でより多くのヘルスチェックがサーバーに送信されることを意味します。接続の観点から見ると、これはより効率が高い方法であるといえます（複数の接続ではなく、接続は1つだけとなる）。

HTTP/1.1 Host (HTTP/1.1ホスト)

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

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

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

HTTP Method (HTTPメソッド)

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

Post Data (Postデータ)

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

Reply 200 Pattern (レスポンス200のパターン)

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



ロードマスターは、サーバーからのレスポンスがコード200の場合のみ、そのフレーズをチェックします。それ以外の場合はフレーズをチェックせず、ページが停止しているものとしてマークします。ただし、レスポンスがリダイレクト（コード302）の場合、そのページが停止しているものとしてマークしません。これは、サービスがダウンしているとみなすとリダイレクトが使い物にならないため、ロードマスターはフレーズが存在しないと仮定するためです。

カラット(^)で始まるパターンの場合、レスポンスのパターンを反転させます。

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

Custom Headers (カスタムヘッダー)

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

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

； . () / + = - _

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

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



1. ユーザー名とパスワードは、“ユーザー名:パスワード”という文字列に結合されます。
2. このようにして得られた文字列は、Base64のRFC2045-MIMEバリエントを用いて符号化されます。ただし、76文字/行の制約はありません。
3. 符号化された文字列の先頭に、認証方式とスペース（すなわち “Basic ”）が追加されます。

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

Authorization:Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

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

Rules (ルール)

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

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

OperationName	Match Type	Options	Header	Pattern
Delete ExampleRule	Regex			Example
Delete ExampleMatchRule	Regex			Example2

Add Rule

Rule:

default

Add

図3-30: ルール

この画面では、実サーバーに割り当てられたルールを追加または削除できます。

3.11.2 バイナリデータによるヘルスチェック

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



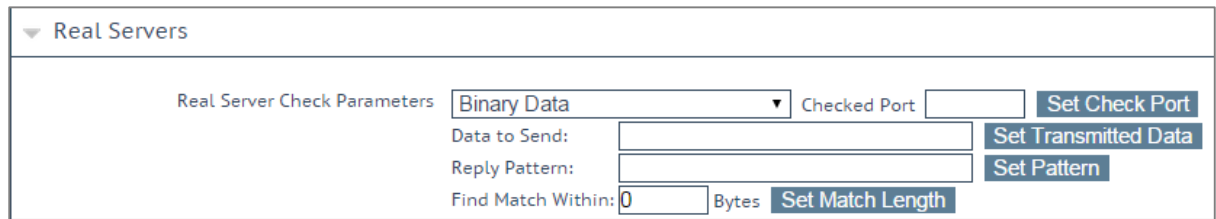


図3-31: バイナリデータによるヘルスチェック

Data to Send (送信データ)

実サーバーに送信する16進文字列を指定します。

この16進文字列には偶数個の文字が含まれている必要があります。

Reply Pattern (応答パターン)

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

この16進文字列には偶数個の文字が含まれている必要があります。

Find Match Within (検索バイト数)

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

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

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

3.11.3 Add a Real Server (実サーバーの追加)

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



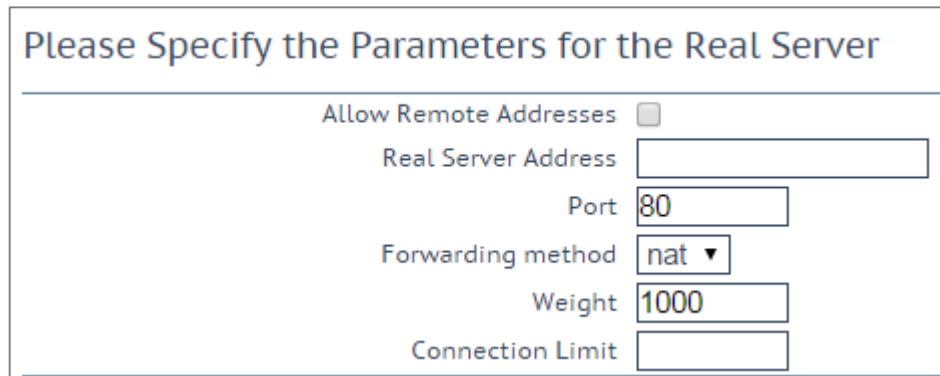


図3-32: 実サーバーのパラメータ

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

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

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

Real Server Address (実サーバーのアドレス) : 実サーバーのIPアドレス。実サーバーの変更中に、このフィールドは編集できません。

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

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

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

Connection Limit (接続上限) :ローテーションから取り出される前に、実サーバーが受け入れられるオープン接続の最大数を設定します。これは、レイヤ7のトラフィックにのみ適用されます。この上限により、新たな接続の作成が制限されます。ただし、サーバーとの間ですでにパーシステントコネクションが確立しているリクエストは許可されます。パーシステンス接続には、セッションブローカーパーシステンスによる仮想サービスへの接続が含まれます。このセッションブローカーパーシステンスには、接続ブローカーにより設定されたセッションブローカークッキーが含まれます。

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

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

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

Critical (重大) :

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

仮想サービス編集画面の実サーバーのセクションには、各実サーバーの“Critical”チェックボックスが用意されています。このオプションが有効な場合、仮想サービスが利用可能であると認識されるためにはこの実サーバーが必要であることを意味します。この



実サーバーが機能しなくなる（または無効になる）と、この仮想サーバーは停止中であるとマークされます。

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

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

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

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

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

Please Specify the Parameters for the Real Server on tcp/10.154.11.61:443 (Id:1)

Real Server Address	10.154.11.92
Port	80
Forwarding method	nat
Weight	1000
Connection Limit	0

図3-33:実サーバーのオプション

Real Server Address (実サーバーのアドレス)

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

Port (ポート)

このフィールドには、実サーバーが使用するポートが表示されます。



Forwarding Method (フォワーディング方式)

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

Weight (重み)

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

Connection Limit (接続上限)

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

3.12 Manage Templates (テンプレートの管理)

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

Name	Comment	Certified	Operation
Adobe Connect HTTPS Offloaded	Handles Adobe Connect Traffic On HTTPS With An HTTP redirect (Version 1.0)	yes	<button>Delete</button>
Adobe Connect RTMP	Handles Adobe Connect Traffic On RTMP (Version 1.0)	yes	<button>Delete</button>

Import Templates

Template file: Choose File No file chosen Add New Template

図3-34: テンプレートの管理

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

テンプレートを削除するには、“Delete”ボタンをクリックします。

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

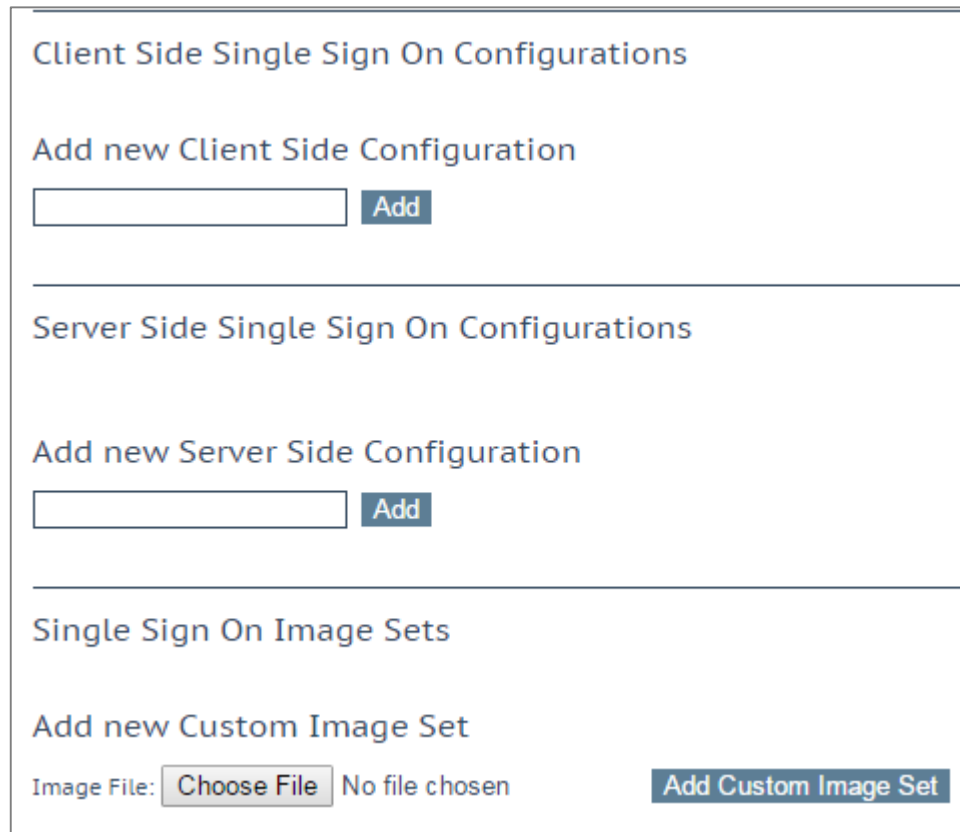
テンプレートに関する詳細（テンプレートを使用して新規仮想サービスの作成と設定を行う方法や、KEMPのテンプレートの入手先など）は、

仮想サービスとテンプレート機能説明ドキュメントを参照してください。

3.13 Manage SSO Domains (SSOドメインの管理)

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

SSOドメインは最大128個まで設定できます。



Client Side Single Sign On Configurations

Add new Client Side Configuration

Add

Server Side Single Sign On Configurations

Add new Server Side Configuration

Add

Single Sign On Image Sets

Add new Custom Image Set

Image File: No file chosen **Add Custom Image Set**

図3-35:SSO管理オプション

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

3.13.1 Single Sign On Domains (SSOドメイン)

クライアントサイドとサーバーサイドの2種類のSSOドメインを作成できます。

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

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

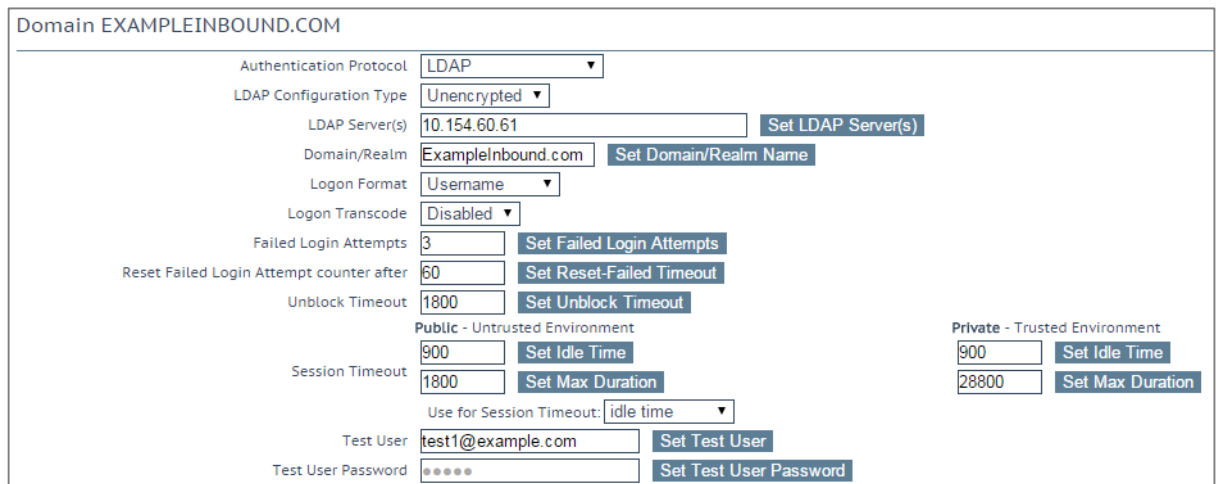
SSOドメインを新規追加するには、“Name”フィールドにドメイン名を入力して“Add”ボタンをクリックします。ここで入力する名前は、SSOドメインでアクセスを許可されたホストと関連している必要はありません。



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

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

3.13.1.1 クライアントサイド (インバウンド) SSOドメイン



Domain EXAMPLEINBOUND.COM

Authentication Protocol	LDAP	
LDAP Configuration Type	Unencrypted	
LDAP Server(s)	10.154.60.61	Set LDAP Server(s)
Domain/Realm	ExampleInbound.com	Set Domain/Realm Name
Logon Format	Username	
Logon Transcode	Disabled	
Failed Login Attempts	3	Set Failed Login Attempts
Reset Failed Login Attempt counter after	60	Set Reset-Failed Timeout
Unblock Timeout	1800	Set Unblock Timeout
Session Timeout	900	Set Idle Time
	1800	Set Max Duration
Use for Session Timeout:	idle time	
Test User	test1@example.com	Set Test User
Test User Password	*****	Set Test User Password

Public - Untrusted Environment

900	Set Idle Time
28800	Set Max Duration

Private - Trusted Environment

図3-36: ドメインの管理画面

Authentication Protocol (認証プロトコル)

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

- LDAP
- RADIUS
- RSA-SecurID
- Certificates (証明書)

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

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

LDAP Configuration Type (LDAP設定タイプ)

LDAPの設定タイプを選択します。以下のオプションが利用できます。

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

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

RADIUS and LDAP (RADIUSおよびLDAPの設定タイプ)

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

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

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

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

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

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



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

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

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

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

RADIUS Shared Secret (RADIUS共有秘密鍵)

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

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

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

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

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

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

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



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

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

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

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

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

Domain/Realm（ドメイン/レルム）

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

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

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

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

このフィールドは、RSA認証マネジャーにエクスポートする必要があります。

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

RSA Node Secret File（RSAノード秘密ファイル）



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

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

Logon Format (ログオンフォーマット)

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

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

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

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

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

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

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

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

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



ロードマスターシリーズ リリースノート (Ver 7.1.34.1)

Copyright © 2002 - 2016 KEMP Technologies, Inc. All Rights Reserved.

実サーバーで認証するためのログオン文字列形式を指定します。

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

- RADIUS
- RSA-SecurID

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

LDAPにより認証されるためのログイン文字列の形式を指定します。

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

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

Logon Transcode (ログオン時のトランスコード)

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

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

Failed Login Attempts (ログイン試行回数)

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

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

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

認証の試行に失敗した後、(新たに試行が行われないまま) この時間 (単位: 秒) が経過すると、試行回数が0にリセットされます。このテキストボックスの有効な値の範囲



は60～86400です。この値は、Unblock timeout（タイムアウトの解除）の値より小さくなければなりません。

Unblock timeout（タイムアウトの解除）

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

Session timeout（セッションタイムアウト）

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

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

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

これらのフィールドの有効な値の範囲は60～86400です。

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

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

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



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

Currently Blocked Users (ブロックされたユーザー)

Currently Blocked Users		
Blocked User	When	Operation
tvaughan@kemptest.com	Fri Sep 18 11:30:23 UTC 2015	<button>unlock</button>
admin@kemptest.com	Fri Sep 18 11:32:09 UTC 2015	<button>unlock</button>

図3-37: ブロックされたユーザー

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

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

3.13.1.2 サーバーサイド (アウトバウンド) SSOドメイン

Authentication Protocol (認証プロトコル)

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

Kerberos Realm (Kerberosレルム)

Kerberosレルムのアドレスです。

このフィールドでは、コロン、スラッシュ、2重引用符は使用できません。

このフィールドは1つのアドレスのみサポートします。



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

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

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

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

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

このフィールドには2重引用符や引用符は使用できません。

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

Kerberosで信頼されたユーザーのパスワードです。

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

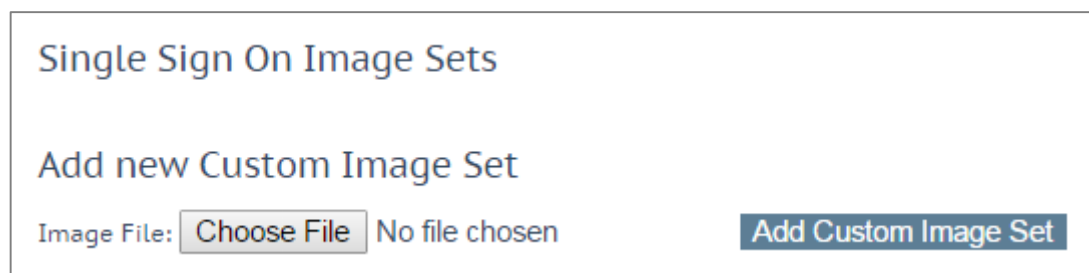


図3-38:SSOの画像設定

新規画像を設定するには、“Choose File”をクリックし、ファイルをブラウザ/選択して“Add Custom Image Set”をクリックします。ファイルを追加すると、追加した画像がこ

のページにリスト表示されます。また、仮想サービス編集画面の“ESP Options”セクションにある“SSO Image Set”ドロップダウンリストでも選択可能です。

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

3.14 WAFの設定

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

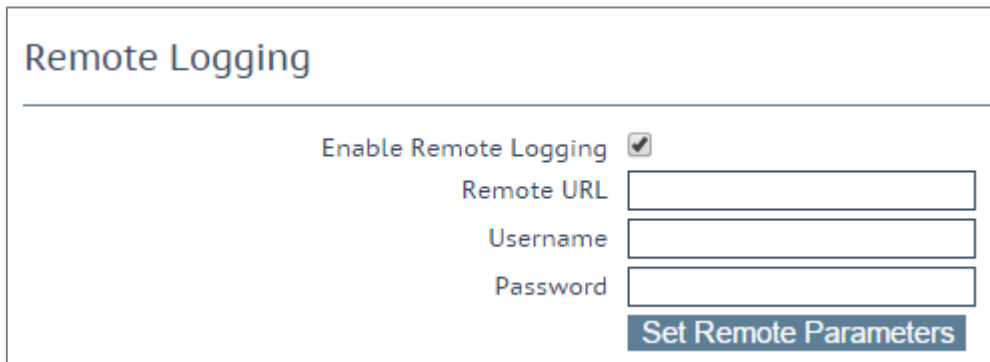


図3-39: Remote Logging (リモートログの作成)

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

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

Remote URL (リモートURL)

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

Username (ユーザー名)

リモートログサーバーのユーザー名を指定します。

Password (パスワード)

リモートログサーバーのパスワードを指定します。



Automated WAF Rule Updates

Enable Automated Rule Updates ☒

Last Updated: Tue 01 Dec 15

[Download Now](#)

[Show Changes](#)

Enable Automated Installs ☒

When to Install

04:00 ▼

Manually Install rules

[Install Now](#)

Last Installed: Tue 01 Dec 15

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

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

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

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

Last Updated (最新更新日)

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

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

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

When to Install (インストール時刻)

毎日何時に最新のルールをインストールするか選択します。

Manually Install rules (ルールを手動インストール)



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

Custom Rules

Installed Rules	Installed Date	Operation
modsecurity_crs_55_marketing	Tue, 01 Dec 2015 13:43:23	Delete Download
modsecurity_crs_55_response_profiling	Tue, 01 Dec 2015 13:43:23	Delete Download
modsecurity_crs_56_pvi_checks	Tue, 01 Dec 2015 13:43:23	Delete Download

Ruleset File: [Choose File](#) No file chosen [Add Ruleset](#)

Custom Rule Data

Installed Data Files	Installed Date	Operation
modsecurity_50_outbound_malware	Tue, 01 Dec 2015 13:43:23	Delete Download

Data File: [Choose File](#) No file chosen [Add Data File](#)

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

Custom Rules (カスタムルール)

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

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

Custom Rule Data (カスタムルールデータ)

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



4 グローバル負荷分散

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

4.1Enable/Disable GSLB (GSLBの有効化/無効化)

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

4.2FQDNの管理

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

Configured Fully Qualified Names								
Fully Qualified Domain Name	Type	IP Address	Cluster	Checker	Availability	Requests/s	Parameters	Operation
Example.com.	Proximity	1.1.1.1	Example	ICMP Ping		0	27°0'0"S 133°0'0"E	Modify Delete

図4-1: グローバルな完全修飾名

この画面から、FQDNの“Add”または“Modify”を選択できます。

4.2.1 Add a FQDN (FQDNの追加)

Add a FQDN

New Fully Qualified Domain Name

www.example1.com

Add FQDN

図4-2: FQDNの追加

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

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

4.2.2 Add/Modify an FQDN (FQDNの追加/変更)

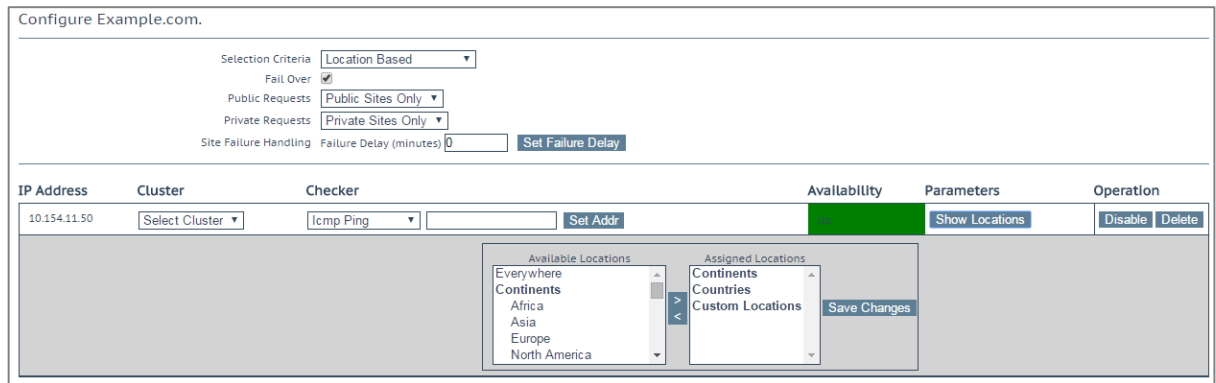


図4-3:FQDNの設定

Selection Criteria (選択条件)

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

- **Round Robin (ラウンドロビン)** - トラフィックはサーバーファーム（クラスター。利用可能なサーバーと同義）全体に順番に分配されます。
- **Weighted Round Robin (重み付けラウンドロビン)** - 受信した要求は、サーバー単位に事前に割り当てできる静的な重み付けを考慮して、クラスター全体に順番に分配されます。
- **Fixed Weighting (固定重み)** - 他の実サーバーに小さい重みの値が与えられている場合限定して、最も重みが大い実サーバーが使用されます。
- **Real Server Load (実サーバーの負荷)** - ロードマスターに用意されているロジックで、設定済みの重み付けとは無関係に、サーバーの状態を一定の間隔でチェックします。
- **Proximity (近接)** - トラフィックはクライアントに最も近接するサイトに分配されます。“Proximity”（近接）スケジューリングを使用する場合、GE0データベースに基づき新しいパブリックサイトが地理的座標に自動的にマッピングされます。新しいプライベートサイトは0°0'0"にマッピングされ、期待どおりに機能します。負荷分散を正しく行うには、この座標を正確な値で上書きする必要があります。クライアントの位置は、そのクライアントのIPアドレスによって判定されます。

- **Location Based (位置ベース)** - トラフィックはクライアントに最も近接するサイトに分配されます。サイトの位置は、セットアップ時にサイトの位置（国名や大陸名）を入力することで設定します。クライアントの位置は、そのクライアントのIPアドレスによって判定されます。同じ国コードを持つ複数のサイトがある場合、リクエストは各サイトにラウンドロビン方式で配信されます。

Fail Over (フェイルオーバー)

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

パブリックリクエスト/プライベートリクエスト

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

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

以下の表に、各設定と設定可能な値の概要を示します。



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

表4-1:パブリック/プライベートリクエストの設定

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

Site Failure Handling (サイト障害時の処理)

デフォルトでは、フェイルオーバーが自動的に実行されます。ただし、複数サイトにまたがるExchange 2010構成など、環境によっては、このような処理は最適ではなく、異



なる処理が必要になる場合があります。“Failure Delay”は分単位で設定します。“Failure Delay”を設定すると、“Site Recovery Mode”という新しいオプションが利用可能になります。

Site Recovery Mode (サイト復旧モード)

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

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

Cluster (クラスター)

必要に応じて、IPアドレスを含むクラスターを選択できます。

Checker (チェッカー)

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

- **None (なし)** : 現在のFQDNに関連するマシン (IPアドレス) の健全性をチェックするためのヘルスチェックを行わないことを意味します。
- **ICMP Ping** : IPアドレスにPingを送信することで健全性をテストします。
- **TCP Connect (TCP接続)** : 指定したポートにてIPアドレスへの接続を試みることで健全性をテストします。
- **Cluster Checks (クラスターチェック)** : このオプションを選択すると、選択したクラスターに関連する手法を用いて健全性がチェックされます。
 - “Slection Criteria”として“Real Server Load”が使用されており、クラスターの“Type”が“Local LM”または“Remote LM”に設定されている場合、“Mapping Menu”ドロップダウンリストが表示されます。“Mapping Menu”ドロップダウンリストには、そのロードマスターからの仮想サービスのIPアドレスのリストが表示されます。ここには、ポートを持たない各仮想サービスのIPアドレス、および仮想IPアドレスとポートのすべての組み合わせがリストされます。このマッピングに割り当てられている仮想IPアドレスを選択してください。ポートをもたない仮想サービスを選択した場合、選択したアドレスと同じIP



アドレスをもつすべての仮想サービスがヘルスチェックによりチェックされます。仮想サービスのいずれかが“UP”（稼働中）の状態であった場合、FQDNは“UP”と表示されます。このとき、ポートは考慮されません。

ポートをもつ仮想サービスを選択した場合、FQDNの健全性を更新するときにその仮想サービスの健全性のみチェックされます。

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

Parameters（パラメータ）

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

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

Delete IP address（IPアドレスの削除）

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

Delete FQDN（FQDNの削除）

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



4.3 クラスターの管理

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

Configured Clusters

IP Address	Name	Coordinates	Type	Checker	Availability	Operation
10.154.11.190	Example	0°0'5"N 0°0'5"E	Default	None	Up	Modify Delete
172.20.0.29	Example2	0°0'0"N 0°0'0"W	Default	None	Up	Modify Delete

Add a Cluster

IP address

Name

Add Cluster

図 4-4: 設定済みのクラスター

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

4.3.1 Add a Cluster（クラスターの追加）

Add a Cluster

IP address

10.154.11.158

Name

ExampleCluster

Add Cluster

図4-5: クラスターの追加

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

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

4.3.2 Modify a Cluster (クラスターの変更)

Modify Cluster ExampleCluster

IP Address	Name	Location	Type	Checkers	Operation
10.154.11.158	ExampleCluster	Location: 0°0'0"N 0°0'0"W	Default	None	Disable
		Show Locations			
		Manually set location: 0°0'0"N 0°0'0"E Resolved location: 0°0'0"N 0°0'0"W			
		000N 000E Set Location			

図 4-6: クラスターの変更

Name (名前)

クラスターの名前。

Location (位置)

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

Type (タイプ)

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

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



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

Checkers (チェッカー)

クラスターのステータスをチェックする目的で使用するヘルスチェック方式。

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

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

Disable (無効)

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

4.3.3 Delete a Cluster (クラスターの削除)

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

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

4.3.4 GEOクラスターのアップグレード

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

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



4.4その他のパラメータ

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

4.4.1 Source of Authority (権限ソース)

Source of Authority

Source of Authority	lm1.example.com.	Set SOA
Name Server	lm1.example.com.	Set Nameserver
SOA Email	hostmaster@example.com	Set SOA Email
TTL	10	Set TTL value

図4-7: 権限ソース

Source of Authority (権限ソース)

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

Name Server (ネームサーバー)

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

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

SOA Email (SOA Emailアドレス)

このテキストボックスは、“@”を“.”に変換して、このゾーンを処理するユーザーまたはロールアカウントのメールアドレスを発行する目的で使用します。ベストプラクティス



として、専用のメールエイリアスを定義（および保持）することを推奨します。たとえば、DNS操作用の“hostmaster” [RFC 2142] の場合、hostmaster@example.comです。

TTL

有効期限（“TTL”）の値は、他のDNSサーバーやクライアントデバイスでGE0ロードマスターからのリプライをキャッシュ可能な期間を規定します。この値は、可能な限り小さく設定する必要があります。このフィールドのデフォルト値は10です。この期間は、秒単位で定義します。

4.4.2 リソースチェックのパラメータ

Resource Check Parameters

Check Interval	120	Set Check Interval
Connection Timeout	20	Set Timeout value
Retry attempts	2	Set Retry Attempts

図4-8: リソースチェックのパラメータ

Check Interval（チェック間隔）

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

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

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

Connection Timeout（接続タイムアウト）

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



Retry Attempts (再試行回数)

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

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

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

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

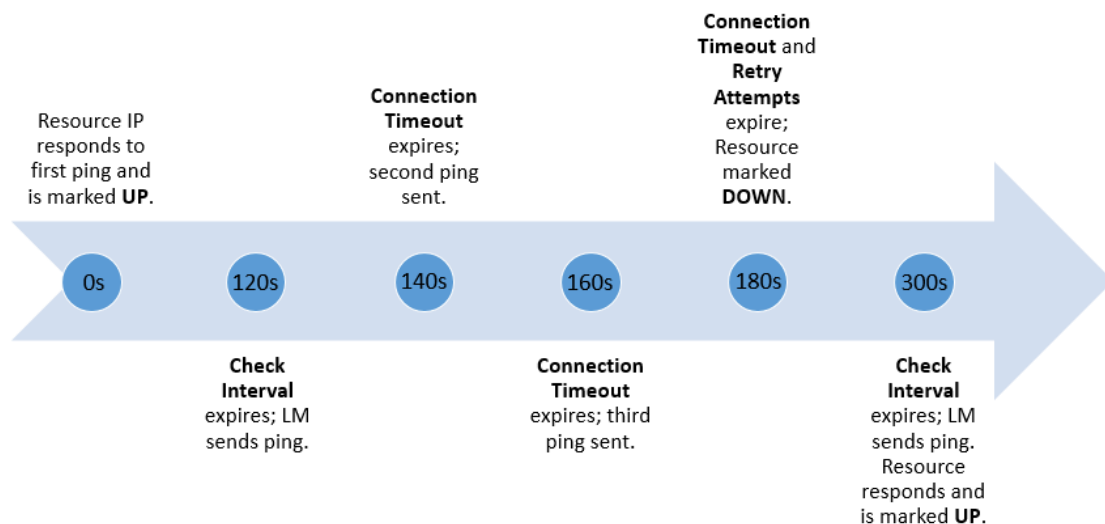


図 4-9: リソースチェックのタイミング図

4.4.3 Stickiness (持続性)



図 4-10:スティッキネス

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

4.4.4 Location Data Update (位置データ更新)

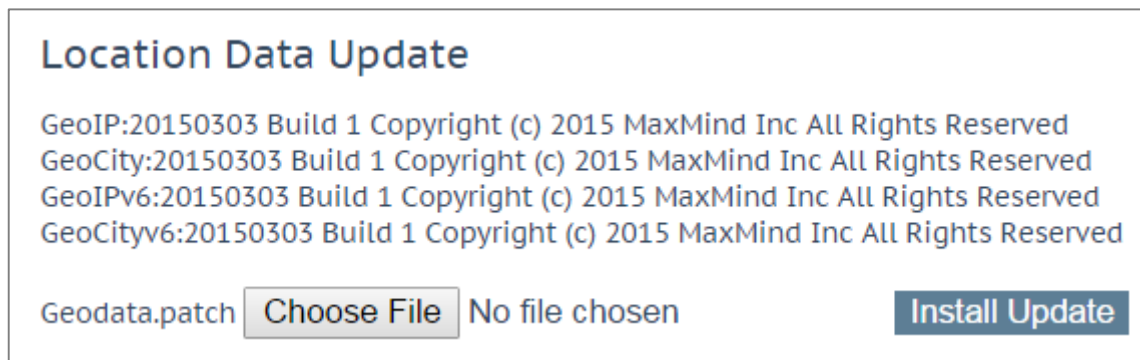


図4-11:位置データ更新

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

4.5 IP範囲の選択条件

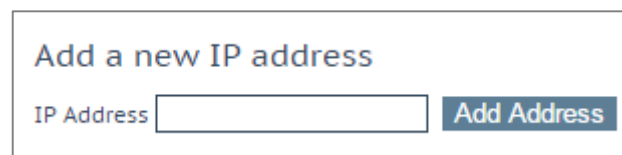


図4-12:新規IPアドレスの追加

このセクションでは、新しいIPアドレス範囲を定義できます。

IP Address Ranges configured			
IP/IPv6 Address Range	Coordinates	Location	Operation
10.154.11.190/32		Ireland	<button>Modify</button> <button>Delete</button>

図 4-13: 設定されたIPアドレス範囲

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

IP Address	Coordinates	Location
10.154.11.190/32	N E	Ireland
Save Delete		

図 4-14: IP範囲の選択条件

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

IP Address (IPアドレス)

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

Coordinates (座標)

位置を示す緯度と経度を入力します。

Location (位置)

アドレスに割り当てる位置を指定します。

Add a new custom location

Add location

図 4-15: カスタムロケーションの追加

Add Custom Location (カスタムロケーションの追加)



このセクションでは、カスタムロケーションを追加できます。

Custom Locations configured	
Custom Location Name	Operation
New York	ModifyDelete

図 4-16: 設定されたカスタムロケーション

このセクションでは、カスタムロケーションの編集と削除も行えます。

5 Statistics (統計情報)

5.1実サーバーの統計情報

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

5.1.1 Global (システム統計)

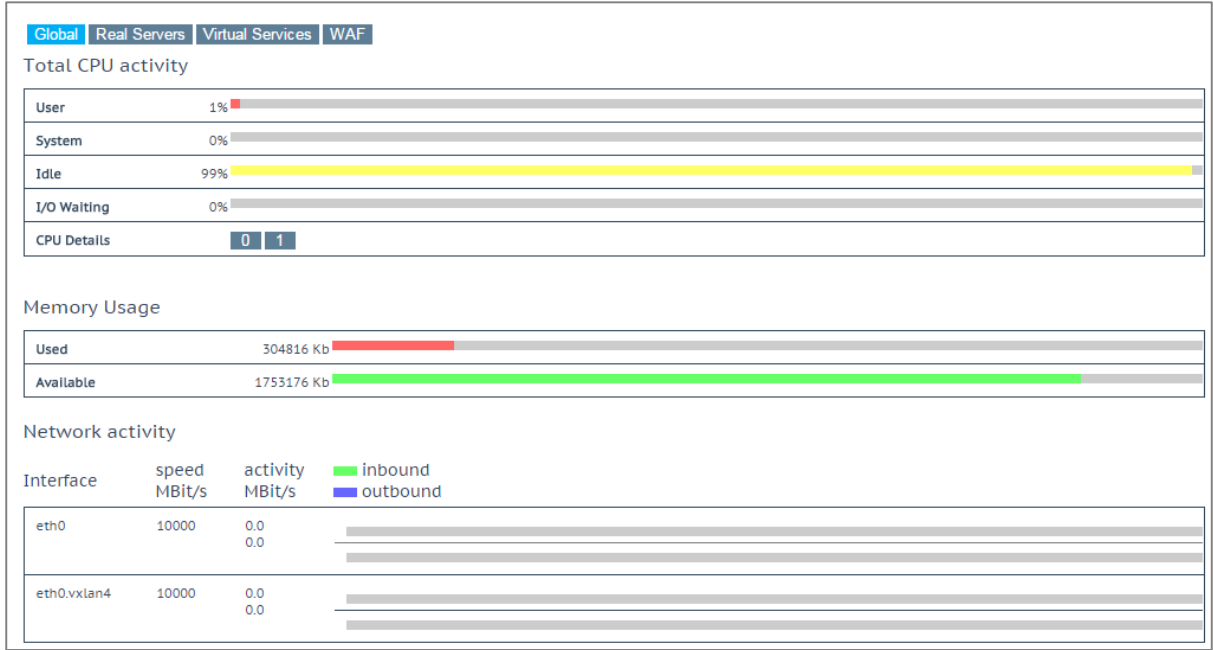


図5-1:統計

Total CPU Activity (合計CPUアクティビティ)

このグラフは、ロードマスターの以下のCPU使用率を表示します。

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



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

この4つのパーセンテージの合計は100%になります。

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

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

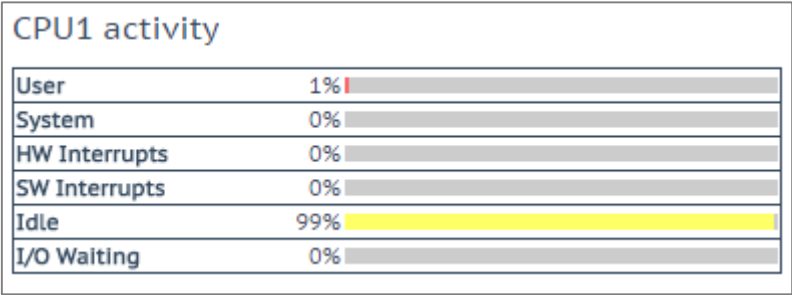


図 5-2:CPUの統計情報

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

Memory usage (メモリ使用率)

この棒グラフには、メモリの使用容量と空き容量が表示されます。

Network activity (ネットワークアクティビティ)

この棒グラフは、各インターフェイスのネットワーク・スループットを示します。



5.1.2 実サーバー

Global Real Servers Virtual Services				
Name	RS-IP	Status	Adaptive	Weight
1⇒	10.154.201.2	Ambiguous	61	1055
2⇒	10.154.201.3	Ambiguous	61	1055
3⇒	10.154.201.4	Up	65	945
4⇒	10.154.201.5	Up	65	972/2
4	System Total Conns			

図 5-3:実サーバー統計情報画面のセクション

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

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

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

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

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

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

図 5-4:実サーバーの統計情報



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

Status (ステータス) : 実サーバーの状態が表示されます。

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

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

Total Conns (トータルの接続数) : トータルの接続数です。

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

5 Mins (5分間) : 過去5分間におけるトータルの接続数

30 Mins (30分間) : 過去30分間におけるトータルの接続数

1 Hour (1時間) : 過去1時間におけるトータルの接続数

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

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

[%] : 1秒当たりの現在の接続率

Conns/sec (接続数/秒) : 1秒当たりの接続数をグラフ表示したもの

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



5.1.3 仮想サービス

GlobalReal ServersVirtual ServicesConnectionsBytesBits										
Name	Virtual IP Address	Protocol	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/s
1	10.154.201.8:80	tcp	Up	0	0	0	0	0	0	0
2	10.154.201.203:80	tcp	Down							
3	10.154.201.254:80	tcp	Down							
3	System Total Conns			0	0	0	0	0	0	0/sec

図5-5:Virtual Services (仮想サービス)

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

Name (名前) : 仮想サービスの名前

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

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

図 5-6:仮想サービスの統計情報



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

Address (アドレス) : 仮想サービスのIPアドレス

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

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

Total Conns (トータルの接続数) : トータルの接続数です。

Total Bytes (トータルのバイト数) : 送信されたトータルのバイト数

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

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

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

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

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

Incidents/Hour (インシデント/時) : 現在の時間内 (xx. 00. 00以降) に発生したイベントの数

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

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

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



5.1.4 WAF

Global Real Servers Virtual Services WAF								
WAF Enabled VS Statistics								
Name	Virtual IP Address	Protocol	Status	Total Requests	Total Events	Events this hour	Events Today	Events over Limit Today
1 Example Virtual Service	172.20.0.207:80	tcp	Down	0	0	0	0	0
1	WAF enabled VS Total			0	0	0	0	0

図 5-7:WAFが有効なVSの統計情報

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

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

Name (名前) :WAFが有効な仮想サービスの名前

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

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

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

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

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

Events this hour (現在の時間内のイベント数) :現在の時間内 (xx. 00. 00以降) に発生したイベントの数

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

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



5.2 履歴グラフ

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

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

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

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

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

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

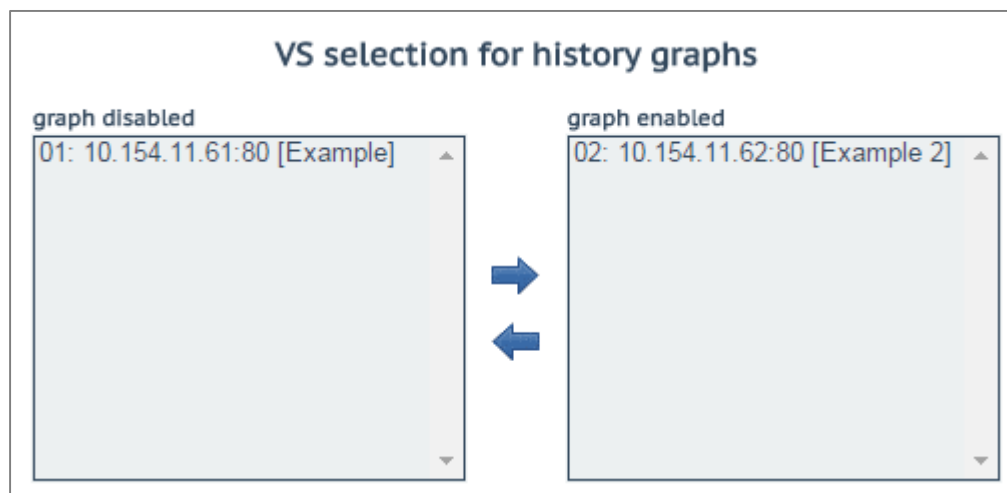


図 5-8: 履歴グラフ用の仮想サービス (VS) の選択

このダイアログで、仮想サービスの統計情報表示を追加/削除できます。

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



最大5個の仮想サービスを同時に表示できます。

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

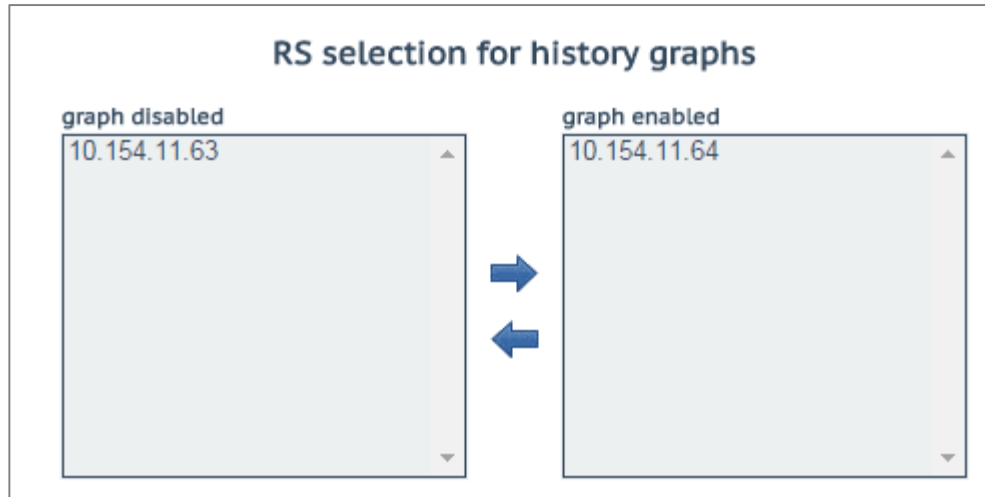


図 5-9: 履歴グラフ用の実サーバー (RS) の選択

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

このダイアログで、実サーバーの統計情報表示を追加/削除できます。

最大5個の実サーバーを同時に表示できます。

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

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

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

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

使用可能な倍率とその接頭辞を以下の表に示します。

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

表5-1: 倍率と接頭辞

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

例:

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

- $10^{-3} = 0.001$
- $200 \times 0.001 = 0.2$ コネクション/秒

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

6 SDN統計情報

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

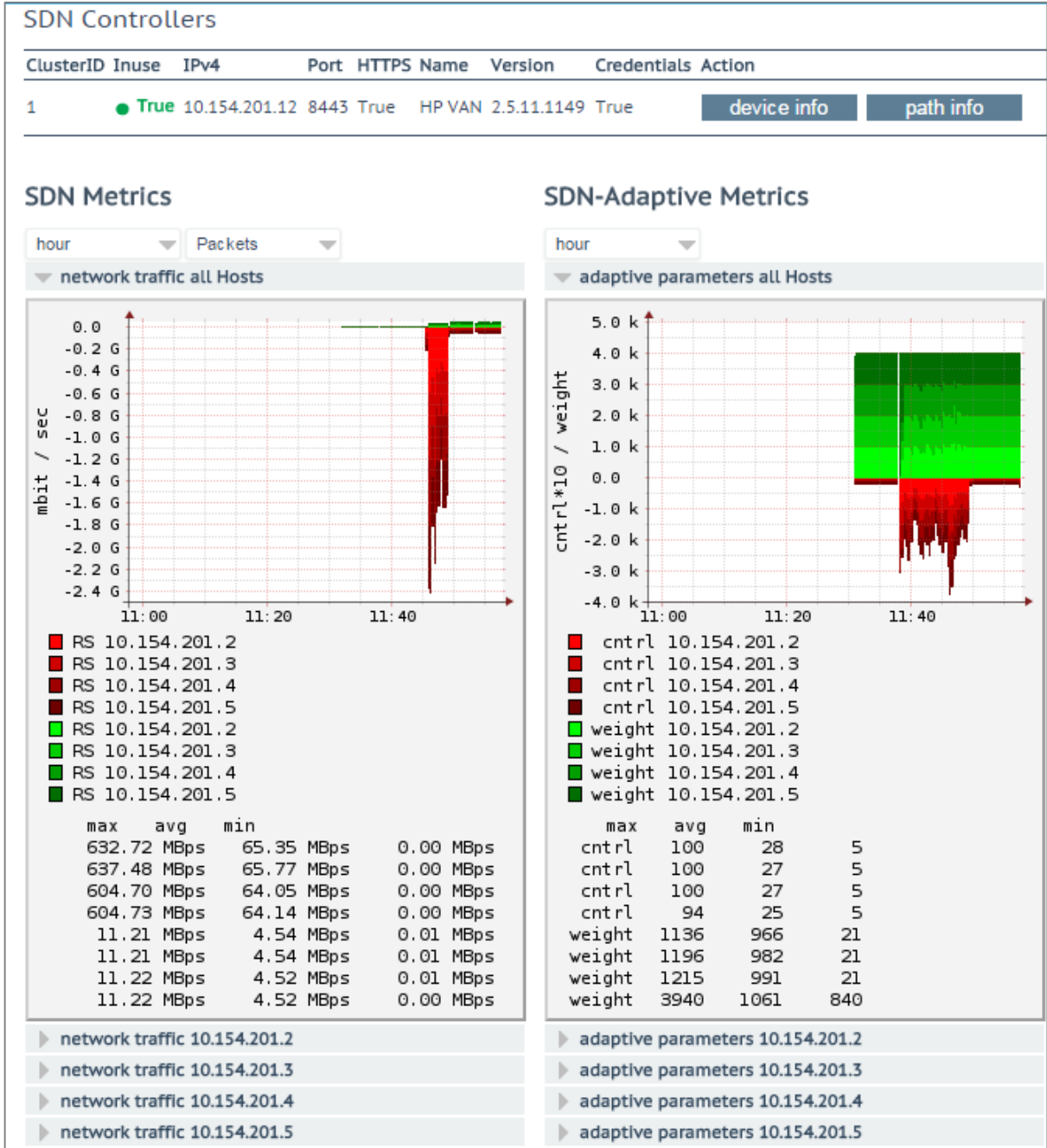


図 6-1:SDNの統計情報



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

Statistics section（統計情報の選択）

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

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

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

6.1.1 デバイス情報

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

図 6-2: デバイス画面のセクション

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



UID	Name	Type	Vendor	Product
▼ 00:00:54:9f:35:1c:c5:30	ovsbr0	Default OpenFlow Switch	Nicira, Inc.	Open vSwitch
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=0xffffffe	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

図 6-3: デバイス画面のセクション - 追加の詳細情報

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



6.1.2 パス情報

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

図 6-4:パス情報画面のセクション

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

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

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



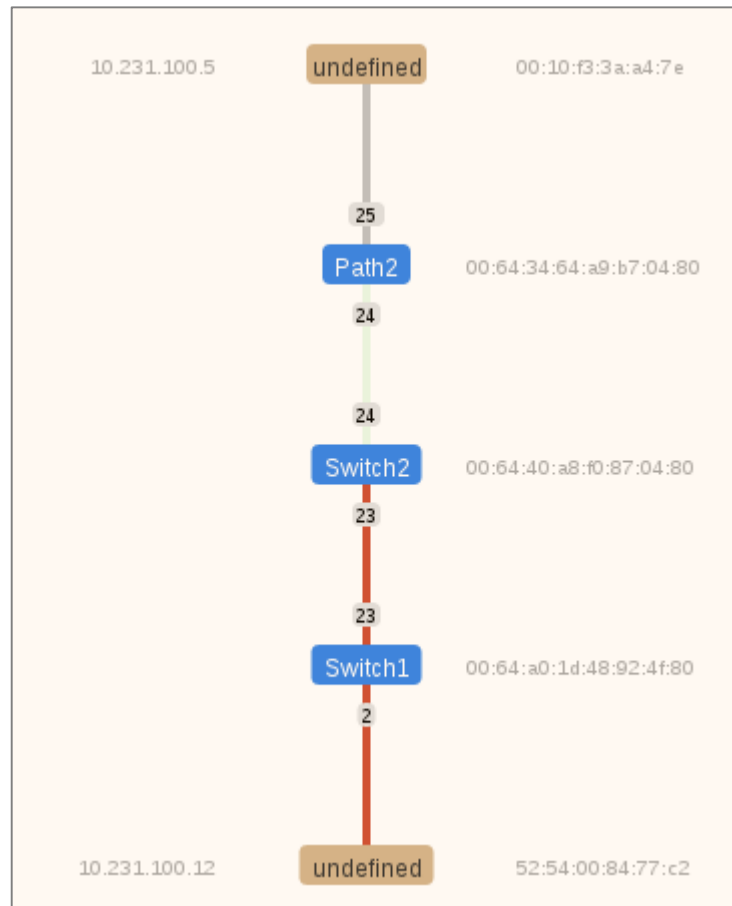


図 6-5:パス情報 - グラフ表示

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

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

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

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

パスの色の意味は以下のとおりです。

- ライトグリーン: トラフィックがアイドル状態で、リンクは正常です。
- 赤: パスのトラフィックが混雑しています。

- グレー:ロードマスターと最初のスイッチとの間のパスはグレーで表示されます。

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

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



7 実サーバー

Real Server	Status	Operation	
☐ 10.154.201.2	Enabled	Enable	Disable
☐ 10.154.201.3	Enabled	Enable	Disable
☐ 10.154.201.4	Enabled	Enable	Disable
☐ 10.154.201.5	Enabled	Enable	Disable
Enable Disable			

図 7-1:実サーバーの画面

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

注意

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

8 Rules & Checking (ルールとチェック)

8.1コンテンツルール

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

Content Matching Rules						Create New
Name	Type	Options	Header	Pattern	Operation	
vmworkspace	RegEx	Must Fail Ignore Case		~/admin*		Modify Delete

図8-1:ルール

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

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

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

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

ルールの種類:

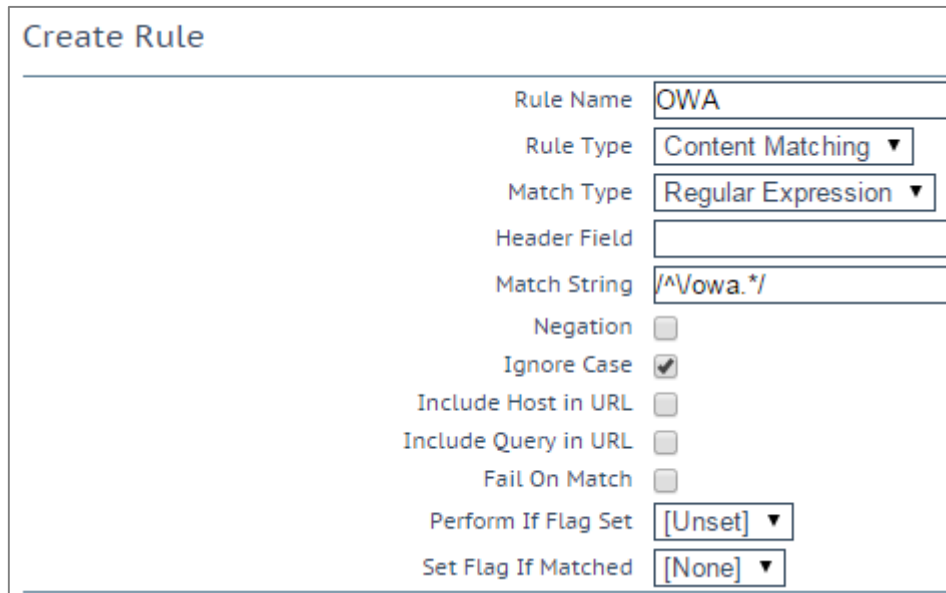
- **Content Matching (コンテンツマッチング)**：ヘッダーまたはボディのコンテンツを照合します。
- **Add Header** - ルールに従ってヘッダーを追加
- **Delete Header (ヘッダーの削除)** -ルールに従ってヘッダーを削除
- **Replace Header** - ルールに従ってヘッダーを置き換え
- **Modify URL** - ルールに従ってURLの変更

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



8.1.2 Content Matching (コンテンツマッチング)

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



Create Rule	
Rule Name	OWA
Rule Type	Content Matching ▼
Match Type	Regular Expression ▼
Header Field	
Match String	/^\/owa.*\/
Negation	☐
Ignore Case	☒
Include Host in URL	☐
Include Query in URL	☐
Fail On Match	☐
Perform If Flag Set	[Unset] ▼
Set Flag If Matched	[None] ▼

図8-2: コンテンツマッチング

Rule Name (ルール名)

ルールの名前です。

Match Type (マッチタイプ) :

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

Header Field (ヘッダーフィールド)



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

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

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

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

Match String (マッチ文字列)

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

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

Negation (反転)

マッチ文の意味を反転します。

Ignore Case (大文字と小文字を区別しない)

文字列の大文字と小文字を区別しません。

Include Host in URL (URLにホスト名を含める)

ルール文のマッチを行う前に、リクエストURLの先頭にホスト名を追加します。

Include Query in URL (URLにクエリ文字列を含める)

ルール文のマッチを行う前に、クエリ文字列をURLに追加します。

Fail On Match (マッチ失敗時の処理)

このルール文にマッチした場合、常に接続しません。

Perform If Flag Set (フラグセット時にマッチ実行)

指定したフラグがセットされている場合のみこのルール文が実行されます。

Set Flag If Matched (マッチ時にフラグをセット)

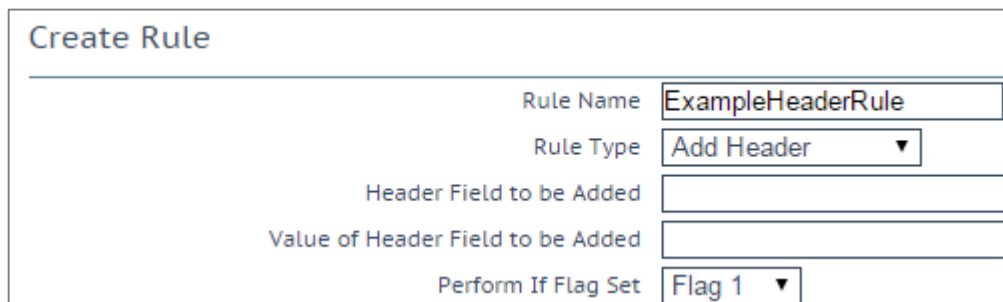
このルール文のマッチに成功すると、指定したフラグがセットされます。



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

8.1.3 Add Header (ヘッダーの追加)

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



The screenshot shows a 'Create Rule' dialog box with the following fields:

- Rule Name:** ExampleHeaderRule
- Rule Type:** Add Header (dropdown menu)
- Header Field to be Added:** (empty text box)
- Value of Header Field to be Added:** (empty text box)
- Perform If Flag Set:** Flag 1 (dropdown menu)

図8-3: ヘッダーの追加

Rule Name (ルール名)

ルールの名前を入力するためのテキストボックスです。

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

追加するヘッダーフィールドの名前を入力するためのテキストボックスです。

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

追加するヘッダーフィールドの値を入力するためのテキストボックスです。

Perform If Flag Set (フラグセット時に実行)

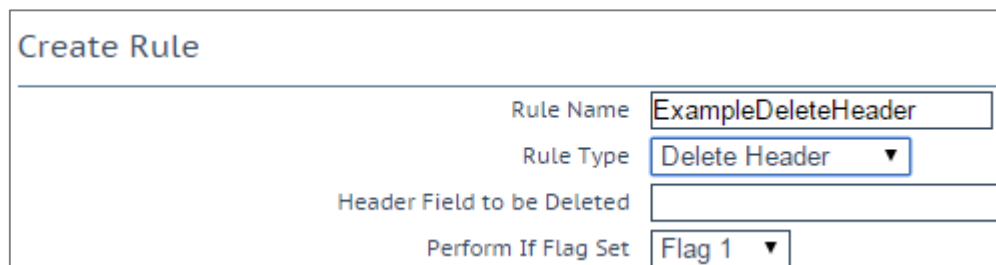
指定したフラグがセットされている場合のみこのルール文が実行されます。

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

8.1.4 Delete Header (ヘッダーの削除)

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





Create Rule	
Rule Name	ExampleDeleteHeader
Rule Type	Delete Header ▼
Header Field to be Deleted	
Perform If Flag Set	Flag 1 ▼

図8-4: ヘッダーの削除

Rule Name (ルール名)

ルールの名前を入力するためのテキストボックスです。

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

削除するヘッダーフィールドの名前を入力するためのテキストボックスです。

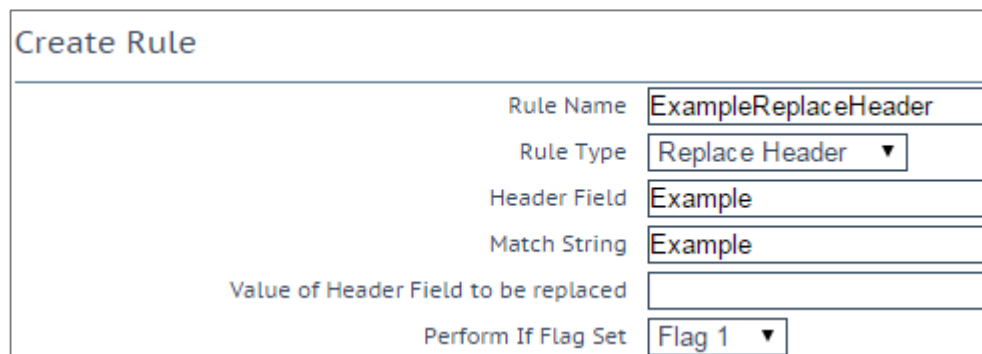
Perform If Flag Set (フラグセット時に実行)

指定したフラグがセットされている場合のみこのルール文が実行されます。

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

8.1.5 Replace Header (ヘッダーの置換)

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



Create Rule	
Rule Name	ExampleReplaceHeader
Rule Type	Replace Header ▼
Header Field	Example
Match String	Example
Value of Header Field to be replaced	
Perform If Flag Set	Flag 1 ▼

図8-5: ヘッダーの置換

Rule Name (ルール名)

ルールの名前を入力するためのテキストボックスです。

Header Field (ヘッダーフィールド)

置換するヘッダーフィールドの名前を入力するためのテキストボックスです。

Match String (マッチ文字列)

マッチを行うパターンを入力します。

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

置換するヘッダーフィールドの値を入力するためのテキストボックスです。

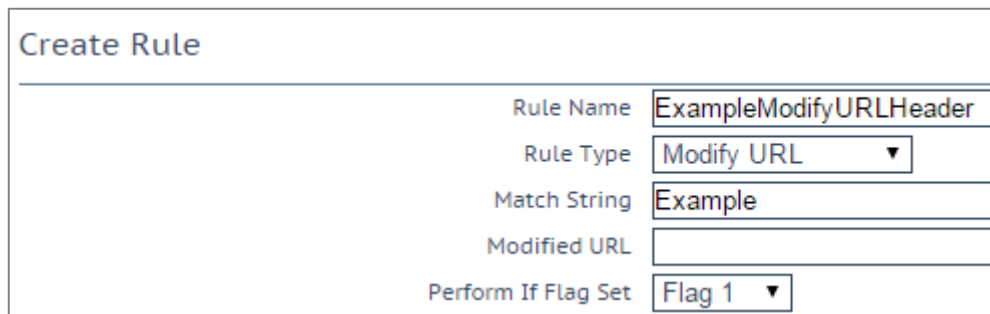
Perform If Flag Set (フラグセット時に実行)

指定したフラグがセットされている場合のみこのルール文が実行されます。

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

8.1.6 Modify URL (URLの変更)

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



The screenshot shows a web form titled "Create Rule". It contains several input fields and a dropdown menu. The "Rule Name" field is filled with "ExampleModifyURLHeader". The "Rule Type" dropdown menu is set to "Modify URL". The "Match String" field is filled with "Example". The "Modified URL" field is empty. The "Perform If Flag Set" dropdown menu is set to "Flag 1".

図8-6:URLの変更

Rule Name (ルール名)

ルールの名前を入力するためのテキストボックスです。

Match String (マッチ文字列)

マッチングするパターンを入力するためのテキストボックスです。

Modified URL (変更後のURL)

変更するURLを入力するためのテキストボックスです。

Perform If Flag Set (フラグセット時に実行)

指定したフラグがセットされている場合のみこのルール文が実行されます。

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

8.1.7 Header Modification (ヘッダーの変更)

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

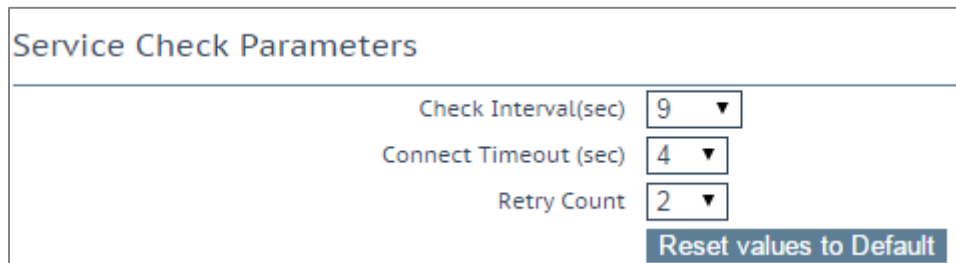
8.2 Check Parameters (チェック用パラメータ)

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

詳細は、以下の関連するセクションを参照してください。

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

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



Service Check Parameters	
Check Interval(sec)	9 ▼
Connect Timeout(sec)	4 ▼
Retry Count	2 ▼
Reset values to Default	

図 8-7: サービスチェック用パラメータ

Check Interval(sec) (チェック周期 (秒))

ヘルスチェックの周期時間を変更できます。デフォルト値は9 秒です。

Connect Timeout (sec) (接続タイムアウト (秒))

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

レイヤのアクセスが確立されるまでどれだけ待つかの設定です。デフォルトは4秒に設定してあります。

Retry Count (リトライ回数)

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

8.2.2 アダプティブ負荷分散方式用パラメータ

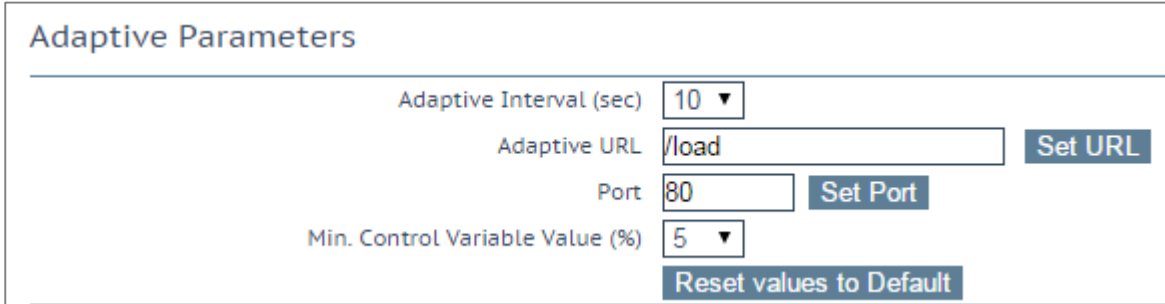


図8-8:アダプティブ負荷分散方式用パラメータ

Adaptive Interval (sec) (インターバル (秒))

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

Adaptive URL (アダプティブ URL)

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

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

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

ファイルロケーションのデフォルトは“/load”です。



このファイルはHTTPを介してアクセスできます。

ファイルはHTTP経由でアクセス可能でなければなりません。

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

Port (ポート)

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

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

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

8.2.3 SDNのアダプティブ負荷分散方式パラメーター

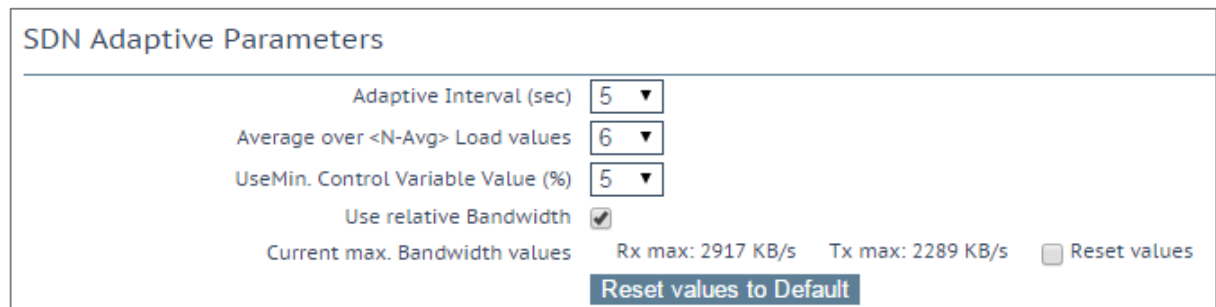


図 8-9:SDNのアダプティブ負荷分散方式パラメーター

Adaptive Interval (sec) (インターバル (秒))

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

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

システムにおける変動を抑制するにはこの値を使用します。



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

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

User Relative Bandwidth (相対帯域幅を使用)

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

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

このセクションには、送受信された現在の最大帯域幅の値が表示されます。

Reset values (値のリセット)

このチェックボックスを使用すると、現在の最大帯域幅の値をリセットできます。

9 証明書とセキュリティ

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

9.1 SSL Certificates (SSL 証明書)

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

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

9.1.1 HSMが有効でない場合

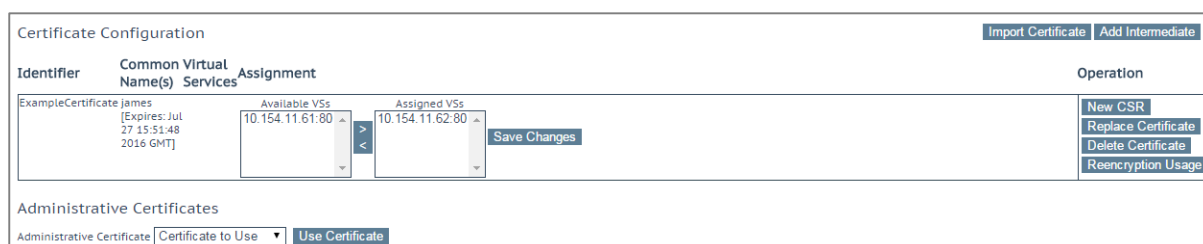


図9-1:SSL証明書

上図は、SSL証明書の管理画面を示します。

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

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

Identifier - 証明書作成時に与えられた証明書名です。

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

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

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

Operations（操作） -

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

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

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

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

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

9.1.2 HSMが有効な場合

Private Key Identifier (秘密鍵識別子)

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

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

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

Private Key (秘密鍵) - この列には秘密鍵名が表示されます。

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

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

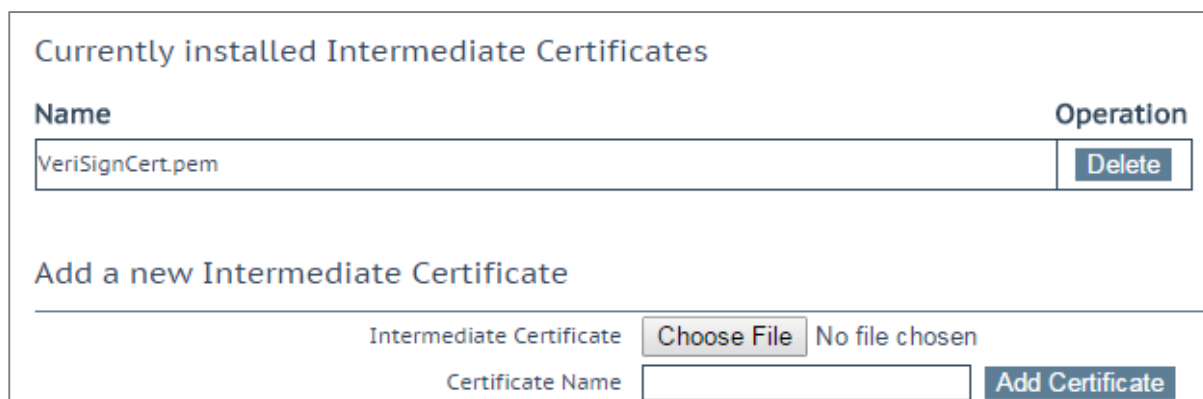
Assignment (割り当て) - 割り当てられた利用可能な仮想サービスのリスト

Operations (操作) -

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



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



Name	Operation
VeriSignCert.pem	<button>Delete</button>

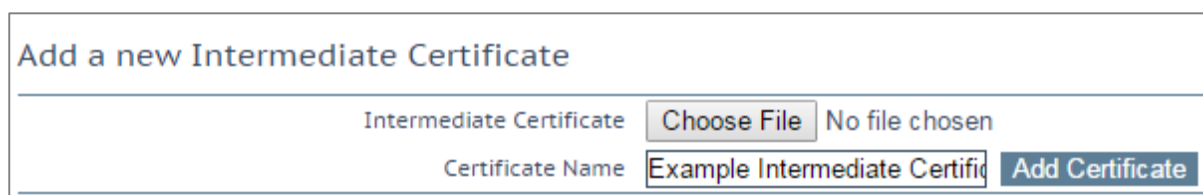
Add a new Intermediate Certificate

Intermediate Certificate No file chosen

Certificate Name

図9-2: インターミディエート証明書

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



Add a new Intermediate Certificate

Intermediate Certificate No file chosen

Certificate Name

図 9-3: 中間証明書のインストール

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

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

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

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

All Fields are optional except "Common Name"

2 Letter Country Code (ex. US)	
State/Province (Full Name - New York, not NY)	
City	
Company	
Organization (e.g., Marketing, Finance, Sales)	
Common Name (The FQDN of your web server)	
Email Address	
SAN/UCC Names	

図 9-4: CSRの作成

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

証明書に含める2文字国コードです。例えば、米国であればUSと入力します。

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

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

City (都市)

証明書に含める都市名です。

Company (企業)

証明書に含める企業名です。

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

証明書に含める部門または組織単位です。

Common Name (コモンネーム)

お使いのWebブラウザの完全修飾ドメイン名 (FQDN) です。

Email Address (Eメールアドレス)



この証明書に関する問い合わせ先の担当者または組織のEメールアドレスです。

SAN/UCC Names (SAN/UCC名)

スペースで区切られた代替名のリストです。

[Create CSR] ボタンをクリックすると、次の画面が表示されます。



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-----
MIIC9zCCA8CAQAwbGExCzAJBgNVBAYTA1VTMRwDwYDVQIEWhOZXcgM9yazER
MA8GA1UEBxMlTMv3IFlvcmsxGjAYBgNVBAoTEUFTVAgVGVjaG5vbG9naWZMR0w
GwYDQQLExRLbm93bGVkZ2UgTWFuYXd1bWVudDEUMBIGA1UEAxMLRXhhbX8sZS5j
b20xKzApBgkqhkiG9w0BCQEWHGpibG9nZ3Naa2VtcHRlY2hub2xvZ2llcy5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+ohZjEwKEQT3jd6y9gN7k
5nu8E0T8bha1LuGCD5mN++u+c+3Vm4r5m6g5pVS16RF4QaRqkuiaekZ5QPWqMV06b
yxvveIhoq1HPVphPOEHBhd1iotC4SLorJ6/A0vwdlRIj1JVJfe7ka6S60xaVgAog
61VohNoDtCRHJOWFvawBhEZh2YzpuoPsmDoZRnuX8qD9DZn1c9s5Kn3YjomY50
2KRyJmFEI98N8sMmiPATvXYZCrTUIfu2nwfpR9ogx7KVyK7Mi/73P41zD3dN4T
1GM0FMxYehg9bNXL27wkUek4994izLpyrv4whSc9QCbfid1BXz6IdxuFbpMJBmdVx
AgMBAAGGAADANBgkqhkiG9w0BAQsFAAOCQAQANRw0oaxj+B6/t+KTMHTVWzZXFDf
79HHQj7ROftqkw+FfijKEAfbhFNAfopmRQEC6twysb70K1acBn2fCI2lr9stsUUC
bq+wXl/crsVs+mc+veQ+p3R3zHlNPU1mZ6sofoQUi1E8NbCRUtdZ+6ixxLZL0ah
Y7a9Nipn5qy2st/yfYhao4rJWuzLXuKaphqyc1JNwvPkFI/4tdbrdD5rgPZfCdDY
PD0xUnD6244HtFkn9ZCqfkatGyTI9qVnPsIdqapKUAVZ4Zk1j+W7zNF6mw2CXK5
Ff97URaPlwEI+VQRv1baJgn3/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-----
MIIEpAIBAAKCAQEAavqIwYXMCHEE943esvYDe5Ep7v8NE/G4QNS7hgg+Zjfvrgvt1
ZuK+Zuo0avUtekREEGkapLomnpM+UD1qjFdom8sb3niIaktrZiaYtzhBwR3dYqLQ
uEi6E5evwNLnZUSI5SVSX3u5GukutMwIYAKIOPvaITaA7QtkRyTs8b2sAYRGYdm
M86bqD0pg6GUZ71/Kg/Q2TdXPbeip92I6JmOTTikcizhRCCPFdLDJojwE712GWQ
q0I1n7tp8H6ufaIMeylciziv+9z+NcwYXTEe9RjNBMTMwHoYPWzV9u8JFHP0Pfe
Isy6cq7+MIUnPUAm33dQV8+iHcbhw6TCWzHVCIDAQABAOIBAQCt/fLA6pDzdVKV
UoNvUzgc1X6p4kyMuHbWlBBDUvxs4T5P9mf1kRCWk5dBULE1zGjeMrAnsaw5Wny
iRu+i9FLK4M495XJLFS3Espi483gHQn7B0/Lw1VQYxCex03rt+nae337eEkyrrH
afkq8PpNoJPmZ4C02jjkvma1trBPLHBhJ0zJ/ot5QtpDu0W+ISysZriUuo1IOPi
1VzKEl1T08oqZRTJTSqIbx12akk3C9QCua/F+BIGF6Tn76epHmPYGuYykoaAZcjAV
H9ryfKANhtz3B/sRza5lfrmqzTmoex03sayhf35x6rU68xGSWN5qCr761RJR7U
4bjopXehAoGBAPr+B51VQyuQ0Gih5fysbqX2sUDX2SEM1m55Ts+Xukrog7kc36XY
xTivObfZfUE6ERQhxmGjUD8ZsvHn6giL5PMSDnvFmIL3vg4ja90zAXHKgoR2kpph
IuGf0UOf/3+ZSTUjflR/OEzD9uiVRBPHeH58iwtZJ2YqmqJzMV0193AoGBAMJv
xFK1RZG7MMVXQ1JFYrk+C5A5VG80VVDYh0K+XNV6ThSHk1XqOrrIkCXzhY1qU14o
IuaS05+8ASbmJgx9LZLCE5xqHqHt1934WFF4G1BNC8hP9UR6ApnAtQwinWA+8k0
Ii/kAOKRAYAa2ENCt4gF/UdM38lhoiD7QSw2B7XXAoGBAIIJZs7Caa0wQ5WuxyT00
ibj/sN68uvNDK40sThXngrSgF0jgae+kGqkZt6wXfp5x/b5q5dCHQoR6330w4z6V
CM6ELilxsYczCu1kz/wNjibzOV16ByFOGUN77Ts8EjTkrbq2+RGUJbzxux6h6/OQ
qSW621F9k8cA3LSovbr2NtR5AoGAYDI7x0+346nhL0FFJWb+uPdhtFr/Li/od9E
bfKSSCNGjhGla1Q/SjoBjRaedKCuL19dJQZaxeqy/QTQvk0QSkroUqwnq6WJBWD
heS2Cl0g4tU6Z4g8bSkZ1TF0z2PJLnqEj30Wlj18ex3M8UaycnHEJYp7DX8oYrAw
RldU7HECgyBX4do2+E6pNLiy7uoXXCyIZdHqapMt+MAaiFmg5cCggXbnby3ftuxH
LDpMa6kZ/Yz10x2UuJi0QXvuh2wL1HlGCB+wJ8GgBI85FtIzaFht70wdR2HzhXY2
m1/RL5hgtSEBdLLDg9DEN27Pr8LnTtF+7RrFFVDWboeDvIm+sqigQ==
-----END RSA PRIVATE KEY-----
```

図9-5: CSR未署名の証明書と秘密鍵

図8 6: CSR未署名の証明書と秘密鍵

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

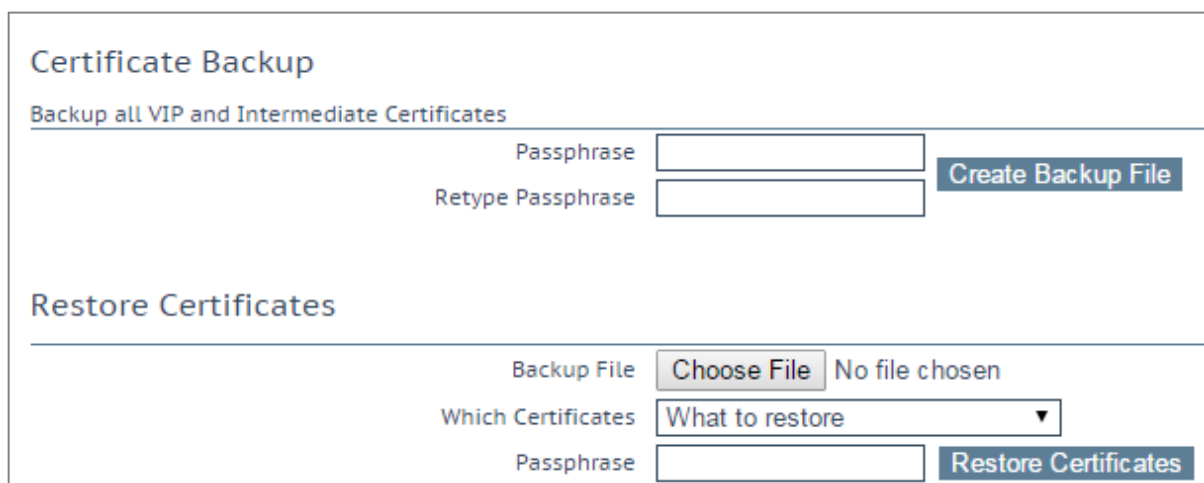


画面下部は、秘密鍵であり、安全な場所に保管する必要があります。秘密鍵は、認証局より送られてくる証明書とペアで使用する必要がありますが、このキーは誰にも渡すべきではありません。秘密鍵をコピーし、プレーンテキストファイルに貼り付けて（Microsoft Wordなど、アプリケーションは使用しないこと）、安全な場所で保管します。

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

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

9.4.1 HSMが有効でない場合



The screenshot shows a web interface for certificate management. It has two main sections: 'Certificate Backup' and 'Restore Certificates'. The 'Certificate Backup' section includes a link 'Backup all VIP and Intermediate Certificates', two input fields for 'Passphrase' and 'Retype Passphrase', and a 'Create Backup File' button. The 'Restore Certificates' section includes a 'Backup File' field with a 'Choose File' button and 'No file chosen' text, a 'Which Certificates' dropdown menu set to 'What to restore', a 'Passphrase' input field, and a 'Restore Certificates' button.

図9-6: 証明書のバックアップ/復元 - HSMが無効な場合

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

注意

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

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

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

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

9.4.2 HSMが有効な場合

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

注意

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

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

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

9.5Cipher Set（暗号セット）

Cipher Set Management

Cipher Set

Default

Available Ciphers

Filter:

Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High

Assigned Ciphers

Filter:

Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High

Save as:

Default

Save

図 9-7:暗号セットの管理

Cipher Set（暗号セット）

表示/編集する暗号セットを選択します。

以下に示すシステム定義の暗号セットが用意されています。

- Default（デフォルト）:現在のデフォルトの暗号セットはLoadMasterです。



- **Default_NoRc4**: Default_NoRc4の暗号にはデフォルトの暗号セットと同じ暗号が含まれますが、RC4暗号は含まれません (RC4は安全ではないとみなされています)。
- **BestPractices**: これは推奨の暗号セットです。この暗号セットは、後方互換性が不要なサービスで使われます。この暗号は、高いレベルのセキュリティを提供します。この設定は、Firefox 27、Chrome 22、IE 11、Opera 14、Safari 7に対応しています。
- **Intermediate_compatibility**: 古いクライアント (多くの場合、Windows XP) との互換性が不要なものの、幅広いクライアントをサポートする必要があるサービスについては、この設定を推奨します。この設定は、Firefox 1、Chrome 1、IE 7、Opera 5、Safari 1に対応しています。
- **Backward_compatibility**: これは古い暗号セットで、Windows XP/IE6のクライアントで動作します。これは最後の手段として使用してください。
- **WUI**: WUIの暗号セットとして使うことを推奨された暗号セットです。WUIの暗号セットは、“Admin WUI Access”画面で選択できます。詳細は[セクション9.7](#)を参照してください。
- **FIPS**: FIPS (連邦情報処理規格) に準拠した暗号です。
- **Legacy**: これは、OpenSSLが更新される前の古いロードマスターのファームウェア (v7.0~10) で使用されていた暗号セットです。

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

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

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

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

設定済みの暗号セットに対する変更は行えません。ただし、設定済みの暗号セットをベースにして必要な変更を行い、その暗号セットを新しいカスタム名で保存することがで



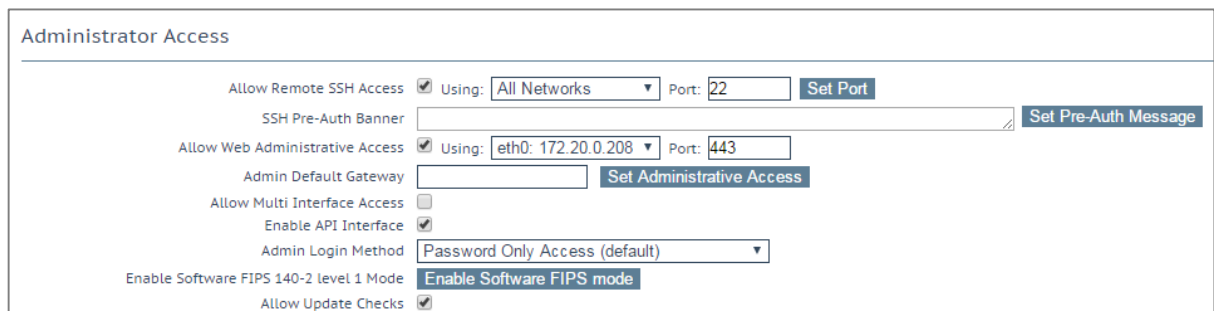
きます。“Save as”テキストボックスに新しい名前を入力し、“Save”ボタンをクリックします。カスタム暗号セットは、複数の仮想サービスで 사용할 수 있습니다。また、WUI의暗号セットとして割り当てることができます。

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

9.6 Remote Access (リモートアクセス)

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

9.6.1 管理者アクセス



The screenshot shows the 'Administrator Access' configuration page. It includes several settings: 'Allow Remote SSH Access' is checked with 'Using' set to 'All Networks' and 'Port' set to '22'; 'SSH Pre-Auth Banner' has a text input field and a 'Set Pre-Auth Message' button; 'Allow Web Administrative Access' is checked with 'Using' set to 'eth0: 172.20.0.208' and 'Port' set to '443'; 'Admin Default Gateway' has a text input field and a 'Set Administrative Access' button; 'Allow Multi Interface Access' is unchecked; 'Enable API Interface' is checked; 'Admin Login Method' is set to 'Password Only Access (default)'; 'Enable Software FIPS 140-2 level 1 Mode' has an 'Enable Software FIPS mode' button; and 'Allow Update Checks' is checked.

図10-37: 管理者アクセス

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

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

Using (使用)

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

Port (ポート)

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

SSH事前認証バナー



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

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

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

Webアクセスを無効にすることは推奨しません。

Using0

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

Port (ポート)

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

管理用デフォルトゲートウェイ

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

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

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

WUIとの接続にデフォルトで使用される証明書では、最初のWUIのIPアドレスが指定されています。そのため、この証明書は、他のインターフェイスにおけるWUIとの接続では機能しません。複数のインタ



ーフェイスのWUIを有効にするには、そのWUIのワイルドカード証明書
をインストールする必要があります。証明書についての詳細は、
アプリケーションファイアウォールパック（AFP）カスタムルールを
参照してください。

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

RADIUS Server (RADIUSサーバー)

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

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

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

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

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

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

応答メッセージ	ロードマスターの権限
real	実サーバー
vs	Virtual Services (仮想サービ ス)
rules	Rules (ルール)
backup	システムバックアップ
certs	証明書の作成



応答メッセージ	ロードマスターの権限
cert3	Intermediate Certificates（インターミディエート証明書）
certbackup	証明書のバックアップ
users	ユーザの管理
geo	OCSPの設定

表9-1: 応答メッセージ/ロードマスターの権限

応答メッセージの値は、“All Permissions”（すべて許可）を除き、図119のようにWUIのユーザー権限のページと対応させる必要があります。

User	Permissions
KEMPUser	Real Servers, Virtual Services, Rules, System Backup, Certificate Creation, Intermediate Certificates, Certificate Backup, User Administration, Geo Control

図 9-8: ユーザー権限のセクション

Windows版のRADIUSを設定するには、KEMPのWebサイトにあるRADIUSの認証と権限設定テクニカルノートを参照してください。

Linux版のFreeRADIUSサーバーを設定する場合、/etc/freeradius/usersの指定されたセクションに、以下のテキストを挿入してください。以下に、“LMUSER”ユーザーの権限を設定する例を示します。

LMUSER Cleartext-Password := “1fourall”

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

また、/etc/freeradius/clients.confを設定してロードマスターのIPアドレスを含める必要があります。このファイルには、RADIUSに接続可能なIPアドレスの一覧が記述されています。

セッション管理が有効になっている場合、この画面で“RADIUS Server”オプションは使用できません。セッション管理が有効なときにRADIUSサーバーを設定する方法については、Section 9.6.4を参照してください。

Enable API Interface (APIインターフェイスを有効にする)

RESTfulアプリケーション・プログラム・インターフェイス (API) を有効/無効にします。



Admin Login Method (ログイン方式の管理)

このオプションは、セッション管理が有効な場合のみ表示されます。セッション管理についての詳細は、**セクション9.7**または**ユーザー管理 機能説明**を参照してください。

ロードマスターWUIにアクセスするためのログインオプションを指定します。以下のオプションが利用可能です。

- **Password Only Access (default) (パスワードのみのアクセス (デフォルト))** : このオプションを選択すると、ユーザー名とパスワードを用いたアクセスのみ可能になります。クライアント証明書によるアクセスはできません。
- **Password or Client certificate (パスワードまたはクライアント証明書)** : ユーザーは、ユーザー名/パスワードまたは有効なクライアント証明書を用いてログインできます。有効なクライアント証明書が存在する場合、ユーザー名とパスワードは必要ありません。

クライアントは、証明書を提供するように求められます。クライアント証明書が提供されると、ロードマスターはその証明書が一致するかチェックします。ロードマスターは、提供された証明書がローカルに保存されている証明書と一致するかチェックします。または、提供された証明書のサブジェクト代替名 (SAN) もしくはコモンネーム (CN) が一致するかチェックします。照合を行う際、CNよりもSANが優先的に使用されます。一致するものがあった場合、ユーザーはそのロードマスターへのアクセスを許可されます。この動作は、APIとユーザーインターフェイスのどちらでも機能します。

証明書が無効な場合はアクセスは許可されません。

クライアント証明書が提供されない場合、ロードマスターは、ユーザー名とパスワードが提供されることを期待します (APIを使用する場合)。または、標準のWUIログインページからパスワードを入力するようユーザーに要求します。

- **Client certificate required (クライアント証明書が必要)** : クライアント証明書を用いたアクセスのみ許可します。ユーザー名とパスワードによるアクセスはできません。SSHのアクセスは、このオプションによる影響を受けません (balユーザーのみSSH経由でログイン可能)。
- **Client certificate required (Verify via OCSP) (クライアント証明書が必要 (OCSP経由で照合))** : これは“Client certificate required”オプションと同じですが、クライアント証明書はOCSPサービス経由で照合されます。このオプション



ンが機能するには、OCSPサーバーを設定する必要があります。OCSPサーバーの設定に関する詳細は、**セクション9.5**を参照してください。

クライアント証明書を用いた方式に関して、以下の点に注意する必要があります。

- balユーザーはクライアント証明書を持っていません。そのため、“Client certificate required”方式を用いてbalとしてロードマスターにログインすることはできません。ただし、bal以外のユーザーを作成し、そのユーザーに“All Permissions”の権限を与えることができます。これにより、balユーザーと同じ機能を実現することができます。
- クライアント証明書でログインした場合、ログアウトすることはできないため（ログアウトしても次回アクセス時に自動的に再度ログインされる）、クライアント証明書でログインしたユーザーに対するログアウトオプションはありません。ページを閉じるかブラウザを再起動すると、セッションが終了します。

クライアント証明書によるWUI認証に関する詳細（ステップバイステップの設定方法など）は、**ユーザー管理 機能説明**を参照してください。

Enable Software FIPS 140-2 level 1 Mode（ソフトウェアFIPS 140-2レベル1モードを有効にする）

セッション管理が無効な場合、FIPSモードを有効にできません。セッション管理についての詳細は、**セクション9.7**を参照してください。

このロードマスターをFIPS 140-2レベル1で認定されたモードに切り替えます。有効にするにはロードマスターを再起動する必要があります。

FIPSを有効にする前に、数多くの警告が表示されます。ロードマスターでFIPSを有効にすると、FIPSを簡単には無効にできません。ロードマスターで有効になっているFIPSを無効にしたい場合は、KEMPのサポートにお問い合わせください。



図 9-9:FIPS-1モード

ロードマスターがFIPSレベル1モードになっている場合、ロードマスターWUIの右上に“FIPS-1”と表示されます。



FIPSレベル1では、非FIPSロードマスターとは異なる暗号セットを持っています。“Default”（デフォルト）の暗号セットが用意されていますが、これ以外のシステム定義の暗号セットを選択することはできません。

Allow Update Checks（アップデートのチェックを許可する）

KEMPのWebサイトにソフトウェアの新しいバージョンがあるかどうかをロードマスターが定期的にチェックするのを許可します。

9.6.2 GEOの設定

GEO Settings	
Remote GEO LoadMaster Access	Set GEO LoadMaster access
GEO LoadMaster Partners	10.154.11.10 172.20.0.184 Set GEO LoadMaster Partners
GEO LoadMaster Port	22 Set GEO LoadMaster Port
GEO Update Interface	eth0: 10.154.11.60

図10-38:GEOの設定

Remote GEO LoadMaster Access（GEOロードマスターのリモートアクセス）

LoadMaster-GEO, LoadMaster-DR、もしくはVLM-DRと併用して使用する時に、状態監視を受け付けるために相手のIPアドレスを設定します。アドレスはスペースで区切ります。HAモードにある場合、共有アドレスの入力のみ必要です。

GEO LoadMaster Partners（GEOロードマスターパートナー）ロードマスターの分散パートナー

GEO機能はGSLB機能パックに含まれており、ロードマスターに適用されているライセンスに基づいて有効になります。GSLB機能パックを利用するには、ライセンスをアップグレードする必要があるので、KEMPにご連絡ください。

パートナーGEOロードマスターのアドレスを設定します。アドレスはスペースで区切ります。このGEOロードマスターは、DNSの設定をシンクに保持しています。



GE0ロードマスターのパートナーを設定する前に、正しい設定/推奨設定を持つ該当するGE0ロードマスターのバックアップを作成する必要があります。そして、このバックアップを、オリジナルのロードマスターのパートナーとなるロードマスターに保存する必要があります。詳細および手順については、GE0 製品概要を参照してください。

最大64個のGE0 HAパートナーのアドレスを追加できます。選択基準の詳細については、を参照してください。

GE0 LoadMaster Port (GE0ロードマスターのポート)

上記“Remote GE0 LoadMaster Access”のポート番号を設定します。SSHプロトコルが使用されますので、通常ポート番号22を使用します。

GE0 update interface (GE0更新インターフェイス)

SHパートナートンネルを作成するGE0インターフェイスを指定します。このインターフェイスを介して、GE0パートナーは情報をやり取りします。

9.6.3 GE0パートナーのステータス

このセクションはGE0パートナーが設定されている場合のみ表示されます。

GE0 Partners Status	
10.154.11.10	■
172.20.0.184	■

図10-39:GE0パートナーのステータス

GE0パートナーの緑のステータスは、2つのパートナーがお互いに見える状態にあることを示しています。

GE0パートナーの赤のステータスは、ロードマスターが通信できないことを示しています。その原因のひとつとして、いずれかのパートナーの電源がオフになっていることが考えられます。この場合、停電が発生しているか、ケーブルが接続されていない可能性があります。



GE0パートナーの更新に失敗すると、そのパートナーに対するGE0の更新が失敗したことを示すエラーメッセージがログに表示されます。このメッセージには、そのパートナーのIPアドレスが表示されます。

9.6.4 WUI Authentication and Authorization (WUIによる認証と権限設定)

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

“Remote Access”（リモートアクセス）画面の“WUI Authorization Options”（WUI認証オプション）ボタンをクリックすると、“WUI Authentication and Authorization”（WUIによる認証と権限設定）画面が表示されます。このオプションは、セッション管理が有効になっているときのみ表示されます。

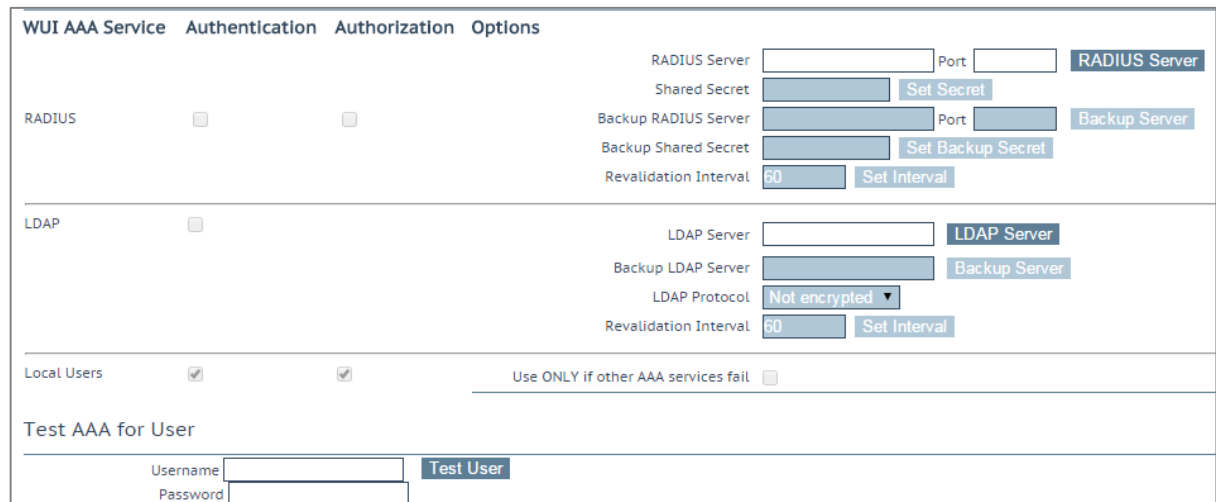


図 9-10: WUIの認証および承認

WUIによる認証と権限設定画面では、認証（ログイン）と権限設定（権限の許可）に関するオプションを管理できます。

Authentication (認証)

ユーザーは、ロードマスターにログインする前に認証を受ける必要があります。ロードマスターでは、ローカルユーザーの認証方式の他に、RADIUSおよびLDAPによる認証方式を用いてユーザー認証を行えます。

すべての認証方式が選択されている場合、ロードマスターは以下の順序でユーザー認証を試みます。

1. RADIUS
2. LDAP

3. ローカルユーザー

例えば、RADIUSサーバーを利用できない場合、LDAPサーバーが使用されます。LDAPサーバーも利用できない場合は、ローカルユーザーの認証方式が使用されます。

RADIUSによる認証方式もLDAPによる認証方式も選択されていない場合は、デフォルトでローカルユーザーの認証方式が選択されます。

Authorization (権限設定)

ロードマスターでは、RADIUSを用いて（またはローカルで）ユーザーに権限を設定できます。ユーザー権限の設定では、ユーザーがロードマスターのどの機能をどのレベルまで使用できるかを設定できます。

RADIUSによる認証方式を使用している場合、RADIUSによる権限設定のみ行えます。

権限設定方式が両方とも選択されている場合、ロードマスターは、まず始めにRADIUSによる権限設定を試みます。RADIUSによる権限設定を利用できない場合、ロードマスターは、ローカルユーザーの権限設定方式を使用します。なお、LDAPによる権限設定はサポートしていません。

RADIUSによる権限設定方式が選択されていない場合は、デフォルトでローカルの権限設定方式が選択されます

以下に示すのは、RADIUSサーバーによる認証が適切に機能する上で必要な設定の例です。

以下の例は、Linux専用です。

“Reply-Message”には、許可する権限の種類をそのまま指定する必要があります。具体的には、“All Permissions”を除く、WUIのユーザー権限のページに対応させる必要があります。

LMUSER Cleartext-Password := “1fourall”

Reply-Message = “real, vs, rules, backup, certs, cert3, certbackup, users” balユーザーは常に、ローカルユーザーの認証および承認方式に基づいて認証および承認されます。



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

RADIUS Server (RADIUSサーバー)

WUIからロードマスターへアクセスするユーザーの認証に使うRADIUSサーバーのアドレスとポート番号を入力します。

Shared Secret (共有秘密鍵)

RADIUSサーバーの共有秘密鍵を入力します。

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

Backup RADIUS Server (バックアップ用RADIUSサーバー)

WUIからロードマスターへアクセスするユーザーの認証に使うバックアップ用RADIUSサーバーのアドレスとポート番号を入力します。このサーバーは、メインのRADIUSサーバーが故障したときに使用されます。

Backup Shared Secret (バックアップ用共有秘密鍵)

このテキストボックスには、バックアップRADIUSサーバーの共有秘密鍵を入力します。

Revalidation Interval (再認証間隔)

RADIUSサーバーがユーザーを再認証する頻度を指定します。

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

LDAP Server (LDAPサーバー)

WUIからロードマスターへアクセスするユーザーの認証に使うLDAPサーバーのアドレスとポート番号を入力します。

Backup LDAP Server (バックアップ用LDAPサーバー)

WUIからロードマスターへアクセスするユーザーの認証に使うバックアップ用LDAPサーバーのアドレスとポート番号を入力します。このサーバーは、メインのLDAPサーバーが故障したときに使用されます。

LDAP Protocol (LDAPプロトコル)

LDAPサーバーとの通信で使用する転送プロトコルを選択します。

“Not encrypted”、“StartTLS”、“LDAPS”のオプションを選択できます。



Revalidation Interval (再認証間隔)

LDAPサーバーがユーザーを再認証する頻度を指定します。

Local Users Configuration (ローカルユーザーの設定)

Use ONLY if other AAA services fail (AAAサービスが失敗したときのみ使用)

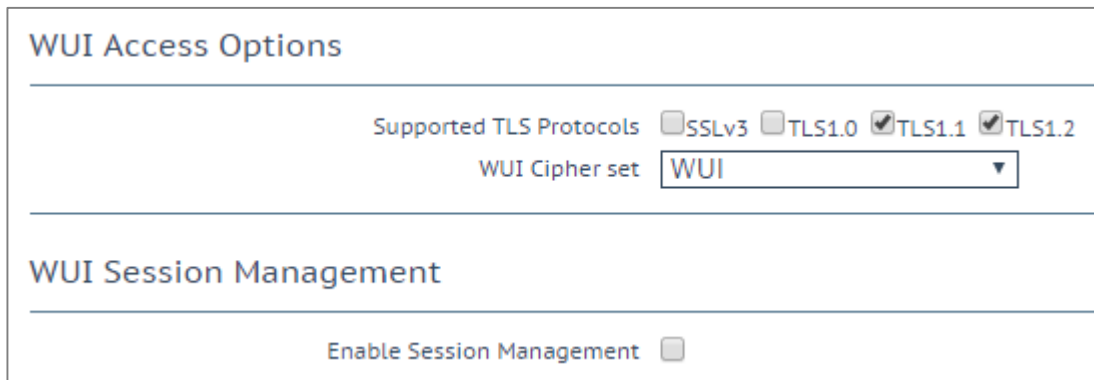
このオプションを選択すると、RADIUSおよびLDAPによる認証/権限設定方式に失敗したときのみ、ローカルユーザーの認証/権限設定方式が使用されます。

Test AAA for User (ユーザーのAAAをテスト)

ユーザーの資格情報をテストするには、“Username”および“Password”フィールドにそのユーザーのユーザー名とパスワードを入力して、“Test User”ボタンをクリックします。

これで、そのユーザーの認証に成功したかどうかを示すメッセージが表示されます。この機能を使用すると、ログイン/ログアウトを必要とせずに、ユーザーの認証情報をチェックできます。

9.7 管理用WUIへのアクセス



The screenshot shows two sections of a configuration interface. The top section, titled "WUI Access Options", contains "Supported TLS Protocols" with checkboxes for SSLv3, TLS1.0, TLS1.1, and TLS1.2. TLS1.1 and TLS1.2 are checked. Below this is a "WUI Cipher set" dropdown menu currently set to "WUI". The bottom section, titled "WUI Session Management", contains an "Enable Session Management" checkbox which is currently unchecked.

図 9-11: 管理用WUIへの設定

Supported TLS Protocols (サポートされているTLSプロトコル)

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

FIPSモードが有効な場合、TLS1.1およびTLS1.2のみ選択可能です。

WUI Cipher set (WUI暗号セット)

WUIへのアクセスに使用する暗号セットを選択します。利用可能な暗号セットについては、[セクション9.5](#)を参照してください。

WUI Session Management (WUIセッション管理)

WUI Session Management

Enable Session Management

☒

Require Basic Authentication

☒

Basic Authentication Password

Please set password

Set Basic Password

Failed Login Attempts

3

Set Fail Limit (Valid values:1-999)

Idle Session Timeout

600

Set Idle Timeout (Valid values: 60-86400)

Limit Concurrent Logins

0 (No limit)

Pre-Auth Click Through Banner

Set Pre-Auth Message

図 9-12:WUIセッション管理 (balユーザー)

ユーザー権限のレベルに応じて、WUIのどのセッション管理フィールドが表示・編集可能になるかが決まります。権限の詳細については以下の表を参照してください。

制御	Balユーザー	‘All Permissions’ (すべての権限)を持つユーザー	‘User Administration’ (ユーザー管理)の権限を持つユーザー	その他のすべてのユーザー
セッション管理	Modify (変更)	表示	表示	None (なし)
Require Basic Authentication (基本認証が必要)	Modify (変更)	表示	表示	None (なし)
Basic Authentication Password (基本認証パスワード)	Modify (変更)	表示	表示	None (なし)
Failed Login Attempts (ログイン試行回数)	Modify (変更)	Modify (変更)	表示	None (なし)
Idle Session Timeout (アイドルセッションのタイムアウト)	Modify (変更)	Modify (変更)	表示	None (なし)



制御	Bal ユーザー	‘All Permissions’ (すべての権限) を持つユーザー	‘User Administration’ (ユーザー管理) の権限を持つユーザー	その他のすべてのユーザー
Limit Concurrent Logins (同時ログインを制限する)	Modify (変更)	Modify (変更)	表示	
Pre-Auth Click Through Banner (事前認証クリックスルーバナー)	Modify (変更)	Modify (変更)	表示	None (なし)
Currently Active Users (現在アクティブなユーザー)	Modify (変更)	Modify (変更)	表示	None (なし)
Currently Blocked Users (ブロックされたユーザー)	Modify (変更)	Modify (変更)	表示	None (なし)

表9-2: WUIセッション管理の権限

WUIセッション管理を使用する場合、1段階認証または2段階認証を使用できます。

“Enable Session Management” (セッション管理を有効にする) チェックボックスがオンになっており、“Require Basic Authentication” (基本認証が必要) が無効になっている場合、ユーザーはローカルのユーザー名とパスワードだけでログインできます。“bal”または“user”を使用してのログインは求められません。

“Enable Session Management” (セッション管理を有効にする) と“Require Basic Authentication” (基本認証が必要) のチェックボックスが両方ともオンになっている場合、ロードマスターWUIにアクセスするには2段階認証が必要です。最初の段階は基本認証で、“bal”または“user”でログインします (これらはシステムで定義されたデフォルトのユーザー名です)。

userユーザーが用意されているのは、管理者がbalユーザーの証明書ではなくuserユーザーの証明書を提供できるようにするためです。userユーザーのパスワードを設定するには、“Basic Authentication Password”テキストボックスを設定します。“Basic Authentication Password”はbalユーザーのみ設定できます。

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

Enable Session Management (セッション管理の有効化)



“Enable Session Management”チェックボックスをオンにすると、WUIセッション管理機能が有効になります。このとき、すべてのユーザーは通常の証明書を使用してセッションにログインする必要があります。

このチェックボックスをオンにした場合、ユーザーは、引き続きロードマスターを使用するためにログインする必要があります。

LDAPユーザーは、ログイン時に完全なドメイン名を入力する必要があります。例えば、LDAPのユーザー名として、**test**ではなく**test@kemp.com**と入力する必要があります。

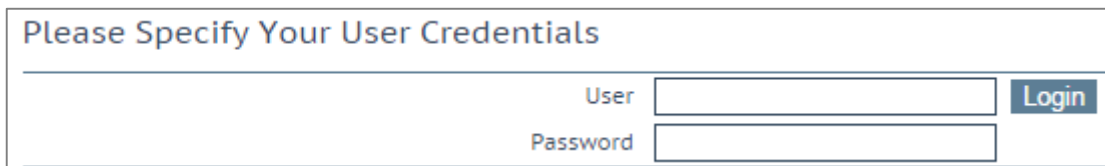


図 9-13: ユーザー資格情報

ログインしたユーザーは、画面の右上隅にある“Logout”ボタンをクリックしてログアウトできます。

WUIのセッション管理機能を有効にすると、WUIのセッション管理オプションがすべて表示されます。

Require Basic Authentication (基本認証が必要)

WUIセッション管理と基本認証が両方とも有効になっている場合、ロードマスターにアクセスするには2段階認証が必要です。最初の段階は基本認証で、“bal”または“user”でログインします（これらはシステムで定義されたデフォルトのユーザー名です）。

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

Basic Authentication Password (基本認証パスワード)

“user”ログイン用の基本認証パスワードを設定するには、“Basic Authentication Password”テキストボックスにパスワードを入力して、“Set Basic Password”ボタンをクリックします。



パスワードは、アルファベットと数字を組み合わせ、8文字以上になるように設定してください。パスワードが弱すぎると判断された場合、新たにパスワードを入力するよう求めるメッセージが表示されます。

“bal” ユーザーのみ、基本認証パスワードを設定できます。

Failed Login Attempts (ログイン試行回数)

このテキストボックスでは、ログインの失敗回数を指定して、この回数を上回ってログインに失敗したユーザーをブロックするよう設定できます。入力できる値の範囲は、1から999までです。

ユーザーがブロックされた場合、“bal” ユーザーまたは“All Permissions”の権限が設定されたユーザーのみ、ブロックされたユーザーのブロックを解除できます。

“bal” ユーザーがブロックされた場合、“bal” ユーザーが再度ログインできるようになるまで10分間の“クールダウン”期間が設けられています。

Idle Session Timeout (アイドルセッションのタイムアウト)

ユーザーがセッションからログアウトされる前に、ユーザーがアイドル状態（何も操作が記録されない状態）でいられる期間を秒で指定します。60～86400（1分～24時間）の値を入力できます。

Limit Concurrent Logins (同時ログインを制限する)

ロードマスターの管理者は、このオプションを使用して、1人のユーザーがロードマスターWUIに1度にログインできる数を制限できます。

この値は0～9の範囲で選択できます。

値を0にすると、ログイン数が制限されなくなります。

入力した値はトータルのログイン数を表します。この値には“bal”ユーザーのログインが含まれます。

Pre-Auth Click Through Banner (事前認証クリックスルーバナー)

ロードマスターのWUIログインページの前に表示される事前認証クリックスルーバナーを設定します。このフィールドにはプレインテキストまたはHTMLコードを入力できます。



このフィールドにはJavaScriptは入力できません。このフィールドには5,000文字まで入力できます。

Active and Blocked Users (アクティブなユーザーおよびブロックされたユーザー)

“bal” ユーザーまたは“All Permissions”の権限が設定されたユーザーのみ、この機能を使用できます。“User Administration”の権限が設定されたユーザーの場合、画面上のボタンや入力フィールドはすべてグレー表示になります。その他のユーザーの場合、この部分は画面上に表示されません。

Currently Active Users		
User	Logged in since	Operation
bal	Tue Sep 8 14:57:20 UTC 2015	Force logout Block user

図9-14: 現在アクティブなユーザー

Currently Active Users (アクティブなユーザー)

このセクションには、ロードマスターにログインしている全ユーザーのユーザー名とログイン時刻がリスト表示されます。

ユーザーを直ちにログアウトさせ、システムに再度ログインするよう強制するには、“Force logout”ボタンをクリックします。

ユーザーを直ちにログアウトさせ、システムにログインできないようそのユーザーをブロックするには、“Block user”ボタンをクリックします。ブロックされたユーザーは、ブロックが解除されるか、ロードマスターが再起動するまで、システムに再度ログインできません。“Block user”ボタンをクリックしても、そのユーザーを強制的にログオフできません。この場合、“Force logout”ボタンをクリックする必要があります。

ユーザーがログオフせずにブラウザを終了した場合、そのセッションは、タイムアウトになるまでアクティブなユーザーのリストでオープンになったままとなります。その後、タイムアウトになる前にそのユーザーが再度ログインすると、そのユーザーは別のセッションでログインされます。

Currently Blocked Users (ブロックされたユーザー)

このセクションには、ユーザーがブロックされた時点でのユーザー名とログイン時刻がリスト表示されます。



ブロックされたユーザーのブロックを解除して、再度システムにログインできるようにするには、“Unblock”ボタンをクリックします。

9.80CSPの設定

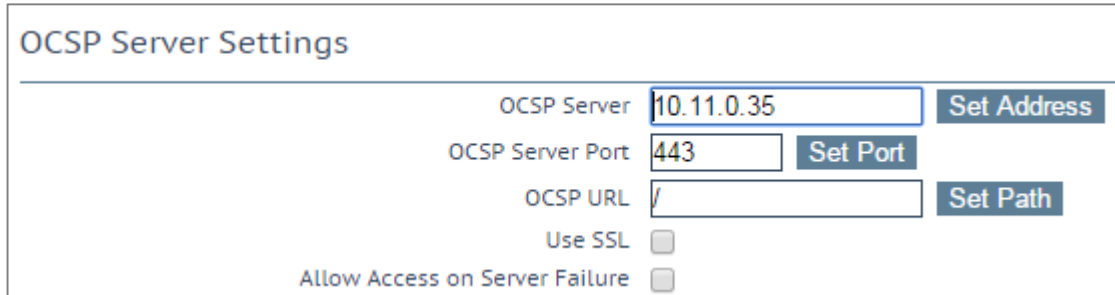


図9-15:OCSPサーバーの設定

OCSP Server (OCSPサーバー)

OCSPサーバーのアドレスです。

OCSP Server Port (OCSPサーバーポート)

OCSPサーバーのポートです。

OCSP URL

OCSPサーバーにアクセスするためのURLです。

Use SSL (SSLを使用する)

SSLを使用してOCSPサーバーに接続する場合はこのオプションを選択します。

Allow Access on Server Failure (サーバー障害発生時のアクセスを許可する)

OCSPサーバーが有効な応答を返したものであるとして（クライアント証明書が有効であるものとして）OCSPサーバー接続障害またはタイムアウトを処理します。

9.9HSMの設定

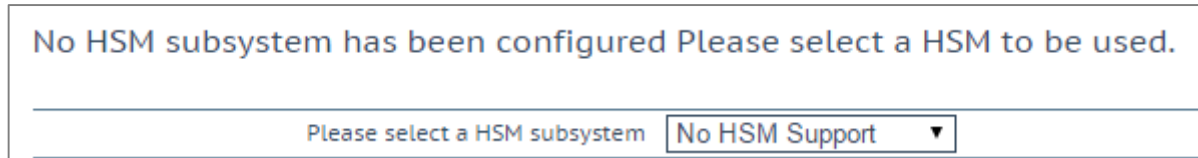


図9-16:HSMをサポートしない場合

Please select a HSM subsystem (HSMサブシステムを選択してください)

このドロップダウンメニューでは2つのオプションが用意されています。

- No HSM Support (HSMをサポートしない)
- Safenet Luna HSM

HSMを使用するには、“**Safenet Luna HSM**”を選択して設定を行ってください。

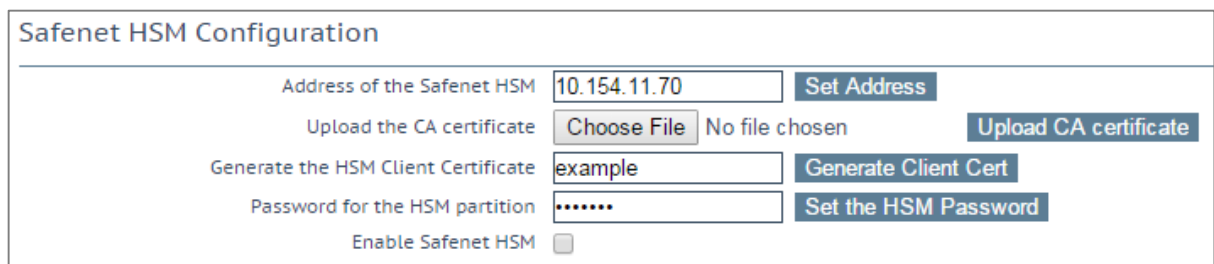


図9-17:Safenet HSMの設定

Address of the Safenet HSM (Safenet HSMのアドレス)

使用するSafenetユニットのIPアドレスを入力します。

Upload the CA certificate (CA証明書のアップロード)

HSMからダウンロードした証明書をアップロードします。

Generate the HSM Client Certificate (HSMクライアント証明書の生成)

HSMにアップロードするローカルクライアントの証明書を生成します。ここで指定する名前は、ロードマスターのFQDN名である必要があります。この名前は、HSMのclient registerコマンドで使用されます。

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

ロードマスターがHSMにアクセスできるように、HSMにおけるパーティションのパスワードを指定します。

証明書を生成するまで、パーティションのパスワードは指定できません。

Enable Safenet HSM (Safenet HSMを有効にする)

このチェックボックスを使用すると、HSMを有効/無効にできます。

HSMの起動には時間がかかる場合があります。

HSMを無効にすると、新たにHSMが追加されるか証明書の設定が変更されるまで、ロードマスターが新たなSSL (HTTPS) 接続を作成できなくなり、既存の接続が直ちにドロップされます。

アクティブなSSL接続が存在しない場合のみHSMの設定を変更することを強く推奨します。

10 System Configuration (システム用設定)

10.1 ネットワークの設定

10.1.1 Interfaces (インターフェイス)

外部ネットワークと内部ネットワークのインターフェイスについて規定します。この画面には、eth0およびeth1イーサネットポートで同じ情報が用意されています。以下の例は、非高可用性（HA）ユニットのeth0の場合です。

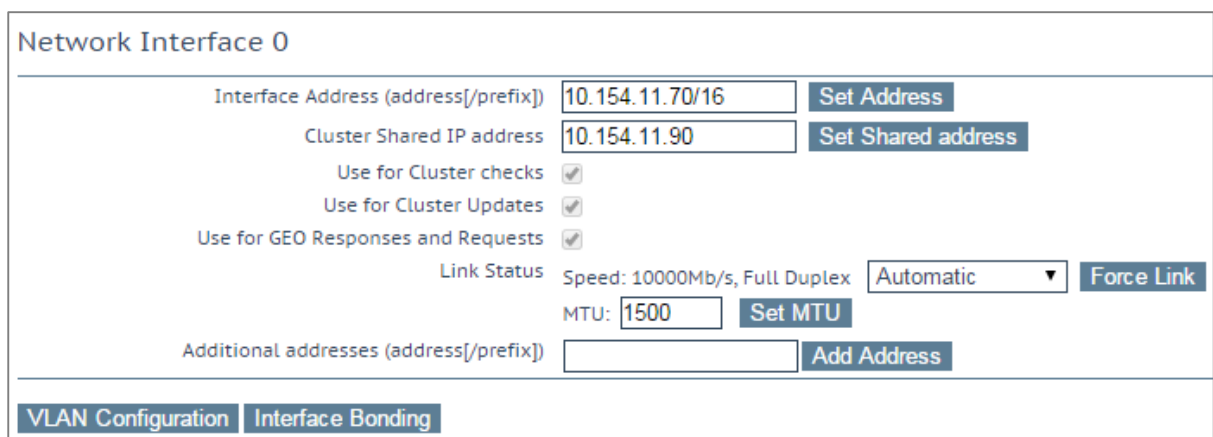


図10-1: ネットワークインターフェイスのオプション

Interface Address (インターフェイスアドレス)

“Interface Address (address[/prefix])”テキストボックスにて、このインターフェイスのインターネットアドレスを指定できます。

Cluster Shared IP address (クラスターの共有IPアドレス)

クラスターへのアクセスに使用できる共有IPアドレスを指定します。これは、サーバーのNATを使用する際のデフォルトのソースアドレスとしても使用されます。

“Clustering”のオプションは、ロードマスターにクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMPの担当者にお問い合わせください。クラスタリングについての詳細は、ロードマスターのクラスタリング 機能説明を参照してください。

Use for Cluster checks (クラスターのチェックで使用)

このオプションを使用すると、ノード間でクラスターのヘルスチェックを行うことができます。少なくとも1つのインターフェイスを有効にする必要があります。

Use for Cluster Updates (クラスターの更新で使用)

これは、クラスターの同期動作のためのインターフェイスです。

Speed (速度)

デフォルトでは、リンクのSpeed (速度) は自動的に検出されます。構成によってはこの速度は適切でない場合があるため、値を指定する必要があります。

Use for Default Gateway (デフォルトゲートウェイで使用)

“Use for Default Gateway”チェックボックスを使用できるのは、“Network Options”画面で“Enable Alternate GW support”が選択されている場合に限定されます。表示対象の設定がデフォルトのインターフェイス用である場合、このオプションは灰色表示で選択されている状態です。このオプションを別のインターフェイスで有効にするには、左側にあるメインメニューでインターフェイスをクリックし、そのインターフェイスに移動します。これで、このオプションを選択できる状態になります。

Allow Administrative WUI Access (管理用WUIへのアクセスを許可)

このオプションは、“Miscellaneous Options > Remote Access”の“Allow Multi Interface Access”チェックボックスがオンの場合のみ利用できます。

これらのオプションを2つとも有効にすると、該当するインターフェイスのIPアドレスと、そのインターフェイスに設定された“Additional addresses” (追加アドレス) からWUIにアクセスできます。

これらの全アドレスに対して1つのインターフェイスのみ割り当てられます。そのため、ワイルドカード証明書以外の証明書を使用すると問題が生じるおそれがあります。証明書についての詳細は、アプリケーションファイアウォールパック (AFP) カスタムルールを参照してください。



最大64個のネットワークインターフェイスを追跡できます。また、トータルで最大1024個のアドレスがシステムによりリッスンされます。

Use for GEO Responses and Requests (GEOの応答/要求に使用)

デフォルトでは、デフォルトゲートウェイを使用してDNS要求をリッスンして応答を返します。このフィールドを使用すると、他のインターフェイスでもリッスンできるようになります。

このオプションは、デフォルトゲートウェイを含むインターフェイスでは無効にできません。デフォルトではeth0に設定されています。

このオプションを有効にすると、GEOはそのインターフェイスで設定された“Additional addresses”でもリッスンします。

MTU

“MTU” フィールドでは、このインターフェイスから送信されるイーサネットフレームの最大サイズを指定できます。有効範囲は512～9216です。

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

Additional addresses (追加アドレス)

“Additional addresses”フィールドを使用すると、ロードマスターから複数のアドレスを各インターフェイスにエイリアスとして提供できます。この機能は、「ルーター・オン・ア・スティック」と呼ばれることがあります。この機能では、標準IP+CIDR形式のIPv4アドレスとIPv6アドレスの両方が使用できるので、同じインターフェイス上でIPv4アドレスとIPv6アドレスが混在するモードも実現できます。ここで追加したサブネットはすべて、仮想IPアドレスと実サーバーIPアドレスの両方で使用できます。



HA

ユニットがHA構成の一部である場合、いずれかのインターフェイスをクリックすると、次の画面が表示されます。

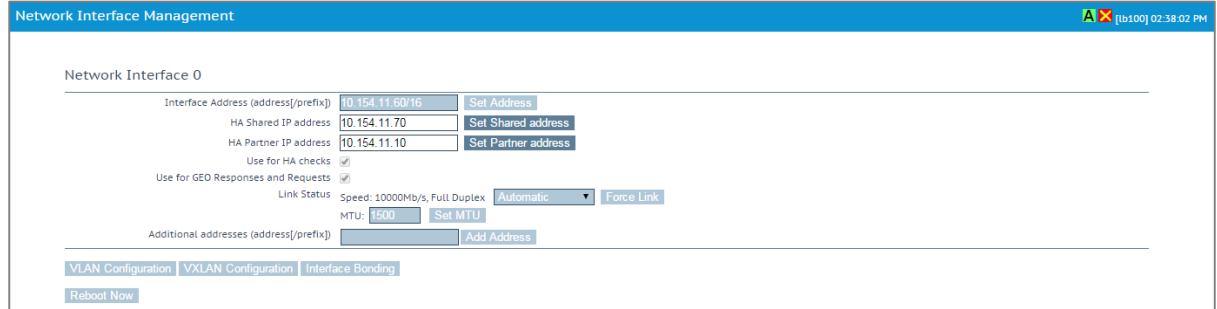


図10-2: ネットワークインターフェイスの管理 - HA

この画面では、ユーザーに下記を示唆します。

- これはペアのマスターマシン（画面の左上）です。
- このシステムは アップ状態であり、ペアを組む相手マシンはダウンしています（緑と赤のアイコン）。
- このインターフェイスアドレスは、このユニット自身のIPアドレスです。
- “HA Shared IP address”。ペアを組む相手マシンのIPアドレスです。
- ペアマシンのIPアドレス
- このインターフェイスは、HAヘルスチェックが有効になっています。
- このインターフェイスは、デフォルトゲートウェイとして使用されています。
- リンクの速度が自動的に検出されています（Link Status）。
- このインターフェイスの代替アドレスは登録されていません（Additional addresses）

ボンディング/チーミングの設定

ボンディングインターフェイスを作成する前に、以下の点に注意してください。

- 親より大きい番号のボンディングインターフェイスのみ作成できます。例えば、ポート10から始まるように指定した場合、ポート11以降のインターフェイスのみ作成できます。
- VLANタギングが必要な場合、まず始めにリンクをボンディングし、ボンディングの設定が終わった後にVLANを追加してください。
- ボンディングされたインターフェイスにリンクを追加するには、まず始めに、追加するリンクからIPアドレスを削除する必要があります。



- 通常、“Active-Backup” モードを有効にする際にスイッチ側の設定は必要ありません。
- eth0とeth1をボンディングすると深刻な問題が発生する可能性があるため、このボンディングは許可されていません。

“Interface Bonding”ボタンをクリックし、ボンディングを要求します。

“Create a bonded interface”ボタンをクリックし、ボンディングの作成を実行します。

警告ダイアログを確認します。

ウェブユーザーインターフェイス (WUI) を使用して、“System Configuration > Interfaces > bndx” メニューオプションを選択します。

“bndX”インターフェイスが表示されない場合、ブラウザの表示を更新し、ボンディングインターフェイスを選択して、“Bonded Devices”ボタンをクリックします。

目的のボンディングモードを選択します。

ボンディングにインターフェイスを追加します。

ボンディングインターフェイスのIPアドレスとサブネットマスクを設定します。

ボンディング／チーミングの解除

ボンディングポートに VLAN が設定されている場合は、まずこれらの設定を削除します。これらを削除しないとボンディングを解除したポートの最初の親ポートにこれらの設定が残ります。

“System Configuration > Interfaces > bndx”メニューオプションを選択します。“bndX”インターフェイスが表示されない場合、ブラウザの表示を更新し、ボンディングインターフェイスを選択して、“Bonded Devices”ボタンをクリックします。

ポートのボンディングを解除するには、“Unbind Port”ボタンをクリックします（すべてのポートのボンディングが解除されるまでこの作業を繰り返します）。

子ポートのボンディングをすべて解除したら、“Unbond this interface”ボタンをクリックして親ポートのボンディングを解除できます。

Adding a VLAN (VLANの追加)

インターフェイスを選択し、“VLAN Configuration”ボタンをクリックします。



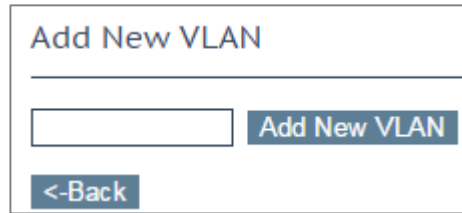


図10-3:VLAN Id

“VLAN Id” に値を入力し、“Add New VLAN” メニューオプションを選択します。

必要に応じて、手順を繰り返します。VLANを表示するには、“System Configuration” > “Network Setup”メニューオプションを選択してドロップダウンリストを展開します。

Removing a VLAN (VLANの削除)

VLANを削除する前に、インターフェイスが他の用途（マルチキャストインターフェイス、WUIインターフェイス、SSHインターフェイス、GEOインターフェイスなど）で使用されていないことを確認してください。

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

VLAN IDを選択したら、IPアドレスを削除して、“Set Address”をクリックします。IPアドレスが削除されたら、“Delete this VLAN”ボタンをクリックし、VLANを削除します。

必要に応じて、手順を繰り返します。VLANを表示するには、“System Configuration > Interfaces”メニューオプションを選択して、ドロップダウンリストから目的のVLAN IDを選択します。

Adding a VXLAN (VXLANの追加)

目的のインターフェイスを選択し、“VXLAN Configuration” (VXLANの設定) ボタンをクリックします。

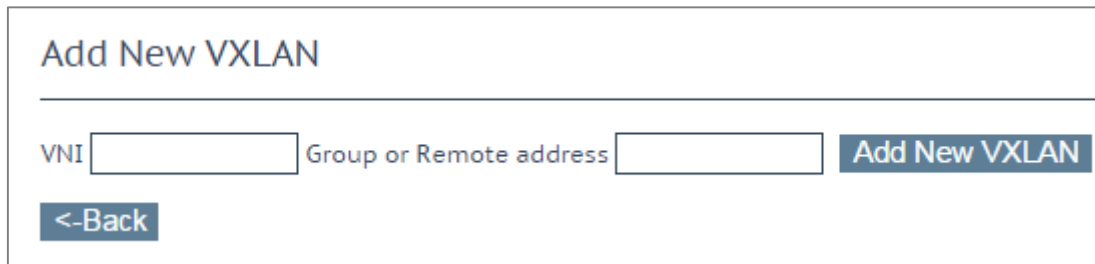


図 10-4:VXLANの新規追加

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

VXLANを編集するには、“System Configuration > Interfaces”を選択して、ドロップダウンリストから目的のVXLANを選択します。

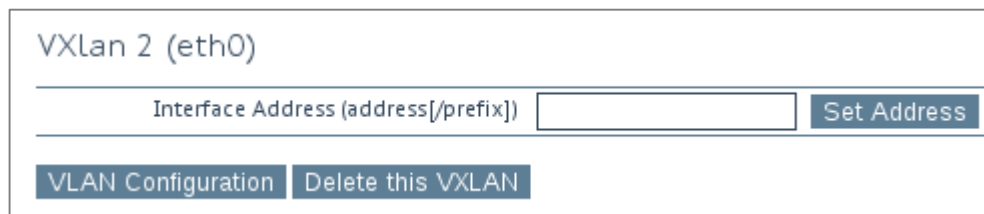


図 10-5:VXLANの編集

この画面では、VXLANのインターフェイスアドレスを指定できます。また、この画面ではVXLANの削除も行えます。

HAが有効になっている場合、VXLANにてHAパラメーターの設定が行えます。

- “HA Shared IP address”。これは、HAペアの設定で使用するIPアドレスです。
- パートナーマシンのIPアドレス
- このインターフェイスをHAヘルスチェックで使用するかどうかを指定します。

10.1.2 ホストとDNSの設定

Set Hostname

Hostname Set Hostname

DNS NameServer (IP Address)

172.20.0.1	Delete
---	---------------------

Add Nameserver

IP Address Add

Add Search Domain

Domain Add

Add/Modify Hosts for Local Resolution

IP Address	Host FQDN	Add/Modify
---------------------------------	--------------------------------	-------------------------

DNSSEC options

Enable DNSSEC Client ☐

図 10-6:ホスト名とDNSの設定

ホスト名の設定

“Hostname”（ホスト名）テキストボックスにホスト名を入力し、“Set Hostname”（ホスト名の設定）ボタンをクリックして、ローカルマシンのホスト名を設定します。使用できるのは、英数字だけです。

Add NameServer（IP Address）（ネームサーバーの追加（IPアドレス））



ロードマスターにてローカルに名前解決するDNSサーバーのIPアドレスを入力し、“Add” ボタンをクリックします。最大3つまでDNSサーバーを指定できます。

Add Search Domain (検索ドメインの追加)

DNSネームサーバーへのリクエストの先頭に追加するドメイン名を入力し、“Add” ボタンをクリックします。最大6つまで検索ドメインを指定できます。

Add/Modify Hosts for Local Resolution (ローカル名前解決ホストの追加/編集)

このフィールドを使用すると、ロードマスターからホストファイルを操作できます。IP アドレスとホストFQDNを指定してください。

DNSSEC options (DNSSECのオプション)

デフォルトでは、ロードマスターのDNSSECクライアントは無効になっています。必要な場合のみこのオプションを有効にしてください。DNSSECの検証は、失敗するまで非常に時間がかかることがあります。これにより、ロードマスターがフリーズまたはハングするおそれがあります。

このオプションを有効にすると、ロードマスターでDNSSEC機能が有効になります。DNSSECを有効にするには、**ネームサーバー**を1つ以上追加する必要があります。この機能を有効/無効にするには、DNSSECオプションを変更後にロードマスターを再起動する必要があります。1度設定を変更すると、ロードマスターを再起動するまで設定を再度変更できません。

HAを使用している場合、両方の機器で個別にDNSSECオプションを設定する必要があります。

DNSSECは、ロードマスターの以下のユーティリティで機能します。

- Vipdump
- Pingおよびping6
- Syslog
- SNMP
- Wget
- NTP



- SMTP

10.1.3 デフォルト・ゲートウェイ

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

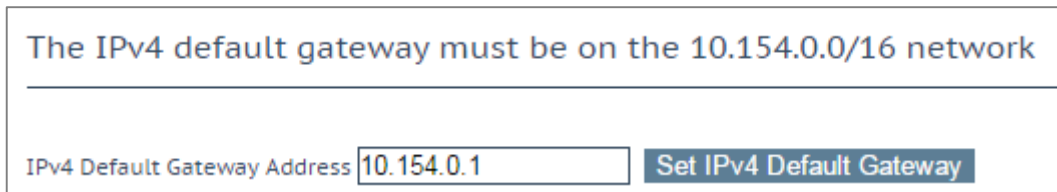


図10-7: デフォルト・ゲートウェイ

ロードマスターでIPv4とIPv6を使用する場合、IPv4とIPv6のデフォルト・ゲートウェイ・アドレスを指定する必要があります。

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

10.1.4 追加ルート

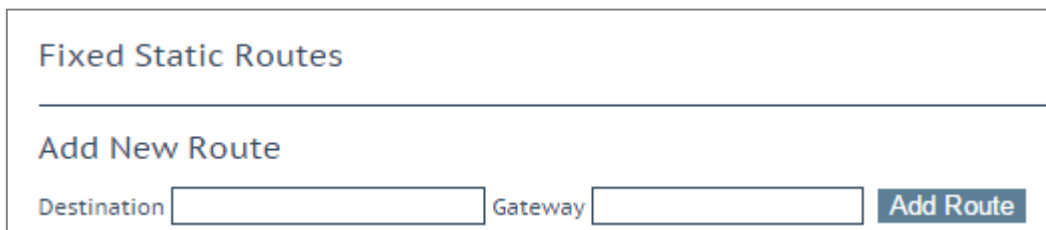


図10-8: 追加ルート

追加のルートを設定できます。これは静的ルーティングであるため、ゲートウェイはロードマスターと同じネットワーク上になければなりません。なお、仮想サービスレベルのデフォルト・ゲートウェイを使用してトラフィックを分割することもできます。

10.1.5 Packet Routing Filter (パケット・ルーティング・フィルター)

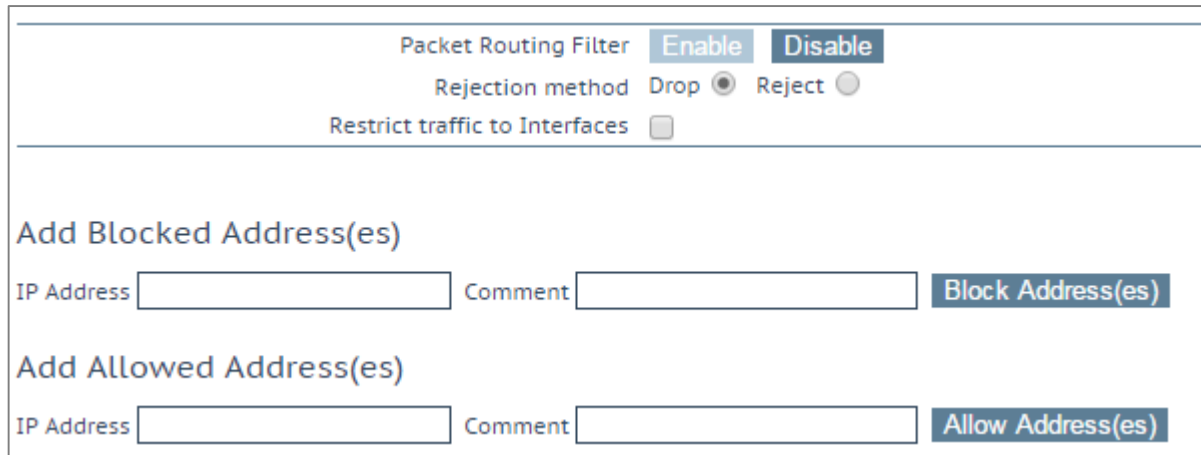


図 10-9:パケットフィルター

Packet Routing Filter (パケット・ルーティング・フィルター)

GE0を有効にすると、“Packet Routing Filter” (パケット・ルーティング・フィルター) はデフォルトで有効に設定され、無効に変更することはできません。GE0を無効にすると、“Packet Routing Filter” (パケット・ルーティング・フィルター) が設定可能になり、有効/無効を切り替えることができます。GE0機能を持つロードマスター上でGE0を無効にするには、メインメニューにて“Global Balancing”を選択し、“Disable GSLB”を選択します。

フィルターが有効になっていない場合、ロードマスターは単純なIPフォワーダーとしても機能します。

フィルターを有効にするとロードマスターへのトラフィックが制限されますが、ロードマスターを経由したクライアントから仮想サービスへのアクセスは影響を受けません。また、実サーバーから送信され、SNATが設定されたロードマスターで処理されたトラフィックも影響を受けません。

Reject/Drop blocked packets (ブロックされたパケットのリジェクト/ドロップ)

ホストから送信されたIPパケットがアクセス制御リスト (ACL) でブロックされた場合、その要求は通常、無視 (ドロップ) されます。ICMP拒否パケットを返すようロードマスターを設定できますが、セキュリティ上の理由から、通常の場合は、ブロックされたパケットをそのままドロップすることを推奨します。

Restrict traffic to Interfaces (インターフェイスへのトラフィックを制限)



接続されているサブネット間のルーティングを制限します。

Add Blocked Address(es) (ブロックされたアドレスを追加)

ロードマスターは、「ブラックリスト」に基づくアクセス制御リスト (ACL) システムをサポートしています。アクセス制御リストに設定されたホストやネットワークは、ロードマスターが提供するサービスへのアクセスをブロックされます。

ACLが有効になるのは、パケットフィルターが有効になっている場合に限定されます。ホワイトリストは、特定のIPアドレスまたはアドレス範囲からのアクセスを許可します。ホワイトリストで指定されたアドレス（またはアドレス範囲）が、ブラックリストで指定された範囲に含まれる場合、ホワイトリストの指定が優先されます。

ブラックリストにアドレスが指定されておらず、ホワイトリストにのみアドレスが指定されている場合、ホワイトリストで指定されたアドレスからの接続のみ許可され、その他のアドレスからの接続はブロックされます。

このオプションでは、ホストまたはネットワークのIPアドレスをアクセス・コントロール・リストに追加（またはリストから削除）できます。また、システムがIPv6アドレスファミリで構成されている場合、IPv4に加えてIPv6のアドレスもリストに指定できます。ネットワークを指定するには、ネットワーク識別子を使用します。

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

アクセスリストにて特定のトラフィックをブロックするよう定義し、それと同じIPアドレスにてワイルドカードの仮想サービスが設定されている場合、静的ポートの仮想サービスは正常に機能しません。静的ポートの仮想サービスにてそのトラフィックが拒否された後に、ワイルドカードの仮想サービスにてそのトラフィックが受け付けられます。

この場合、上記の相互作用により予期せぬ動作が引き起こされるのを防ぐため、別々のIPアドレスを使用するようにしてください。

10.1.6 VPN管理

“VPN Management”のリンク/画面は、ロードマスターにIPsecトンネリングのライセンスが与えられている場合のみ利用できます。



IPsecトンネリングに関する詳細（セットアップ手順を含む）は、**IPsecトンネリング機能説明**を参照してください。

Connection Endpoints Configuration			Refresh
Connection Name	Status	Operation	
AWS2	Down	View/Modify	Delete
vCloudAir	Down	View/Modify	Delete
Azure	Up	View/Modify	Delete
AWS1	Up	View/Modify	Delete
Connection Name		Create	

図 10-10:VPNの管理

Connection Name (接続名)

接続を識別するための一意の名前を指定します。

Create (作成)

指定した名前を使用して、一意に識別可能な接続を作成します。

View/Modify (表示/変更)

この接続の設定パラメーターを表示/変更します。

Delete (削除)

この接続を削除します。

関連する設定が完全に削除されます。接続は、それが動作中であってもいつでも削除できます。

10.1.6.1 VPN接続の表示/変更

Connection Details

Local IP Address

10.154.11.10

Set Local IP Address

Local Subnet(s)

10.154.11.10/32

Set Local Subnet(s)

Remote IP Address

10.154.11.20

Set Remote IP Address

Remote Subnet(s)

10.154.11.30/32

Set Remote Subnet(s)

Perfect Forward Secrecy

☐

Connection Secrets

Local ID

10.154.11.10

Remote ID

10.154.11.20

Pre Shared Key(PSK)

Save Secret Information

<-Back

図 10-11: 接続の変更

最初に接続を作成するとき、または接続を変更するときに“View/Modify VPN Connection”画面が表示されます。

Local IP Address (ローカルIPアドレス)

接続のローカル側のIPアドレスを設定します。

非HAモードの場合、“Local IP Address”はロードマスターのIPアドレス（デフォルトゲートウェイのIPアドレス）である必要があります。

HAモードの場合、“Local IP Address”は共有IPアドレスである必要があります。HAが設定済みの場合、このアドレスは自動的に設定されます。HA構成におけるトンネリングのセットアップに関する詳細は、次のセクションを参照してください。

Local Subnet Address (ローカルサブネットアドレス)

“Local IP Address”が“Local Subnet Address”に設定されている場合、テキストボックスに値が自動的に設定されます。/32 CIDRが与えられている場合、ローカルIPが唯一のパーティシパントとなります。必要に応じて“Local Subnet Address”を確認してください。アドレスを変更したかどうかにかかわらず、必ず“Set Local Subnet Address”をク



リックして設定を適用してください。複数のローカルサブネットを指定するには、カンマ区切りのリストを使用します。最大10個のIPアドレスを指定できます。

Remote IP Address (リモートIPアドレス)

接続のリモート側のIPアドレスを設定します。Azureエンドポイントの場合、このIPアドレスは、仮想プライベートネットワーク (VPN) のゲートウェイ機器におけるパブリック側のIPアドレスである必要があります。

Remote Subnet Address (リモートサブネットアドレス)

接続のリモート側のサブネットを設定します。複数のリモートサブネットを指定するには、カンマ区切りのリストを使用します。最大10個のIPアドレスを指定できます。

Perfect Forward Secrecy (前方秘匿性)

前方秘匿性のオプションを有効/無効にします。

使用されているクラウドプラットフォームに応じて、“Perfect Forward Secrecy” (前方秘匿性) のどのオプションを設定すべきかが決まります。“Perfect Forward Secrecy” (前方秘匿性) は、それが必要なプラットフォームもあれば、それをサポートしていないプラットフォームもあります。お使いのクラウドプラットフォームで何が機能するかは、**IPsecトンネリング 機能説明**を参照してください。

Local ID (ローカルID)

接続のローカル側の識別子です。通常、ローカルIPアドレスが使用されます。ロードマスターがHAモードでない場合、このフィールドにはLocal IP Addressと同じアドレスが自動的に設定されます。

ロードマスターがHAモードにある場合、Local IDフィールドは自動的に%anyに設定されます。ロードマスターがHAモードにあるとき、この値は更新できません。



Remote ID (リモートID)

接続のリモート側の識別子です。通常、リモートIPアドレスが使用されます。

Pre Shared Key (PSK) (プレシェアードキー)

プレシェアードキーの文字列を入力します。

Save Secret Information (秘密情報を保存)

接続の識別子および秘密情報を生成/保存します。

10.2 Cluster Control (クラスターの制御)

“Cluster Control”のオプションは、ロードマスターにクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMPの担当者にお問い合わせください。クラスタリングについての詳細は、[ロードマスターのクラスタリング 機能説明](#)を参照してください。

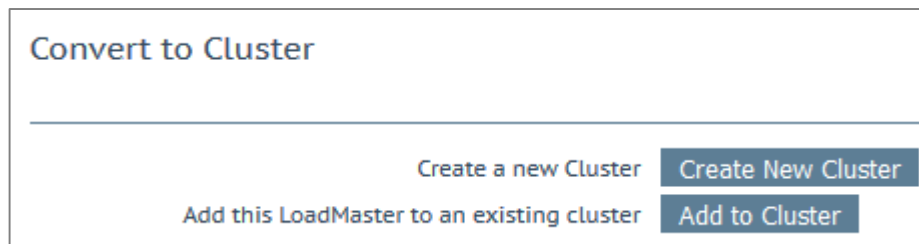


図 10-12:Cluster Control (クラスターの制御)

クラスタリングを設定する前に、“Cluster Control”メニュー項目をクリックします。すると、クラスターを新たに作成するか、このロードマスターをクラスターに追加するかを選択するオプションが表示されます。

Create New Cluster (クラスターの新規作成) : クラスターを新たに設定するには、このボタンをクリックします。

Add to Cluster (クラスターに追加) : このロードマスターを既存のロードマスターに追加します。

Convert to Cluster

Cluster Shared Address 10.154.11.90 Set Shared Address

Cancel Create a Cluster

図 10-13:Creating a New Cluster (クラスターの新規作成)

“Create New Cluster”ボタンをクリックすると、上記の画面が表示され、クラスターの共有IPアドレスを設定するよう求められます。この共有IPアドレスは、クラスターの管理に使用されます。

Rebooting and switching to the Shared Address to finish the conversion to Cluster mode

Please reconnect to 10.154.11.90

Continue

図 10-14:Rebooting (再起動)

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

Current Cluster Configuration

ID	Address	Status	Operation
1	10.154.11.70	Admin	Disable Delete

IP Address 10.154.0.0 Add New Node

図 10-15:Cluster Control (クラスターの制御)

クラスターを作成すると、共有IPアドレスのWUIの“Cluster Control”画面にて、ロードマスターのノードをクラスターに追加できるようになります。

ロードマスターの追加は、クラスターが利用可能であり、そのクラスターがクラスターの追加を待っている場合のみ行えます。詳細な情報と手順については、ロードマスターのクラスタリング 機能説明を参照してください。



ID	Address	Status	Operation
1	10.154.11.110	Admin	Disable Delete
2	10.154.11.120	Up	Disable Delete

図 10-16:Cluster Control (クラスターの制御)

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

Show Options (オプションの表示) : “Show Options”ボタンをクリックすると、“Cluster Parameters”セクションが表示されます。このセクションには、Cluster Virtual ID (クラスターの仮想ID) とNode Drain Time (ノードドレイン時間) を設定するための2つのフィールドが用意されています。詳細については、ロードマスターのクラスタリング 機能説明を参照してください。

ID: クラスターのID

Address (アドレス) : ロードマスターノードのIPアドレス。最初のIPアドレスの後ろに括弧で囲まれた2番目のIPアドレスが表示されている場合、2番目のIPアドレスはインターフェイスポートのIPアドレスを表します。IPアドレスとステータスの文字は、ステータスに応じて色分けされます。

- 青: このノードはマスターノードです。
- 黄: このノードは無効です。
- 緑: このノードは稼働しています。
- 赤: このノードは停止しています。

Status (ステータス) : ノードの状態以下の状態があります。

- Admin (管理) : このノードはプライマリ制御ノードです。
- Up (稼働中) : このノードは稼働しています。
- Down (停止中) : このノードは停止しています。
- Drain stopping (ドレイン停止中) : このノードは無効になっており、正しい手順で接続をシャットダウンしている最中です。ドレイン停止は、デフォルトで10秒間継続します。この値は、“Cluster Control”画面の“Node Drain Time”の値を変更することで更新できます。詳細は、ロードマスターのクラスタリング 機能説明を参照してください。
- Disabled (無効) : このノードは無効になっています。このノードには接続は送信されません。



Operation (動作) : このノードに関して実行可能な各種動作

- **Add new node (ノードの新規追加)** : 指定されたIPを持つ新しいノードをこのクラスターに追加します。
- **Disable (無効化)** : ノードを無効にします。無効化されたノードに対し、まず始めにドレイン停止が行われます。ドレイン停止時間中に、正しい手順で接続がシャットダウンされます。ドレイン終了後、このノードは無効になり、このノードにトラフィックが送信されなくなります。
- **Enable (有効化)** : ノードを有効にします。ノードが起動すると、そのノードは直ちにローテーションに組み込まれます。ノードは、30秒間稼働してからオンラインになります。
- **Delete (削除)** : クラスターからノードを削除します。ノードを削除すると、そのノードは単体動作する通常のロードマスターインスタンスになります。その後、ロードマスターをクラスターに戻すと、共有IPアドレスに対して行われた変更が、ノードのロードマスターに反映されます。
- **Reboot (再起動)** : クラスター全体のファームウェアを更新する際、ファームウェアの更新パッチをアップロードすると、“Reboot”ボタンが画面に表示されます。クラスター全体のファームウェアを更新するための具体的な手順については、**ロードマスターのクラスタリング 機能説明**を参照してください。

10.2.1 Cluster Parameters (クラスターのパラメーター)

Cluster Parameters

Cluster Virtual ID

1

Set Cluster Virtual ID (Valid Values: 1-255)

Node Drain Time

10

Set Node Drain Time (Valid Values: 1-600)

図 10-17:Cluster Parameters (クラスターのパラメーター)

“Show Options”ボタンをクリックすると、“Cluster Parameters”画面が表示されます。このセクションには、“Cluster Virtual ID”と“Node Drain Time”の2つのWUIオプションが用意されています。

Cluster Virtual ID (クラスターの仮想ID)

同じネットワーク上で複数のクラスターまたはロードマスターHAシステムを使用する場合、仮想IDにより各クラスターが識別されます。そのため、望ましくない干渉は発生しません。クラスターの仮想IDはデフォルトで1に設定されていますが、この値は必要に



応じて変更できます。仮想IDは1～255の範囲で設定できます。管理用ロードマスターに対して行われた変更は、そのクラスター内のすべてのノードに反映されます。

Node Drain Time (ノードドレイン時間)

ノードが無効になっても、“Node Drain Time”テキストボックスで指定された秒数だけ、そのノードにより提供される接続を継続することができます。この間、ノードにより新たな接続は処理されません。“Node Drain Time”はデフォルトで10に設定されていますが、この値は必要に応じて変更できます。有効な値の範囲は1～600（単位：秒）です。

ドレン期間中は、指定されたドレン時間が経過するまで、ステータスは「ドレイン中」になります。

ドレイン時間が経過すると、ステータスが「無効」になります。

10.3 System Administration (システム管理)

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

10.3.1 ユーザの管理

以下、ユーザー管理用の各種WUIフィールドについて説明します。ユーザー管理とWUI認証の詳細については、**ユーザー管理 機能説明**を参照してください。

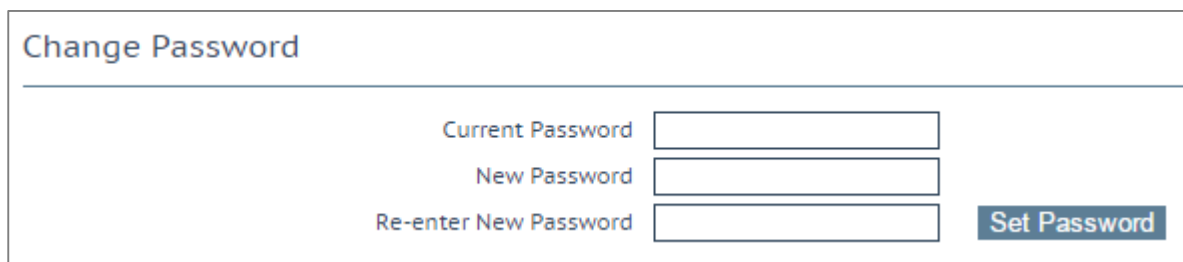
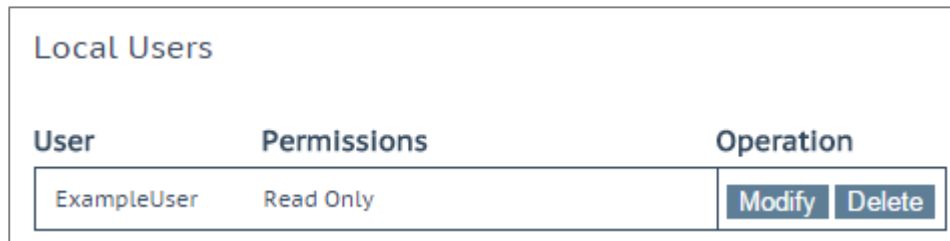


図 10-18: パスワードの変更

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



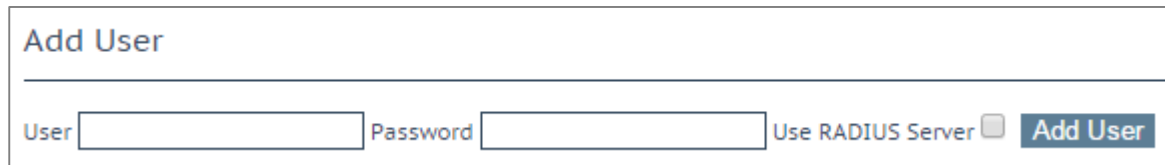


User	Permissions	Operation
ExampleUser	Read Only	<button>Modify</button> <button>Delete</button>

図 10-19: ユーザーの管理

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

- **Modify (変更)** : 既存のローカルユーザーの詳細を変更します (権限やパスワードなど)。詳細は[セクション10.3.1.1](#)を参照してください。
- **Delete (削除)** : 目的のユーザーを削除します。



Add User

User Password Use RADIUS Server ☐ Add User

図 10-20: ユーザーの追加

“Add User”セクションでは、新規ユーザーを追加できます。

ユーザー名には最大64文字まで使用できます。ユーザー名は数字で始めることができます。また、以下の特殊文字に加えて英数字を含めることができます。

=~^._+#@¥/-

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

“Use RADIUS Server” (RADIUSサーバーを使用する) オプションを使用すると、ユーザーがロードマスターにログインするときにRADIUSサーバによる認証を行うかどうかを決定できます。このオプションを使用する前に、RADIUSサーバの詳細を設定する必要があります。

RADIUSサーバーによる認証を行う場合、ロードマスターからRADIUSサーバーにユーザーの情報が渡され、RADIUSサーバーからロードマスターにそのユーザーが認証されたかどうか通知されます。RADIUSサーバーの設定に関する詳細は、[セクション9.6.4](#)および[RADIUSの認証と権限設定](#) テクニカルノートを参照してください。

セッション管理が有効になっている場合、この画面で “Use RADIUS Server” オプションは使用できません。セッション管理が有効なときにRADIUSサーバーを設定する方法については、Section9. 6. 4を参照してください。

セッション管理が有効になっている場合、“Add User”セクションに“No Local Password”チェックボックスが表示されます。ユーザがロードマスターにアクセスするときに、クライアント証明書を用いてそのユーザーを認証する場合、このオプションを有効にできます。クライアント証明書による認証を有効にするには、“Remote Access”画面で“Admin Login Method”を設定します。詳細はセクション9. 6またはユーザー管理 機能説明を参照してください。

10.3.1.1 ユーザーの編集

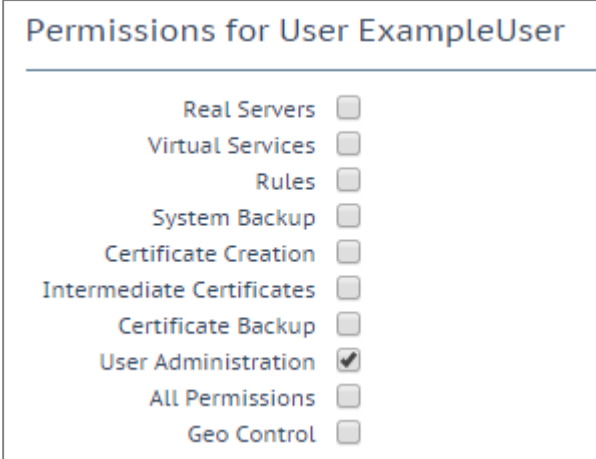
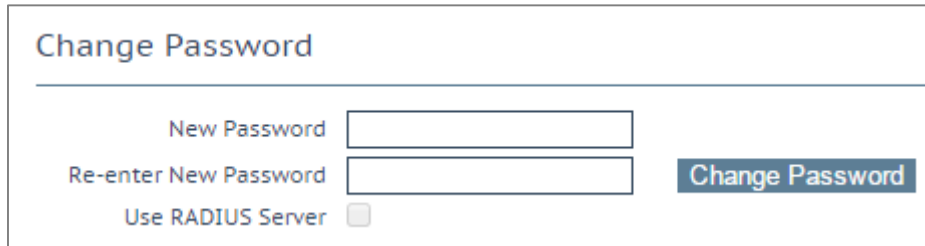


図 10-21: 権限

この画面では、ユーザー権限のレベルを設定できます。この設定に基づいて、ユーザーに実行を許可する設定変更の範囲が決まります。プライマリユーザー（bal）は、常にすべての機能を使用する権限を持っています。セカンダリユーザーは、一部の機能が制限される場合があります。

ユーザー権限の詳細については、KEMPロードマスター 製品概要を参照してください。



The form is titled "Change Password". It contains three input fields: "New Password", "Re-enter New Password", and "Use RADIUS Server" (a checkbox). A "Change Password" button is located to the right of the input fields.

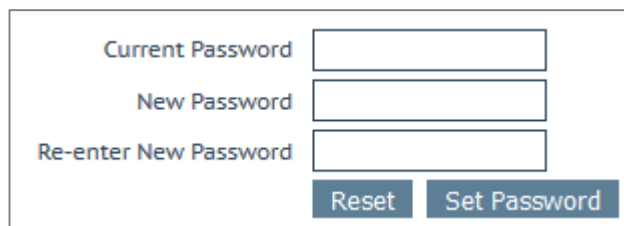
図 10-22:パスワードの変更

“Change Password”セクションでは、ユーザーのパスワードの変更が行えます。また、RADIUSサーバーによるユーザー認証を有効/無効にできます。

セッション管理が有効になっている場合、この画面で“Use RADIUS Server”オプションは使用できません。セッション管理が有効なときにRADIUSサーバーを設定する方法については、Section 9.6.4を参照してください。

セッション管理が有効になっている場合、“Change Password”セクションに“No Local Password”チェックボックスが表示されます。ユーザがロードマスターにアクセスするときに、クライアント証明書を用いてそのユーザーを認証する場合、このオプションを有効にできます。クライアント証明書による認証を有効にするには、“Remote Access”画面で“Admin Login Method”を設定します。詳細はセクション9.6またはユーザー管理機能説明を参照してください。

名前付きユーザーは、ユーザー管理権限を持っていなくても、自分のパスワードを変更できます。名前付きユーザーが“System Administration > User Management”メニューオプションをクリックすると、“Change Password”画面が表示されます。



The form contains three input fields: "Current Password", "New Password", and "Re-enter New Password". Below the input fields are two buttons: "Reset" and "Set Password".

図 10-23:パスワードの変更

ユーザーは、この画面で自分のパスワードを変更できます。パスワードは8文字以上64文字以下でなければなりません。¥” `を除いてすべての文字を使用できます。パスワードを変更すると、確認画面が表示されます。その後、ユーザーは、新しく設定したパスワードでロードマスターに再度ログインするよう求められます。

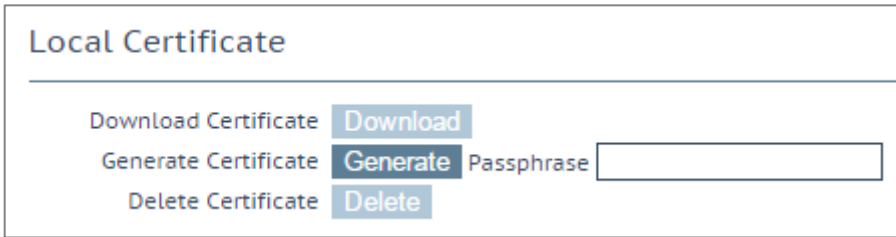


図 10-24: ローカル証明書

“Local Certificate”セクションでは、そのユーザーの証明書を生成できます。オプションとして、秘密鍵の暗号化で使用するパスフレーズを“Passphrase”に設定できます。証明書をダウンロードすると、その証明書をクライアント証明書として使うことができます。これにより、ロードマスターのAPIにパスワードなしでアクセスできます。“User Administration”の権限が設定されたユーザーは、自分または他のユーザーのローカル証明書を管理できます。

クライアント証明書によるロードマスターへのアクセス認証を有効にするには、“Remote Access”画面で“Admin Login Method”を設定します。詳細はセクション9.6またはユーザー管理 機能説明を参照してください。

10.3.2 Update License (ライセンスの更新)

この画面には、現在のライセンスが有効になった日付と、現在のライセンスの有効期限が表示されます。ロードマスターのライセンスを更新する前に、KEMPの担当窓口にお問い合わせいただくか、“Upgrade”オプションを使用する必要があります。KEMPへのお問い合わせ後または“Upgrade”オプション使用後に、オンラインとオフラインの2つの方法でライセンスを更新できます。各方式の画面に関する詳細は、以下のセクションを参照してください。

詳細および手順については、ライセンス 機能説明を参照してください。

10.3.2.1 オンライン方式

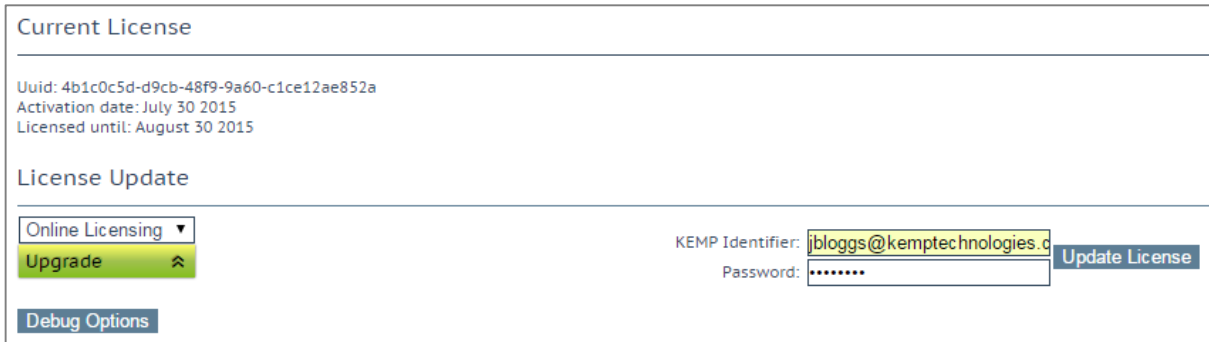


図 10-25: ライセンスの更新 - オンライン方式



オンライン方式でライセンスをアップグレードするには、ロードマスターをインターネットに接続する必要があります。オンライン方式でライセンスを設定するには、“KEMP ID”と“Password”（パスワード）を入力する必要があります。

10.3.2.2 オフライン方式

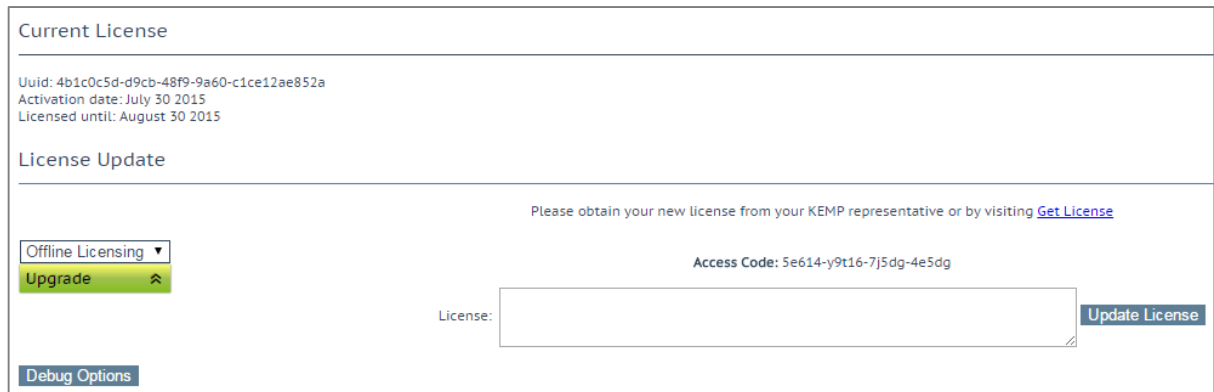


図 10-26: ライセンスの更新 - オフライン方式

オフライン方式でライセンスをアップグレードするには、ロードマスターにライセンステキストを入力する必要があります。ライセンステキストは、KEMPから入手するか、“Get License”（ライセンスの取得）のリンクから入手することができます。

適用するライセンスの種類によっては、再起動が必要になる場合があります。ESPライセンスへのアップグレードの場合、更新後に再起動が必要です。

10.3.2.3 Debug Options (デバッグオプション)

“Update License”（ライセンスのアップグレード）画面には、ライセンス設定に関する問題のトラブルシューティングに役立つ、いくつかのデバッグオプションが用意されています。

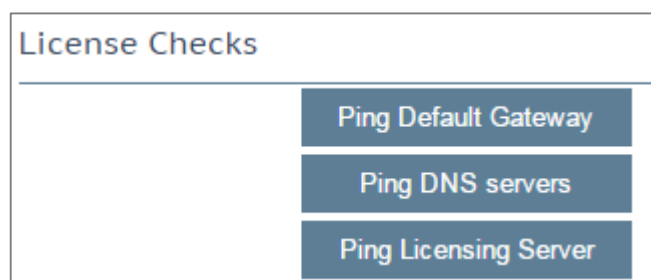


図 10-27: 利用可能なデバッグオプション

“Debug Options”（デバッグオプション）ボタンをクリックすると、以下の3つのデバッグオプションが表示されます。

- Ping Default Gateway (デフォルトゲートウェイにpingを送信する)
- Ping DNS Servers (DNSサーバーにpingを送信する)
- Ping Licensing Server (ライセンスサーバーにpingを送信する)

License Checks			
Ping Default Gateway	Host FQDN	10.154.0.1	
	IP Address	10.154.0.1	
	Packets details	1 packets transmitted, 1 received, 0% packet loss, time 0ms	
	RTT details	rtt min/avg/max/mdev = 4.373/4.373/4.373/0.000 ms	
Ping DNS servers			
Ping Licensing Server	Host FQDN	alsi-qa.kemptechnologies.com	
	IP Address	ping: unknown host alsi-qa.kemptechnologies.com	
	Packets details		
	RTT details		
Clean ping logs			

図 10-28:pingの結果

pingボタンをクリックすると、右側の列にpingの結果が表示されます。

“Clean ping logs” (pingのログをクリアする) ボタンをクリックすると、右側の列にある情報がクリアされます。

10.3.3 System Reboot (システムリブート)

Reboot	Reboot
Shutdown	Shutdown
Reset To Factory Defaults	Reset Machine

図10-29: システムリブート

Reboot (リブート)

アプライアンスをリブートします。

Shutdown (シャットダウン)

このボタンをクリックすると、ロードマスターの電源を切る処理が行われます。何らかの理由で電源を切る処理に失敗した場合でも、CPUは停止します。

Reset Machine (マシンのリセット)

ライセンス、ユーザー名、およびパスワードの情報を除く、アプライアンスの設定をリセットします。適用の対象は、HAペアのアクティブなアプライアンスに限定されます。



10.3.4 Update Software (ファームウェア更新)

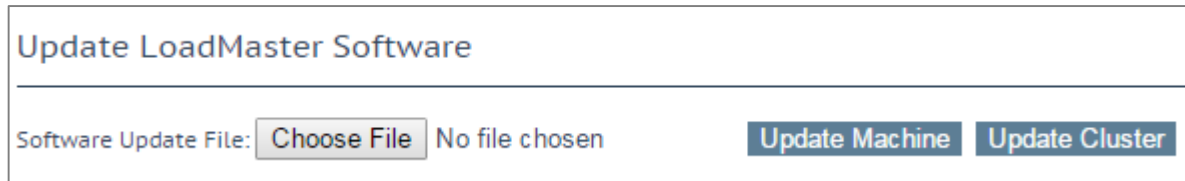


図10-30: ソフトウェアの更新

ファームウェアの更新につきましては、弊社販売店までお問い合わせ願います。ファームウェアをダウンロードするにはインターネットにアクセスする必要があります。パッチ情報の詳細は、<http://forums.kemptechnologies.com/>でご覧いただけます。

Update Machine (マシンの更新)

ファームウェアの更新を行えます。パッチは、新しいファームウェアとしてリリースされますので、一旦ローカルディスクへダウンロードした後、ここにそのロケーションを指定します。このファームウェアは、ロードマスターで解凍して有効化します。パッチが有効になると、リリース情報を確認するよう求められます。更新を完了するには、機器を再起動する必要があります。必要に応じて、このリブートは保留できます。

Update Cluster (クラスターの更新)

“Update Cluster”のオプションは、ロードマスターにクラスタリングのライセンスが設定されている場合のみ利用できます。お使いのライセンスにクラスタリング機能を追加する場合は、KEMPの担当者にお問い合わせください。クラスタリングについての詳細は、**ロードマスターのクラスタリング 機能説明**を参照してください。

“Update Cluster”ボタンをクリックすると、クラスターにあるすべてのロードマスターのファームウェアを共有IPアドレス経由で更新できます。クラスター全体のソフトウェアを更新するための具体的な手順については、**ロードマスターのクラスタリング 機能説明**を参照してください。

Restore Software (ファームウェア復旧)

ロードマスターのファームウェア更新が完了した場合、このオプションを使用して、以前のビルドに戻すことができます。



Installed Addon Packages			
Package	Version	Installation Date	Operation
Vmtoolsd	7.1-27-1139	Tue Apr 28 15:07:38 2015	Delete

図 10-31: Installed Addon Packages (インストールされているアドオンパッケージ)

Installed Addon Packages (インストールされているアドオンパッケージ)

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

アドオンパッケージは、KEMP TechnologiesのWebサイト (www.kemptechnologies.com) から入手できます。 www.kemptechnologies.com

アドオンパッケージをインストールするには、“Choose File”をクリックしてファイルをブラウズ/選択し、“Install Addon Package”をクリックします。アドオンパッケージのインストールを完了するには再起動する必要があります。同じ名前のアドオンパッケージをアップロードした場合、既存のパッケージが上書き/更新されます。

インストールしたアドオンを起動できない場合、テキストが赤で表示され、そのパッケージを起動できなかったことが吹き出し文字で示されます。

10.3.5 Backup/Restore (設定バックアップ／リストア)

Create a Backup

Backup the LoadMaster [Create Backup File](#)

Restore Backup

Backup File [Choose File](#) No file chosen

☐ LoadMaster Base Configuration
☐ VS Configuration
☐ Geo Configuration

[Restore Configuration](#)

Automated Backups

Enable Automated Backups ☒

When to perform backup

00 : 00

Day of week

Daily

[Set Backup Time](#)

Remote user

[Set Remote User](#)

Remote password

[Set Remote Password](#)

Remote host

[Set Remote Host](#)

Remote Pathname

[Set Remote Pathname](#)

Test Automated Backups

[Test Backup](#)

図 10-32: バックアップと復元

Create Backup File (バックアップファイルの作成)

仮想サービスの設定およびローカルアプライアンスの情報を含むバックアップを生成します。ライセンス情報とSSL証明書情報はバックアップに含まれません。

容易に識別できるように、バックアップファイル名にはロードマスターのホスト名が含まれています。

Restore Backup (バックアップの復元)

リモートマシンから復元を実行する場合、ユーザーは復元する情報の種類（“VS Configuration”、“LoadMaster Base Configuration”、“Geo Configuration”、またはこの3つのオプションの組み合わせ）を選択できます。

HAマシンにシングルマシンの設定をリストアすることはできません（その逆も不可）。



ESPが有効になっている仮想サービスの設定を、ESPが無効になっているマシンにリストアすることはできません。

Automated Backups (自動バックアップ)

“Enable Automated Backups”チェックボックスがオンになっている場合、毎日または週単位で自動バックアップを実行するよう、システムを設定できます。

容易に識別できるように、バックアップファイル名にはロードマスターのホスト名が含まれています。

しかるべき時刻に自動バックアップが実行されない場合、NTPが正しく設定されているか確認してください。詳細は[セクション10.3.6](#)を参照してください。

When to perform backup (バックアップの実行タイミング)

バックアップの時間（24時間制）を指定します。同時に、バックアップを毎日実行するか、特定の曜日に実行するかを選択します。選択が終わったら、“Set Backup Time”ボタンをクリックします。

場合によっては、以下のような偽のエラーメッセージがシステムログに表示されることがあります。

```
Dec 8 12:27:01 KEMP_1 /usr/sbin/cron[2065]:(system) RELOAD (/etc/crontab)
```

```
Dec 8 12:27:01 KEMP_1 /usr/sbin/cron[2065]:(CRON) bad minute (/etc/crontab)
```

これらを見ても支障ありません。このような場合でも、通常、自動バックアップは正しく行われます。

Remote user (リモートユーザー)

リモートホストにアクセスするユーザー名

Remote password (リモートパスワード)



リモートホストにアクセスするためのパスワード。このフィールドには、英数字およびほとんどの非英数字が使用できます。以下の文字は使用できません。

- 制御文字
- ‘ (アポストロフィー)
- ` (グループ)
- 削除文字

Remote host (リモートホスト)

リモートホスト名

Remote Pathname (リモートパス名)

バックアップファイルを格納するリモートホスト上の場所

Test Automated Backups (自動バックアップのテスト)

“Test Backup”ボタンをクリックすると、自動バックアップの設定が正しく機能するかどうかチェックするテストが実行されます。テストの結果は、システムメッセージファイルで確認できます。

現在、自動バックアップの転送プロトコルはFTPのみサポートしています。

10.3.6 Date/Time (日付／時間)

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



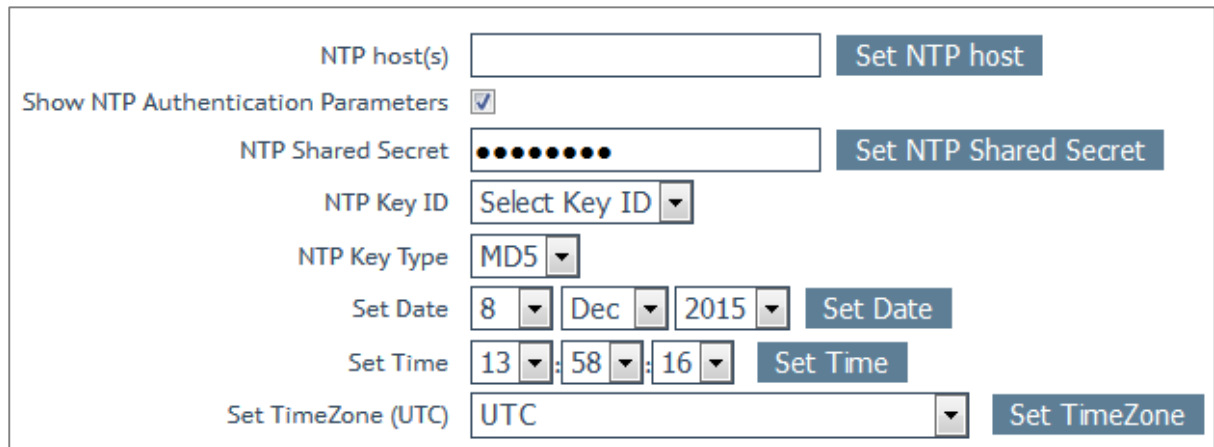


図10-33: 日付および時刻の設定

NTP host(s) (NTPホスト)

NTPサーバーとして使用するホストを指定します。NTPは、HA構成では強く推奨されるオプションです。単一ユニットの場合は、ユーザーが任意に設定できます。“Set NTP host”ボタンをクリックすると、設定された詳細に基づき時刻が更新されます。

ローカルNTPサーバーがない場合は、www.pool.ntp.orgにアクセスし、使用可能な公開NTPサーバープールの一覧を参照してください。

タイムゾーンは、常に手動で設定する必要があります。

Show NTP Authentication Parameters (NTP認証パラメーターの表示)

ロードマスターは、暗号化された署名を用いて安全なNTPサーバーに問い合わせを行うNTPv4をサポートします。このプロトコルは、簡単な認証方式を使用します。この方式では、共有秘密鍵を使用して、サーバーからの応答が正規のものであるかを確認します。“Show NTP Authentication Parameters”チェックボックスをオンにすると、NTPにより認証された要求をサポートするのに必要なパラメーターが表示されます。

NTP Shared Secret (NTP共有秘密鍵)

NTP共有秘密鍵の文字列です。NTPの秘密鍵は、ASCII文字で20文字（または16進数で40文字）まで使用できます。

NTP Key ID (NTP鍵ID)



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

NTP Key Type (NTP鍵タイプ)

NTP鍵タイプを選択します。

NTPv4を機能させるには、サーバー上に以下の形式を持つファイル (/etc/ntp.keys) を作成する必要があります。

<鍵ID> M <秘密鍵の文字列>

...

<鍵ID> M <秘密鍵の文字列>

鍵IDを有効にするには、/etc/ntp.confのtrustkeyの行に鍵IDを指定する必要があります。すなわち、鍵IDが5の場合、“trustedkey5”と指定する必要があります。trustedkeyは複数の値を持つことができます (例: trustedkey 1 2 3 4 5 9 10)

10.4 Logging Options (ログオプション)

ロードマスターのログには、アプライアンスからのプッシュと、プルによる両方のイベントが出力されます。ロードマスターのログ情報は、アプライアンスが再起動した場合、リセットされ、維持されないことに注意してください。システム上のイベント出力記録の維持が重要な場合には、SNMPマネージャー、Syslogサーバー、SMTPサーバーなどを使用した外部デバイスへの蓄積をお勧めします。



10.4.1 System Log Files (システムのログファイル)

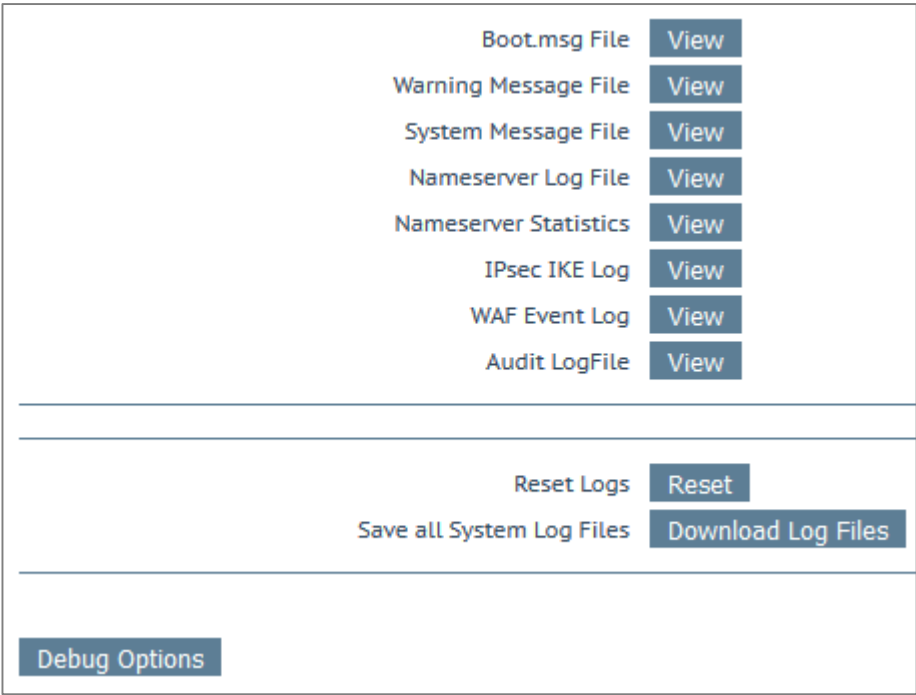


図10-34: システムのログファイル

Boot.msg File - システムがブートした時のメッセージを記録したファイルをレビューできます。

Warning Message File (警告のメッセージファイル) - ロードマスターの運用中に記録された警告を含んでいます。

System Message File (システムのメッセージファイル) - ロードマスターの運用中に記録されたシステムイベントを含んでいます。オペレーティングシステムレベルのイベントとロードマスターの内部イベントの両方が対象です。

Nameserver Log File (ネームサーバーのログファイル) - DNSネームサーバーのログを表示します。

Nameserver Statistics (ネームサーバーの統計情報) - ネームサーバーの最新の統計情報を表示します。

IPsec IKE Log (IPsec IKEのログ) - IPsec IKEのログを表示します。

WAF Event Log - 最後にトリガーされたWAFルールログが格納されます。

Audit LogFile - ユーザーによりAPI経由またはWUI経由で行われる各アクションのログが格納されます。これは、セッション管理が有効な場合のみ機能します。セッション管理についての詳細は、**セクション9.7**を参照してください。

Reset Logs - すべてのメッセージを消去します。

Save all System Log Files (システムのログファイルをすべて保存) - サポート対応の一環として、KEMPのサポート部門にログを送付する必要がある場合に使用します。このボタンをクリックすることで、使用中のPCにファイルを保存した後で、販売店のサポートにそれらを転送できます。

10.4.1.1 *Debug Options (デバッグオプション)*

ロードマスターには、接続関連の問題を診断する際に、ユーザーやKEMPのサポート部門のスタッフを支援するため、さまざまな機能が用意されています。**[Debug Options]** ボタンをクリックすると、そのための下記画面が表示されます。

Debug Options

Disable All Transparency	Disable Transparency
Enable L7 Debug Traces	Enable Traces
Perform an l7adm	l7adm
Enable WAF Debug Logging	Enable Logging
Enable IRQ Balance	Enable IRQ Balance
Enable TSO	Enable TSO
Enable Bind Debug Traces	Enable Bind Traces
Perform a PS	ps
Display Meminfo	Meminfo
Display Slabinfo	Slabinfo
Perform an Ifconfig	Ifconfig
Perform a Netstat	Netstat
Reset Statistic Counters	Reset Statistics
Flush OCSPD Cache	Flush Cache
Enable SSOMGR Debug Traces	Enable Traces
Flush SSO Authentication Cache	Flush SSO Cache
SSO LDAP server timeout	5 Set Timeout
Linear SSO Logfiles	☐
Start IPsec IKE Daemon	Start IPsec IKE Daemon
Perform an IPsec Status	IPsec Status
Enable IKE Debug Level Logs	Enable Logs
Netconsole Host	Interface eth0 Set Netconsole Host
Ping Host	Interface eth0 Ping
Traceroute Host	Traceroute
Kill LoadMaster (441872)	Kill LoadMaster

図10-35: デバッグオプション



Disable All Transparency (すべてのトランスペアレンシーを無効化)

各仮想サービス上のトランスペアレンシーを無効にし、レイヤ7を使用するよう強制します。注意して使用してください。

Enable L7 Debug Traces (レイヤ7のデバッグトレースを有効にする)

メッセージファイルにてログトラフィックを生成します。大量のファイルが記録されるため、レイヤ7の処理が遅くなります。

Perform an l7adm (l7admの実行)

L7の仮想サービスの詳細情報をテーブル形式で表示します。

Enable WAF Debug Logging (WAFのデバッグログを有効にする)

WAFのデバッグトレースを有効にします。

このオプションは大量のトラフィックを生成します。また、WAFの処理速度も低下します。KEMPの技術サポートからこのオプションを使用するように要求された場合のみ、このオプションを有効にしてください。実稼働環境でこのオプションを有効にするのは推奨しません。

AFPデバッグログはクローズされません。ログが大きくなりすぎたときは、循環して使用されます。デバッグログを再度有効にするには、WAFが有効なすべての仮想サービスの設定において、WAFを無効にしてから再度有効にする必要があります。または、それらの仮想サービスに関連するルールを更新してください。

Enable IRQ Balance (IRQの負荷分散を有効にする)

IRQ負荷分散を有効にします。販売店サポート要員の指示で有効にしてください。

Enable TS0 (TS0を有効化)

TCPセグメンテーションオフロード (TS0) を有効にします。



このオプションを変更する場合は、必ずKEMPの技術サポートにご相談ください。このオプションの変更は再起動後に有効になります。

Enable Bind Debug Traces (バインドデバッグトレースの有効化)

GE0に対するバインドデバッグトレースのログを有効にします。

Perform a PS (PSの実行)

システムのプロセス状態をレポートします。

Display Meminfo (メモリ情報の表示)

システムのメモリ使用状態を表示します。

Display Slabinfo (スラブ情報の表示)

システムのSlab情報を表示します。

Perform an Ifconfig (Ifconfigの実行)

システムが持つすべてのイーサネットポートの情報を表示します。

Perform a Netstat (Netstatの実行)

Netstatの出力を表示します。

Reset Statistic Counters (統計カウンタのリセット)

統計カウンタをすべてゼロにします。

Flush OCSPD Cache (OCSPDのキャッシュを消去)



OCSPを使用してクライアント証明書を検証する場合、OCSPサーバーから取得した応答がOCSPDキャッシュされます。このボタンを押すと、このキャッシュを消去できます。OCSPDのキャッシュの消去は、試験を行うときや、証明書失効リスト（CRL）が更新されたときに役に立ちます。

Enable SSOMGR Debug Traces (SSOMGRによるデバッグトレースを有効にする)

このオプションを有効にすると、ロードマスター上で設定されたSSOドメインへのログイン試行が記録されます。このオプションを有効にすると、“Extended Log Files”画面の“SSOMGR Audit Logs”にログが保存されます。ログファイルの詳細については、セクション10.4.2を参照してください。

Stop IPsec IKE Daemon (IPsec IKEデーモンの停止)

ロードマスターのIPsec IKEデーモンを停止します。

このボタンをクリックすると、すべてのトンネルの接続が停止します。

Perform an IPsec Status (IPsecステータスの表示)

生のIPsecステータス出力を表示します。

Enable IKE Debug Level Logs (IKEのデバッグレベルのログ表示を有効化)

IPsec IKEのログレベルを制御します。

Flush SSO Authentication Cache (SSO認証のキャッシュの消去)

“Flush SSO Cache” ボタンをクリックすると、ロードマスターに保存されているシングルサインオンのキャッシュが消去されます。また、認証サーバーのステータスがすべてリセットされ、（KCDドメインが関係している場合は）KCDドメインがリセットされて、



設定が再度読み込まれます。これにより、シングルサインオンを使用してロードマスターに接続しているすべてのクライアントがログオフされます。

Linear SS0 Logfiles (SS0ログファイルをリニアに拡張する)

デフォルトでは、新しいログファイルを保存できるように、古いログファイルは削除されます。これにより、ファイルシステムが一杯になるのを防ぐことができます。“Linear SS0 Logfiles” チェックボックスをオンにすると、古いファイルが削除されないようになります。

“Linear SS0 Logging”を使用する場合、ログファイルを定期的に削除せずにファイルシステムが一杯になると、ログに記録されないまま仮想サービスにアクセスされるのを防ぐため、ESPが有効になっている仮想サービスへのアクセスがブロックされます。ESPが無効になっている仮想サービスへのアクセスは、“Linear SS0 Logfile”機能による影響を受けません。

Netconsole Host (netconsoleホスト)

指定したホストで動作するsyslogデーモンにより、重要なカーネルメッセージがすべて受信されます。syslogサーバーはローカルLAN上に置く必要があります。また、メッセージはUDPで送信されます。

“Interface” プルダウンメニューにて、どのインターフェイスにネットコンソールホストを設定するかを選択できます。

指定したネットコンソールホストが、選択したインターフェイス上にあることを確認してください（そうでない場合はエラーが発生します）。

Ping Host (pingホスト)

指定したホストにてpingを実行します。pingの送信元インターフェイスは、“Interface” ドロップダウンリストにて指定できます。“Automatic” オプションを選択すると、特定のネットワーク上にあるアドレスにpingを送信するための適切なインターフェイスが選択されます。



インターフェイスは、pingを行うアドレスがIPv4とIPv6のどちらのアドレスかを判断し、pingを実行するための正しいコマンドを選択します。数値形式のアドレスの場合は簡単ですが、数値でないアドレスは処理できないため、常にIPv4アドレスとして処理されます。

Traceroute Host (tracerouteホスト)

特定のホストのトレースルートを実行します。

Kill LoadMaster (ロードマスターを停止する)

ロードマスターのすべての機能を恒久的に無効にします。ライセンスを再度設定すると、ロードマスターの機能を再度使用できるようになります。

ロードマスターの機能を無効にする場合は、必ずKEMPの技術サポートにご相談ください。

“Kill LoadMaster”オプションは、KEMP Condorのテナントのロードマスターでは利用できません。

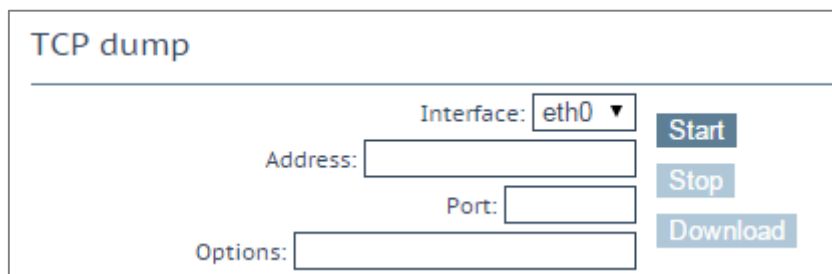


図 10-36: TCPダンプ

TCPダンプ

TCPダンプは1つまたはすべてのイーサネットポートで取り込むことができます。アドレス、ポートパラメーター、およびオプションのパラメーターを指定できます。“Options”テキストボックスには最大255文字まで入力できます。

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



詳細は、VMwareツールのアドオンパッケージ **機能説明**を参照してください。

10.4.2 Extended Log Files (拡張ログファイル)

“Extended Log Files”画面では、ESPのAFP機能に関するログのオプションが用意されています。これらのログは永続的に保存され、ロードマスターの再起動後も利用できます。オプションをすべて表示するには、 アイコンをクリックします。

WAFのログはリアルタイムでは作成されません。このログは、WAFのエンジンが実際に処理を行ってから最大2分後に作成されます。

File	Action	Selection
ESP Connection Log	View	from  to  filter
ESP Security Log	View	from  to  filter
ESP User Log	View	from  to  filter
WAF Audit Logs	View	 filter
SSOMGR Audit Logs	View	 filter
Clear Extended Logs	Clear	from  to 
Save Extended Logs	Save	from  to 

図 10-37:ESPオプション

さまざまなログファイルがロードマスターに保存されます。

- ESP Connection Log (ESP接続ログ) : 各接続を記録
- ESP Security Log (ESPセキュリティログ) : セキュリティ警告をすべて記録
- ESP User Log (ESPユーザーログ) : 全ユーザーのログイン情報を記録
- WAF Audit Logs (WAF監査ログ) : 仮想サービス設定画面の“WAF Options”セクションの“Audit mode”ドロップダウンリストで選択した内容に従ってWAFのログを作成します。各ログエントリにリストされる番号は、仮想サービスIDに対応します。

す。仮想サービスIDを取得するには、APIインターフェイスが有効になっていることを確認し (“System Configuration” > “Miscellaneous Options” > “Remote Access” > “Enable API Interface”) から、Webブラウザのアドレスバーに `https://<LoadMasterIPAddress>/access/listvs` と入力します。Webブラウザのアドレスバーで、`https://<LoadMasterIPAddress>/access/listvs` と入力します。仮想サービスのindex (インデックス) をチェックしてください。これが、監査ログエントリの番号に対応する番号です。

- **SSOMGR Audit Logs (SSOMGR監査ログ)** :SSO認証試行に関するログ。このログを有効にするには、“Debug Options”画面で“SSOMGR Debug Traces”オプションを有効にします。

ログを表示するには、目的のオプションを選択して“View”ボタンをクリックします。

一部のログは、さまざまな方法でフィルターできます。特定の日付範囲のログを表示するには、“from”フィールドと“to”フィールドで日付を選択し、“View”ボタンをクリックします。また、アーカイブされたログファイルを表示するには、ファイル名一覧から目的のファイルを選択し、“View”ボタンをクリックします。さらに、“filter”フィールドに単語や正規表現を入力し、“View”ボタンをクリックしても、ログファイルをフィルターできます。

SSOMGRログファイルが空でない場合 (“Debug Options”画面の“SSOMGR Debug Traces”が有効な場合)、毎日午前0時にこのファイルが圧縮されます。圧縮ファイル (.gz) が作成されると、そのファイルに日付スタンプで名前が付けられます。SSOMGRファイルが圧縮されると、新しいSSOMGRファイルが作成されます。その後、該当するログが生成されると、この新しいファイルにログが書き込まれます。ロードマスターは、圧縮されたSSOMGRファイルを最大6個まで同時に保持します。ファイルが圧縮されてから7日間経過すると、そのファイルは削除されます。

Clear Extended Logs (拡張ログのクリア)

“Clear”ボタンをクリックすると、拡張ログをすべて削除できます。

日付範囲を指定するか、ログファイル一覧から個々のログファイルを選択するか、ログファイル一覧からログの種類 (たとえば、接続、セキュリティ、ユーザー) を選択し、ログファイルをフィルターしてから “Clear” ボタンをクリックすると、特定のログファイルを削除できます。警告メッセージが表示された場合は、“OK” をクリックしてください。

Save Extended Logs (拡張ログの保存)



“Save”ボタンをクリックすると、拡張ログをすべてファイルに保存できます。

日付範囲を指定するか、ログファイル一覧から個々のログファイルを選択するか、ログファイル一覧からログの種類（例えば、接続、セキュリティ、ユーザー）を選択し、ログファイルをフィルターしてから “Save” ボタンをクリックすると、特定のログファイルを削除できます。

10.4.3 Syslog Options (シスログ・オプション)

ロードマスターは、syslogプロトコルを使い、色々な警告とエラーメッセージを出力できます。これらのメッセージは、通常ローカルメモリーに蓄積されます。

Emergency Host	10.154.190.112
Critical Host	
Error Host	
Warn Host	
Notice Host	
Info Host	

図10-38: シスログ・オプション

該当するフィールドに該当するIPアドレスを入力し、“Change Syslog Parameters”をクリックすることで、このエラーメッセージをリモートのsyslogサーバーに送信するようにロードマスターを設定することもできます。

6つの異なるレベルのエラーメッセージが定義されています。各レベルのメッセージを、異なるサーバーへと送れます。レベルは、INFO、NOTICE、WARN、ERROR、CRITICAL、EMERGENCY です。

各Syslogフィールドでは、最大10個までのIPアドレスを指定できます。IPアドレスは、スペース区切りリストで区切ってください。

Syslogサーバーのセットアップ後、表示される可能性があるメッセージのタイプの例は、以下のとおりです。

- **Emergency (緊急)** : カーネル関連の重大なエラーメッセージ
- **Critical (重大)** : ユニット1で障害が発生し、ユニット2がマスターとして処理を引き継いだ状況 (HAセットアップの場合)
- **Error (エラー)** : 192.168.1.1からのルートの認証エラー
- **Warn (警告)** : インターフェイスの稼働/停止
- **Notice (注意)** : 時刻の同期済み



- Info (情報) : ローカルでアドバタイズされたイーサネットアドレス

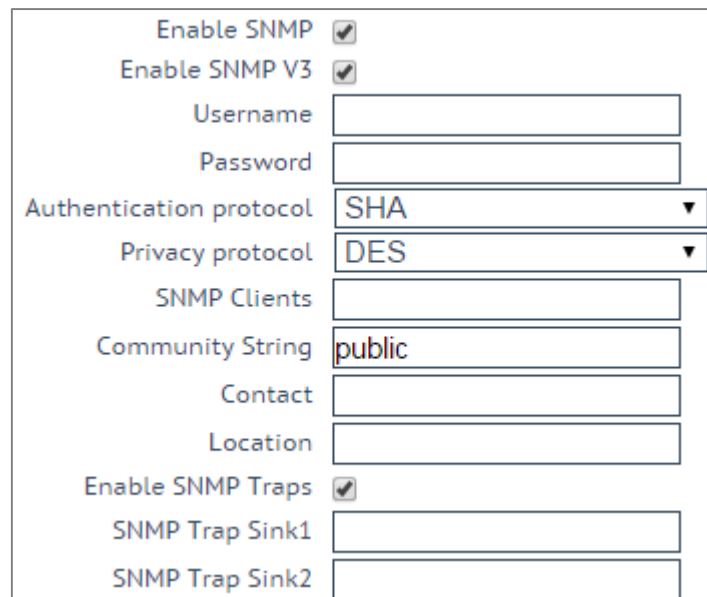
syslogメッセージで1つ注意する点は、それらが上方向にカスケード接続されているということです。つまり、ホストがWARNのメッセージを受信するように設定されている場合、ログのメッセージファイルには、WARN以下のレベルのすべてのメッセージが含まれて出力されます。

もし、WARNとその一つ下のNOTICEに同じシスログサーバーを指定した場合、NOTICEレベルのメッセージは同じホストに二回送信されます。よって、同じホストを一つ以上のレベルに設定しないことをお勧めします。

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

10.4.4 SNMP Options (SNMP オプション)

このメニューでは、SNMPの設定を変更できます。



The image shows a web form for configuring SNMP. It includes checkboxes for 'Enable SNMP' and 'Enable SNMP V3', both of which are checked. There are input fields for 'Username' and 'Password'. Two dropdown menus are present: 'Authentication protocol' set to 'SHA' and 'Privacy protocol' set to 'DES'. Below these are input fields for 'SNMP Clients', 'Community String' (containing 'public'), 'Contact', and 'Location'. At the bottom, there is a checked checkbox for 'Enable SNMP Traps' and two empty input fields for 'SNMP Trap Sink1' and 'SNMP Trap Sink2'.

図 10-39:SNMPオプション

Enable SNMP (SNMPの有効化)

このチェックボックスは、SNMPメトリクスを有効/無効にします。たとえば、このオプションを使用すると、ロードマスターがSNMP要求に応答するよう設定できます。

デフォルトでは、SNMPは無効になっています。

機能が有効になっている場合、次のトラップが生成されます。

- ColdStart (SNMPサブシステムの開始/停止)
- VsStateChange (仮想サービス状態の変更)
- RsStateChange (実サーバー状態の変化)
- HaStateChange (HAの状態変更) : (HA構成のみ:ロードマスターのフェイルオーバー)

テンプレートで作成した、ESPが有効になっている仮想サービスの監視にSNMPを使用する場合、マスターサービスに頼るのではなく、各サブVSを直接監視するようにしてください。これは、認証プロキシのサブサービスは常に稼働中であるとしてマークされるため、その結果、そのマスターサービスも同様に稼働中であるとしてマークされることによるものです。

すべてのロードマスター固有のデータ・オブジェクトに関する情報は、3つのエンタープライズ固有のMIB（管理情報ベース）に格納されます。

MIBファイル	関連するデータ
IPVS-MIB. txt	仮想サーバーの統計
B-100-MIB. txt	L7ロードマスターの設定およびステータス情報
ONE4NET-MIB. txt	エンタープライズID

表10-1:MIBファイル

SNMPを介してロードマスターの性能/コンフィギュレーションのデータを要求できるようにするには、これらのMIBファイル（このファイルはKEMPのドキュメントページ<http://kemptechnologies.com/documentation>にあります）をSNMPマネジャーにインストールする必要があります。

各カウンタの説明は、ロードマスターのMIBから採取することができます。MIB情報を読み込むためには、LinuxでNADucdsnmpコマンドを使用して下記のように行います。



```
snmptranslate -Td -OS <oid>
```

ここでの < OID >は、オブジェクト識別子です。

例:<oid> = .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

```
snmptranslate -Td -Ov .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns
```

```
.1.3.6.1.4.1.12196.12.2.1.12
```

RSConns	OBJECT-TYPE
---------	-------------

— FROM	IPVS-MIB
--------	----------

SYNTAX	Counter32
--------	-----------

MAX-ACCESS	read-only
------------	-----------

STATUS	current
--------	---------

DESCRIPTION	“the total number of connections for this RS”
-------------	---

```
::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12) ipvsRSTable(2) rsEntry(1) 12 }
```

KEMP OIDは、従来化の互換性を保つため、one4netと呼ばれます。

ロードマスターMIBで定義されたデータオブジェクトは、WUIで表示されるカウンタのスーパーセットです。

ロードマスター上のデータオブジェクトは、書き込み可能ではありません。よって、GETリクエスト (GET、GET-NEXT、GETBULKなど) のみ使用してください。

Enable SNMP V3 (SNMP V3を有効にする)

このチェックボックスは、SNMPv3メトリクスを有効にします。SNMPv3は、SNMPと比べ、主にセキュリティやリモート設定機能が強化されています。

このオプションを有効にすると、2つのフィールド、すなわち“Username” (ユーザー名) と“Password” (パスワード) のフィールドが新たに利用できるようになります。



SNMPv3が機能するには、“Username”（ユーザー名）と“Password”（パスワード）を設定する必要があります。

パスワードは8文字以上でなければなりません。

Authentication protocol (認証プロトコル)

目的の“Authentication protocol”（認証プロトコル）（MD5またはSHA）を選択します。
SHAを推奨します。

Privacy protocol (プライバシープロトコル)

目的の“Privacy protocol”（プライバシープロトコル）（AESまたはDES）を選択します。
AESを推奨します。

SNMP Clients (SNMPクライアント)

このオプションにより、管理者はロードマスターが特定の SNMP管理ホストへのみ応答を返すかの指定を行います。1つ以上のホストを指定する場合は、空白で区切って入力します。

クライアントを指定しない場合は、ロードマスターはSNMP管理リクエストに対しての応答を不特定のホストへ返します。

SNMP Community String (SNMPコミュニティ文字列)

このオプションは、SNMPコミュニティ・ストリングの変更を許します。デフォルト値は“public”です。

“Community String”（コミュニティ文字列）では以下の文字を使用できます。a-z, A-Z, 0-9, _ . - @ () ? # % ^ + ~ ! .

Contact (SNMPコンタクト)

このオプションは、SNMPコンタクト名列の変更を許します。例えば、ロードマスター管理者のE-Mailアドレスなどです。



SNMP Location (SNMPロケーション)

このオプションは、SNMPロケーション名列を入力します。

このフィールドには、下記の文字列が使用できます。

a-z A-Z 0-9 _ . - ; , = : { } @ () ? # % ^ + ~ !

“Location”では先頭の文字にハッシュタグ記号（#）を入力しないでください。

SNMP traps (SNMPトラップ)

ロードマスターの仮想サービスや実サーバーへの重要なイベントが発生した場合、トラップが作られます。これらは、SNMPトラップシンクへ送られます。変更を行うと、ロードマスターはすべての変更が完了するまで待ち、その後、5秒待ってからその値を読み込みます。その時点ですべての変更が安定し、SNMPトラップを送信できるようになります。この5秒の待ち時間中に何らかの状態変化が生じると、その状態変化が処理されて、待ち時間が再度スタートします。

Enable/Disable SNMP Traps (SNMPトラップの有効／無効化)

このトグル・オプションは、SNMPトラップの送信を有効／無効にします。

SNMPトラップは、デフォルトでは無効です。

Send SNMP traps from the shared address (SNMPトラップを共有アドレスから送信する)

このチェックボックスは、ロードマスターがHAモードにあるときのみ表示されます。

デフォルトでは、SNMPトラップは、マスターHAユニットのIPアドレスをソースアドレスとして送信されます。このオプションを有効にすると、SNMPトラップは、マスターHAユニットから共有IPアドレスを使用して送信されます。



SNMP Trap Sink1 (SNMPトラップシンク1)

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

SNMP Trap Sink2 (SNMPトラップシンク2)

このオプションは、管理者がトラップの発生時に、SNMPv2トラップをどのホストに送信するかを指定します。

10.4.5 Email Options (E-Mail オプション)

この画面では、Emailによるロードマスター関連イベントの警告通知を設定できます。Email通知は、事前に定義された6つの情報レベルに基づいて配信できます。レベルごとに異なる受信者を設定でき、各レベルは複数の受信者を設定できます。Eメール警告は、メールサーバーによりますが、ノンセキュア、もしくはセキュア (SSL) 両方の通信をサポートしています。設定と発信試験は、WUIの“System Configuration”サブメニュー下の“System Administration”オプションの“E-Mail Options”から行えます。

Enable Email Logging	☒				
SMTP Server		Set Server	Port		Set Port
Server Authorization (Username)		Set			
Authorization Password		Set Password			
Local Domain		Set Domain			
Connection Security	None				
Emergency Recipients					
Critical Recipients					
Error Recipients					
Warn Recipients					
Notice Recipients					
Info Recipients					
Send Test Email to All Recipients					

図10-40:Email Options (E-Mail オプション)

SMTP Server (SMTPサーバー)



メールサーバーのFQDNまたはIPアドレスを入力します。FQDNを使用する場合は、DNSサーバーを設定してください。

Port (ポート)

Eメールイベントを処理するSMTPサーバーのポートを指定します。

Server Authorization (Username) (サーバー認証 (ユーザー名))

指定した SMTPサーバーが、メール配信を行うために特定権限を必要とするならば、その権限を持ったユーザー名を入力します。もし権限を必要としないならば空白のままとします。

AuthorizationPassword (認証パスワード)

上記ユーザーのためのパスワードを入力します。パスワードは、半角文字で8文字から16文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組み合わせて指定できます。

Local Domain (ローカルドメイン)

SMTPサーバーが、ドメインに属しているならば最上位のドメイン名を入力します。必要がなければ空白のままとします。

Connection Security (接続セキュリティ)

接続のセキュリティの種類を選択します。

- None (なし)
- STARTTLS (利用可能な場合)
- STARTTLS
- SSL/TLS

Set Email Recipient (Eメール受信者の設定)

目的の通知レベルに対応する“Recipients”テキストボックスに、それぞれ担当者のEメールアドレスを入力します。その重大度に加え、より高い重大度をもつものに対して通知



が送信されます。そのため、複数のテキストボックスにEメールアドレスを入力する必要はありません。複数のテキストボックスに入力すると、通知が重複して送信されます。例えば、“Critical Recipients”テキストボックスに入力されたEメールアドレスには、重大なEメールだけでなく緊急のEメールも送信されます。

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

Info Recipients (情報受信者) : info@kemptechnologies.com, sales@kemptechnologies.com

Error Recipients (エラー受信者) : support@kemptechnologies.com

リストに登録されたすべてのEメール受信者にテストメールを送信するには、“Send Test Email to All Recipients” ボタンをクリックします。



10.4.6 SDN Log Files (SDNログファイル)

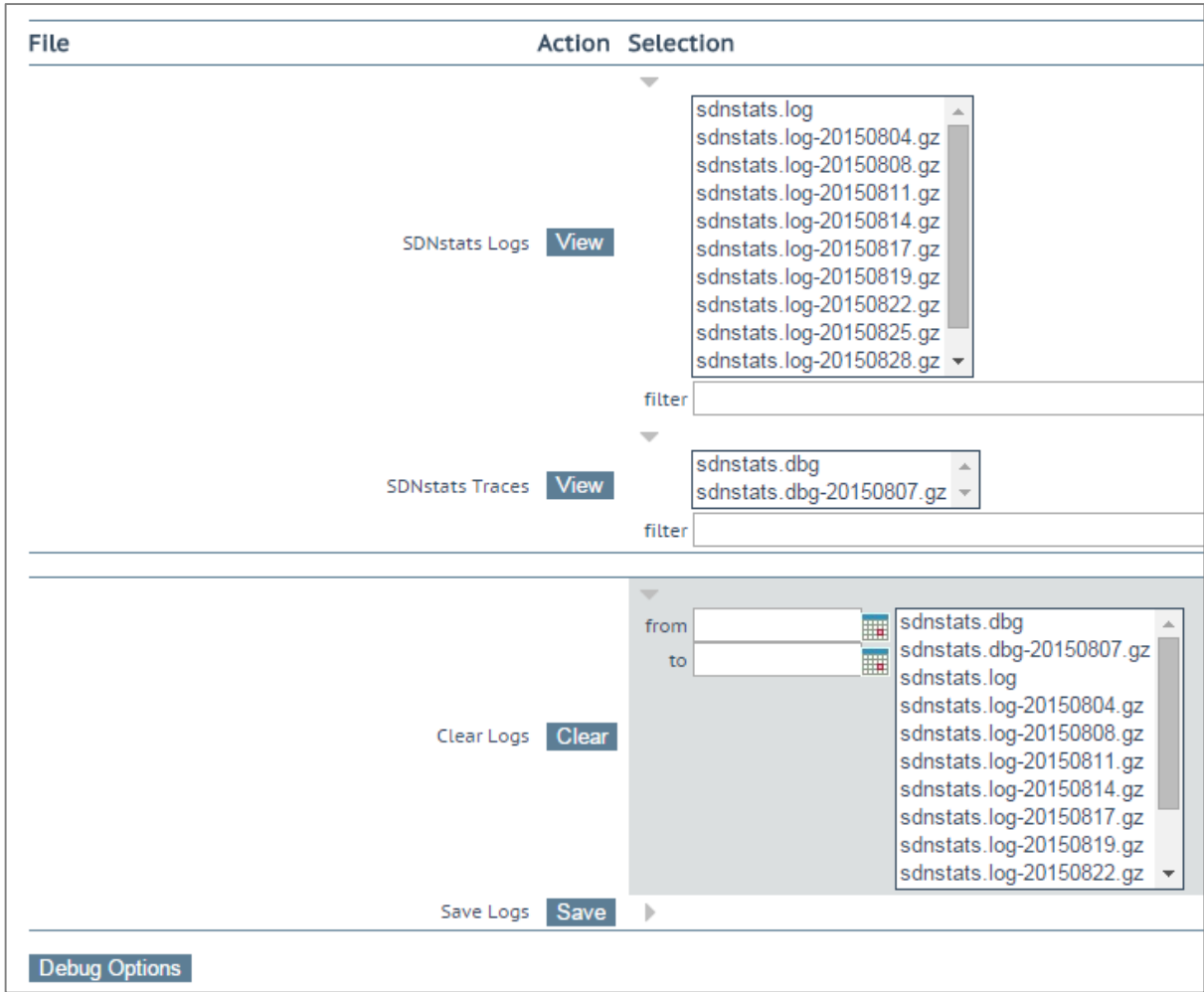


図10-41:SDNログファイル

“SDN Log Files”画面には、SDN機能に関するログのオプションが用意されています。すべてのオプションを表示するには、 アイコンをクリックします。

View SDNstats Logs (SDNstatsログの表示)

SDNstatsログを表示するには、目的のログファイルを選択して“View”ボタンをクリックします。

sdnstats.logがメインの循環ログファイルです。.gzファイルは、ある特定の日にけるログのバックアップです。



また、アーカイブされたログファイルを表示するには、ファイル名一覧から目的のファイルを選択し、“View” ボタンをクリックします。“filter” フィールドに単語または正規表現を入力して“View” ボタンをクリックすると、ログファイルをフィルターできます。

View SDNstats Traces (SDNstatsトレースの表示)

このオプションは、SDNstatsのデバッグログが有効のときのみ利用できます (“System Configuration > Logging Options > SDN Log Files > Debug Options > Enable Debug Log”)。

SDNstatsログを表示するには、目的のログファイルを選択して“View” ボタンをクリックします。

ファイル名一覧から目的のファイルを選択して“View” ボタンをクリックすることで、アーカイブされた1つまたは複数のログファイルを表示できます。“filter” フィールドに単語または正規表現を入力して“View” ボタンをクリックすると、ログファイルをフィルターできます。

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

図 10-42: 成功

トレースには検査結果が表示されます。この検査結果には、ロードマスターがSDNコントローラーと正しく通信できたかが示されます。

Clear Logs (ログのクリア)

“Clear” ボタンをクリックすると、すべてのSDNログをクリアできます。

“from” (開始) および“to” (終了) フィールドで日付を指定すると、特定の範囲のログファイルを抽出できます。日付範囲を指定すると、右側のボックスにて目的のログファイルが選択されます。その場合でも、右側のボックスで個々のログファイルを選択/選択解除できます。



重要: sdnstats. logを選択すると、日付範囲フィールドで選択した日付にかかわらず、そのファイルに記録されているすべてのログが消去されます。

Save Extended Logs (拡張ログの保存)

“Save”ボタンをクリックすると、すべてのSDNログをファイルに保存できます。

特定の日付範囲を指定してフィルターするか、ログファイル一覧にて1つまたは複数のログファイルを個々に選択して“Save”ボタンをクリックすると、特定のログファイルを保存できます。

10.4.6.1 Debug Options (デバッグオプション)

“SDN Debug Options” (SDNデバッグオプション) 画面を開くには、“SDN Log Files” (SDNログファイル) 画面にて“Debug Options” (デバッグオプション) ボタンをクリックします。

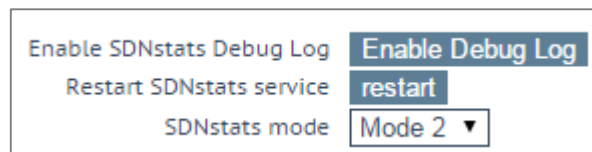


図 10-43: デバッグオプション

Enable Debug Log (デバッグログを有効にする)

SDNstatsのデバッグログを有効にします。

SDNの統計値のログを表示するには、“System Configuration > Logging Options > SDN Log Files”を選択し、表示したいログファイルを選択して“View” (表示) ボタンをクリックします。

デバッグログはロードマスターのパフォーマンスに影響を与えるため、トラブルシューティング時のみ有効にしてください。

Restart SDNstats service (SDNstatsサービスの再起動)

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



再起動すると、“Process ID” (プロセスID) が新しいIDに変わります。

“Process ID” (プロセスID) を調べるには、“System Configuration > Logging Options > System LogFiles”の“Debug” (デバッグ) ボタンをクリックし、“ps”ボタンをクリックします。

このオプションは、SDNコントローラーに割り当てられているすべての接続を再起動します。

SDNstats mode (SDNstatsモード)

SDNの統計情報を収集するための2つのモードが用意されています。

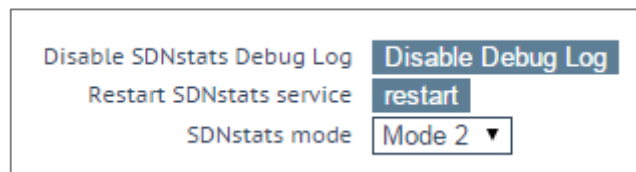


図 10-44:SDNstats mode (SDNstatsモード)

モードを設定するには、“System Configuration > Logging Options > SDN Log Files > Debug Options”を選択し、“SDNstats mode” (SDNstatsモード) を設定します。

各モードについて、以下で説明します。

- **Mode 1 (モード1)** :モード1に設定すると、サーバーに接続されているスイッチから統計情報が取り出され、その統計情報が中継されてロードマスターに返されます。
- **Mode 2 (モード2)** :モード2に設定すると、経路上にあるすべてのスイッチポートから統計情報が取り出されます。

10.5 Miscellaneous Options (その他のオプション)

10.5.1 WUI Settings (WUIの設定)

“bal” ユーザーまたは“All Permissions” の権限が設定されたユーザーのみ、この機能を使用できます。それ以外のユーザーの場合、画面上のボタンや入力フィールドはすべてグレー表示になります。



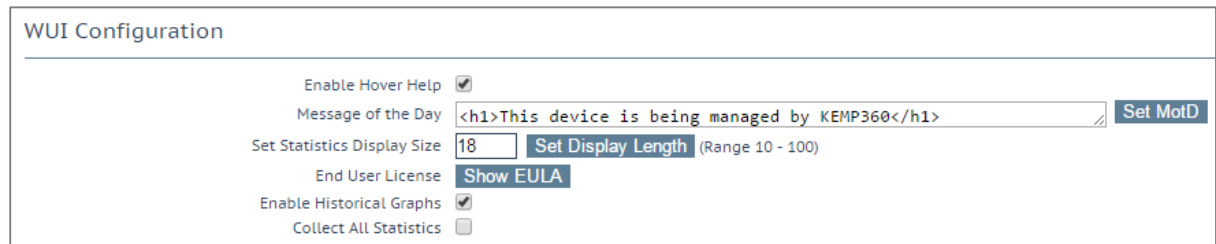


図10-45:WUI設定の画面

Enable Hover Help (ホバーヘルプの有効化)

フィールドの上にマウスポインターを置いたときに、青いホバーヘルプが表示されるようにします。

Message of the Day (MOTD) (本日のメッセージ (MOTD))

フィールドにテキストを入力して、“Set MotD”ボタンをクリックします。このメッセージは、ロードマスターのホーム画面に表示されます。

WUIのセッション管理が有効になっている場合、MOTDはHOME画面ではなくログイン画面に表示されます。

メッセージは最大5,000文字まで入力できます。HTMLはサポートされていますが、必須ではありません。引用符（'）と二重引用風（"）は使用できません。ただし、これらと等価のHTML文字コードは使用できます。たとえば、"it's allowed"と入力すると、“it’s allowed”というMOTDが表示されます。

Set Statistics Display Size (統計情報の表示サイズ設定)

統計情報のページに表示可能な最大行数を設定します。10～100行の範囲でページに表示できます。

End User License (エンドユーザーライセンス)

“Show EULA” ボタンをクリックすると、ロードマスターのエンドユーザーライセンス契約が表示されます。

Enable Historical Graphs (履歴グラフを有効にする)



仮想サービスと実サーバーに関する過去の統計情報の収集を有効にします。

Collect All Statistics (全統計情報の収集)

デフォルトでは、このオプションは無効になっています。つまり、ホームページに表示するよう設定されている仮想サービスと実サーバーの統計情報だけが収集されることを意味します。このオプションを有効にすると、ロードマスターでは、すべての仮想サービスと実サーバーを対象として統計情報が収集されます。

数多くの仮想サービスや実サーバーの統計情報を収集すると、CPUの使用率が高まる可能性があります。

10.5.2 レイヤ7設定

Allow connection scaling over 64K Connections	☐
Always Check Persist	No
Add Port to Active Cookie	☐
Conform to RFC	☒
Close on Error	☐
Add Via Header In Cache Responses	☐
Real Servers are Local	☐
Drop Connections on RS failure	☐
Drop at Drain Time End	☐
L7 Authentication Timeout (secs)	30 Set Timeout (Valid values:30 - 300)
L7 Connection Drain Time (secs)	300 Set Time (Valid values:0, 60 - 86400)
Additional L7 Header	X-ClientSide
100-Continue Handling	RFC-2616 Compliant
Allow Empty POSTs	☐
Least Connection Slow Start	0 Set Slow Start (Valid values:0 - 600)
Share SubVS Persistence	☐
Log Insight Message Split Interval	10 Set Log Split Interval (Valid values:1 - 100)

図 10-46: レイヤ7設定

Allow Connection Scaling over 64K Connections (64Kを超える接続への拡張を許可する)

高トラフィックにおいては、VSごとのTCP接続数が1ポートの上限である64,000 以上必要になることがあります。このオプションを使用することで、他のIPアドレスのポートを振り分けることで上限を拡張できます。他のIPアドレスの指定は、仮想サービスの属



性パラメータの“Alternate Source Addresses”内に指定できます。1つ以上のIPアドレスを指定する場合は、空白で区切って入力します。

64Kを超える同時接続が必要な場合は、“Allow Connection Scaling over 64K Connections” オプションを有効にし、“Alternate Source Addresses” フィールドに代替アドレスとなる仮想サービスのIPアドレスを入力します。これにより、各仮想サービスがソースポートのプールを持てるようになります。

透過仮想サービスについては、同時接続数を64Kより大きくできません。この制限は、仮想サービスごとに適用されます。

このオプションを選択した後に代替ソースアドレスを設定した場合、“Allow connection scaling over 64K Connections”オプションを無効にできません。

Always Check Persist (パーシステンスを常にチェック)

デフォルトでは、L7モジュールはHTTP/1.1接続における最初のリクエストに対してのみパーシステンスをチェックします。このオプションで“**Yes**”を選択すると、全てのリクエストに対してパーシステンスをチェックします。“**Yes - Accept Changes**”を選択すると、接続の途中でであってもパーシステンスの全ての変更が保存されます。

Add Port to Active Cookie (アクティブクッキーにポートを追加)

アクティブクッキーを使用している場合、ロードマスターは（数ある情報の中から）クライアントのIPアドレスに基づいてクッキーを作成します。ただし、プロキシサーバー経由で接続しているクライアントはすべて、同じIPアドレスで接続していることになります。このオプションをオンにすると、クライアントのソースポートが追加されるので、クッキーのランダム性が向上します。

Conform to RFC (RFCへの準拠)

このオプションは、HTTP要求のヘッダー解析をRFC 1738に準拠させます。



この要求は3つの部分で構成されています。このオプションをオンにすると、ロードマスターはHTTPリクエストの3つの部分から構成されている ‘GET /’ ‘パス名’ ‘HTTP / 1.1’ を、パス名の最後尾としてのスペースが見つかるまでスキャンします。そして、そのスペースが見つかり、その後続く部分が HTTP/1.xであるとみなします。パス名にスペースが含まれており、ブラウザがRFCに準拠している場合、そのパス名のスペースは“%20”にエスケープされるので、スペースのスキャンは正しく機能します。

ただし、規格に準拠していない一部のブラウザでは、スペースがエスケープ処理されず、間違ったパス名として処理されます。そして、システムはHTTP/1.xを見つけることができないことより、ロードマスターは要求を拒否します。

この機能をオフにすると、ロードマスターは強制的にスペースはパス名の最後尾と見まします。そして、その後のパス名を HTTP/1.xの指定として処理してしまうために、リクエストは正しく処理されません。スペースを含むパス名を使用可能にするためには、RFC 1738非準拠にしなければなりません。

Close on Error (エラー時にクローズする)

キャッシュ内のファイルの方が新しい場合など、ロードマスターがクライアントにエラーレポートを返す必要がある場合、このオプションはロードマスターによる応答の送信後に接続を強制的に終了します。このオプションを使用しないで、エラーレポートを送信した後でも、接続を継続して使用できますが、いくつかのシステムは混乱する可能性があります。このオプションは、処理を継続せずに強制的に終了します。

Add Via Header In Cache Responses (キャッシュ応答へのViaヘッダーの追加)

関連するHTTP RFCでは、キャッシュから応答が帰ってきた場合には、プロキシがViaヘッダーを追加する必要があると規定されています。残念ながら、ロードマスターの古いバージョンは、この機能に対応していませんでした。このチェックボックスは、（必要に応じて）古いバージョンとの下位互換性を有効にする目的で使用します。

Real Servers are Local (実サーバーをローカルとみなす)



ロードマスターは、透過性（選択的透過性）を目的として、ローカル/非ローカルクライアントを自動検出しています。この機能は、ほとんどのケースで問題なく動作しますが、クライアントが実サーバーである場合には適切に動作しません。このオプションをオンにすることで、実サーバーがローカルであることをロードマスター側で判定できるようになるので、選択的透過性が適切に機能します。

2アーム環境（クライアントと実サーバーが2番目のインターフェイス上にある環境）にてこのオプションを有効にすると、実サーバーはクライアントから見てローカルであるかのように（非透過的に）扱われます。実サーバーが全く異なるネットワーク上にある場合、そのサーバーはローカルになることはできず、常に非ローカルとして扱われます。ローカルとは、同じネットワーク上にあることをいいます。

このオプションを有効にする際は、ネットワークトポロジーを慎重に計画してください。また、このオプションを有効にする前に、KEMPのサポートチームに必ずお問い合わせください。

Drop Connections on RS Failure (実サーバー障害時に接続をドロップする)

Microsoft Outlookユーザーに有用なオプションであり、実サーバーの障害が検出された時点で、直ちに接続を終了します。

これは、MS Outlookユーザーのために非常に有用なオプションです。それと同時に、“Idle Connection Timeout”オプションが86400に設定されます。詳細については、*Microsoft Exchange 2010 展開ガイド*を参照してください。

Drop at Drain Time End (ドレイン時間終了時にドロップする)

このオプションを有効にすると、無効化された実サーバーへのオープンな接続が、実サーバーのドレイン停止時間終了時にすべてドロップされます（実サーバーに継続時間が設定されていない場合は直ちにドロップされます）。

L7 Authentication Timeout (secs) (L7認証タイムアウト (秒))

このオプションは、2次処理（SMSや電話による確認など）を備えたサードパーティの多要素認証ソリューションとの統合をサポートします。この設定は、認証時の確認がタイムアウトするまでの、SSOフォームの待ち時間（単位：秒）を規定します。



L7 Connection Drain Time (secs) (L7接続ドレイン時間 (秒))

“L7 Connection Drain Time” は、新規接続にのみ影響します。既存の接続は、その接続が終了するまで（ただし“Drop at Drain Time End” チェックボックスがオンになっている場合を除く）、無効化された実サーバーにアプリケーションのデータを中継し続けます。

“L7 Connection Drain Time (secs)”を0に設定すると、実サーバーが無効化された時点で、直ちにすべての接続がドロップされます。

サーバーがレイヤ4で動作している場合は、ドレインの停止は適用されません。この場合、パーシステンスレコードが破棄され、その接続は有効かつ正常に動作しているサーバーに送信されるようスケジュールされ、新たにパーシステンスレコードが作成されます。

以下の場合、新規のTCP接続は無効化されたサーバーには送信されず、有効かつ正常に動作しているサーバーに送信されます。

- パーシステンスが無効になっている。または
- その接続のパーシステンスレコードの有効期限が切れていない。または
- 実サーバーが停止している。または
- ドレイン停止時間が過ぎている

上記の条件がすべて当てはまらない場合、その接続は指定したサーバーに送信され、パーシステンスレコードが更新されます。

ドレイン停止時間は、既存の接続には影響しません。

Additional L7 Header (レイヤ7 追加ヘッダー)

HTTP/HTTPS仮想サービスのレイヤ7ヘッダー挿入を有効にします。ヘッダー挿入の設定は、“X-ClientSide” (KEMPロードマスター専用)、“X-Forwarded-For”、または“None”のいずれかを選択できます。

100-Continue Handling (100-Continueの処理)

100-Continue Handling メッセージをどのように処理するかを設定します。以下のオプションを選択できます。

- **RFC-2616 Compliant (RFC-2616準拠)** : RFC-2616で規定された動作に準拠します
- **Require 100-Continue (100-Continueが必要)** : 100-Continueメッセージを待機するよう、ロードマスターを設定



- **RFC-7231 Compliant (RFC-7231準拠)** : ロードマスターが100-Continueメッセージを待たないようにします

システムにより100 Continueメッセージがどのように処理されるかを
変更するには、上記のRFCに記載されている関連技術を理解する
必要があります。これらの設定を変更する前に、KEMPの技術サポ
ートエンジニアにご相談ください。

Allow Empty POSTs (空のPOSTを許可)

デフォルトでは、リクエストペイロードの長さを示すContent-LengthヘッダーまたはTransfer-Encodingヘッダーを含まないPOSTは、ロードマスターによってブロックされます。“Allow Empty POSTs”オプションを有効にすると、そうしたリクエストはペイロードデータがないものとみなされ、拒絶されなくなります。

バージョン7.1-24以降のリリースでは、サポートされるコンテンツ
長の上限が2GBから2TBに増えました。

Least Connection Slow Start (最小接続のスロースタート)

最小接続方式または重み付け最小接続方式を使用する場合、実サーバーがオンラインになったときにそのサーバーへの接続数を制限する期間を指定し、その後、徐々に接続数を増やすように設定できます。これにより、実サーバーがオンラインになったときに接続が殺到するのを防いで、サーバーが過負荷になるのを防げます。

スロースタート期間は0～600秒の範囲で設定できます。

Share SubVS Persistence (共有サブVSパーシステンス)

デフォルトでは、仮想サービスの各サブVSは個別のパーシステンステーブルを持っています。このオプションを有効にすると、サブVS間でその情報を共有できるようになります。この機能が動作するには、その仮想サービス内にあるすべてのサブVSのパーシステンスモードが同じでなければなりません。このオプションを有効にするには再起動が必要です。



Persistence Mode (パーシステンスモード) のうち、SSL Session ID (SSLセッションID) だけは共有できません。

共有サブVSパーシステンス設定時、この機能を完全に動作させるにはいくつかの要件があります。

- そのサブVSのすべての実サーバーが同じでなければならない
- すべてのサブVSにおいて、“Persistence Mode” (パーシステンスモード) が同じでなければならない
- タイムアウト値を同じ値に設定する必要がある

上記の要件が満たされない場合、そのサブVSまたは複数のサブVSのいずれにおいても、そのパーシステンスは正しく機能しません。

10.5.3 Network Options (ネットワーク関連オプション設定) ネットワークオプション

Enable Server NAT ☒	
Connection Timeout (secs) 660	Set Time (Valid values:0, 60-86400)
Enable Non-Local Real Servers ☐	
Enable Alternate GW support ☐	
Enable TCP Timestamps ☐	
Enable TCP Keepalives ☒	
Enable Reset on Close ☐	
Subnet Originating Requests ☐	
Enforce Strict IP Routing ☐	
Handle non HTTP Uploads ☐	
Enable Connection Timeout Diagnostics ☐	
Enable SSL Renegotiation ☒	
Size of SSL Diffie-Hellman Key Exchange 2048 Bits	
Use Default Route Only ☐	
HTTP(S) Proxy	Set HTTP(S) Proxy

図 10-10-47:Network Options (ネットワーク関連オプション設定) ネットワークオプション

Enable Server NAT (サーバーNATの有効化)

このオプションを選択すると、サーバーネットワークアドレス変換 (SNAT) が有効になります。このオプションを無効にすると、接続時に実サーバーのIPアドレスが使用されます。

Connection Timeout (secs) (接続タイムアウト (秒))



接続が閉じられる前に、接続がアイドル状態でいられる時間を秒で指定します。この値は、パーシステンスタイムアウトの値とは独立しています。

0を設定すると、デフォルトの設定（660秒）にリセットされます。

Enable Non-Local Real Servers (リモートサーバーの有効化)

非透過モード (Non transparent) 仮想サービスで、ローカルサブネット以外のサーバーを、実サーバーとして追加できます。透過モード (Transparent) の仮想サービスへは有効になりません。このパラメータを “Yes” にすると、VS内のRS追加時に新たなパラメータとして “Allow Remote Addresses” が表示されますので、チェックマークをいれた後でリモートRSのIPアドレスを入力します。ロードマスターがインターフェイスを1つしか持つことができず、実サーバーがそのインターフェイスとは異なるネットワーク上にある場合に、このオプションが必要になります。

Enable Alternate GW support (ポート 0 以外のゲートウェイの有効化)

複数のインターフェイスが有効になっている場合、このオプションは、デフォルトゲートウェイを別のインターフェイスに移行する機能を提供します。

このオプションを有効にすると、“Interfaces”画面に“Use for Default Gateway”オプションが追加されます。

“Enable Alternate GW support”オプションは、GE0のみのロードマスターの画面に別途表示されます。

Enable TCP Timestamps (L7タイムスタンプの有効化)

ロードマスターは、デフォルトにおいてTCP接続パケット (SYN) にタイムスタンプを含みません。L7モードでの接続で、パフォーマンス試験などでタイムスタンプの必要がある時は、Onにしてください。それ以外の一般の通常オペレーションでは、このパラメータはオフにしておくことを推奨します。

販売店のサポート要員からの要求に応じてこれを有効にしてください。

Enable TCP Keepalives (TCP接続のキープアライブの有効化)



アプリケーションによっては、TCPを開いたままではタイムアウトを起こしてしまうものがあります。一般に、通常のHTTP/HTTPSサービスではキープアライブは必要ありませんが、FTPサービスなどで必要になります。

キープアライブメッセージは、ロードマスターから実サーバーとクライアントに送信されます。したがって、クライアントがモバイルネットワーク上にある場合、データトラフィックの増加が問題になる可能性があります。

Enable Reset on Close (Reset使用によるTCP接続クローズの有効化)

このオプションを有効にすると、ロードマスターは通常のクローズハンドシェイクの代わりにRESETを使用して、実サーバーとの接続を終了します。このオプションによる効果が現れるのは、接続数が多く、負荷が高い場合に限定されます。

Subnet Originating Requests (非透過モードでのソースアドレス変更)

このオプションを有効にすると、非透過リクエストのソースIPアドレスが、該当するサブネット（すなわち、実サーバーがあるサブネット、または、静的ルートの背後にある非ローカルな実サーバーにルーティング可能なゲートウェイがあるサブネット）上のロードマスターのアドレスに設定されます。

これはグローバルなオプション/設定です。

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

このグローバルオプションを無効にすると、各仮想サービスの“Subnet Originating Requests”オプションが優先されます。すなわち、仮想サービスごとに有効/無効にできます。このオプションは、仮想サービスのプロパティ画面の“Standard Options”セクションで設定できます（“Transparency”が無効の場合）。仮想サービスごとのオプションに関する詳細は、**セクション3.4**を参照してください。

SSLの再暗号化が有効な仮想サービスに対してこのスイッチをオンにすると、その接続を処理しているプロセスを終了して再起動する必要があるため、その仮想サービスを使用しているすべての接続が切断されます。

Enable Strict IP Routing (厳密なIPルーティングの有効化)



このオプションを選択すると、アウトバウンドインターフェイスと同じインターフェイスを介してマシンに到達したパケットだけが許容されます。

これを実現するには、“Use Default Route Only”オプションの方が適しています。

Handle non HTML Uploads (非HTMLのアップロード処理)

このオプションを有効にすると、非HTMLのアップロード (FTPによるアップロードなど) が正しく機能するようになります。

Enable Connection Timeout Diagnostics (接続タイムアウト診断を有効にする)

デフォルトでは、接続タイムアウトログは無効になっています。これは、不要なログが大量に記録されるためです。接続タイムアウトに関するログを作成したい場合は、“Enable Connection Timeout” (接続タイムアウトを有効にする) チェックボックスをオンにします。

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

このオプションをオフにすると、クライアントにより再ネゴシエーションが要求されたときにSSL接続が終了します。

Size of SSL Diffie-Hellman Key Exchange (SSLのディフィー・ヘルマン鍵交換のサイズ)

ディフィー・ヘルマン鍵交換で使用する鍵の強度を選択します。この値を変更した場合、新しい値を使用するには再起動する必要があります。デフォルトは2048です。

Use Default Route Only (デフォルトルートのみ使用)

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



このオプションを有効にすると、同じネットワーク上にあるすべての仮想サービスが影響を受けます。

HTTP(S) Proxy (HTTPSプロキシ)

このオプションを使用すると、ロードマスターがインターネットに接続する際に使用するHTTPプロキシサーバーとポートをクライアントが指定できます。

10.5.4 AFE Configuration (アプリケーション・フロント・エンド機能設定)
OCSPの設定

Cache Configuration

Maximum Cache Size

100

Set Size (Valid values:1 - 409)

Cache Virtual Hosts

☒

File extensions that should not be cached:

Add

.aspx .jsp .php .shtml

No Entry ▾

Delete

Compression Options

File extensions that should not be compressed:

Add

.asf .gif .gz .jpeg .jpg .mov .mp3 .mp4 .mpe .mpeg .mpg .pdf .png .swf .tgz .wav .wma .wmv .z .zip

No Entry ▾

Delete

Intrusion Detection Options

Detection Rules

Choose File

No file chosen

Install new Rules

Detection level

Default - Only Critical problems are rejected ▾

Client Limiting

Client Connection Limiter

0

Set Limit (Valid values:0 - 1000000)

図 10-48:アプリケーション・フロント・エンド機能設定

Maximum Cache Size (最大キャッシュサイズ)

キャッシュで利用可能なメモリ容量をメガバイト単位で定義します。“Maximum Cache Size”は、どのくらいのメインメモリをキャッシュに割り当てるかを定義します。マシンの総メモリ容量の50%を越えて設定することはできません。より多くのメモリをキャッシュに割り当てると、接続やパースシステムのエントリで利用可能なメモリ量が減少します。システムが正しく設定されていれば、十分なキャッシュのためのメモリ、およびシステムにより処理されると予想されるすべての接続のためのメモリが十分用意されているはずです。そうでない場合、システムのメモリが不足する可能性があります。



Cache Virtual Hosts (仮想ホストをキャッシュする)

このオプションが無効になっている場合、キャッシュ処理では、実サーバーでサポートされている仮想ホストが1台だけであると想定します。もし、このオプションが有効になっている場合は、実サーバーが異なるコンテンツを持つ複数の仮想ホストを持つものとしてキャッシュの処理を行います。

File Extensions Not to Cache (キャッシュしないファイル拡張子)

キャッシュされるべきではないファイルタイプのリスト。

File Extensions Not to Compress (圧縮しないファイルの拡張子)

圧縮されるべきではないファイルタイプのリスト。

Detection Rules (検出ルール)

検出ルールをインストールするには、関連する検出ルールを選択して、“Install New Rules”ボタンをクリックします。

SNORTルールをインストールする場合、以下の点に注意してください。

- 宛先ポートは\$HTTP_PORTSとしてください
- オプションで ‘msg’ を設定できます。
- フローは ‘to_server, established’ と設定してください
- 実際のフィルターは ‘content’ または ‘pcre’ のいずれかを選択できます
- ‘http_’ パラメータを追加で設定できます。
- classtypeには有効な値を設定してください

最新のカスタムSNORTルールを取得するには、SNORTのウェブサイト (<https://www.snort.org/>) を参照してください。 <https://www.snort.org/>

Detection Level (検出レベル)

侵入防止システムのルールのアップグレード、および検出レベルの設定変更を行えます。

- Low - 無拒絶、ログのみ



- **Default** - 重要な問題を含むアクセスのみ拒否
- **High** - 深刻かつ重大な問題を含むアクセスのみ拒否
- **Paranoid** - 問題が検出されたすべてのアクセスを拒否

Client Limiting (クライアントの制限) :

与えられたホストからの秒あたりの接続数の制限を設定可能です。(100Kまで制限が可能)。システムに“デフォルト値の制限”を設定した後、特定のホスト/ネットワークのために異なる制限を設定できます。

ネットワークとそのネットワーク上のホストを設定する場合は、表示されるリストの順番による処理が行われるため、優先順位の高いホストより設定する必要があります。

クライアントの上限をオフにするには、“Client Connection Limiter”の値を0に設定します。

10.5.5 HAのパラメータ

ロードマスターfor Azureを使用する場合は、**セクション10.5.6**を参照してください。

各ユニットのロールは、「HAモード」パラメータを設定し直すことで変更することができます。“HA (First) Mode”または“HA (Second) Mode”を“HA Mode”として選択した場合、共有IPアドレスを追加するよう促すプロンプトが表示されます。“HA Mode”を変更すると再起動が必要になるので、詳細を設定したら、画面の“Reboot”ボタンをクリックします。ロードマスターが再起動すると、ロールが“Non HA Mode”ではない場合、“System Configuration > Miscellaneous Options”セクションで“HA Parameters”メニューオプションが使用可能になります。2台を両方とも同じHAモードにすると正しいペアとして構成されません。

HAペアにログインして、完全な機能の表示および設定を行うには、共有（シェアード）IPアドレスを使用します。ユニットに与えられたIPアドレスに直接ログインした場合、WUIとして表示されるメニューが異なります（下記のメニューを参照してください）。各ユニットのIPアドレスでの直接ログインは、通常そのユニットのみのメンテナンスを行うために行います。





図 10-49:ダイレクトIPメニュー

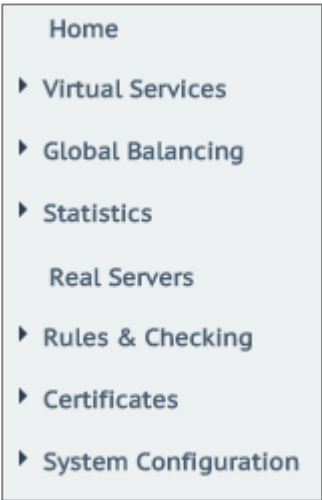


図 10-50:共有IPメニュー

ロードマスターがHAモードになっている場合、“HA Parameters” メニューオプションを選択したときに以下の画面が表示されます。

HA Mode	HA (First) Mode ▼
HA Timeout	9 Seconds ▼
HA Initial Wait Time	0 Set Delay (Valid Values: 0, 10-180)
HA Virtual ID	1 Set Virtual ID (Valid Values: 1-255)
Switch to Preferred Server	No Preferred Host ▼
HA Update Interface	eth0: 10.154.11.70 ▼
Force Partner Update	Force Update
Inter HA L4 TCP Connection Updates	☐
Inter HA L7 Persistency Updates	☐

図 10-51:HAの設定

HA Status (HA状態)

画面上部の時刻表示の隣にあるアイコンは、クラスター内のロードマスターユニットのリアルタイムステータスを示しています。左側のアイコンは、HA-1、右側は HA-2 に対



応しています。該当するステータスアイコンをクリックすると、1番目または2番目のHAユニットのWUIを開くことができます。



可能なアイコンとして、下記のパターンがあります。

緑 ('A' の文字 あり)		ユニットは、オンラインで正常に稼動しています。 中央に 'A' の文字が表示された四角は、マスターユニットであることを表します。
緑 ('A' の文字 なし)		ユニットは、オンラインで正常に稼動しています。 中央に 'A' の文字が表示されていない四角は、マスターユニットではないことを表します。
赤で黄 色の X		ユニットはオフラインです。正しいHA構成がなされていません。
青		両方のマシンがアクティブモードとなっています。すなわち、何らかの設定間違いが何かで両方がマスターで立ち上がっています。両ユニットのイーサネットポートの設定を確認後、一つのユニットを再起動してみると解決するかもしれません。
灰		3分以内に二回以上のリブートが発生したためにパッシブファイ (管理者対応を要求し、システムはホルト状態) モードです。原因究明、そしてその対処後、再起動が必要です。 KEMPのサポートにご連絡ください。

HAモードでは、各ユニットは、自身の直接診断目的でのみ使用する、独自のIPアドレスを持ちます。そして、単一のエンティティとしてHA構成の設定および管理を行うために使用されるWUI上の共有IPアドレスを持ちます。

HA1とHA2の両方が同一のデフォルトゲートウェイと同じサブネット上に存在し、同じ物理サイト内に存在する必要があります。サイト内リンクで区分されることなく、同じゲートウェイを使用してトラフィックを返す必要があります。

HA Mode (HA構成モード)

スタンドアローン、HA-1 (HA First)、もしくは HA-2 (HA Second) の選択ができます。同じ HAモードでは、正しいHA 構成が組めません。この設定を変更するときにはシステムリブートが必要です。

KEMPIはHA対応のライセンスをHAユニットごとに提供し、ユニット1とユニット2として規定しています。したがって、KEMPのサポート部門と問題について話し合わずに、このオプションを変更することは推奨しません。

HA Timeout (HAタイムアウト)

スイッチオーバーが発生する前にマスターマシンを利用できなくする時間です。このオプションを使用すると、HAクラスターが障害を検出するのに要する時間を3秒から15秒まで3秒刻みで調整できます。デフォルト値は9秒です。値を低くすると、障害がより早く検出されます。一方、値を高くすると、DOS攻撃に対する防御が強くなります。

HA Initial Wait Time (HA起動待機時間)

ロードマスターの初回起動後、マシンをアクティブにすべきであるとマシンが判断するまでの時間です。パートナーのマシンが動作している場合、この値は無視されます。この値を変更すると、（一部のインテリジェントスイッチにより）ロードマスターが起動して接続状態になったと判断されるまでの時間を短縮できます。

HA Virtual ID (HA仮想ID)

このオプションは、CARPプロトコルの選択時（デフォルト）に、同じネットワーク上に1つ以上のHAペアが設置されていて、間違った干渉が起こるのを防止するために必要です。そういう場合は、必ずHAペアに異なるID番号を設定するようにしてください。

ネットワーク上でHAペアとして設定されている（またはHAペアとして設定する予定の）ロードマスターには、すべて一意のHA仮想ID番号を割り当てる必要があります。

Switch to Preferred Server (アクティブ固定)



デフォルトでは、HAクラスターのいずれのパートナーも優先権を持っていません。そのため、スイッチオーバー後にマシンが再起動すると、そのマシンがスレーブになり、マスターになるよう強制されるまでその状態を維持します。優先ホストを指定すると、このマシンは再起動時に常にマスターになろうと試みます。そして、このマシンがマスターになると、パートナーはスレーブモードに戻ります。推奨サーバーが指定されている場合、マスターユニットで障害が発生したときスレーブユニットがマスターとなり、その後、推奨ユニットが復帰したときその推奨ユニットがマスターとなるため、フェイルオーバーイベントが二重に発生します。

HA Update Interface (HA情報転送インターフェイス)

この設定は、HA間の情報転送にどのインターフェイスを使用するかを指定できます。1アーム構成では他の選択はできませんが、2アーム、マルチアームでは他のインターフェイスへの変更ができます。

Force Partner Update (パートナーへの設定情報更新)

このパラメータは、HAが正しく同期している時のみ使用できます。“Force Update” ボタンをクリックすると、アクティブ側の設定ファイルをスタンバイ側へ強制的に上書きします。

Inter HA L4 TCP Connection Updates (L4ステータスフル切り替え)

L4サービス使用時、更新を有効にすると、接続テーブルが共有され、HAのスイッチオーバー時にL4の接続が維持されます。このオプションはレイヤ7のサービスでは無視されます。

Inter HA L7 Persistence Updates (L7ステータスフル切り替え)

L7サービス使用時、このオプションを有効にすると、HAパートナー間でパーシステンス情報の共有が可能になります。HAのフェイルオーバーが発生すると、パーシステンス情報が失われます。このオプションを有効にすると、パフォーマンスが大きく影響を受けます。

HA Multicast Interface (HAマルチキャストインターフェイス)



HA間のアップデートが有効になっている場合、マルチキャストトラフィック用のネットワークインターフェイスを用いてレイヤ4とレイヤ7のトラフィックの同期が行われます。

Use Virtual MAC Addresses (仮想MACアドレスを使用)

このオプションを有効にすると、スイッチオーバー時にHAペア間でMACアドレスが強制的に交換されます。これは、HAのIPアドレスの変更をスイッチに通知するのに使用されるグラテュイタスARPが許可されていない場合に役に立ちます。

このオプションは、ハードウェアのロードマスターに対してのみ利用可能です。

10.5.6 AzureのHAパラメータ

このメニューオプションは、ロードマスターfor Azureでのみ利用できます。

Azure HA Mode	Master HA Mode ▼	
Partner Name/IP	qa-azure-ha2.cloudapp.net	Set Partner Name/IP
Health Check Port	8444	Set Health Check Port

図 10-52: AzureのHAパラメータ

Azure HA Mode (AzureのHAモード)

このユニットで必要なHAモードを選択します。3つのオプションが用意されています。

- Master HA Mode (マスターHAモード)
- Slave HA Mode (スレーブHAモード)
- Non HA Mode (非HAモード)

ロードマスターを1台だけ使用する場合、“Non HA Mode”を選択してください。

HAモードを使用する場合、1台目のマシンを“Master”に設定し、2台目のマシンを“Slave”に設定します。

2台のユニットで同じ“Azure HA Mode”の値を選択した場合、HAは機能しません。

仮想サービスの設定の同期は、マスターからスレーブの方向でのみ行われます。マスターに対する変更はスレーブに複製されます。ただし、スレーブに対する変更はマスターには複製されません。

マスターユニットに障害が発生すると、接続はスレーブユニットに向けられます。障害が発生しても、マスターユニットはあくまでマスターであり、スレーブにはなりません。同様に、スレーブユニットはマスターにはなりません。マスターユニットが復旧すると、接続は自動的にマスターユニットに向けられます。

MASTER (ACTIVE) 04:12:10 PM

図 10-53: Master unit (マスターユニット)

ロードマスターのトップバーに表示されるモードをチェックすれば、どのユニットがマスターでどのユニットがスレーブなのかが一目で分かります。

Partner Name/IP (パートナー名/IP)

HAパートナーユニットのホスト名またはIPアドレスを指定します。

Health Check Port (ヘルスチェックポート)

ヘルスチェックを実行するポートを設定します。HAを正しく機能させるには、マスターユニットとスレーブユニットで同じポートを指定する必要があります。

10.5.7 AWSのHAパラメーター

このメニューオプションは、ロードマスター for Amazon Web Services (AWS) でのみ利用できます。

AWS HA Mode	Master HA Mode	
Partner Name/IP	172.31.0.197	Set Partner Name/IP
Health Check Port	8444	Set Health Check Port

図 10-54: AWSのHAパラメーター

AWS HA Mode (AWSのHAモード)

このユニットで必要なHAモードを選択します。3つのオプションが用意されています。

- Master HA Mode (マスターHAモード)
- Slave HA Mode (スレーブHAモード)



- Non HA Mode (非HAモード)

ロードマスターを1台だけ使用する場合、“Non HA Mode”を選択してください。

HAモードを使用する場合、1台目のマシンを“Master”に設定し、2台目のマシンを“Slave”に設定します。

2台のユニットで同じ“AWS HA Mode”の値を選択した場合、HAは機能しません。

仮想サービスの設定の同期は、マスターからスレーブの方向でのみ行われます。マスターに対する変更はスレーブに複製されます。ただし、スレーブに対する変更はマスターには複製されません。

マスターユニットに障害が発生すると、接続はスレーブユニットに向けられます。障害が発生しても、マスターユニットはあくまでマスターであり、スレーブにはなりません。同様に、スレーブユニットはマスターにはなりません。マスターユニットが復旧すると、接続は自動的にマスターユニットに向けられます。



図 10-55: Master unit (マスターユニット)

ロードマスターのトップバーに表示されるモードをチェックすれば、どのユニットがマスターでどのユニットがスレーブなのかが一目で分かります。

Partner Name/IP (パートナー名/IP)

HAパートナーユニットのホスト名またはIPアドレスを指定します。

Health Check Port (ヘルスチェックポート)

ヘルスチェックを実行するポートを設定します。HAを正しく機能させるには、マスターユニットとスレーブユニットで同じポートを指定する必要があります。



10.5.8 SDNの設定

SDN Controllers		
ClusterID	ControllerID	Inuse
1	23	 True
Add New		

図10-56:SDN設定画面のセクション

新規追加

SDNコントローラー接続を新規に追加します。

Modify (変更)

既存のSDNコントローラー接続を変更します。

Delete (削除)

既存のSDNコントローラー接続を削除します。

10.5.8.1 SDNコントローラーの設定

SDN-Controller Settings

Cluster

1

IPv4

10.154.201.12

Set IPV4

Port

8443

Set Port

HTTPS

True

User

sdn

Set User

Password

Set Password

図 10-57:SDNコントローラーの設定

SDNコントローラーの接続を新たに追加する際、始めに、Cluster（クラスター）、IPv4 アドレス、Port（ポート）を尋ねる画面が表示されます。SDNコントローラーの接続を追加後、“SDN Statistics”画面の“Modify”をクリックすることで設定を更新できます。

Cluster（クラスター）



SDNコントローラーがメンバーとなるクラスターです。

“Cluster”フィールドはデフォルトのままにしてください。

IPv4

SDNコントローラーのIPv4アドレス。

Port (ポート)

SDNコントローラーWUIのポートです。

HP VANコントローラーのデフォルトのポートは8443です。

OpenDaylight SDNコントローラーのデフォルトのポートは8181です。

HTTPS

SDNコントローラーへのアクセスにHTTP/HTTPSを使用します。

User (ユーザー)

SDNコントローラーへのアクセスで使用するユーザー名です。

Password (パスワード)

SDNコントローラーへのアクセスで使用するパスワードです。



参考ドキュメント

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



[仮想サービスとテンプレート機能説明](#)

[RSAの2要素認証 機能説明](#)

[コンテンツルール機能説明](#)

[ロードマスター5.1から6.0への移行 テクニカルノート](#)

[ヘッダー変更ガイド テクニカルノート](#)

[GEO 製品概要](#)

[GEO Sticky DNS 機能説明](#)

[パケットトレースガイド テクニカルノート](#)

[VMwareツールのアドオンパッケージ 機能説明](#)

[カスタム認証フォーム テクニカルノート](#)

[ポートフォロウィング 機能説明](#)

[SSLアクセラレーションサービス 機能説明](#)

[アプリケーションファイアウォールパック \(AFP\) カスタムルール](#)

[Kerberos Constrained Delegation 機能説明](#)

[ハードウェアセキュリティモジュール \(HSM\) 機能説明](#)

[IPsecトンネリング 機能説明](#)

[KEMPロードマスター 製品概要](#)

[SDNアダプティブ負荷分散 機能説明](#)

[DoD共通アクセスカード \(CAC\) 認証 機能説明](#)

[RESTful API インターフェイス説明](#)

[ライセンス 機能説明](#)

[RADIUSの認証と権限設定 テクニカルノート](#)



ロードマスターのクラスタリング 機能説明

Microsoft Exchange 2010 展開ガイド

RADIUSの認証と権限設定 テクニカルノート

ユーザー管理 機能説明

Document History

Date	Change	Reason for Change	Ver.	Resp.
June 2015	Release updates	Updates for 7.1-28 release	1.34	LB
July 2015	Release updates	Updates for 7.1-28a release	3.0	LB
Aug 2015	Minor changes	Enhancements made	4.0	LB
Sep 2015	Release updates	Updates for 7.1-30 release	5.0	LB
Dec 2015	Minor changes	Enhancements made	6.0	LB
Jan 2016	Minor changes	Updated Copyright Notices	7.0	LB
Mar 2016	Minor changes	Enhancements made	8.0	LB
May 2016	Minor changes	Enhancements made	9.0	LB

