



RESTful API

インターフェイス

マニュアル

バージョン : 13.0
更新 : 2016年5月

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. The RESTful API Interfaceインターフェイス.....	11
2.1 RESTful APIとは.....	11
2.2 セキュリティ.....	12
2.3 RESTful APIインターフェイスの有効化.....	12
2.4 getおよびsetコマンドの使用.....	13
2.5 エラーレポート.....	13
2.6 表記.....	13
3. RESTful API コマンド.....	15
3.1 コマンドの構文.....	15
3.2 getallコマンド.....	15
3.3 Home画面の情報.....	15
3.3.1 ロードマスターのファームウェアバージョンの取得.....	15
3.3.2 シリアル番号の取得.....	15
3.3.3 仮想サービスと実サーバーの状態取得.....	16
3.3.4 ライセンス情報の取得.....	16
3.4 初期設定.....	16
3.4.1 EULAの読み込み.....	16
3.4.2 EULAの承諾とライセンスタイプの設定.....	17
3.4.3 ホーム呼び出し機能の使用の有無の指定.....	17
3.4.4 ロードマスターのライセンス設定.....	18
3.4.5 初期パスワードの設定.....	18
3.5 Virtual Services (仮想サービス).....	18



3.5.1	仮想サービス (VS) の制御.....	18
3.5.2	テンプレートを用いた仮想サービスの追加.....	47
3.5.3	Manage Templates (テンプレートの管理)	48
3.5.4	SSOの管理.....	48
3.5.5	WAFの設定.....	53
3.6	グローバル負荷分散.....	59
3.6.1	完全修飾ドメイン名 (FQDN) の管理.....	59
3.6.2	クラスタの管理.....	66
3.6.3	その他のパラメータ.....	68
3.6.4	IP範囲の選択条件.....	69
3.6.5	GE0の有効化/無効化.....	71
3.7	Statistics (統計情報)	72
3.8	SDN統計情報.....	76
3.9	実サーバー.....	83
3.9.1	実サーバーの有効化 / 無効化.....	86
3.10	ルールとチェック.....	86
3.10.1	ルールの表示.....	86
3.10.2	ルールのシステムよりの削除.....	87
3.10.3	ルールは、delrule コマンドにより削除できます。.....	87
3.10.4	実サーバーへのルールの追加/削除.....	89
3.10.5	サブVSのルールの追加/削除.....	89
3.10.6	仮想サービスのルールの追加.....	90
3.10.7	仮想サービスのルールの削除.....	91
3.10.8	Check Parameters (チェック用パラメータ)	91
3.11	証明書とセキュリティ.....	92
3.11.1	証明書の管理.....	92
3.11.2	暗号セット.....	94



3.11.3	Remote Access (リモートアクセス)	96
3.11.4	管理用WUIへのアクセス	97
3.11.5	OCSPの設定	100
3.11.6	ハードウェアセキュリティモジュール (HSM) の設定	100
3.12	Interfaces (インターフェイス)	102
3.12.1	インターフェイス詳細の取得	102
3.12.2	インターフェイス詳細の変更	102
3.12.3	追加アドレス	103
3.12.4	ボンディングインターフェイス	104
3.12.5	VLANs	104
3.12.6	VXLANs	104
3.13	ホストとDNSの設定	105
3.13.1	ローカル名前解決ホスト	105
3.14	Route Management (ルート管理)	106
3.14.1	デフォルト・ゲートウェイ	106
3.14.2	追加ルート	106
3.14.3	Packet Routing Filter (パケット・ルーティング・フィルター)	106
3.14.4	VPN管理	107
3.15	Access Lists (アクセスリスト)	110
3.16	Cluster Control (クラスターの制御)	112
3.16.1	クラスタリングに関するAPI コマンド	112
3.16.2	RESTful APIを用いたクラスタリングの例	114
3.17	System Administration (システム管理)	115
3.17.1	ユーザの管理	115
3.17.2	ライセンス設定	118
3.17.3	System Reboot (システムリブート)	121
3.17.4	Update Software (ファームウェア更新)	122



3.17.5	バックアップ/復元.....	123
3.17.6	Date/Time (日付/時間)	124
3.18	Logging Options (ログオプション)	125
3.18.1	システムログの管理.....	125
3.18.2	Ping Host (pingホスト)	125
3.18.3	tracerouteの実行.....	125
3.18.4	Debug Options (デバッグオプション)	126
3.18.5	Extended Log Files (拡張ログファイル)	127
3.18.6	Syslog Options (シスログ・オプション)	128
3.18.7	SNMPオプション.....	129
3.18.8	Email Options (E-Mail オプション)	130
3.18.9	SDN Log Files (SDNログファイル)	131
3.19	その他のオプション.....	131
3.19.1	WUI Settings (WUIの設定)	131
3.19.2	WUIの認証および承認オプション.....	132
3.19.3	レイヤ7設定.....	134
3.19.4	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 137	
3.19.5	アプリケーションフロントエンド (AFE) の設定.....	139
3.19.6	HA管理.....	141
3.19.7	AzureのHAパラメータ.....	144
3.19.8	AWSのHAパラメーター.....	144
3.19.9	SDNの設定.....	145
3.20	RESTful APIによるHAの設定.....	149
3.20.1	RESTful APIを使用して通常のロードマスターにHAを設定する.....	149
3.20.2	RESTful APIを使用してロードマスターfor AzureにHAを設定する.....	150
4.	ロードマスターRESTful APIのスク립ト例文.....	152
5.	付録A - パラメータの取得と設定.....	153



6. 参考ドキュメント.....	158
Document History.....	159

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, SP



ECIAL, 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.

(参考訳)

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。

ソースファイルへのリンクは、KEMP米国ウェブサイトのProduct MatrixページとSupportページを参照ください。

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



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.

(参考訳)

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

このソフトウェアの一部（1995年発行 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。
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。



1. はじめに

KEMPテクノロジーは、アプリケーション提供と負荷分散に関して、価格/性能比に優れた製品群をお求めやすい価格でお客様にご提供しています。当社の製品はさまざまな用途に対応できる高性能なアーキテクチャを採用しており、最高の価値をもたらすとともに、インターネットベースのインフラストラクチャに依存するビジネスを最適化して、当社のお客様が顧客、従業員、およびパートナーと連携してビジネスを行えるようになります。

KEMPテクノロジーの製品は、高可用性（HA）、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るように、Webおよびアプリケーションのインフラストラクチャを最適化します。また、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ロードマスターへのRESTful APIインターフェイスについて説明します。本ドキュメントでは、RESTful API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。

本ドキュメントでは、個々の機能やオプションについては詳しく説明していません。詳細については、www.kemptechnologies.com/documentationにある機能説明のドキュメントを参照してください。

1.2 対象読者

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



2. The RESTful API Interfaceインターフェイス

このドキュメントは、ロードマスターへのリモートアクセスを容易に行う為にデザインされたインターフェイスであるRESTful APIに関して記述しています。このインターフェイスは、REST (Representational State Transfer) に類似したものです。REST (Representational State Transfer) は、分散システム用ソフトウェア・アーキテクチャの1つのスタイルで、卓越したウェブサービスのデザインモデルの一つです。

2.1 RESTful APIとは

ロードマスターのRESTful APIは、ユーザもしくはアプリケーションがHTTPSリクエストをロードマスターに送るのを許可させるインターフェイスです。ロードマスターは、そのHTTPSリクエストに対してXMLフォーマットのレスポンスを返します。HTTPSリクエストは、下記のようなフォーマットとなります。

`https://<LoadMaster IP Address>/access/<command>?<parameter1>=value&<parameter2>=value`

基本的なインターフェイスは、URLによって指定されるコマンドをHTTPS GETにて送信します。もし、パラメータが必要なものは、クエリ用パラメータとして渡します。

下記は、このHTTPSリクエストのフォーマットについての注意点です。

- 一回に一つのコマンドのみ送信できます。
- ‘?’ キャラクターは、コマンドの最後を意味します。
- ‘&’ キャラクターは、パラメータ/バリューのペアの最後を意味します。
- もし不必要なパラメータ/バリューのペアを含んでいる場合は、それらは無視されます。
- コマンドに続くパラメータ/バリューのペアの順序はありません。
- クエリ内にスペースはありません。ただし、ブラウザなどのアプリケーションでは、文字列をLoadMasterに送信する前にスペースがHTMLコードに変換されます。
- 複数のパラメータは、同じコマンド内であれば変更可能です。

例えば、下記のクエリはIPアドレス10.11.0.20のロードマスターより最大キャッシュメモリーサイズを求めるものです。

`https://10.11.0.20/access/get?param=cachesize`

このクエリに対するロードマスターからのレスポンスは、下記のように容易にデコードできるXMLフォーマットです。



```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="200" code="ok">
  <Success>
    <Data>
      <cachesize>
        100
      </cachesize>
    </Data>
  </Success>
</Response>
```

本ドキュメントに記載されているすべてのコマンドがすべてのロードマスターで使用できるわけではありません。コマンドによっては、ロードマスターの一部のライセンスでのみ使用可能なものもあります。

2.2セキュリティ

アプリケーションは、一般的なWUI用IPアドレスを介してロードマスターにアクセス可能です。セキュリティとして、HTTPSを介してWUIへアクセスする時と同じ有効なユーザー資格をアクセスする毎にHTTPベーシック認証を使用して渡す必要があります。

ユーザー名“bal”は、すべての機能へのアクセスが可能です。他のユーザーは、そのユーザーに与えられているサブシステムにのみへのアクセスだけが認められます。

現状では、このインターフェイスによるユーザーの権限変更はできません。

セキュリティの設定にもよりますが、WUIへのログインが既になされていない場合は、ログイン情報を追加しなければなりません。通常の既にログインがなされている場合のコマンドフォーマットは下記ですが、

`https://<LoadMaster IP address>/access/<command>?params`

もし、ユーザー情報を含ませなければならない場合は下記のフォーマットになります。

エラー! ハイパーリンクの参照に誤りがあります。Name>:<UserPassword>@<LoadMaster IP address>/access/<command>?params

2.3RESTful APIインターフェイスの有効化

RESTful APIインターフェイスは、ロードマスターのWUIから有効化/無効化を行います。デフォルトでは、このインターフェイスは無効になっています。

RESTful APIインターフェイスを使用できるようにするには、下記の手順で行います。



1. WUIのメニューよりSystem Configuration > Miscellaneous Options > Remote Access オプションに移動します。
2. “Enable API Interface” チェックボックスをオンにします。

2.4 getおよびsetコマンドの使用

ロードマスターのパラメータの多くは、setおよびgetコマンドを使用して管理できます。各パラメータについては、このドキュメント全体を通して説明します。パラメーターのリストは付録A - パラメータの取得と設定にも記載されています。

パラメータの値は、以下のようなフォーマットのgetコマンドで取得できます。

```
https://<LoadMaster IP Address>/access/get?param=<ParameterName>
```

パラメータの値は、以下のようなフォーマットのsetコマンドで設定できます。

```
https://<LoadMaster IP Address>/access/set?param=<ParameterName>&value=<ParameterValue>
```

2.5 エラーレポート

必要なパラメータが不足していたり、バリューが正しくない場合は、システムが下記のようなエラーレポートを返します。

```
-----
<?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="400" code="fail">
  <Error>
    param:String Value missing
  </Error>
</Response>
-----
```

リクエストのHTTPステータスや、レスポンスコードがこのレポート内に反映されます。

2.6 表記

このドキュメント全体を通して、パラメータのタイプは以下のように定義されます。

種類	省略形	標準値
Boolean	B	YまたはN、yまたはn、1または0
整数	I	<最小値>-<最大値>



種類	省略形	標準値
String	S	“値”
アドレス	A	IPアドレス
ファイル	F	同じ種類のファイル

表2-1:Parameter Notation

3. RESTful API コマンド

3.1 コマンドの構文

リクエストは、コマンドとパラメータの2つの部分より成り立っています。

```
https://<LoadMaster IP address>/access/<command>?params
```

リクエスト内に複数のパラメータがある場合は、各パラメータをアンパサンド記号 (&) で区切ります。

すべてのコマンドは、矛盾があってはなりません。例えば、仮想サービス (VS) 関連のすべてのコマンドにおいては、下記のようにVSは '**vs=<ipaddr>**' のフォーマットでVIPアドレスを指定する必要があります。

```
https://<LoadMaster IPAddress>/access/showvs?vs=10.0.0.10&port=80&prot=tcp
```

VS上の特定RSを指定する場合は、下記のように '**rs=<ipaddress>**' のフォーマットになります。

```
https://<LoadMaster IPAddress>/access/showrs?vs=10.0.0.10&port=80&prot=tcp&rs=99.1.1.1&rsport=80
```

3.2 getall コマンド

getall コマンドは、利用可能な (かつnullでない) すべてのパラメータのリストを返します。

```
https://<LoadMaster IPAddress>/access/getall
```

3.3 Home画面の情報

ロードマスターWUIで利用可能な一部の情報は、APIでも利用できます。詳細は以下のサブセクションを参照してください。

3.3.1 ロードマスターのファームウェアバージョンの取得

ロードマスターのファームウェアのバージョンは、get コマンドと version パラメータを使用して取得できます。

```
https://<LoadMaster IPAddress>/access/get?param=version
```

3.3.2 シリアル番号の取得

ロードマスターのシリアル番号を取得するには、serialnumber パラメータの get コマンドを実行します。



`https://<LoadMaster IP Address>/access/get?param=serialnumber`

3.3.3 仮想サービスと実サーバーの状態取得

稼働中、停止中、および管理者により無効にされている仮想サービス、サブVS、実サーバーのトータルの数を取得するには、`vstotals`コマンドを実行します。

`https://<LoadMaster IP Address>/access/vstotals`

3.3.4 ライセンス情報の取得

ロードマスターのライセンスに関する詳細を取得するには、`licenseinfo`コマンドを実行します。

`https://<LoadMaster IP Address>/access/licenseinfo`

3.4 初期設定

初期設定のAPIコマンドは、ロードマスター for Amazon Web Services (AWS) では現在利用できません。

ロードマスターを初めて展開する場合、エンドユーザーライセンス契約 (EULA) の承諾やユニットのライセンス設定など、さまざまな手順が必要です。ロードマスターを完全に利用可能な状態にするには、EULAを表示して承諾する必要があります。初期設定手順は、WUIまたはAPIのいずれからでも行えます。初期設定関連のAPIコマンドは、以下のセクションで示します。

このコマンドは順番に実行する必要があります。

3.4.1 EULAの読み込み

`ReadEula`コマンドは、EULAとマジッククッキーを表示します。

マジッククッキーは、セキュリティ上の理由から使用されます。これは、リモート攻撃の可能性を抑えます。(以下のセクションの他のコマンドのように) コマンドがマジッククッキーを必要とし、その前のコマンドから正しいマジッククッキーを取得できない場合、そのコマンドは正しく実行されません。

`https://<LoadMaster IP Address>/access/readeula`



マジックストリングは、自動的に生成されたランダムな文字列です（例：c0a6fccc-1c53-4a26-8ed3-e0d0bb8e23f3）。次のコマンドでライセンスタイプを設定するのに必要となるため、この文字列をコピーしておいてください。

3.4.2 EULAの承諾とライセンスタイプの設定

現在、3つのライセンスタイプが用意されています。以下の3つです。

- 試用版（制限なし）
- 永久
- 無償（制限付き）

AcceptEULAコマンドは、EULAを承諾して使用するライセンスの種類（試用、永久、無償など）を設定するため、readEulaコマンドにより返されたマジッククッキーキーを入力するのに使用します。

<https://<LoadMaster IPAddress>/access/accepteula?magic=<CorrectMagicString>&type=free>

値	WUIにおける名前	説明
Trial	試用版（制限なし）	KEMPロードマスターを評価するための一時ライセンス
Perm	永久	購入して恒久的に使用するロードマスター
Free	無償（制限付き）	無償のロードマスター

表3-1: ライセンスタイプのパラメーターで有効な値

ライセンスタイプはマルチテナントロードマスターから継承されるため、マルチテナントロードマスターで作成された仮想ロードマスター（VLM）上でこのコマンドを実行した場合、ここで設定したライセンスタイプは意味を持ちません。ただし、次のコマンド（AcceptEula2）を実行するのに必要な別のマジックストリングを取得する場合は、このコマンドを実行する必要があります。

3.4.3 ホーム呼び出し機能の使用の有無の指定

AcceptEULA2コマンドは、ホーム呼び出し機能の使用の有無を指定するのに使用します。

<https://<LoadMaster IPAddress>/access/accepteula2?magic=<CorrectMagicString>&accept=<yes/no>>



3.4.4 ロードマスターのライセンス設定

ロードマスターにライセンスを設定するには、`license`コマンドまたは`alsilicense`コマンドを使用します。詳細はセクション3.17.1.8を参照してください。

3.4.5 初期パスワードの設定

`SetInitialPasswd`コマンドは、ロードマスターのデフォルトユーザー（`bal`）のパスワードを設定するのに使用します。

`https://<loadMasterIPAddress>/access/set_initial_passwd?passwd=<password1>`

パラメーター	パラメーターの種類	説明	必須
Passwd	String	これは、デフォルトの管理者ユーザー（ <code>bal</code> ）のパスワードです。パスワードには8文字以上の英数字が含まれていなければなりません。	Yes

表3-2: SetInitialPasswdのパラメーター

3.5 Virtual Services (仮想サービス)

3.5.1 仮想サービス (VS) の制御

仮想サービスコマンドの基本形式を以下に示します。仮想サービスは、IPアドレスとインデックス (ID) のいずれでも指定できます。インデックスとは、仮想サービスを内部で追跡するための値です。

Properties for tcp/10.154.11.71:80 (Id:1) - Operating at Layer 7

図 3-1: 仮想サービスID

インデックスを表示するには、`showvs`コマンドまたは`listvs`コマンドを使用するか、WUIの仮想サービスプロパティ画面（ここに仮想サービスIDが表示されます）をチェックします。

`https://<LoadMasterIPAddress>/access/listvs`

`https://<LoadMasterIPAddress>/access/showvs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>`

`https://<LoadMasterIPAddress>/access/showvs?vs=<index>`

`https://<LoadMasterIPAddress>/access/addvs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp> [&...]`

`https://<LoadMasterIPAddress>/access/delvs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>`



```
https://<LoadMaster IPAddress>/access/delvs?vs=<index>
```

```
https://<LoadMaster IPAddress>/access/modvs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>
[&...]
```

```
https://<LoadMaster IPAddress>/access/modvs?vs=<index>[&...]
```

‘delvs’ コマンドによるVSの削除が成功した場合は、OKのステータスを返しますが、それ以外はVSの現設定情報を返します。

addvsコマンドとmodvsコマンドは、いずれも仮想サービスのすべての設定を変更できます。addvsコマンドは、はじめに仮想サービスを作成します。一方、modvsコマンドは既存の仮想サービスを編集します。

listvsコマンドは、ロードマスターにあるすべての仮想サービスの一覧を表示します。

(新しい仮想サービスが作成される場合、udpプロトコルでの指定以外はL7のトランスペアレンシーモードのデフォルトの設定が適用されます。)

仮想サービスのステータスが返される時に、付属する実サーバー (RS) 情報も返されません。

コマンドによっては、他のコマンドの実行が必須条件となっているものがあります。その条件が満たされない場合、指定したコマンドを実行しても何も起こりません。

すべてのパラメータがすべての設定に使用できるとは限りません。パラメータが使用できるかどうかは、設定する環境により変化します。

Sub-Virtual Services (SubVSs)

仮想サービスのコマンドはSubVSでも使用できます。ただし、SubVSはIPアドレスを持っていないため、SubVSのインデックスを使用する必要があります。SubVSのインデックスを調べるにはlistvsコマンドを使用します。

```
Properties for subVS 1 (Id:2) of tcp/10.154.11.71:80 - Operating at Layer 7
```

図 3-2:サブVS ID

または、サブVSの“modify” (編集) をクリックし、WUIのサブIDプロパティ画面をチェックします。上記の例ではサブIDは2になっています。



特定のSubVSに関する詳細を表示するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/showvs?vs=<SubVS index>
```

次のいずれかのコマンドを実行することで、SubVSを新規に追加できます。

```
https://<LoadMaster IP Address>/access/modvs?vs=<VS IP>&port=<Port>&prot=<tcp/udp>&create subvs=
```

```
https://<LoadMaster IP Address>/access/modvs?vs=<index>&createsubvs=
```

次のコマンドを実行することで、仮想サービスからSubVSを削除できます。

```
https://<LoadMaster IP Address>/access/delvs?vs=<VS index>
```

次のコマンドを実行することで、SubVSから実サーバーを削除できます。

```
https://<LoadMaster IP Address>/access/delrs?vs=<SubVS index>&rs=%21<RS index>
```

SubVSの設定を変更するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/modvs?vs=<SubVS index> [&...]
```

SubVSのインデックスは整数値です。

以下のセクションで、**addvs**コマンドおよび**modvs**コマンドで設定可能なパラメーターについて説明します。使いやすさを考えて、パラメーターに対応するフィールドがWUIのどこに表示されるかに基づきパラメーターを分割してあります。

3.5.1.1 プロパティ

名前	種類	デフォルト	範囲	説明
VSPort	I	<未設定>	3-65530	仮想サービスのポート
Protocol	S	<未設定>	udp, tcp	仮想サービスで使用するプロトコル
VSAAddress	A	アドレス		仮想サービスのIPアドレス
MasterVS	I (読み取り専用)	<未設定>	0 - 親仮想サービスではない 1 - 親仮想サービスである	仮想サービスが親仮想サービスであるかどうか (1つ以上のSubVSを持つかどうか) を表します。

表3-3: APIパラメーターのプロパティ

3.5.1.2 Basic Properties

名前	種類	デフォルト	範囲	説明
Enable	B	Y		仮想サービスのアクティブ化または非アクティブ化



名前	種類	デフォルト	範囲	説明
VStype	S	<ポートに依存>	gen - 汎用 http - HTTP/HTTPS http2 - HTTP/2 ts - リモートターミナル tls - STARTTLSプロトコル log - Log Insight	負荷分散を行うサービスの種類を指定します。
NickName	S	<未設定>		サービスのニックネームを指定します。 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。

表3-4:APIパラメーターの基本プロパティ

3.5.1.3 Standard Options (標準的なオプション)

名前	種類	デフォルト	範囲	説明
Cookie	S	<未設定>		このパラメーターは、パーシステンスモードがcookie、active-cookie、cookie-src、active-cook-srcに設定されている場合のみ必要です。チェックするクッキーの名前を入力してください。
ForceL7	B	Y (if not UDP)	0 = 無効 1 = 有効	ForceL7を有効にすると、レイヤ4ではなくレイヤ7で仮想サービスが実行されます。さまざまな理由でこの設定が必要になります（レイヤ7のサービスのみ非透過にできる場合など）。
IdleTime	I	0	0-86400	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。このパラメーターの範囲は0~86400です。0は無制限を意味します。



名前	種類	デフォルト	範囲	説明
Persist	S	none (なし)	関連するパーシステンス値は以下のとおりです。 ssl cookie (クッキー) active-cookie cookie-src active-cook-src cookie-hash cookie-hash-src url query-hash host (ホスト) header (ヘッダー) super (スーパー) super-src src rdp rdp-src rdp-sb rdp-sb-src	この仮想サービスで使用するパーシステンス (スティッキネス) の種類を指定します。
SubnetOriginating	B	0	0 - 無効 1 - 有効	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。
PersistTimeout	I	0	0-86400	最後に接続してからロードマスターがパーシステンス情報を保持する時間 (単位: 秒)
QueryTag	S	<未設定>		これは、Persist typeがquery-hashに設定されているときに照合されるクエリタグです。



名前	種類	デフォルト	範囲	説明
Schedule	S	rr	rr wrr lc wlc fixed (固定) daptive (アダプティブ) sh dl sdn-adaptive	<p>実サーバーに新規接続を行うスケジューリングの種類を指定します。この値は以下のように記述します。</p> <p>rr = round robin (ラウンドロビン)</p> <p>wrr = weighted round robin (加重ラウンドロビン)</p> <p>lc = least connection (最小接続)</p> <p>wlc = weighted least connection (加重最小接続)</p> <p>fixed = 固定加重</p> <p>daptive = (リソースベース (適応))</p> <p>sh = source IP hash (ソースIPハッシュ)</p> <p>dl = 重み付け応答時間</p> <p>sdn-adaptive = リソースベース (SDNアダプティブ)</p>



名前	種類	デフォルト	範囲	説明
ServerInit	I	0	0-6	<p>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。</p> <p>仮想サービスが以下のいずれかのプロトコルを使用する場合は、ServerInitパラメーターを使用してプロトコルを指定し、そのプロトコルが正しく機能するようにします。</p> <p>0 = 通常プロトコル 1 = SMTP 2 = SSH 3 = その他のサーバー初期化 4 = IMAP4 5 = MySQL 6 = POP3</p>
Transparent	B	Y	0 - 無効 1 = 有効	<p>レイヤー7を使用している場合、このオプションを有効にすると、実サーバーに到達する接続がクライアントから直接来ているように見えます。または、接続を非透過にすることも可能で、その場合、実サーバーへの接続はロードマスターから来ているように見えます。</p>



名前	種類	デフォルト	範囲	説明
UseforSnat	B	N	0 - 無効 1 - 有効	<p>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。</p> <p>このオプションを有効にすると、仮想サービスを使用するよう設定された実サーバーがソースIPアドレスとして使用されます。</p> <p>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を構成した場合、宛先ポート80への接続のみ、この仮想サービスをソースIPアドレスとして使用します。</p>
QoS	S	0 - 通常のサービス	0 - 通常のサービス 1 - コストを最小にする 2 - 信頼性を最大にする 4 - スループットを最大にする 8 - 遅延を最小にする	<p>Quality of Service (QoS) パラメーターは、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。</p> <p>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。</p>
StartTLSMode	I		0-6	<p>0 = HTTP/HTTPS (この機能を動作させるには、Service TypeをHTTP/HTTPSに設定する必要があります)</p> <p>残りの値を設定するには、Virtual Service TypeをSTARTTLSに設定する必要があります。</p> <p>1 = SMTP (必要な場合STARTTLS) 2 = SMTP (常にSTARTTLS) 3 = SSH 4 = SSH 6 = POP3</p>



名前	種類	デフォルト	範囲	説明
ExtraPorts	S	<未設定>	3-65530	仮想サービスがリッスンする追加ポートを指定します。既存の追加ポートを削除するには、ExtraPortsパラメーターに空の文字列を設定します。

表3-5:APIパラメーターの標準オプション

パーシステンス方式をcookie、active-cookie、cookie-src、active-cook-srcに設定した場合、コマンドでクッキー名も指定する必要があります。

例：

エラー! ハイパーリンクの参照に誤りがあります。LoadMasterIPAddress>/access/modvs?vs=10.0.2.194&port=80&prot=tcp&persist=cookie&cookie=<cookie name>&

3.5.1.4 SSL Properties (SSLのプロパティ) 画面

名前	種類	デフォルト	範囲	説明
CertFile	S	<未設定>		インストールされている証明書のID。



名前	種類	デフォルト	範囲	説明
Ciphers	S	Default assignment	All supported ciphers	<p>コロンで区切るにより、複数の暗号化方式を割り当てることができます。この方法で暗号化方式を割り当てた場合、Custom_<Virtual/ServiceID>と呼ばれる暗号セットが作成/更新されます。</p> <p>注:この方法で暗号化方式を追加した場合、暗号化方式の割り当てリストが上書きされます。割り当てる暗号化方式がすべて含まれていることを確認してください。</p> <p>デフォルトで割り当てられている暗号化方式のリスト、およびサポートされている暗号化のリストについては、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。</p> <p>注:CipherSetとCiphersを同時に設定しないでください（いずれか1つを使用してください）。別のコマンドを使用して、カスタム暗号セットを作成できます。詳細はセクション3.11.2.1を参照してください。</p>



名前	種類	デフォルト	範囲	説明
CipherSet	S	デフォルト	利用可能な暗号セット	<p>このパラメーターを使用すると、仮想サービスに暗号セットを割り当てることができます。このパラメーターを使用して、システム定義の暗号セットとカスタム暗号セットを割り当てることができます。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> - デフォルト - Default_NoRc4 - BestPractices - Intermediate_compatibility - Backward_compatibility <ul style="list-style-type: none"> - WUI - FIPS - Legacy - <i><NameOfCustomCipherSet></i> <p>注: CipherSetとCiphersを同時に設定しないでください（いずれか1つを使用してください）。別のコマンドを使用して、カスタム暗号セットを作成できます。詳細はセクション3.11.2.1を参照してください。</p>
ClientCert	I	0	0-6	<p>0 = クライアント証明書が不要 1 = クライアント証明書が必要 2 = クライアント証明書と、ヘッダの追加 3 = クライアント証明書と、SSL-CLIENT-CERTとしてのDERの受け渡し 4 = クライアント証明書と、X-CLIENT-CERTとしてのDERの受け渡し 5 = クライアント証明書と、SSL-CLIENT-CERTとしてのDERの受け渡し 6 = クライアント証明書と、X-CLIENT-CERTとしてのPEMの受け渡し</p>



名前	種類	デフォルト	範囲	説明
SSLReencrypt	B	N	0 = 無効 1 = 有効	このパラメーターは、SSLアクセラレーションが有効のときのみ関係します。 このオプションを有効にすると、実サーバーに送信される前にSSLのデータストリームが再暗号化されます。
SSLReverse	B	N	0 = 無効 1 = 有効	このパラメーターを有効にすると、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。
SSLRewrite	S	<未設定>	<未設定>、http、https	HTTPリダイレクトを含むリクエストが実サーバーにより拒否される場合、HTTPではなくHTTPSを指定するように、リクエスト先のロケーションURLを変換する必要があります（この逆も同様）
ReverseSNIHostname	S	<未設定>		このオプションを有効にすると、TLSクライアントのHelloメッセージにてホスト名を送信する必要があります。送信しない場合、接続がドロップされます。
SSLAcceleration	B	N	0 = 無効 1 = 有効	この仮想サービスでSSLの処理を有効にします。
OCSPVerify	B	0 - 無効	0 - 無効 1 - 有効	（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。
TLSType	B	SSLアクセラレーションが有効でないときは無効になります。 SSLアクセラレーションが有効なときは有効になります。	0 = 無効 1 = 有効	このオプションを選択すると、SSL v3のサポートが無効になり、TLS1.xプロトコルのみサポートされます。

表3-6: APIパラメーターのSSLプロパティ

3.5.1.5 Advanced Properties (高度なプロパティ)

名前	種類	デフォルト	範囲	説明
----	----	-------	----	----



名前	種類	デフォルト	範囲	説明
AddVia	I		0 = Legacy Operation 1 = X-フォワーディングされる 2 = なし 3 = X-クライアントサイド 4 = X-クライアントサイド (Viaなし) 5 = X-Forwarded-For (No Via) 6 = Via Only	これは、WUIの Add HTTP Headers フィールドに対応します。HTTP リクエストに追加されるヘッダを選択します。X-ClientSide およびX-Forwarded-Forが追加されるのは、非トランスペアレンシー接続に限定されます。
Cache	B	N	0 = キャッシング無効 1 = キャッシング有効	URLのキャッシングを有効または無効にします。
Compress	B	N	0 = 無効 1 = 有効	このオプションを有効にすると、ロードマスターから送信されるファイルがGzipで圧縮されます。
CachePercent	I	0	0-100	このパラメータは、キャッシングが有効のときのみ関係します。この仮想サービスで許容されるキャッシュ空間の最大使用率を指定してください。
DefaultGW	A	<未設定>		クライアントに応答を返すために使用する、仮想サービス固有のデフォルトゲートウェイを指定します。このパラメータを設定しない場合、グローバルのデフォルトゲートウェイが使用されます。
ErrorCode	I	0	200-505	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。このパラメータでエラーコード番号を指定してください。エラーコードの設定を解除するには、パラメータに空の文字列を設定します。



名前	種類	デフォルト	範囲	説明
ErrorUrl	S	<未設定>		実サーバーが利用可能で、クライアントにエラー応答が返された場合、リダイレクトURLを指定できます。
PortFollow	I	<未設定>	0 and 3-65530	このパラメーターは、バージョン7.1-24において存在価値が低下しました。バージョン7.1-24以降のロードマスターでは、FollowVSIDパラメーターを使用してポートフォロウィングを設定してください。 フォローする仮想サービスのIDを指定します。この値を0に設定すると、ポートフォロウィングが無効になります。1と2は無効な値であるため、フォローする仮想サービスが3~65530の値を持っていることを確認してください。
FollowVSID	I	<未設定>		フォローする仮想サービスのIDを指定します。
LocalBindAddr	A	<未設定>	スペースで区切られたIPアドレスのリストです。	これはWUIの“Advanced Properties”（高度なプロパティ）セクションにある“Alternate Source Address”（代替ソースアドレス）に対応します。この機能を動作させるには、Allow connections scaling over 64K ConnectionsをL7 Configurationで有効にする必要があります。
NRequestRules	I（読み取り専用）	<未設定>		HTTPヘッダ変更リクエストルールの数を表示します。
NResponseRules	I（読み取り専用）	<未設定>		HTTPヘッダ変更レスポンスルールの数を表示します。
RequestRules	リスト（読み取り専用）			仮想サービスに割り当てるリクエストルールのリスト
ResponseRules	リスト（読み取り専用）			仮想サービスに割り当てる応答ルールのリスト



名前	種類	デフォルト	範囲	説明
StandbyAddr	A	<未設定>		他の実サーバーが利用できないときに使用される“Sorry”サーバーのIPアドレスを指定します。このサーバーに対してはヘルスチェックは行われません。このサーバーは常に利用可能とみなされます。
StandbyPort	I	<未設定>		“Sorry”サーバーのポートを指定します。
Verify	I	0	0~7 (ビットマスク)	Verifyパラメーターの詳細については、 セクション3.5.2 を参照
AltAddress	A	<未設定>	IPアドレス	この仮想サービスの代替アドレスを指定します。
AddVia	I		0-6	HTTP リクエストに追加されるヘッダを指定します。X-ClientSide およびX-Forwarded-Forが追加されるのは、非トランスペアレンシー接続に限定されます。 0 = 従来の操作 (X-Forwarded-For) 1 = X-Forwarded-For (+ Via) 2 = なし 3 = X-ClientSide (+ Via) 4 = X-ClientSide (Viaなし) 5 = X-Forwarded-For (No Via) 6 = Via Only
PreProcPrecedence	S	<未設定>		このパラメーターは、PreProcPrecedencePosと組み合わせて使う必要があります。このパラメーターは、そのポジションを変更したい既存のルールの名前を指定するのに使用します。 このパラメーターは、Content Matching Rules (コンテンツ照合規則) にのみ関係します。



名前	種類	デフォルト	範囲	説明
PreProcPrecedencePos	Int16	<未設定>		<p>このパラメーターは、パラメーター PreProcPrecedence とともに使用し、一連のルールにおいてそのルールのポジションを変更するのに使用します。例えば、ポジション2はルールが2番目にチェックされることを意味します。</p> <p>このパラメーターは、Content Matching Rules (コンテンツ照合規則) にのみ関係します。</p>
RequestPrecedence	String	<未設定>		<p>このパラメーターは、RequestPrecedencePos と組み合わせて使う必要があります。このパラメーターは、そのポジションを変更したい既存のリクエストの名前を指定するのに使用します。</p> <p>このパラメーターは、以下の種類のルールに関係します。</p> <p>Content Matching (コンテンツマッチング)</p> <p>Add Header (ヘッダーの追加)</p> <p>Delete Header (ヘッダーの削除)</p> <p>Replace Header (ヘッダーの置換)</p> <p>Modify URL (URLの変更)</p>
RequestPrecedencePos	Int16	<未設定>		<p>このパラメーターは、パラメーター RequestPrecedence とともに使用し、一連のルールにおいてそのルールのポジションを変更するのに使用します。例えば、ポジション2はルールが2番目にチェックされることを意味します。</p>



名前	種類	デフォルト	範囲	説明
ResponsePrecedence	String	<未設定>		<p>このパラメーターは、ResponsePrecedencePosと組み合わせて使う必要があります。このパラメーターは、そのポジションを変更したい既存の応答の名前を指定するのに使用します。</p> <p>このパラメーターは、以下の種類のルールに関係します。</p> <p>Content Matching (コンテンツマッチング)</p> <p>Add Header (ヘッダーの追加)</p> <p>Delete Header (ヘッダーの削除)</p> <p>Replace Header (ヘッダーの置換)</p>
ResponsePrecedencePos	Int16	<未設定>		<p>このパラメーターは、パラメーターResponsePrecedenceとともに使用し、一連のルールにおいてそのルールのポジションを変更するのに使用します。例えば、ポジション2はルールが2番目にチェックされることを意味します。</p>

表3-7: APIパラメーターの高度なプロパティ

3.5.1.5.1 パラメーターの検証

Verifyはビットマスクです。Verifyパラメータの有効な値は以下のとおりです。

- ビット0: 侵入検知を有効にするにはこのビットを1にします。

他の2つのビットを使用するにはビット0を1に設定する必要があります。

- ビット1は、接続をリジェクトするかドロップするかを決定します。1にセットすると接続がドロップされます。
- ビット2は、不正な要求や悪意ある（ただし無効ではない）要求に対して単に警告を与えるだけにするかどうかを決定します。



以下の表に、有効な整数値、およびそれらが使用されたときにフィールドに設定される値を示します。

整数	Detect Malicious Requests (IDS機能の追加)	侵入時の処理	警告チェックボックス
0	無効	N/A	N/A
1	有効	接続のドロップ	チェックオフ
2	有効	拒否を送信	チェックオフ
3	有効	拒否を送信	チェックオフ
4	有効	接続のドロップ	チェックオン
5	有効	接続のドロップ	チェックオン
6	有効	拒否を送信	チェックオン
7	有効	拒否を送信	チェックオン

表3-8: パラメーター整数値の検証

3.5.1.6 WAFの設定

名前	種類	デフォルト	範囲	説明
Intercept	B	0	0 - 無効 1 - 有効	この仮想サービスのWebアプリケーションファイアウォール (WAF) を有効/無効にします。
InterceptOpts	S	<未設定>		このパラメーターを使用すると、ロードマスターの仮想サービス変更画面の“WAF Options” (WAFのオプション) セクションにあるほとんどのフィールドを設定できます。詳細はセクション3.5.1.6.1を参照してください。
AlertThreshold	I	0 = 無効	0 - 100000	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。

表3-9: APIパラメーターのWAF設定



3.5.1.6.1 AFPのInterceptOptsパラメーター

AFPのInterceptOptsは特殊なパラメーターです。このパラメーターを使用すると、他の多くのパラメーターのように1つのフィールドではなく、複数のフィールドに値を設定できます。InterceptOptsパラメーターを使用すると、ロードマスターの仮想サービス変更画面のWAF Optionsセクションにあるほとんどのフィールドを指定できます。

WAFを有効にするには、Interceptパラメーターを1に設定します。

InterceptOptsパラメーターに関連するWUIフィールドの名前を以下の表に示します。

1つのコマンドで1つ以上のフィールド値を設定できます。値をセミコロンで区切ることで、1つのコマンドで複数の値を設定できます。例:

```
https://<LoadMaster IPAddress>/access/modvs?vs=<VirtualServiceIPAddress>&port=<Port>&prot=<tcp/udp>&InterceptOpts=opnormal;auditnone;reqdataenable;resdataenable;jsondisable;xmldisable
```

以下の表に、各値が何を意味するかの概要を示します。

同じWUIオプションに関する値は同時には設定できません。例えば、Basic Operationにopnormalとopblockの両方を設定することはできません。表: InterceptOptsのパラメーター値

値	関連するWUIオプション	デフォルト	意味
opnormal	Default Operation (デフォルト動作)	Audit Only (監査のみ)	Basic OperationをAudit Onlyに設定します。
opblock	Default Operation (デフォルト動作)	Audit Only (監査のみ)	Basic OperationをBlock Modeに設定します。
auditnone	Audit mode (監査モード)	No Audit (監査なし)	Basic OperationをNo Auditに設定します。データは記録されません。
auditrelevant	Audit mode (監査モード)	No Audit (監査なし)	Audit modeをAudit Relevantに設定します。警告レベル以上のデータを記録します。
auditall	Audit mode (監査モード)	No Audit (監査なし)	Audit modeをAudit Allに設定します。仮想サービス経由のすべてのデータを記録します。 通常の動作ではAudit Allオプションは推



値	関連するWUIオプション	デフォルト	意味
			奨めません。Audit Allは、特定の問題を解決する場合のみ使用してください。
reqdataenable	Inspect HTML POST Request Content (HTML POST要求の内容を検査する)	無効	Inspect HTML POST Request Contentオプションを有効にします。
reqdatadisable	Inspect HTML POST Request Content (HTML POST要求の内容を検査する)	無効	Inspect HTML POST Request Contentオプションを無効にします。
resdataenable	Process Response Data (応答データを処理する)	無効	Process Response Dataオプションを有効にします。
resdatadisable	Process Response Data (応答データを処理する)	無効	Process Response Dataオプションを無効にします。
jsondisable	Disable JSON Parser (JSONパーサーを無効にする)	無効	JSONパーサーを無効にします。このオプションは、Inspect HTML POST Request Contentオプションが有効な場合に限り関係してきます。
jsonenable	Disable JSON Parser (JSONパーサーを無効にする)	無効	JSONパーサーを有効にします。このオプションは、Inspect HTML POST Request Contentオプションが有効な場合に限り関係してきます。
xmldisable	Disable XML Parser (XMLパーサーを無効にする)	無効	XMLパーサーを無効にします。このオプションは、Inspect HTML POST Request Contentオプションが有効な場合に限り関係してきます。
xmlenable	Disable XML Parser (XMLパーサーを無効にする)	無効	XMLパーサーを有効にします。このオプションは、Inspect HTML POST Request Contentオプションが有効な場合に限り関係してきます。

表3-10: InterceptOptsのパラメータ値

3.5.1.6.2 仮想サービスへのAFPルールの割り当て

次のコマンドを実行することで、仮想サービスにAFPルールを割り当てられます。

```
https://<LoadMaster IP Address>/access/vsaddwafrule?vs=<VS IP Address>&port=<Port>&prot=<tcp/udp>&rule=<Prefix>/<RuleName>
```

例 :



```
https://10.11.0.30/access/vsaddwafrule?vs=10.11.0.35&port=80&prot=tcp&rule=C/modsecurity_crs_13_xml_enabler
```

<RuleName>の前にはしかなるべき文字（または単語）とスラッシュを記述する必要があります。この文字/単語は、追加するルールの種類によって決まります。

大文字と小文字が区別されます。コマンドを正しく機能させるには、文字/単語の大文字と小文字を正しく指定する必要があります。

- CまたはCustom（カスタム）
- ZまたはApplicationGeneric（アプリケーション汎用）
- AまたはApplicationSpecific（アプリケーション固有）
- GまたはGeneric（汎用）

vsaddwafruleコマンドでは、上記のコマンド例に示したすべてのパラメーターが必要です。いずれかのパラメーターを省略すると、String value missing（文字列値がありません）のエラーが表示されません。

スペース（または%20）で区切ることで、1つのコマンドに複数のルールを割り当てることができます。例：

```
https://10.11.0.30/access/vsaddwafrule?vs=10.11.0.35&port=80&prot=tcp&rule=C/modsecurity_crs_13_xml_enabler%20C/modsecurity_crs_10_ignore_static
```

この方法で複数のルールを割り当てるときは注意が必要です。既に割り当て済みのルールを追加すると、WAF Misconfigured（WAFの設定が間違っている）状態になります。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。

関連するWUI項目

Virtual Services > View/Modify Services > Modify > WUI Options > Assign Rules

3.5.1.6.3 仮想サービスからのAFPルールの割り当て解除

次のコマンドを実行することで、仮想サービスからAFPルールの割り当てを解除できます。このコマンドは、WUIのModify Virtual Service（仮想サービスの変更）画面のAvailable RulesフィールドおよびAssigned Rulesフィールドに関係しています。



`https://<LoadMasterIPAddress>/access/vsremoveafrule?vs=<VSIPAddress>&port=<Port>&prot=<tcp/udp>&rule=C/<RuleName>`

例 :

`https://10.11.0.30/access/vsremoveafrule?vs=10.11.0.35&port=80&prot=tcp&rule=C/modsecurity_crs_13_xml_enabler`

<RuleName>の前にはしかるべき文字（または単語）とスラッシュを記述する必要があります。この文字/単語は、削除するルールの種類によって決まります。

- CまたはCustom（カスタム）
- ZまたはApplicationGeneric（アプリケーション汎用）
- AまたはApplicationSpecific（アプリケーション固有）
- GまたはGeneric（汎用）

vsremoveafruleコマンドでは、上記のコマンド例に示したすべてのパラメーターが必要です。いずれかのパラメーターを省略すると、String value missing（文字列値がありません）のエラーが表示されます。

関連するWUI項目

Virtual Services > View/Modify Services > Modify > WAF Options > Assign Rules



3.5.1.7 ESPオプション

名前	種類	デフォルト	範囲	説明
AllowedHosts	S	<未設定>		このパラメーターは、ESPが有効のときのみ関係します。この仮想サービスからアクセス可能な仮想ホストを指定してください。
AllowedDirectories	S	<未設定>		このパラメーターは、ESPが有効のときのみ関係します。この仮想サービスからアクセス可能なすべての仮想ディレクトリを指定してください。
Domain	S	<未設定>		この仮想サービスが動作するシングルサインオン (SSO) ドメイン
Logoff	S	<未設定>		このパラメーターは、ESPが有効かつクライアント認証モードがフォームベースに設定されているときのみ関係します。ロードマスターがログアウトイベントを検出するのに使用する文字列を指定してください。 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。



名前	種類	デフォルト	範囲	説明
ESPLogs	I	7	整数 (0~7)	ESPログの有効化有効な値は以下のとおりです。 0 = ログを記録しない 1 = ユーザーアクセス 2 = セキュリティ = ユーザーアクセスとセキュリティ 4 = 接続 5 = ユーザーアクセスと接続 6 = セキュリティと接続 7 = ユーザーアクセス、セキュリティ、接続 注:SMTPサービスの場合、0と4のみ有効です。SMTPサービスではセキュリティの問題は常に記録されません。ログインされないため、ユーザーアクセスは記録されません。
SMTPAllowedDomains	S	<未設定>		仮想サービスによる受信を許可するすべてのドメインを指定します。
EspEnabled	B	N	0 - 無効 1 = 有効	エッジセキュリティパック (ESP) 機能を有効/無効にします。
InputAuthMode	I	0	0-4	使用するクライアント認証方式を指定します。 0 = サーバーに委任 1 = 基本認証 2 = フォームベース 3 = 将来的に使用 4 = Client Certificates (クライアント証明書) 5 = SMTP
OutputAuthMode	I	Dependant on InputAuthMode value	0-2	使用するサーバー認証方式を指定します。 0 = なし 1 = 基本認証 2 = KCD
OutConf	S	<未設定>		アウトバウンドSSOドメイン名を入力



名前	種類	デフォルト	範囲	説明
SingleSignOnDir	S	<未設定>		このパラメーターは、仮想サービス編集画面の“ESP Options” (ESPのオプション) セクションにある“SSO Image Set” (SSO画像セット) ドロップダウンリストに関係しています。ログイン画面で使用する画像セットの名前を指定します。画像セットを指定しない場合、デフォルトのExchange画像セットが使用されます。
AllowedGroups	S	<未設定>		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。
IncludeNestedGroups	B	0 = 無効	0 - 無効 1 = 有効	このパラメーターは、AllowedGroupsパラメーターに関係します。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。
ExcludedDomains	String	<未設定>		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。複数の除外ドメインを指定するには、スペース区切りのリストを使用します。
AltDomains	String	<未設定>		複数のドメインの認証を設定する際に仮想サービスに割り当てる代替ドメインを指定します。複数の代替ドメインを指定するには、スペース区切りのリストを使用します。

表3-11: APIパラメーターのESPオプション



3.5.1.8 実サーバー

名前	種類	デフォルト	範囲	説明
CheckType	S	<tcp>	デフォルト値は仮想サービスのポートにより異なります。値の一覧を以下に示します。 <ul style="list-style-type: none"> - icmp - https - https - tcp - smtp - nntp - ftp - telnet - pop3 - imap - rdp - bdata - none (なし) 	Real Serverのヘルスチェックに使用されるプロトコルを指定します。
CheckHost	A	<未設定>		CheckHostの値を設定するには、CheckUse1.1を有効にする必要があります。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。
CheckPattern	S	<未設定>		CheckTypeがhttpまたはhttpsに設定されている場合 - これは、WUIのReply 200 Patternに対応しません。このパラメーターは、HTTP MethodがGETまたはPOSTに設定されている場合のみ適用されます。CheckTypeがbdataに設定されている場合: 応答内で検索する16進文字列を指定します。



名前	種類	デフォルト	範囲	説明
CheckUrl	S	<未設定>		<p>CheckTypeがhttpまたはhttpsに設定されている場合 - デフォルトで、ヘルスチェッカーはURL"/"へのアクセスを試み、これによりそのマシンが利用可能かどうかを判定します。CheckUrlパラメーターにて他のURLを設定できます。</p> <p>Check Typeがbdataに設定されている場合:実サーバーに送信する16進文字列を指定します。</p>
CheckCodes	S	<未設定>	300-599	<p>実サーバーから受信したときに成功として処理する必要のある、スペースで区切られたHTTPステータスコードのリスト</p>
CheckHeaders	S	<未設定>		<p>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。この組はパイプで区切ります (例: Host:xyz UserAgent:prq)。</p>
MatchLen	S	0	0-8000	<p>このパラメーターは、CheckTypeがbdataに設定されているときのみ関係します。CheckPatternを検索するバイト数を指定してください。</p>
CheckUse1.1	B	N	0 - 無効 1 = 有効	<p>デフォルトでは、ヘルスチェッカーはHTTP/1.0を使用して実サーバーの状態をチェックします。CheckUse1.1を有効にすると、HTTP/1.1が使用されます (こちらの方が効率的です)。</p>
CheckPort	I	<未設定>	3-65530	<p>チェックするポートです。ポートを指定しない場合、実サーバーのポートが使用されます。</p>
NumberOfRSs	I (読み取り専用)	<未設定>		<p>仮想サービスに割り当てられている実サーバーの数を表示します。</p>
NRules	I (読み取り専用)	<未設定>		<p>コンテンツスイッチが有効なときにReal Serverに割り当てられるルールの数を表示します。</p>



名前	種類	デフォルト	範囲	説明
RuleList	リスト (読み取り専用)			実サーバーに割り当てるコンテンツルールのリスト
CheckUseGet	I	N	0 - HEAD 1 - GET 2 - POST	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。
ExtraHdrKey	S	<未設定>		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を指定します。
ExtraHdrValue	S	<未設定>		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値を指定します。
CreateSubVS		<未設定>		このパラメーターを使用すると、仮想サービス内にSubVSを作成できます。このパラメーターは値を持ちません (createsubvsと入力するとSubVSが作成されます)。
SubVS	I (読み取り専用)		0 - 無効 1 - 有効	このパラメーターは、仮想サービスに存在するサブVSの詳細を表示します。
CheckPostData	S	<未設定>	2047文字まで入力できます。	このパラメーターは、HTTP MethodがPOSTに設定されている場合のみ適用されます。POSTメソッドを使用した場合、最大2047文字のPOSTデータをサーバーに送信できません。
RSRulePrecedence	String	<未設定>		このパラメーターは、RSRulePrecedencePosと組み合わせて使う必要があります。このパラメーターは、そのポジションを変更したい既存のルールの名前を指定するのに使用します。
RSRulePrecedencePos	Int16	<未設定>		このパラメーターは、パラメーターRSRulePrecedenceとともに使用し、一連のルールにおいてそのルールのポジションを変更するのに使用します。例えば、ポジション2はルールが2番目にチェックされることを意味します。



名前	種類	デフォルト	範囲	説明
EnhancedHealthchecks	Boolean	0 - 無効	0 - 無効 1 - 有効	EnhancedHealthchecksパラメーターを有効にすると、ヘルスチェックに関する追加のパラメーター (RsMinimum) が現れます。EnhancedHealthchecksパラメーターが無効な場合、1つ以上の実サーバーが利用可能であれば、仮想サービスが利用可能であるとみなされます。EnhancedHealthchecksパラメーターが有効な場合、仮想サービスが利用可能であると認識されるのに必要な最低限の実サーバー数を指定できます。
RsMinimum	整数	1	1～実際の実サーバーの数まで設定できます。	このパラメーターは、EnhancedHealthchecksパラメーターが有効な場合のみ、modvsコマンドを用いて設定できます。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指定してください。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。一部の实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。 このパラメーターの値を取得する際、仮想サービスに実サーバーがない場合は0（デフォルト値）になり、仮想サービスに実サーバーがある場合は1になります。ただし、実際には最小値は常に1になります。

表3-12: 実サーバーのAPIパラメーター



3.5.1.9 その他

名前	種類	デフォルト	範囲	説明
Adaptive	S (Read only)	<未設定>		このパラメータは読み取り専用であり、表示されるのはScheduling Methodがresource based (adaptive) に設定されている場合に限定されます。
MultiConnect	B	0	0 = 無効 1 = 有効	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。このパラメーターは、“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、一部の状況では有効にできません。
Non-local	B	0 = 無効	0 - 無効 1 - 有効	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。 このオプションは、関連する仮想サービスにおいて、Enable Non-Local Real Serversが有効になっており、Transparencyが無効になっているときのみ利用できます。

表3-13: その他のAPIパラメーター

3.5.2 テンプレートを用いた仮想サービスの追加

テンプレートを使用して、仮想サービスの追加と自動設定を行うには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/addvs?vs=<VS IP Address>&port=<port>&prot=<tcp/udp>&template=<TemplateName>
```



ポートとプロトコルのパラメーターが必要ですが、テンプレートによりポートが設定される場合、コマンドで入力した値は無視されます。

テンプレートを追加/削除/表示するコマンドについては、[セクション3.5.3](#)を参照してください。

3.5.3 Manage Templates (テンプレートの管理)

3.5.3.1 テンプレートとして仮想サービスをエクスポートする

以下のコマンドを実行すると、既存の仮想サービスをテンプレートとしてエクスポートできます。

```
https://<LoadMaster IP Address>/access/exportvstmpl?vs=<VirtualService IP Address>&port=<VirtualServicePort>&prot=<tcp/udp>
```

vsパラメーターには、仮想サービスのインデックスも入力できます（この場合、その他のパラメーターは必要ありません）。仮想サービスのIDを取得するには、`listvs`コマンドを実行します。詳細は[セクション3.5.1](#)を参照してください。

3.5.3.2 テンプレートのアップロード

次のcURLコマンドを実行することで、テンプレートをアップロードできます。

```
curl -X POST --data-binary "@<TemplateFileName.templ>" -k https://bal:<password>@<LoadMaster IP Address>/access/uploadtemplate
```

3.5.3.3 インストールされているテンプレートのリスト表示

ロードマスターに存在するテンプレートのリストを表示するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/listtemplates
```

3.5.3.4 テンプレートの削除

ロードマスターからテンプレートを削除するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/deletetemplate?name=<TemplateName>
```

3.5.4 SSOの管理

3.5.4.1 SSO ドメイン

SSOドメインは、以下のコマンドで管理できます。



https://<LoadMaster IPAddress>/access/adddomain?domain=<DomainName>

SSO ドメインは最大128個まで設定できます。

https://<LoadMaster IPAddress>/access/deldomain?domain=<DomainName>

https://<LoadMaster IPAddress>/access/showdomain

https://<LoadMaster IPAddress>/access/showdomain?domain=<domain.name>

https://<LoadMaster IPAddress>/access/moddomain?domain=<domain.name>[¶mname=value...]

moddomainには以下の追加（オプション）パラメータを指定できます。

名前	種類	デフォルト	範囲	追加情報
auth_type	S	“LDAP-StartTLS”	LDAP-Unencrypted LDAP-StartTLS LDAP-LDAPS RADIUS RSA-SECURID KCD Certificates（証明書） RADIUS and LDAP-Unencrypted RADIUS%20and%20LDAP-StartTLS S RADIUS%20and%20LDAP-LDAPS RSA-SECURID%20and%20LDAP-Unencrypted RSA-SECURID%20and%20LDAP-StartTLS RSA-SECURID%20and%20LDAP-LDAPS	認証サーバーとの通信で使用する転送プロトコルを指定します。
radius_shared_secret	S（マスク）	<未設定>		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。



名前	種類	デフォルト	範囲	追加情報
logon_fmt	S	Principalname (プリンシパル名)	“not%20specified” “Principalname” “Username” “Username%20only”	LDAP/RADIUSサーバー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。 Username%20only の値は、 auth_type が RADIUS プロトコルまたは RSA-SecurID プロトコルに設定されている場合のみ利用できます。 auth_type が RADIUS または RADIUS and LDAP プロトコルに設定されている場合、 Username の値は利用できません。
logon_fmt2	S	Principalname (プリンシパル名)	“Not%20specified” “Principalname” “Username”	サーバー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_domain	S	<未設定>		このパラメータは、WUIの Domain/Realm フィールドに対応しています。使用するログインドメインです。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。 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>
logon_transcode	B	0	0 = 無効 1 = 有効	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。
max_failed_auths	I	0	0-999	ユーザーがロックアウトされるまでの最大のログイン試行回数 0 - ロックアウトしない
sess_tout_idle_pub	I	900	60-86400	セッションアイドルタイムアウト値 (単位:秒)。この値はパブリック環境で使用されます。
sess_tout_duration_pub	I	1800	60-86400	セッションがタイムアウトするまでの最大のセッション継続時間 (単位:秒)。この値はパブリック環境で使用されます。
sess_tout_idle_priv	I	900	60-86400	セッションアイドルタイムアウト値 (単位:秒)。この値はプライベート環境で使用されます。



名前	種類	デフォルト	範囲	追加情報
sess_tout_duration_priv	I	2800	60-86400	セッションがタイムアウトするまでの最大のセッション継続時間（単位:秒）。この値はプライベート環境で使用されます。
sess_tout_type	S	Idle time (アイドル時間)	Idle time (アイドル時間) Max duration (最大継続時間) :	使用するセッションタイムアウトの種類を指定します。
testuser	S	<未設定>		認証サーバーのチェックで使用されるユーザー名
testpass	S (マスク)	<未設定>		認証サーバーのチェックで使用されるパスワード
reset_fail_tout	I	60	60-86400	Failed Login Attemptsカウンターを0にリセットするまでに必要な時間（単位:秒）。この値はunlock_toutより小さくなければなりません。
unlock_tout	I	1800	60-86400	ブロックされたアカウントが自動的にブロック解除されるまでの時間（単位:秒）。この値はreset_fail_toutより大きくなければなりません。
server	S	<未設定>		このドメインを有効にするのに使用されるサーバーのアドレス
server2	A	<未設定>	有効なIPアドレス	2要素認証を使用する場合、パラメーターserverを使用してRADIUSサーバーのアドレスを設定し、パラメーターserver2を使用してLDAPのサーバーのアドレスを設定します。
kerberos_domain	S	<未設定>		Kerberosレルム
kerberos_kdc	S	<未設定>		Kerberosキー配信センター
kcd_username	S	<未設定>		kcd_usernameには、二重引用符または一重引用符を含めることはできません。
kcd_password	S	<未設定>		kcd_passwordには、二重引用符または一重引用符を含めることはできません。
ldap_admin	S	<未設定>		データベースにログインして証明書に含まれているユーザーが存在するかどうかをチェックするため、ldap_passwordとともに使用されます。



名前	種類	デフォルト	範囲	追加情報
ldap_password	S	<未設定>		データベースにログインして証明書に含まれているユーザーが存在するかどうかをチェックするため、ldap_adminとともに使用されます。
cert_check_asl	B	0 = 無効	0 = 無効 1 = 有効	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altSecurity Identities (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。
cert_check_cn	B	0 = 無効	0 = 無効 1 = 無効	このパラメーターを有効にすると、SANを利用できないときに、フォールバックによる共通ネーム (CN) のチェックを許可します。
server_side	B	Y - アウトバウンドKCD SSOドメイン N = インバウンド構成	Y = アウトバウンドKCD SSOドメイン N = インバウンド構成	構成がインバウンドまたはアウトバウンドのどちらであるかを指定します。

表3-14:Moddomainパラメーター

`https://<LoadMaster IP Address>/access/showdomainlockedusers?`

`https://<LoadMaster IP Address>/access/unlockdomainusers?domain=<example.com>&users=<exampleuser>`

3.5.4.1.1 RSAファイルのアップロード

認証プロトコルとしてRSA-Secur IDを使用する場合、認証を正しく機能させるにはロードマスターにファイルをアップロードする必要があります。

RSA認証マネージャー設定ファイルをアップロードするには、以下のコマンドを実行します。

```
curl -X POST --data-binary "@<RSAConfigFileName.zip>" -k https://<username>:<password>@<LoadMaster IP Address>/access/setrsaconfig
```

RSAノード秘密鍵ファイルをアップロードするには、以下のコマンドを実行します。



```
curl -X POST --data-binary "@<NodeSecretFileName.zip>" -k https://<username>:<password>@<LoadMaster IP Address>/access/setrsanodesecret?rsanspwd=<RSANodeSecretPassword>
```

3.5.4.2 SS0画像の設定

以下のコマンドを使用してカスタムのSS0画像を管理できます。

```
https://<LoadMaster IP Address>/access/listssimages
```

```
https://<LoadMaster IP Address>/access/delssoimage?name=<Imagesetname>
```

SS0画像をアップロードするには以下のコマンドを使用します。

```
curl -X POST --data-binary "@<pathToImageSet>" -k https://<LoadMaster IP Address>/access/ssimages?
```

カスタムのSS0画像は、tarファイルの形式で設定する必要があります。テンプレートのtarファイルは、KEMPサポートサイトから入手できます。<https://support.kemptechnologies.com/hc/en-us/articles/202220783-Custom-Image-Set>.

このパラメーターを編集すると、目的の外観と使い勝手を得ることができます。詳細については、[ポートフォロウィング 機能説明](#)を参照してください。

3.5.5 WAFの設定

以下のコマンドは、AFPが有効なライセンスを保有するロードマスターでのみ機能します。

KEMPは、AFPライセンスとAFPサポートを保有するユーザーに対し、**ip reputation**などのさまざまな商用ルールを提供します。このルールは、毎日自動的にダウンロード/更新するよう設定できます。この商用ルールは、特定の脅威から保護することを目的としています。KEMPが提供する商用ルールは、AFPサポートに申し込むと利用可能になります。

また、ModSecurityコアルールセットなどの汎用の攻撃検出ルールをアップロードすることもできます。これらのルールは、各Webアプリケーションに基本レベルの保護を提供します。

必要であれば、ユーザー独自のカスタムルールを記述してアップロードすることも可能です。

AFPが有効なロードマスターでは、KEMPが提供したルールを使用するか、アップロード可能なカスタムルールを使用するか、またはそれらを組み合わせて使用するかを選択できます。以下のセクションでは、商用ルールやカスタムルールに特有のコマンド、およびその両方に関するコマンドについて詳しく説明します。



3.5.5.1 商用ルールファイルに関するコマンド

本セクションのコマンドは、すべて商用ルールファイルに関係します。

3.5.5.1.1 WAF商用ルールの設定の表示

`getwafsettings`コマンドを使用すると、ロードマスターWUIのWAF Settings画面に表示される商用ルールに関するWAFオプションの値が表示されます。

`https://<LoadMaster IP Address>/access/getwafsettings`

関連するWUI項目

Virtual Services > WAF Settings

3.5.5.1.2 商用ルールファイルの自動更新の有効化

`setwafautoupdate`コマンドを使用すると、最新の商用AFPルールファイルの自動ダウンロードが有効になります。このオプションを有効にすると、最新のルールがKEMPから毎日ダウンロードされます。最新ルールのデフォルトのインストール時刻は午前4時です。最新ルールのインストール時刻は、`SetWafInstallTime`コマンドを実行することで設定できます。詳細はセクション3.5.5.1.4を参照してください。

`GetWafSetting`コマンドを実行することで、現在の設定を確認できます。詳細はセクション0を参照してください。

`https://<LoadMaster IP Address>/access/setwafautoupdate?enable=<yes/no>`

関連するWUI項目

Virtual Services > WAF Settings > Enable Automatic Rule Updates

3.5.5.1.3 最新の商用ルールファイルの自動インストールを有効/無効にする

次のコマンドを実行することで、最新の商用ルールファイルの自動インストールを有効/無効にできます。

`https://<LoadMaster IP Address>/access/setwafautoinstall?enable=<yes/no>`

関連するWUI項目

Virtual Services > WAF Settings > Enable Automated Installs

3.5.5.1.4 商用ルールファイルの自動インストール時刻の設定

次のコマンドを実行することで、商用ルールファイルの自動インストール時刻を設定できます。これは、WUIのWAF Settings画面にあるWhen to Installドロップダウンメニューに関連しています。



`https://<LoadMaster IP Address>/access/setwafinstalltime?hour=<hour>`

hoursは24時間制の時刻（0～23）です。例えば、13は午後1時を表します。

`https://10.11.0.31/access/setwafinstalltime?hour=13`

範囲は0～23です。分は指定できません。

関連するWUI項目

Virtual Services > WAF Settings > When to Install

3.5.5.1.5 AFP商用ルールファイルを直ちにダウンロードする

次のコマンドを実行することで、最新のAFP商用ルールファイルを手動でダウンロードできます。これは、WUIのWAF Settings画面にあるDownload Nowボタンに関連しています。

`https://<LoadMaster IP Address>/access/downloadwafrules`

関連するWUI項目

Virtual Services > WAF Settings > Download Now

既に最新のルールがダウンロードされていてそれ以上新しいデータが存在しない場合は、**No updates available**（最新データを利用できません）のメッセージが表示されます。

3.5.5.1.6 WAFルールの変更ログの表示

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ダウンロードするには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/getwafchangelog`

3.5.5.1.7 商用ルールファイルの手動インストール

次のコマンドを実行することで、商用ファイルを手動でインストールできます。これは、WUIのWAF Settings画面にあるInstall Nowボタンに関連しています。

`https://<LoadMaster IP Address>/access/maninstallwafrules`

関連するWUI項目

Virtual Services > WAF Settings > Install Now

ルールをインストール中に問題が発生すると、エラーメッセージが表示されます。



3.5.5.2 カスタムルールファイルに関するコマンド

本セクションのコマンドは、すべてカスタムルールに関係します。

3.5.5.2.1 カスタムルールファイル/ルールセットのアップロード

`addwafcustomrule`コマンドと`filename`パラメーター（必須）とともに`cURL`コマンドを使用すると、AFPのカスタムルールをアップロードできます。例：

```
curl -X POST --data-binary "@<FileName.conf>" -k https://bal:<BalPassword>@<LoadMasterIPAddress>/access/addwafcustomrule?filename=<FileName.conf>
```

また、カスタムルールファイルの個別アップロードに加え、カスタムルールセット（.tar.gzファイル）もアップロードできます。OWASPコアルールセットのアップロードの例を以下に示します。

```
curl -X POST --data-binary "@owasp-modsecurity-crs-master.tar.gz" -k https://bal:<BalPassword>@<LoadMasterIPAddress>/access/addwafcustomrule?filename=SpiderLabs-owasp-modsecurity-crs-2.2.9-5-gebe8790.tar.gz
```

これは、ロードマスターWUIのWAF Settings画面にあるCustom Rulesセクションに関連しています。

関連するWUI項目

Virtual Services > WAF Settings > Custom Rules

3.5.5.2.2 カスタムルールファイルの削除

次のコマンドを実行することで、カスタムルールファイルを削除できます。

```
https://<LoadMasterIPAddress>/access/delwafcustomrule?filename=<filename>
```

例：

```
https://10.11.0.30/access/delwafcustomrule?filename=modsecurity_crs_10_ignore_static
```

この操作では関連するデータファイルは削除されません。

関連するWUI項目

Virtual Services > WAF Settings > Custom Rules > Delete

3.5.5.2.3 カスタムルールファイルのダウンロード

次のコマンドを実行することで、お使いのローカルマシンにカスタムルールファイルをダウンロードできます。



`https://<LoadMasterIPAdress>/access/downloadwafcustomrule?filename=<filename>`

例 :

`https://10.11.0.30/access/downloadwafcustomrule?filename=modsecurity_crs_55_response_profiling`

cURLを使用してこのコマンドを実行すると、Linuxの作業ディレクトリにファイルがダウンロードされます。

関連するWUI項目

Virtual Services > WAF Settings > Custom Rule Data > Download

3.5.5.2.4 カスタムルールデータファイルのアップロード

`addwafcustomdata`コマンドと`filename`パラメーター（必須）とともにcURLコマンドを使用すると、カスタムルールデータファイルをアップロードできます。例:

`curl -X POST --data-binary "@<FileName.data>" -k https://bal:<BalPassword>@<LoadMasterIPAdress>/access/addwafcustomdata?filename=<filename.data>`

関連するWUI項目

Virtual Services > WAF Settings > Custom Rule Data > Add Data File

3.5.5.2.5 カスタムルールデータファイルの削除

次のコマンドを実行することで、カスタムルールデータファイルを削除できます。

エラー! ハイパーリンクの参照に誤りがあります。>

関連するWUI項目

Virtual Services > WAF Settings > Custom Rule Data > Delete

3.5.5.2.6 カスタムルールデータファイルのダウンロード

次のコマンドを実行することで、カスタムルールデータファイルをダウンロードできます。

エラー! ハイパーリンクの参照に誤りがあります。>

例 :

`https://10.11.0.30/access/downloadwafcustomdata?filename=modsecurity_35_bad_robots`

関連するWUI項目



Virtual Services > WAF Settings > Custom Rule Data > Download

3.5.5.3 カスタムルールと商用ルールに関するコマンド

本セクションのコマンドは、商用ルールとカスタムルールの両方に関係します。

3.5.5.3.1 AFPルールのリスト表示

`listwafrules` コマンドは、インストールされているすべてのルール（商用ルールとカスタムルール）をリスト表示します。

また、タグ名に **Active** または **Inactive** が表示され、ルールがアクティブかどうかを示されます。アクティブなルールとは、1つ以上の仮想サービスに割り当てられているルールのことです。

`https://<LoadMasterIPAddress>/access/listwafrules`

関連するWUI項目

Virtual Services > WAF Settings > Custom Rules

Virtual Services > View/Modify Services > Modify > WAF Options > Available Rules

3.5.5.4 リモートログ作成に関するコマンド

このセクションのコマンドは、WAFのリモートログ作成機能に関係します。この機能を使用すると、WAF監査ログを中央のログリポジトリに送信することができます。

3.5.5.4.1 リモートログの作成を無効にする

WAFのリモートログ作成を無効にするには、次のコマンドを実行します。

`https://<LoadMasterIPAddress>/access/disablewafremote logging`

3.5.5.4.2 リモートログの作成を有効にする

WAFのリモートログ作成を有効にするには、次のコマンドを実行します。

`https://<LoadMasterIPAddress>/access/enablewafremote logging?remotouri=<RemoteServerConsoleURI>&username=<RemoteUsername>&passwd=<RemotePassword>`



3.6 グローバル負荷分散

3.6.1 完全修飾ドメイン名 (FQDN) の管理

3.6.1.1 FQDNの追加

次のコマンドを実行することで、FQDNを追加できます。

```
https://<LoadMaster IPAddress>/access/addfqdn?fqdn=<FQDNName>
```

このコマンドでは、fqdnが必須パラメータです。

3.6.1.2 Delete FQDN (FQDNの削除)

次のコマンドを実行することで、FQDNを削除できます。

```
https://<LoadMaster IPAddress>/access/delfqdn?fqdn=<FQDNName>
```

このコマンドでは、fqdnが必須パラメータです。

3.6.1.3 FQDNのリスト表示

次のコマンドを実行することで、既存のFQDNのリストを表示できます。

```
https://<LoadMaster IPAddress>/access/listfqdns
```

3.6.1.4 FQDNの表示

showfqdnコマンドを使用すると、指定したFQDNに関する各種詳細が表示されます。

```
https://<LoadMaster IPAddress>/access/showfqdn?fqdn=<FQDNName>
```

3.6.1.5 FQDNの変更

次のコマンドを実行することで、既存のFQDNを変更できます。

```
https://<LoadMaster IPAddress>/access/modfqdn?fqdn=<FQDNName>
```

modfqdnコマンドでは、次のオプションパラメータを使用できます。



名前	種類	デフォルト	範囲	追加情報
SelectionCriteria	S	“rr”	rr = round robin (ラウンドロビン) wrr = weighted round robin (加重ラウンドロビン) fw = 固定重み rsr = 実サーバー負荷 prx = 近接性 lb = ロケーションベース	FQDNに関連付けられたアドレスの選択基準
FailTime	I	0	0-1440	障害遅延が設定されていない場合、通常のヘルスチェックが実行されます。設定されている場合、このパラメータによって、障害後、最終的に無効化するまでに待機する時間（分単位）を定義します。無効化された時点で、通常は元の動作に戻りません。
siterecoverymode	S	auto (自動)	auto - 自動 manual - 手動	このパラメータによって、Site Recovery Mode (サイトリカバリモード) を定義します。 automaticに設定されている場合、サイトリカバリ後、サイトは即座に元の動作に戻ります。 manualに設定されている場合、サイトで障害が発生した時点で、サイトは無効化されます。通常動作に復旧するには手動の作業が必要になります。



名前	種類	デフォルト	範囲	追加情報
failover	B	0 - 無効	0 - 無効 1 - 有効	このパラメーターは、 SelectionCriteria が lb （ロケーションベース）に設定されているときのみ関係します。 FQDNフェイルオーバーを有効/無効にします。
publicRequestValue		0 - パブリックサイトのみ	0 - パブリックサイトのみ 1 - パブリックサイトを推奨 2 - プライベートサイトを推奨 3- 任意のサイト	パブリックIPアドレスからクライアントへの応答を、指定したクラスのサイトに制限します。各種設定とその値についての説明は、「パブリックリクエスト/プライベートリクエスト」のセクションの表3-16などを参照してください。パブリック/プライベートリクエストに関するパラメーターの設定
privateRequestValue		0 - プライベートサイトのみ	0 - プライベートサイトのみ 1 - プライベートサイトを推奨 2 - パブリックサイトを推奨 3 - 任意のサイト	プライベートIPアドレスからクライアントへの応答を、指定したクラスのサイトに制限します。各種設定とその値についての説明は、「パブリックリクエスト/プライベートリクエスト」のセクションの表3-16などを参照してください。パブリック/プライベートリクエストに関するパラメーターの設定

表3-15: ModFQDNのパラメーター

パブリックリクエスト/プライベートリクエスト

“Public Requests & Private Requests”（パブリックリクエスト/プライベートリクエスト）オプションは、ファームウェアバージョン7.1-28までのロードマスターで用意されていた古いオプションである“Isolate Public/Private Sites”（パブリック/プライベートサイトを隔離する）に取って代わるものです。この新しい設定により、管理者は、FQDNに関して非常に柔軟性の高い設定を行うことができます。



この新しい設定を使用すると、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るようになります。例えば、管理者はプライベートなクライアントのみプライベートなサイトに転送することができます。

以下の表に、各設定と設定可能な値の概要を示します。

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

表3-16:パブリック/プライベートリクエストに関するパラメーターの設定

3.6.1.6 マップの追加

次のコマンドを実行することで、FQDNにマップを追加できます。

```
https://<LoadMaster IP Address>/access/addmap?fqdn=<FQDNName>&ip=<IP Address To Add>&clust=<ClusterName>
```

clustパラメーターは任意です。

3.6.1.7 マップの変更

マップを変更するには、次のコマンドを実行します。



`https://<LoadMaster IP Address>/access/modmap?fqdn=<FQDN Name>&ip=<IP Address To Modify>`

modmapコマンドでは、次のオプションパラメータを使用できます。

名前	種類	デフォルト	範囲	追加情報
Checker (チェッカー)	S	"icmp"	none (なし) icmp tcp	このIPアドレスに対して実行するチェックの種類を指定します。
Weight (重み)	I	1000	1-65535	IPアドレスに関連付ける加重を指定します。最も高い加重を持つアドレスが返されます。このパラメータが関連するのは、FQDNのSelection CriteriaがWeighted Round RobinまたはFixed Weightingに設定されている場合に限定されます。
Enable	B	1 - 有効	1 - 有効 0 - 無効	IPアドレスを有効化または無効化します。
Cluster (クラスター)	I	<未設定>		このIPアドレスに関連付けるクラスターのID番号を指定します。
MapAddress	A	<未設定>		これは、SelectionCriteriaがReal Server Loadに、CheckerがCluster Checksに設定されていて、クラスターの種類がRemote LMまたはLocal LMのときのみ関係します。関連するロードマスターからマッピングされる仮想サービスのIPアドレスを入力してください。



名前	種類	デフォルト	範囲	追加情報
MapPort	I	<未設定>		<p>これは、SelectionCriteriaがReal Server Loadに、CheckerがCluster Checksに設定されていて、クラスターの種類がRemote LMまたはLocal LMのときのみ関係します。</p> <p>このパラメーターは、MapAddressパラメーターとともに使用し、マッピングするIPアドレスとポートの組み合わせを指定します。</p> <p>このパラメーターが設定されていない場合、選択したアドレスと同じIPアドレスを持つすべての仮想サービスに対してヘルスチェックが行われます。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。ポートが指定されている場合、FQDNのヘルスチェック時にその仮想サービスに対してのみヘルスチェックが行われます。</p>

表3-17: ModMapのパラメーター

3.6.1.8 マップの削除

マップを削除するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/deletemap?fqdn=<FQDN Name>&ip=<IP Address To Delete>
```

3.6.1.9 マップのロケーションの変更

マップのロケーションを変更するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/changemaploc?fqdn=<FQDN Name>&ip=<IP Address>&lat=<Latitude Degrees And Minutes>&long=<Longitude Degrees And Minutes>
```

このコマンドが関連するのは、FQDNのSelection CriteriaがProximityに設定されている場合に限定されます。

3.6.1.10 ロケーションの追加

国または大陸を追加するには、次のコマンドを実行します。



エラー! ハイパーリンクの参照に誤りがあります。countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>

このコマンドが関連するのは、FQDNのSelection CriteriaがLocation Basedに設定されている場合に限定されます。Selection Criteriaの変更方法に関する詳細は、セクション3.6.1.5を参照してください。

FQDN名は大文字と小文字が区別されます。

使用される国コードと大陸コードは、ISOの標準コードです。

国を追加するには、パラメーターiscontinentをnoに設定する必要があります。

大陸を追加するには、パラメーターiscontinentをyesに設定する必要があります。

countrycodeの値は大文字でなければなりません。

カスタムロケーションを追加するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/addcountry?fqdn=<FQDN Name>&ip=<IP Address>&customlocation=<Custom Location Name>
```

また、コマンドですべてのパラメーターを指定すると、1つのコマンドで国/大陸およびカスタムロケーションを追加できます。例:

```
https://<LoadMaster IP Address>/access/addcountry?fqdn=<FQDN Name>&ip=<IP Address>&countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>&customlocation=<Custom Location Name>
```

3.6.1.11 ロケーションの削除

国を削除するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/removecountry?fqdn=<FQDN Name>&ip=<IP Address>&countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>
```

このコマンドが関連するのは、FQDNのSelection CriteriaがLocation Basedに設定されている場合に限定されます。

FQDN名は大文字と小文字が区別されます。



国を削除するには、パラメーター `iscontinent` を `no` に設定する必要があります。

大陸を削除するには、パラメーター `iscontinent` を `yes` に設定する必要があります。

`countrycode` の値は大文字でなければなりません。

カスタムロケーションを削除するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/removecountry?fqdn=<FQDN Name>&ip=<IP Address>&customlocation=<Custom Location Name>
```

また、コマンドですべてのパラメーターを指定すると、1つのコマンドで国/大陸およびカスタムロケーションを削除できます。例:

```
https://<LoadMaster IP Address>/access/removecountry?fqdn=<FQDN Name>&ip=<IP Address>&countrycode=<Two Character Country/Continent Code>&iscontinent=<yes/no>&customlocation=<Custom Location Name>
```

3.6.1.12 チェッカーアドレスの変更

チェッカーのアドレスを変更するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/changecheckeraddr?fqdn=<FQDN Name>&ip=<IP Address>
```

`changecheckeraddr` コマンドでは、次のオプションパラメータを使用できます。

名前	種類	デフォルト	範囲	追加情報
ip	S	<未設定>		IPアドレスのヘルスチェックに使用されるアドレスを指定します。
port	I	80	1-65530	IPアドレスのヘルスチェックに使用されるポートを指定します。

表3-18: ChangeCheckerAddrのパラメーター

3.6.2 クラスターの管理

3.6.2.1 クラスタのリスト表示

次のコマンドを実行することで、既存のクラスタのリストを表示できます。

```
https://<LoadMaster IP Address>/access/listclusters
```



3.6.2.2 クラスタの表示

次のコマンドを実行することで、特定のクラスタについての詳細を表示できます。

`https://<LoadMaster IP Address>/access/showcluster?id=<Cluster ID>`

このコマンドでは、`id`が必須パラメータです。

3.6.2.3 クラスタの追加

次のコマンドを実行することで、クラスタを追加できます。

`https://<LoadMaster IP Address>/access/addcluster?ip=<Cluster IP Address>&name=<Cluster Name>`

このコマンドでは、`ip` および `name`が必須パラメータです。

3.6.2.4 クラスタの削除

次のコマンドを実行することで、クラスタを削除できます。

`https://<LoadMaster IP Address>/access/deletecluster?id=<Cluster ID>`

このコマンドでは、`id`が必須パラメータです。

3.6.2.5 クラスターの変更

次のコマンドを実行することで、クラスタを変更できます。

`https://<LoadMaster IP Address>/access/modcluster?id=<Cluster ID>`

`modcluster` コマンドでは、次のオプションパラメータを使用できます。

名前	種類	デフォルト	範囲	追加情報
種類	S	Default (デフォルト) :	デフォルト remoteLM localLM	クラスタの種類を変更します。
name (名前)	S			クラスタの名前を指定します。
checker	S	None (なし) :	none (なし) tcp icmp	クラスタのステータスチェックに使用される方法を指定します。



名前	種類	デフォルト	範囲	追加情報
checkerport	I	“0”	1-65530	クラスタのチェックに使用されるポートを設定します。このパラメータが関連するのは、checkerがtcpに設定されている場合に限定されます。
enable	B	1 - 有効	1 = 有効 0 = 無効	クラスタを有効化または無効化します。

表3-19: ModClusterのパラメーター

3.6.2.6 クラスタのロケーションの変更

クラスタのロケーションを変更するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/clustchange loc?ip=<Cluster IP Address>&latsecs=<LatitudeSeconds>&longsecs=<LongitudeSeconds>
```

3.6.3 その他のパラメータ

3.6.3.1 その他のパラメータのリスト表示

GEOのその他のパラメータのリストを表示するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/listparams
```

3.6.3.2 その他のパラメータの変更

次のコマンドを実行することで、GEOのその他のパラメータを変更できます。

```
https://<LoadMaster IP Address>/access/modparams
```

modparamsコマンドでは、次のオプションパラメータを使用できます。

名前	種類	デフォルト	範囲	追加情報
SourceOfAuthority	S	<未設定>		Source of Authorityリクエストに対する応答を設定します。
namesrv	S	<未設定>		Name Serverリクエストに対する応答を設定します。
SOAEmail	S	<未設定>		Source of Authorityリクエストに対して送信するEメール文字列を設定します。
TTL	I	<未設定>	1-86400	ロードマスターから返信された応答のTime To Live (TTL) (単位:秒) を設定します。



名前	種類	デフォルト	範囲	追加情報
persist	I	0	0-86400	これは、WUIのStickinessフィールドに対応します。特定の応答をホストに返す時間（単位:秒）を設定します。
CheckInterval	I	120	9-3600	デバイスをチェックする頻度（単位:秒）を設定します。 注:インターバルの値は、ConnTimeoutとRetryAttemptsの値の積より大きくなければなりません（インターバル>タイムアウト×リトライ+1）。これは、現在のヘルスチェックが完了する前に次のヘルスチェックが開始されないようにするためです。タイムアウト値またはリトライ値を増やしてこのルールが破られた場合、インターバルの値が自動的に増やされます。
ConnTimeout	I	20	4-60	チェックリクエストのタイムアウト時間（単位:秒）を設定します。
RetryAttempts	I	2	2-10	デバイス故障としてマークされるまでのチェック回数を設定します。

表3-20: ModParamsパラメーター

3.6.3.3 ロケーションデータパッチファイルのアップロード

ロケーションデータ更新ファイルをアップロードできます。これを行うにはcURLコマンドを実行します。

```
curl -X POST --data-binary "@<GEOPatchFileName>" -k https://<username>:<password>@<LoadMaster IPAddress>/access/locdataupdate
```

3.6.4 IP範囲の選択条件

3.6.4.1 IPアドレスのリスト表示

IP範囲の選択基準用に設定されたIPアドレスのリストを表示するには、次のコマンドを実行します。

エラー! ハイパーリンクの参照に誤りがあります。



3.6.4.2 IPアドレスの詳細表示

IP範囲の選択基準用に設定された特定のIPアドレスの詳細を表示するには、次のコマンドを実行します。

エラー! ハイパーリンクの参照に誤りがあります。>

3.6.4.3 IPアドレスの追加

IPアドレスをIP範囲の選択基準に追加するには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/addip?ip=<IP Address>`

3.6.4.4 IPアドレスの削除

IPアドレスをIP範囲の選択基準から削除するには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/delip?ip=<IP Address>`

3.6.4.5 IPアドレスのロケーションの変更

IPアドレスのロケーションを変更するには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/modiploc?ip=<IP Address>&lat=<Latitude Minutes>&long=<Longitude Minutes>`

3.6.4.6 IPアドレスのロケーションの削除

IPアドレスのロケーションを削除するには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/deliploc?ip=<IP Address>`

3.6.4.7 IPアドレスに関連付けられた国の追加

既存のIPアドレスに国を割り当てるには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/addipcountry?ip=<IP Address>&<param>=<value>`

名前	必須	種類	デフォルト	範囲	追加情報
countrycode	No	S	<未設定>	有効な国コード	大文字で記された有効な2桁の国コードを使用してください。
customloc	No	S	<未設定>	既存のカスタムロケーション	既存のカスタムロケーションの名前。

このコマンドを実行するには、**countrycode**または**customloc**のいずれかのパラメータを入力する必要があります。



3.6.4.8 IPアドレスに関連付けられた国の削除

IPアドレスに関連付けられた国を削除するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/removeipcountry?ip=<IP Address>
```

3.6.4.9 カスタムロケーションの追加

次のコマンドを実行することで、カスタムロケーションを追加できます。

エラー! ハイパーリンクの参照に誤りがあります。>

locationは必須パラメータです。

3.6.4.10 カスタムロケーションの編集

既存のカスタムロケーションの名前を変更するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/editcustomlocation?cldname=<OldCustomLocationName>&cldnewname=<NewCustomLocationName>
```

3.6.4.11 カスタムロケーションの削除

既存のカスタムロケーションを削除するには、以下の書式でdeletcustomlocationコマンドを実行します。

```
https://<LoadMaster IP Address>/access/deletecustomlocation?cldname=<CustomLocationName>
```

3.6.5 GEOの有効化/無効化

3.6.5.1 GEOが有効であるかどうかのチェック

GEOが有効であるかどうかをチェックするには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/isgeoenabled
```

3.6.5.2 GEOの有効化

次のコマンドを実行することで、GEOを有効化できます。

エラー! ハイパーリンクの参照に誤りがあります。

3.6.5.3 GEOの無効化

次のコマンドを実行することで、GEOを無効化できます。

エラー! ハイパーリンクの参照に誤りがあります。



3.7 Statistics (統計情報)

仮想サービスおよび実サーバーのあらゆる統計情報は、**stats**コマンドで取得できます。

ロードマスターのクラスタリングを使用している場合、管理用ノードにて**stats**コマンドを実行すると、すべてのマシンに関するトータルの結果が出力されます。

https://<LoadMaster IP Address>/access/stats

コマンドが正常に実行された場合、仮想サービスおよび実サーバーのあらゆる統計情報が以下のフォーマットで返されます。

実サーバーの統計情報は、仮想サービス単位に返されます。

```
<Response stat="200" code="ok">
  <Success>
    <Data>
      <CPU>
        <total>
          <User>3</User>
          <System>2</System>
          <Idle>93</Idle>
          <IOWaiting>2</IOWaiting>
        </total>
        <cpu0>
          <User>2</User>
          <System>3</System>
          <HWInterrupts>0</HWInterrupts>
          <SWInterrupts>0</SWInterrupts>
          <Idle>94</Idle>
          <IOWaiting>2</IOWaiting>
        </cpu0>
        <cpu1>
          <User>5</User>
          <System>2</System>
          <HWInterrupts>0</HWInterrupts>
          <SWInterrupts>0</SWInterrupts>
          <Idle>92</Idle>
          <IOWaiting>2</IOWaiting>
        </cpu1>
      </CPU>
      <Memory>
        <memused>280848</memused>
        <percentmemused>13</percentmemused>
      </Memory>
    </Data>
  </Success>
</Response>
```




```
<memfree>1777144</memfree>
<percentmemfree>87</percentmemfree>
</Memory>
<Network>
  <eth0>
    <ifaceID>0</ifaceID>
    <speed>10000</speed>
    <in>0.0</in>
    <inbytes>828</inbytes>
    <inbytesTotal>63644014</inbytesTotal>
    <out>0.0</out>
    <outbytes>5329</outbytes>
    <outbytesTotal>93841381</outbytesTotal>
  </eth0>
  <eth0.vxlan4>
    <ifaceID>2</ifaceID>
    <speed>10000</speed>
    <in>0.0</in>
    <inbytes>0</inbytes>
    <inbytesTotal>0</inbytesTotal>
    <out>0.0</out>
    <outbytes>0</outbytes>
    <outbytesTotal>472</outbytesTotal>
  </eth0.vxlan4>
</Network>
<TPS>
  <Total>0</Total>
  <SSL>0</SSL>
</TPS>
<VStotals>
  <ConnsPerSec>0</ConnsPerSec>
  <TotalConns>0</TotalConns>
  <BitsPerSec>0</BitsPerSec>
  <TotalBits>0</TotalBits>
  <BytesPerSec>0</BytesPerSec>
  <TotalBytes>0</TotalBytes>
  <PktsPerSec>0</PktsPerSec>
  <TotalPackets>0</TotalPackets>
</VStotals>
<Vs>
  <VAddress>172.20.0.207</VAddress>
  <VSPort>80</VSPort>
  <VSProt>tcp</VSProt>
  <Index>12</Index>
  <ErrorCode>0</ErrorCode>
  <Enable>1</Enable>
  <TotalConns>0</TotalConns>
```



```

    <TotalPkts>0</TotalPkts>
    <TotalBytes>0</TotalBytes>
    <TotalBits>0</TotalBits>
    <ActiveConns>0</ActiveConns>
    <BytesRead>0</BytesRead>
    <BytesWritten>0</BytesWritten>
    <ConnsPerSec>0</ConnsPerSec>
    <WafEnable>1</WafEnable>
    <Requests>0</Requests>
    <Incidents>0</Incidents>
    <Incidents_Hour>0</Incidents_Hour>
    <Incidents_Day>0</Incidents_Day>
    <Incidents_Dayover>0</Incidents_Dayover>
  </Vs>
</Vs>
  <VSAddress>172.20.0.237</VSAddress>
  <VSPort>443</VSPort>
  <VSProt>tcp</VSProt>
  <Index>7</Index>
  <ErrorCode>0</ErrorCode>
  <Enable>1</Enable>
  <TotalConns>0</TotalConns>
  <TotalPkts>0</TotalPkts>
  <TotalBytes>0</TotalBytes>
  <TotalBits>0</TotalBits>
  <ActiveConns>0</ActiveConns>
  <BytesRead>0</BytesRead>
  <BytesWritten>0</BytesWritten>
  <ConnsPerSec>0</ConnsPerSec>
  <WafEnable>0</WafEnable>
</Vs>
</Data>
</Success>
</Response>

```

統計情報について以下の表で説明します。

セクション	名前	追加情報
CPU	User (ユーザー)	ユーザーモードでの処理に消費されたCPUのパーセンテージ
	System (システム)	システムモードでの処理に消費されたCPUのパーセンテージ
	Idle (アイドル)	アイドル状態のCPUのパーセンテージ
	IOWaiting	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
	HWInterrupts	ハードウェア割り込みの割合



セクション	名前	追加情報
メモリ	SWInterrupts	ソフトウェア割り込みの割合
	Memused	使用されているメモリ量
	Percentmemused	使用されているメモリの割合
	Memfree	空きメモリ量
	Percentmemfree	空きメモリの割合
	ifaceID	インターフェイスのID番号
ネットワ ーク	Speed (速度)	リンクの速度
	In	インバウンド
	Out	アウトバウンド
VStotals	Total (TPS) (トータル (TP S))	1秒当たりのトータルのトランザクション数 (TPS)
	SSL (TPS)	1秒当たりのトータルのSSLトランザクション数 (TPS)
	ConnsPerSec	1秒当たりの接続数
	BitsPerSec	1秒当たりのビット数
	BytesPerSec	1秒当たりのバイト数
	PktsPerSec	1秒当たりのパケット数
	VSAAddress	仮想サービスのIPアドレス
	VSPort	仮想サービスのポート
	VSProt	仮想サービスのプロトコルtcpまたはudpを選択できます。
	Index	仮想サービスのインデックス (ID) 番号
Vs	ErrorCode	エラーコード
	Enable	仮想サービスが有効 (1) か無効 (0) かを表示します。
	TotalConns	トータルの接続数
	TotalPkts	トータルのパケット数
	TotalBytes	トータルのバイト数
	TotalBits	トータルのビット数
	ActiveConns	現在アクティブな接続のトータルの数
	BytesRead	読み込まれたトータルのバイト数
	BytesWritten	書き込まれたトータルのバイト数
	WafEnable	WAFが有効 (1) か無効 (0) かを表示します。仮想サービスでWAFが有効になっている場合、以下に示すWAF統計情報のみ表示されます。



セクション	名前	追加情報
	リクエスト	WAFにより処理されたトータルの要求数（ブロックされたかどうかにかかわらず、すべての要求が表示されます）。各接続につき2つの要求が記録されます（1つは受信要求、1つは送信要求）。
	Incidents	WAFにより処理されたトータルのイベント数（ブロックされた要求）
	Incidents_Hour	現在の時間内（xx. 00. 00以降）に発生したイベントの数
	Incidents_Day	真夜中（ローカル時刻）以降に発生したイベントの数
	Incidents_Dayover	1日のうちに、設定された警報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、AlertThresholdパラメーターを設定することで、仮想サービスごとに設定できます。詳細はセクション3.5.1を参照してください。

表3-21:統計情報の説明

3.8SDN統計情報

指定されたSDNコントローラーのデバイス情報を取得するには、次のコマンドを実行します。

`https://<LoadMasterIPAddress>/access/sdndeviceinfo?cid=<ControllerID>`

sdndeviceinfoコマンドの出力例を以下に示します。

```
<Response stat="200" code="ok">
  <Success>
    <Data>
      <controller id="62">
        <deviceinfo>
          <uid>openflow:151936205333838</uid>
          <name>br3</name>
          <type/>
          <vendor>Nicira, Inc.</vendor>
          <product>Open vSwitch</product>
          <firmware>2.3.1</firmware>
          <serial>None</serial>
          <ip>10.35.8.47</ip>
          <ifcount>3</ifcount>
          <status/>
          <portinfo>
            <port>
```



```
<id>1</id>
<name>prt3</name>
<state/>
<mac>52:34:63:89:05:17</mac>
<cur speed>current_speed=0</cur speed>
<max speed>max_speed=0</max speed>
</port>
<port>
  <id>2</id>
  <name>vnet5</name>
  <state/>
  <mac>fe:54:00:79:04:75</mac>
  <cur speed>current_speed=10000</cur speed>
  <max speed>max_speed=0</max speed>
</port>
<port>
  <id>local</id>
  <name>br3</name>
  <state/>
  <mac>8a:2f:67:8c:25:4e</mac>
  <cur speed/>
  <max speed/>
</port>
</port info>
</device info>
<device info>
  <uid>openflow:60003129350209</uid>
  <name>br1</name>
  <type/>
  <vendor>Nicira, Inc.</vendor>
  <product>Open vSwitch</product>
  <firmware>2.3.1</firmware>
  <serial>None</serial>
  <ip>10.35.8.47</ip>
  <if count>4</if count>
  <status/>
  <port info>
    <port>
      <id>3</id>
      <name>vnet6</name>
      <state/>
      <mac>fe:54:00:ed:2d:aa</mac>
      <cur speed>current_speed=10000</cur speed>
      <max speed>max_speed=0</max speed>
    </port>
    <port>
      <id>2</id>
      <name>prt11</name>
      <state/>
      <mac>de:8f:f3:cc:58:7a</mac>
      <cur speed>current_speed=0</cur speed>
      <max speed>max_speed=0</max speed>
```



```
</port>
<port>
  <id>1</id>
  <name>prt1</name>
  <state/>
  <mac>5e:b2:61:21:c8:20</mac>
  <cur speed>current_speed=0</cur speed>
  <max speed>max_speed=0</max speed>
</port>
<port>
  <id>local</id>
  <name>br1</name>
  <state/>
  <mac>36:92:91:35:d8:41</mac>
  <cur speed/>
  <max speed/>
</port>
</port info>
</device info>
<device info>
  <uid>openflow:130736296040257</uid>
  <name>br2</name>
  <type/>
  <vendor>Nicira, Inc.</vendor>
  <product>Open vSwitch</product>
  <firmware>2.3.1</firmware>
  <serial>None</serial>
  <ip>10.35.8.47</ip>
  <if count>4</if count>
  <status/>
  <port info>
    <port>
      <id>2</id>
      <name>vnet7</name>
      <state/>
      <mac>fe:54:00:85:ca:9f</mac>
      <cur speed>current_speed=10000</cur speed>
      <max speed>max_speed=0</max speed>
    </port>
    <port>
      <id>1</id>
      <name>prt2</name>
      <state/>
      <mac>8a:8d:81:78:10:8b</mac>
      <cur speed>current_speed=0</cur speed>
      <max speed>max_speed=0</max speed>
    </port>
    <port>
      <id>3</id>
      <name>prt22</name>
      <state/>
      <mac>d2:10:88:e8:98:f6</mac>
```



```

        <curspeed>current_speed=0</curspeed>
        <maxspeed>max_speed=0</maxspeed>
    </port>
    <port>
        <id>local</id>
        <name>br2</name>
        <state/>
        <mac>76:e7:6a:7c:17:41</mac>
        <curspeed/>
        <maxspeed/>
    </port>
</portinfo>
</deviceinfo>
<deviceinfo>
    <uid>openflow:217995646047043</uid>
    <name>br4</name>
    <type/>
    <vendor>Nicira, Inc.</vendor>
    <product>Open vSwitch</product>
    <firmware>2.3.1</firmware>
    <serial>None</serial>
    <ip>10.35.8.47</ip>
    <ifcount>4</ifcount>
    <status/>
    <portinfo>
        <port>
            <id>2</id>
            <name>vnet4</name>
            <state/>
            <mac>fe:54:00:ab:30:91</mac>
            <curspeed>current_speed=10000</curspeed>
            <maxspeed>max_speed=0</maxspeed>
        </port>
        <port>
            <id>1</id>
            <name>prt4</name>
            <state/>
            <mac>f2:fc:c5:31:1e:a0</mac>
            <curspeed>current_speed=0</curspeed>
            <maxspeed>max_speed=0</maxspeed>
        </port>
        <port>
            <id>3</id>
            <name>vnet8</name>
            <state/>
            <mac>fe:54:00:6a:f8:4e</mac>
            <curspeed>current_speed=10000</curspeed>
            <maxspeed>max_speed=0</maxspeed>
        </port>
        <port>
            <id>local</id>
            <name>br4</name>

```



```

    <state/>
    <mac>c6:44:11:0b:93:43</mac>
    <cursspeed/>
    <maxspeed/>
  </port>
</portinfo>
</deviceinfo>
</controller>
</Data>
</Success>
</Response>

```

この出力について以下の表で説明します。

セクション	名前	追加情報
デバイス情報	uid	デバイスの一意識別子 (UID)
	name (名前)	デバイスの名前
	vendor	デバイスのメーカー
	product	デバイスの種類
	firmware	デバイスのファームウェアバージョン
	serial	デバイスのシリアル番号
	ip	デバイスのIPアドレス
	ifcount	デバイス上のインターフェイスの数
ポート情報	status	デバイスの状態
	id	ポートのID番号
	name (名前)	ポートの名前
	mac	ポートのMACアドレス
	cursspeed	ポートの現在の速度
	maxspeed	ポートの最大速度

表3-22:SDNデバイス情報出力の説明

指定されたSDNコントローラー（およびロードマスター上で設定されている該当する仮想サービスの設定）のパス情報を取得するには、次のコマンドを実行します。

`https://<LoadMaster IPAddress>/access/sdnpathinfo?cid=<Controller ID>`

sdnpathinfoコマンドの出力例を以下に示します。

```

<Response stat="200" code="ok">
  <Success>
    <Data>
      <pathinfo>
        <path>
          <dir>fwd</dir>

```




```
<source>10.35.8.49</source>
<dest>10.35.8.89</dest>
<pathelem>
  <switch>
    <idx>0</idx>
    <name>baloo</name>
    <dpid>00:08:a0:1d:48:92:4f:80</dpid>
  </switch>
  <inport>
    <idx>25</idx>
    <name>25</name>
    <byte>3397596</byte>
  </inport>
  <outport>
    <idx>14</idx>
    <name>14</name>
    <byte>3395099</byte>
  </outport>
</pathelem>
<pathelem>
  <switch>
    <idx>1</idx>
    <name>bagheera</name>
    <dpid>00:08:40:a8:f0:87:04:80</dpid>
  </switch>
  <inport>
    <idx>15</idx>
    <name>15</name>
    <byte>3388430</byte>
  </inport>
  <outport>
    <idx>6</idx>
    <name>6</name>
    <byte>1566302</byte>
  </outport>
</pathelem>
</path>
<path>
  <dir>rev</dir>
  <source>10.35.8.89</source>
  <dest>10.35.8.49</dest>
  <pathelem>
    <switch>
      <idx>0</idx>
      <name>baloo</name>
      <dpid>00:08:a0:1d:48:92:4f:80</dpid>
    </switch>
    <inport>
      <idx>25</idx>
      <name>25</name>
      <byte>3397596</byte>
    </inport>
```



```

    <outport>
      <idx>14</idx>
      <name>14</name>
      <byte>3395099</byte>
    </outport>
  </pathelem>
<pathelem>
  <switch>
    <idx>1</idx>
    <name>bagheera</name>
    <dpid>00:08:40:a8:f0:87:04:80</dpid>
  </switch>
  <inport>
    <idx>15</idx>
    <name>15</name>
    <byte>3388430</byte>
  </inport>
  <outport>
    <idx>6</idx>
    <name>6</name>
    <byte>1566302</byte>
  </outport>
</pathelem>
</path>
</pathinfo>
</Data>
</Success>
</Response>

```

この出力について以下の表で説明します。

セクション	名前	追加情報
path	dir	経路の方向
	source	送信元IPアドレス
	dest	宛先IPアドレス
switch	idx	経路上にあるスイッチのインデックス番号
	name (名前)	スイッチの名前
	dpid	スイッチのデータパスID (DPID)



セクション	名前	追加情報
inport	idx	受信トラフィックのスイッチポート番号
	name (名前)	受信ポートの名前
	byte	このポートで送信されたバイト数
outport	idx	送信トラフィックのスイッチポート番号
	name (名前)	送信ポートの名前
	byte	このポートで送信されたバイト数

表3-23: SDN経路情報出力の説明

3.9実サーバー

実サーバーは、下記のいずれかのコマンドを使って管理できます。

```
https://<LoadMaster IP Address>/access/showrs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPAddr>&rsport=<RS-Port>
```

```
https://<LoadMaster IP Address>/access/de/rs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPAddr>&rsport=<RS-Port>
```

```
https://<LoadMaster IP Address>/access/de/rs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=!<RSIndex>
```

```
https://<LoadMaster IP Address>/access/addrs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPAddr>&rsport=<RS-Port>
```

```
https://<LoadMaster IP Address>/access/modrs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPAddr>&rsport=<RS-Port>
```

rsパラメーターには、整数 (ID)、(サブVSの) サービス名、IPアドレスを使用できます。showrsコマンドを使用すると、<RSIndex>エレメントにIDが設定されます。例:

```
...
<Rs>
<Status>Up</Status>
<VSIndex>1</VSIndex>
<RsIndex>3</RsIndex>
<Addr>10.154.201.3</Addr>
```



```

<Port>80</Port>
<Forward>nat</Forward>
<Weight>1000</Weight>
<Limit>0</Limit>
<Enable>Y</Enable>
<Critical>N</Critical>
</Rs>
...

```

Id	IP Address	Port	Forwarding method	Weight	Limit	Rules Status	Operation
5	10.154.11.73	80	nat	1000	0	1 Enabled	Disable Modify Delete

図 3-3: 実サーバーID

または、WUIの“Modify Virtual Service”（仮想サービスの編集）画面をチェックします。この画面にある“Real Servers”（実サーバー）セクションの“Id”列に、サーバーIDの一覧が表示されます。

rsパラメーターで<RSIndex>を使用する場合、その先頭に必ず感嘆符（‘!’）が追加されます。

例：

```
https://<LoadMaster IPAddress>/access/showrs?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=!<RSIndex>
```

実サーバーのIPアドレス（rsパラメーターに設定可能なIPアドレス）は、IPv4形式またはIPv6形式を使用できます。

- IPv4のアドレスの例：10.11.0.24
- IPv6のアドレスの例：fdce:9b36:e54f:110::40:14

criticalなどの一部のサブVSパラメーターは、サブVSのRsIndexを用いて編集する必要があります。例：

```
https://<LoadMaster IPAddress>/access/modrs?vs=<ParentVSIndex>&rs=!<RsIndexOfTheSubVS>&critical=<0/1>
```

サブVSに追加された実サーバーの設定を編集するには、サブVSの仮想サービスIndexおよび実サーバーのRsIndexを使用します。例：

```
https://<LoadMaster IPAddress>/access/modrs?vs=<SubVSIndex>&rs=!<RsIndex>&critical=<0/1>
```

‘addr’ と ‘modrs’ は、オプションとして下記のパラメータが許されます。

名前	種類	デフォルト	範囲	説明
----	----	-------	----	----



名前	種類	デフォルト	範囲	説明
weight	I	1000	1-65535	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。 サブVSの重みはmodrsコマンドで更新できません（親仮想サービス編集画面に表示される目的のサブVSの“Id”列に表示される値をrsに設定します）。
newport	I	<未設定>	3-65535 (change the Port of the Real Server)	実サーバーで使用されるポート
forward	S	nat	nat, route	使用されるフォワーディング方式の種類。デフォルトの方式はNATです。サーバーからの直接返信は、レイヤ4サービスでのみ使用可能です。
enable	B	1		実サーバーを有効/無効にします。
limit	I	0	0-100000	実サーバーがローテーションから外される前に、実サーバーに送信可能なオープン接続の最大数
non_local	B	0	0 = 無効 1 = 有効	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。 このオプションは、関連する仮想サービスにおいて、 Enable Non-Local Real Servers が有効になっており、 Transparency が無効になっているときのみ利用できます。
critical	B	0	0 = 無効 1 = 有効	このパラメーターが有効な場合、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。

表3-24: 実サーバーのパラメータ

もし、仮想サービスがL7モードならば、“forward”パラメータを‘route’に設定しても何の効果もありません。



3.9.1 実サーバーの有効化 / 無効化

3.9.1.1 実サーバーのグローバルな有効化/無効化

実サーバーをグローバルに有効化/無効化する（全ての仮想サービスを有効化/無効化する）には、以下のコマンドを使用します。

```
https://<LoadMaster IP Address>/access/enablers?rs=<IPAddr>
```

または、

```
https://<LoadMaster IP Address>/access/disablers?rs=<IPAddr>
```

実サーバーのIPアドレス（rsパラメーターに設定可能なIPアドレス）は、IPv4形式またはIPv6形式を使用できます。

- IPv4のアドレスの例: 10.11.0.24
- IPv6のアドレスの例: fdce:9b36:e54f:110::40:14

3.9.1.2 実サーバーのローカルな有効化/無効化

実サーバーをローカルに有効化/無効化する（ある1つの仮想サービスを無効化/有効化）するには、以下のコマンドを使用します。

```
https://<LoadMaster IP Address>/access/modrs?vs=<VirtualService IP Address>&port=<Port>&prot=<tcp/udp>&rs=<RealServer IP Address>&rport=<port>&enable=n
```

または、

```
https://<LoadMaster IP Address>/access/modrs?vs=<VirtualService IP Address>&port=<Port>&prot=<tcp/udp>&rs=<RealServer IP Address>&rport=<port>&enable=y
```

実サーバーのIPアドレス（rsパラメーターに設定可能なIPアドレス）は、IPv4形式またはIPv6形式を使用できます。

- IPv4のアドレスの例: 10.11.0.24
- IPv6のアドレスの例: fdce:9b36:e54f:110::40:14

3.10 ルールとチェック

コンテンツルールは、RESTful APIで管理できます。

3.10.1 ルールの表示

システムに設定しているルールは、下記のshowruleコマンドを使用して表示が可能です。

```
https://<LoadMaster IP Address>/access/showrule?[name=<Rule Name>]&[type=<0-4>]
```



パラメーターなしで `showrule` コマンドを実行すると、既存のルールがすべてリスト表示されます。表示されるリストは、ルール名、もしくはルールのタイプを指定することでフィルターができます。

ルールのタイプを下記に示します。

値	種類	説明
0	MatchContentRule	オリジナルのルール
1	AddHeaderRule	Rule to Add header field
2	DeleteHeaderRule	Rule to Delete a header field.
3	ReplaceHeaderRule	Rule to modify a header field.
4	ModifyURLRule	URL書き換えルール

表3-25: ルールのタイプ

3.10.2 ルールのシステムよりの削除

ルールは、`delrule` コマンドにより削除できます。

`https://<LoadMasterIPAddress>/access/delrule?name=<Rule Name>`

3.10.3 ルールは、`delrule` コマンドにより削除できます。

`addrule` コマンドおよび `modrule` コマンドを使用すると、ルールを追加/変更できます。

`https://<LoadMasterIPAddress>/access/delrule?name=<Rule Name>`

`https://<LoadMasterIPAddress>/access/delrule?name=<Rule Name>`

ルールの種類によりますが、下記のパラメータを設定できます。ルール作成時に“type”を指定しなかった場合、デフォルト値の0 (MatchContentRule) になります。ルール変更コマンドの使用時、“Type”を指定しなかった場合は、タイプは変更されません。

Type 1のAddHeaderRuleの追加/変更以外は、`pattern` パラメータを付加しなければなりません。

Type 0 (MatchContentRule)

名前	種類	デフォルト	範囲	追加情報
----	----	-------	----	------



名前	種類	デフォルト	範囲	追加情報
matchtype	S	regex	<ul style="list-style-type: none"> - regex - prefix - postfix 	ルールにより実行される照合の種類
inchoost	B	N		照合を行う前に、リクエストURIの先頭にホスト名を追加します。
nocase	B	N		文字列比較の際に大文字と小文字を区別しません。
negate	B	N		マッチ文の意味を反転します。
incquery	B	N		照合を行う前に、URIにクエリ文字列を追加します。
header (ヘッダー)	S	<未設定>	以下を参照	照合するヘッダーフィールド名。ヘッダーフィールドが設定されていない場合、デフォルトでURLにて照合が行われます。リクエストの本文と照合するには、これをbodyに設定します。
pattern	S	<未設定>		照合パターン

表3-26: ルールのタイプ0のパラメータ

“header” パラメータは、オプションでヘッダー名がマッチした場合のみValueとしての“pattern”を変更可能です。

Type 1 (AddHeaderRule)

名前	種類	デフォルト	追加情報
header (ヘッダー)	S	<未設定>	追加するヘッダーフィールド名
replacement	S	<未設定>	置換文字列

表3-27: ルールのタイプ1のパラメータ

Type 2 (DeleteHeaderRule)

名前	種類	デフォルト	追加情報
pattern	S	<未設定>	照合パターン

表3-28: ルールのタイプ2のパラメータ

Type 3 (ReplaceHeaderRule)



名前	種類	デフォルト	追加情報
header (ヘッダー)	S	<未設定>	置換対象のヘッダーフィールド名
replacement	S	<未設定>	置換文字列
pattern	S	<未設定>	照合パターン

表3-29: ルールのタイプ3のパラメータ

Type 4 (ModifyURLRule)

名前	種類	デフォルト	追加情報
replacement	S	<未設定>	URL変更方法
pattern	S	<未設定>	照合パターン

表3-30: ルールのタイプ4のパラメータ

3.10.4 実サーバーへのルールの追加/削除

ルールは、`addrerule` と `delrrule` コマンドを使用して実サーバーに追加、もしくは実サーバーより削除できます。

```
https://<LoadMaster IP Address>/access/addrerule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPAddr>&rsport=<RS-Port>&rule=<RuleName>
```

```
https://<LoadMaster IP Address>/access/delrrule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPAddr>&rsport=<RS-Port>&rule=<RuleName>
```

`rs`パラメーターには整数 (ID) も使用できます。`showvs`コマンドを使用すると、`<RSIndex>`エレメントにID (実サーバーのインデックス) が設定されます。例:

```
...
<Rs>
<Status>Up</Status>
<VSIndex>1</VSIndex>
<RsIndex>3</RsIndex>
<Addr>10.154.201.3</Addr>
<Port>80</Port>
<Forward>nat</Forward>
<Weight>1000</Weight>
<Limit>0</Limit>
<Enable>Y</Enable>
<Critical>N</Critical>
</Rs>
...
```

3.10.5 サブVSのルールの追加/削除

`addrerule`コマンドおよび`delrrule`コマンドを使用すると、コンテンツルールをサブVSに追加 (またはコンテンツルールをサブVSから削除) することができます。



```
https://<LoadMaster IP Address>/access/addrerule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=!<Rs Index Of Sub VS>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/delrsrule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rs=!<Rs Index Of Sub VS>&rule=<Rule Name>
```

サブVSに割り当てられている実サーバーにコンテンツルールを追加するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/addrerule?vs=<VS Index Of Sub VS>&rs=<Real Server IP Address>&rport=<Real Server Port>&rule=<Rule Name>
```

コンテンツルールをサブVSに追加するには、追加するルールの種類に応じて、`addprerule` コマンド、`addresponserule` コマンド、`addrequestrule` コマンドを使用します。

```
https://<LoadMaster IP Address>/access/addprerule?vs=<VS Index Of Sub VS>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/addresponserule?vs=<VS Index Of Sub VS>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/addrequestrule?vs=<VS Index Of Sub VS>&rule=<Rule Name>
```

コンテンツルールをサブVSから削除するには、削除するルールの種類に応じて、`delprerule` コマンド、`delresponserule` コマンド、`delrequestrule` コマンドを使用します。

```
https://<LoadMaster IP Address>/access/delprerule?vs=<VS Index Of Sub VS>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/delresponserule?vs=<VS Index Of Sub VS>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/delrequestrule?vs=<VS Index Of Sub VS>&rule=<Rule Name>
```

`Rs Index` または `Vs Index` を取得するには、`listvs` コマンドを実行します。詳細は [セクション 3.5.1](#) を参照してください。

3.10.6 仮想サービスのルールの追加

ルールは、`addprerule`、`addresponserule`、および `addrequestrule` コマンドで仮想サービスに追加できます。

```
https://<LoadMaster IP Address>/access/addprerule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/addresponserule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rule=<Rule Name>
```

```
https://<LoadMaster IP Address>/access/addrequestrule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rule=<Rule Name>
```



3.10.7 仮想サービスのルールの削除

ルールは、`delprerule`、`delresponserule`、および`delrequestrule`コマンドで仮想サービスから削除できます。

```
https://<LoadMaster IP Address>/access/delprerule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rule=<RuleName>
```

```
https://<LoadMaster IP Address>/access/delresponserule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rule=<RuleName>
```

```
https://<LoadMaster IP Address>/access/delrequestrule?vs=<IPAddr>&port=<Port>&prot=<tcp/udp>&rule=<RuleName>
```

3.10.8 Check Parameters (チェック用パラメータ)

Service Checkパラメータは、以下のコマンドで取得できます。

```
https://<LoadMaster IP Address>/access/showhealth?
```

`showhealth`コマンドの出力には、`RetryInterval`、`Timeout`、`RetryCount`の値が表示されます。

Service Checkパラメータは、以下のコマンドで変更できます。

```
https://<LoadMaster IP Address>/access/modhealth?RetryInterval=<Interval Value>&Timeout=<Timeout Value>&RetryCount=<Count Value>
```

名前	種類	範囲	デフォルト	追加情報	必須
RetryInterval	I	9-3600	120	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。	N
Timeout	I	4-60	20	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。	N
RetryCount	I	2-15	2	ダウン状態として記録され、負荷分散プールから削除されるヘルスチェックの連続失敗回数です。	N

表3-31: modhealthのパラメータ

Adaptive Checkパラメータは、以下のコマンドで取得できます。



`https://<LoadMaster IP Address>/access/showadaptive?`

Adaptive Checkパラメータは、以下のコマンドで変更できます。

`https://<LoadMaster IP Address>/access/modadaptive?AdaptiveURL=<URL>&AdaptivePort=<Port>
&<AdaptiveInterval=<Interval>&MinPercent=%Value>`

3.11 証明書とセキュリティ

3.11.1 証明書の管理

証明書は、以下のコマンドで管理できます。

現在インストールされている証明書のリストを表示するには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/listcert`

証明書をアップロードするには、次のcURLコマンドを実行します。

`curl -X POST --data-binary "@<Filename>.<Extension>" -k https://<LoadMaster IP Address>/
access/addcert?cert=<Filename>.<Extension>&password=<Password>&replace=<0/1>`

名前	種類	デフォルト	追加情報	必須
cert	F	<未設定>	このパラメーターは、ファイル名とそれに続く拡張子を設定します（例： certname.pem ）。証明書のキーをアップロードする場合、証明書とキーを同じファイル内に置いてください。	Y
password	S	<未設定>	証明書作成時に使用した、証明書を保護するための（任意の）パスワード	N
replace	B	<未設定>	0 - 置き換えない 1 - 置き換える ロードマスターにすでに存在する証明書を置き換える場合、パラメーター replace を1に設定します。新たに証明書をアップロードする場合、 replace を0に設定します。	N

表: パラメーター-addcert

`https://<LoadMaster IP Address>/access/delcert?cert=<CertName>`



仮想サービスに割り当てられている証明書削除することはできません。証明書を削除する前に、仮想サービスに対する証明書の割り当てを解除してください。

`https://<LoadMaster IPAddress>/access/addintermediate?cert=<CertName>`

`https://<LoadMaster IPAddress>/access/delintermediate?cert=<CertName>`

`https://<LoadMaster IPAddress>/access/backupcert?password=<Password>`

`https://<LoadMaster IPAddress>/access/restorecert?password=<Password>&Type=<type>`

パスワード（パスフレーズ）は英数字で指定する必要があり、大文字と小文字が区別されます。文字数の下限は7、上限は64です。

`type`パラメーターには3つの値を指定できます。

- `Full` - すべての仮想サービス証明書とインターミディエート証明書
- `Third` - インターミディエート証明書のみ
- `Vs` - 仮想サービス証明書のみ

`type`パラメーターの値は、大文字と小文字が区別されます。このパラメーターを設定する際は、小文字を使用してください。

`Replace`は、既存の証明書を同じ名前で置き換えるかどうかをロードマスターに通知するためのブール値です。

`get`および`set`コマンドで管理できる証明書関連のパラメータの詳細については、表3-32を参照してください。

名 種 前 類	追加情報
a	S
d	
m	
i	
n	
c	
e	
r	
t	



名前	種類	追加情報
sslcertificate	B	
sslcertificate	S	このパラメーターは、HAを使用しているときのみ関係します。

表3-32: 証明書のパラメータ

3.11.2 暗号セット

以下のコマンドを使用して、カスタム暗号セットを編集することができます。

システム定義の暗号セットを編集したり削除したりすることはできません。

3.11.2.1 カスタム暗号セットの編集/カスタム暗号セットの新規作成

`modifycipherset` コマンドを使って、既存のカスタム暗号セットの更新またはカスタム暗号セットの新規作成が行えます。

既存のカスタム暗号セット名を指定すると、その暗号セットが更新されます。新しい名前を使用すると、カスタム暗号セットが新たに作成されます。



例：

```
https://<LoadMaster IP Address>/access/modifycipherSet?name=<CustomCipherSetName>&value=<Cipher(s)>
```

コロン（“:”）で区切って複数の暗号化方式を割り当てることができます。

3.11.2.2 既存の暗号セットに関する詳細の取得

getcipherSetコマンドを使って、指定した暗号セットに含まれる暗号化方式の一覧を取得することができます。例：

エラー！ハイパーリンクの参照に誤りがあります。>

パラメーターnameの有効な値は以下のとおりです。

- デフォルト
- Default_NoRc4
- BestPractices
- Intermediate_compatibility
- Backward_compatibility
- WUI
- FIPS
- Legacy
- <NameOfCustomCipherSet>

この値は大文字と小文字が区別されます。

3.11.2.3 カスタム暗号セットの削除

delcipherSetコマンドは使って、既存の暗号セットを削除することができます。例：

```
https://<LoadMaster IP Address>/access/delcipherSet?name=<CustomCipherSetName>
```

仮想サービスに割り当てられているカスタム暗号セットは削除できません。仮想サービスに割り当てられている暗号セットに対してこのコマンドを実行すると、“Command Failed: Cipher set in use”（コマンドの実行に失敗しました：暗号セットは使用中です）というエラーメッセージが表示されます。暗号は使用中です。



3.11.3 Remote Access (リモートアクセス)

`get`および`set`コマンドで管理できるリモートアクセス関連のパラメータの詳細については、表3-33を参照してください。`get`および`set`コマンドについてはセクション2.4を参照してください。

名前	種類	範囲	追加情報
<code>admingw</code>	A		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。
<code>enableapi</code>	B		プログラム可能なコマンドAPIインターフェイスを有効にします。 注:これを無効にすると、APIにアクセスできなくなります。
<code>geoclients</code>	A		ロードマスターからサービスステータス情報を取得可能なGEOロードマスターのアドレスを設定します。
<code>geosshport</code>	I	3-65530	GEOロードマスターが相互に通信するのに使用するポート
<code>sshaccess</code>	B		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。
<code>sshiface</code>	S		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。
<code>sshport</code>	I	3-65530	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。
<code>wuiaccess</code>	B		WUIへのアクセスを有効/無効にします。
<code>wuiiface</code>	I		WUIへのインターフェイスを指定します。
<code>wuiport</code>	I		WUIにアクセスするためのポートを指定します。 デフォルト値は443
<code>geopartners</code>	A		GEOロードマスターパートナーのIPアドレスを設定します。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。 注:GEOロードマスターのパートナーを設定する前に、正しい設定/推奨設定を持つ該当するGEOロードマスターのバックアップを作成する必要があります。そして、このバックアップを、オリジナルのロードマスターのパートナーとなるロードマスターに保存する必要があります。詳細および手順については、 GEO 機能説明 を参照してください。



名前	種類	範囲	追加情報
multihomedwui	B		複数のインターフェイスからのWUIへのアクセスを許可します。このオプションを有効にすると、メインの管理用インターフェイスを除き、WUIへのアクセスを許可するかどうかをインターフェイスごとに設定できるようになります。
SSHPreAuth	S	5,000文字まで入力できます。	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。空白文字は、%20を入力してエスケープする必要があります。 このフィールドには5,000文字まで入力できます。5,000文字を超える部分は表示されません。

表3-33: リモートアクセスのパラメータ

3.11.3.1 管理用アクセスの設定

関連するパラメーターとともに以下のコマンドを実行すれば、Webの管理用アクセスインターフェイスおよび管理用デフォルトゲートウェイを1つの手順で設定できます。

```
https://<LoadMaster IP Address>/access/setadminaccess?wuiiface=<WUI Interface address>&wuiport=<Port>&wuidefaultgateway=<Default Gateway Address>
```

以下の表に、setadminaccessコマンドに関するパラメーターを示します。

パラメーター	種類	範囲	追加情報	必須
wuiiface	I	有効なインターフェイスのインデックス	既存のインターフェイスのインデックスこのインデックス番号は、ロードマスターWUIにおけるインターフェイス番号に対応します。例えば、eth0のインデックスは0です。	Y
wuiport	I	3-65535	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。	Y
wuidefaultgateway	S	有効なIPアドレス	デフォルトでないインターフェイスからロードマスターを管理する場合、管理用トラフィックの他のデフォルトゲートウェイはこのパラメーターでのみ指定できます。	N

表3-34: パラメーターSetAdminAccess

3.11.4 管理用WUIへのアクセス

getコマンドおよびsetコマンドで管理できる管理用WUIアクセス関連のパラメーターの詳細については、表3-35を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	範囲	説明
----	----	----	----



名前	種類	範囲	説明
wuicipherset	S	有効な値は以下のとおりです。 <ul style="list-style-type: none"> - デフォルト - Default_NoRc4 - BestPractices - Intermediate_compatibility - Backward_compatibility - WUI - FIPS - Legacy - <NameOfCustomCipherSet> 	ロードマスターWUIで使用する暗号セットを指定します。
sessioncontrol	B		セッション管理を有効/無効にします。
sessionbasicauth	B	0 - 無効 1 - 有効	sessioncontrol パラメーターと sessionbasicauth パラメーター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）。
sessionidletime	I	60-86400	ユーザーがログアウトされる前に、WUIがアイドル状態でいられる時間を秒で指定します。60~86400秒の範囲で設定できます。
sessionmaxfailattempts	I	1-999	ユーザーアカウントがロックされるまでの試行回数
sessionconcurrent	S	0-9	1人のユーザーがロードマスターに同時に接続可能な最大の接続数を制限します（値0は制限なしを意味します）。



名前	種類	範囲	説明
WUIPreAuth	S	5,000文字 まで入力 できます。	<p>ロードマスターの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。このパラメーターにはプレーンテキストまたはHTMLコードを設定することができます。このフィールドにはJavaスクリプトは入力できません。空白文字は%20に置き換える必要があります。</p> <p>このフィールドには5,000文字まで入力できます。5,000文字を超える部分は表示されません。</p>
WUITLSProtocols	I	0 - 14 ビットマスク	<p>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します。このプロトコルは、ビットマスク値を用いて有効/無効にできます。どの値がどの設定に対応するかは、表3-36を参照してください。</p>

表3-35: 管理用WUIへのアクセスに関するパラメーター

Number	SSLv3	TLS1.0	TLS1.1	TLS1.2
0	有効	有効	有効	有効
1	無効	有効	有効	有効
2	有効	無効	有効	有効
3	無効	無効	有効	有効
4	有効	有効	無効	有効
5	無効	有効	無効	有効
6	有効	無効	無効	有効
7	無効	無効	無効	有効
8	有効	有効	有効	無効
9	無効	有効	有効	無効
10	有効	無効	有効	無効
11	無効	無効	有効	無効
12	有効	有効	無効	無効
13	無効	有効	無効	無効
14	有効	無効	無効	無効

表3-36: WUITLSProtocolsビットマスクの値



3.11.5 OCSPの設定

`get`コマンドと`set`コマンドで管理可能なオンライン証明書状態プロトコル（OCSP）に関するパラメーターの詳細を以下の表に示します。`get`および`set`コマンドについてはセクション2.4を参照してください。

名前	種類	追加情報
OCSPPort	I	OCSPサーバーのポートです。
OCSPUseSSL	B	SSLを使用してOCSPサーバーに接続します。
OCSPOnServerFail	B	OCSPサーバーが有効な応答を返したのものとして（クライアント証明書が有効であるものとして）OCSPサーバー接続障害またはタイムアウトを処理します。
OCSPServer	A	OCSPサーバーのアドレスです。
OCSPUrl	S	OCSPサーバーにアクセスするためのURLです。

3.11.6 ハードウェアセキュリティモジュール（HSM）の設定

3.11.6.1 HSM詳細の取得

HSMの詳細は、以下のコマンドで取得できます。

```
https://<LoadMaster IP Address>/access/showhsm
```

3.11.6.2 HSMの設定

HSMは以下のコマンドで設定できます。

```
https://<LoadMaster IP Address>/access/hsmconfig?<parameter>=<value>&<parameter>=<value>...</pre>

```

`hsmconfig`コマンドでは以下のオプションパラメーターが使用できます。

名前	種類	説明
safeaddr	A	使用するSafenet HSM ユニットのアドレスを指定します。



名前	種類	説明
clpass	S	<p>ロードマスターがHSMにアクセスできるように、HSMのパーティションの管理者パスワードを指定します。</p> <p>HSMは複数のユーザーを扱うことができます。各ロードマスターは、指定された名前でHSMにアクセスします。そのため、複数のロードマスターが複数の名前を使用して同じパーティションにアクセスできます。</p> <p>また、複数のパーティションを用意して、設定されたパーティションのいずれかに各ロードマスターがアクセスするようにすることもできます。</p>
enable	B	<p>Safenet HSMを有効/無効にします。</p> <p>0 - 無効</p> <p>1 - 有効</p>

表3-37: hsmconfigコマンドのオプションパラメーター

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。

3.11.6.3 CA証明書のアップロード

HSMからダウンロードされたCA証明書をアップロードするには、以下のcURLコマンドを実行します。

```
curl -X POST --data-binary "@<CertificateName.extension>" -k https://<LoadMasterIPAddress/access/hsmuploadca
```

3.11.6.4 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証明書を生成するには、以下のコマンドを使用します。



ロードマスターのFQDNにclcertnameを設定する必要があります。指定したclcertnameは、HSMのclient registerコマンドで使用されません。

`https://<LoadMaster IP Address>/access/hsmclientcert?clcertname=<name>`

3.12 Interfaces (インターフェイス)

3.12.1 インターフェイス詳細の取得

インターフェイスの詳細は、以下のコマンドで取得できます。

`https://<LoadMaster IP Address>/access/showiface?interface=<InterfaceID>`

各インターフェイスのインターフェイスIDを表示するには、statsコマンドを実行します。インターフェイスIDは、XML出力でifaceIDとして表示されます。statsコマンドの詳細については、[セクション3.7](#)を参照してください。

3.12.2 インターフェイス詳細の変更

インターフェイスのパラメータは、以下のコマンドで変更できます。

`https://<LoadMaster IP Address>/access/modiface?interface=<InterfaceID>&<parameter>=<value>`

1回の呼び出しにつき1つのパラメータのみ変更できます。このパラメータは以下の順序でチェックされます。

名前	種類	説明	追加情報
interface	I	変更するインターフェイスの番号	各インターフェイスのインターフェイスIDを表示するには、statsコマンドを実行します。インターフェイスIDは、XML出力でifaceIDとして表示されます。statsコマンドの詳細については、 セクション3.7 を参照してください。
addr	S	IPアドレス	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します。
mtu	I	MTUサイズ 範囲: 512-9216	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変更します。



名前	種類	説明	追加情報
hacheck	B	0 - HAチェックで使 しない 1 - HAチェックで使 用する	このパラメーターは、HA構成でのみ必要です。このインターフェイスをHAチェックで使用するかどうかを指定します。
gwiface	B	このインターフェイスをデフォルトゲートウェイとして使用する	これがネットワークゲートウェイインターフェイスの場合に指定します。
bondmode	I	1 = active-backup 4 = 802.3ad	bondmodeは、ボンディングされたインターフェイスから送信されたトラフィックが実際のインターフェイスでどのように分散されるかを決定します。
partner	A	パートナーマシンのIPアドレス (HAのみ)	このパラメーターは、HAモードのロードマスターにのみ関係します。
shared	A	共有アドレスのIPアドレス (HAのみ)	このパラメーターは、HAモードのロードマスターにのみ関係します。
adminwuienable	B	このオプションは、“multi homedwui”パラメータがyesに設定されているときのみyes (1)にできる。	adminwuienableとmultihomedwuiのパラメーターを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、およびそのインターフェイスに設定された追加アドレスからWUIにアクセスできます。 パラメーターmultihomedwuiの詳細については、セクション3.11.3を参照してください。
geotraffic	B	0 - GEOのリクエストと応答で使 用しない 1 - GEOのリクエストと応答で使 用する	このインターフェイスをGEOのリクエストと応答で使用するかどうかを指定します。

表3-38: インターフェイスパラメータの変更

3.12.3 追加アドレス

追加アドレスは、以下のコマンドでインターフェイスに追加できます。

```
https://<LoadMaster IP Address>/access/addadditional?interface=<InterfaceID>&addr=<AdditionalAddressIP/prefix>
```

追加アドレスは、以下のコマンドでインターフェイスから削除できます。

```
https://<LoadMaster IP Address>/access/deladditional?interface=<InterfaceID>&addr=<AdditionalAddressIP/prefix>
```



3.12.4 ボンディングインターフェイス

ボンディングインターフェイスは、以下のコマンドで作成できます。

```
https://<LoadMaster IP Address>/access/createbond?interface=<InterfaceID>
```

インターフェイスは、以下のコマンドでボンディングインターフェイスから削除できます。

```
https://<LoadMaster IP Address>/access/unbond?interface=<InterfaceID>
```

インターフェイスは、以下のコマンドでボンディングインターフェイスに追加できます。

```
https://<LoadMaster IP Address>/access/addbond?interface=<InterfaceID>&bond=<BondID>
```

各インターフェイスのインターフェイスIDを表示するには、**stats**コマンドを実行します。インターフェイスIDは、XML出力で **ifaceID** として表示されます。**stats**コマンドの詳細については、[セクション3.7](#)を参照してください。

BondIDは、WUIのメインメニューの**Interfaces**セクションにおけるボンディング番号です。例えば、**bnd2**は値2のBondIDを持ちます。

3.12.5 VLANs

VLANは、以下のコマンドで削除できます。

```
https://<LoadMaster IP Address>/access/delbond?interface=<InterfaceID>
```

新しいVLANは、以下のコマンドでインターフェイスに追加できます。

```
https://<LoadMaster IP Address>/access/addvlan?interface=<InterfaceID>&vlanid=<ID>
```

VLANは、以下のコマンドでインターフェイスから削除できます。

```
https://<LoadMaster IP Address>/access/delvlan?interface=<InterfaceID>&vlanid=<ID>
```

3.12.6 VXLANs

次のいずれかのコマンドを実行することで、VXLANを追加できます。

```
https://<LoadMaster IP Address>/access/addvxlan?interface=<InterfaceID>&vnid=<VXLANNetworkIdentifier>&group=<GroupMulticastIP>
```

```
https://<LoadMaster IP Address>/access/addvxlan?interface=<InterfaceID>&vnid=<VXLANNetworkIdentifier>&remote=<RemoteVTEPIPAddress>
```

次のコマンドを実行することで、VXLANを追加できます。

```
https://<LoadMaster IP Address>/access/delvxlan?interface=<InterfaceID>
```



VXLANの詳細の編集（IPアドレスの設定など）を行うには、**modiface**コマンドを使用してください。詳細は**セクション3.12.2**を参照してください。

VXLANの詳細を取得するには、**showiface**コマンドを使用します。詳細は**セクション3.12.1**を参照してください。

3.13 ホストとDNSの設定

ホストとDNSの設定に関するパラメーターは、**get**コマンドと**set**コマンドで管理できます。例：

`https://<LoadMaster IPAddress>/access/get?param=hostname`

名前	種類	追加情報
Hostname	S	ローカルマシンのホスト名を設定します。
ha1hostname	S	マスター側ロードマスターのホスト名を設定します。
ha2hostname	S	スレーブ側ロードマスターのホスト名を設定します。
namserver	A	ロードマスターでローカルに名前解決するためのDNSサーバーのIPアドレス
searchlist	S	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指定します。
dnssecclient	B	ロードマスターのDNSSECクライアント機能を有効または無効にします。DNSSECを有効にするには、ネームサーバーを1つ以上設定する必要があります。この設定を変更後、変更内容を適用するには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、両方のデバイスで個別にパラメーターを設定してください。 0 = 無効 1 = 有効

表3-39: ローカルDNSのパラメータ

3.13.1 ローカル名前解決ホスト

既存のローカル名前解決ホストのリストを表示するには、**gethosts**コマンドを実行します。例：

`https://<LoadMaster IPAddress>/access/gethosts`



ホストIPアドレスおよびホストFQDNを追加するには、以下の書式でaddhostsentryコマンドを実行します。

```
https://<LoadMaster IP Address>/access/addhostsentry?hostip=<Host IP Address>&hostfqdn=<Host FQDN>
```

ホストIPアドレスおよびホストFQDNを削除するには、以下の書式でdelhostsentryコマンドを実行します。

```
https://<LoadMaster IP Address>/access/delhostsentry?hostip=<Host IP Address>
```

3.14 Route Management (ルート管理)

3.14.1 デフォルト・ゲートウェイ

getコマンドおよびsetコマンドで管理できるルート管理関連のパラメーターの例を以下に示します。

```
https://<LoadMaster IP Address>/access/get?param=dfiltgw
```

名前	種類	デフォルト	追加情報
dfiltgw	A (IPv4)	<未設定>	インターネットとの接続に使用するIPv4デフォルトゲートウェイを指定します。
dfiltgwv6	A (IPv6)	<未設定>	インターネットとの接続に使用するIPv6デフォルトゲートウェイを指定します。

表3-40: ルート管理のパラメータ

3.14.2 追加ルート

追加ルートは、以下のコマンドで追加または削除できます。

```
https://<LoadMaster IP Address>/access/addroute?dest=<Dest IP Address>&gateway=<Gateway IP Address>
```

```
https://<LoadMaster IP Address>/access/delroute?dest=<Dest IP Address>
```

3.14.3 Packet Routing Filter (パケット・ルーティング・フィルター)

このセクションのコマンドは、全体的なパケットルーティングフィルターオプションに関係しています。パケットフィルターはデフォルトで有効になっています。GEOが有効な場合、パケットルーティングを無効にすることはできません。GEOを有効/無効にするコマンドについては、Section 3.6.5を参照してください。

パケットルーティングが有効かどうかを確認するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/acicontrol?isenabled
```



パケットルーティングフィルターを有効/無効にするには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/aclcontrol?enable=<0/1>`

GEOが有効な場合、パケットルーティングを無効にすることはできません。

3.14.4 VPN管理

3.14.4.1 VPN接続の新規作成

仮想プライベートネットワーク（VPN）接続を新規に作成するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/createvpncon?name=<VPNname>`

3.14.4.2 既存のIPsec接続の削除

以下のコマンドを実行すると、既存のIPsec接続を削除できます。

`https://<LoadMaster IP Address>/access/deletevpncon?name=<VPNname>`

3.14.4.3 VPNアドレスの設定

以下のコマンドを実行すると、すべてのVPNアドレスを一度に設定できます。

`https://<LoadMaster IP Address>/access/setvpnaddr?name=<VPNname>&localip=<Local IP Address>&localsubnets=<Local Subnet Address(es)>&remoteip=<Remote IP Address>&remotesubnets=<Remote Subnet Address(es)>`

setvpnaddrコマンドを実行する際は、以下に示すパラメーターがすべて必要です。

名前	種類	デフォルト	追加情報
localip	String	追加情報を参照	非HAモードの場合、デフォルト値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インターフェイスのIPアドレス）になります。 HAモードの場合、デフォルト値は共有IPアドレスになります。



名前	種類	デフォルト	追加情報
localsubnets	String	追加情報を参照	接続のローカル側のサブネットを設定します。/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。localipが設定されている場合、localsubnetは自動的に設定されます。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。
remoteip	String	<未設定>	接続のリモート側のIPアドレスを設定します。
remotesubnets	String	<未設定>	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。

表3-41: setvpnaddrパラメーター

これらのパラメーターは、以下のコマンドを使用して個別に設定することもできます。

Local IP Addressを設定するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/setvpnlocalip?name=<VPNname>&localip=<Local IP Address>
```

Local Subnet Addressを設定するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/setvpnlocalsubnets?name=<VPNname>&localsubnets=<Local Subnet Address(es)>
```

Remote IP Addressを設定するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/setvpnremoteip?name=<VPNname>&remoteip=<Remote IP Address>
```

Remote Subnet Addressを設定するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/setvpnremotesubnets?name=<VPNname>&remotesubnets=<Remote Subnet Address(es)>
```

3.14.4.4 前方秘匿性オプションの設定

特定の接続に対してPerfect Forward Secrecy (前方秘匿性) オプションを有効にするには、以下のオプションを実行します。



```
https://<LoadMaster IP Address>/access/setvpnpfsenable?name=<ConnectionName>
```

特定の接続に対してPerfect Forward Secrecy（前方秘匿性）オプションを無効にするには、以下のオプションを実行します。

```
https://<LoadMaster IP Address>/access/setvpnpfsdisable?name=<ConnectionName>
```

3.14.4.5 秘密鍵

秘密鍵の詳細を設定するには、以下のコマンドを実行します。

エラー! ハイパーリンクの参照に誤りがあります。>

このコマンドを機能させるには、すべてのパラメーターが必要です。

名前	種類	デフォルト	追加情報
localid	String	localipと同じ。	接続のローカル側のID。
remoteid	String	<未設定>	接続のリモート側のID。これはremoteipと同じ値を使用できます。
key	String	<未設定>	プレシェアードキー（PSK）の文字列。これは、Azure側で生成/管理されるプレシェアードキーです。キーの長さは、16文字以上64文字以下でなければなりません。

表3-42: 秘密鍵のパラメータ

3.14.4.6 接続の開始

接続を開始するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/startvpncon?name=<VPNName>
```

3.14.4.7 接続の停止

接続を停止するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/stopvpncon?name=<VPNName>
```

3.14.4.8 接続状態の取得

接続状態を表示するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/getvpnstatus?name=<VPNName>
```

3.14.4.9 既存の全接続の表示

既存のすべてのVPN接続に関する詳細を表示するには、以下のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/listvpns
```



3.14.4.10 IKEデーモンの停止

インターネット鍵交換（IKE）デーモンを停止するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/stopikedamon`

3.14.4.11 IKEデーモンの起動

IKEデーモンを起動するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/startikedamon`

3.14.4.12 IKEデーモンの状態取得

IKEデーモンの状態を表示するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/statusikedamon`

3.15 Access Lists (アクセスリスト)

アクセス制御リスト（ACL）コマンドでは、ACLのオン/オフの切り替えと、関連パラメータの設定および取得を実行できます。仮想サービスIPアドレスの指定なしでACLコマンドを実行すると、グローバルACLに対して実行されます。仮想サービスIPアドレスが設定されている場合、このコマンドは特定の仮想サービスのACLに対してのみ実行されます。

‘All Permissions’ の権限を持つユーザーのみグローバルコマンドを実行できます。

‘All Permissions’ および ‘Virtual Service’ の権限を持つユーザーは、仮想サービス固有のコマンドを実行できます。

全体的なブラック/ホワイトリストのアドレスの表示:

`https://<LoadMaster IP Address>/access/aclcontrol?list=<ListType>`

リストの種類
black (ブラック)
white (ホワイト)

表3-43: アクセスリストの種類

全体的なブラック/ホワイトリストへの（または全体的なブラック/ホワイトリストからの）アドレスの追加/削除:



`https://<LoadMaster IP Address>/access/aclcontrol?add=<ListType>&addr=<IP Address/CIDR>`

`https://<LoadMaster IP Address>/access/aclcontrol?del=<ListType>&addr=<IP Address/CIDR>`

addrにはIPv4またはIPv6のアドレスを指定できます。

特定の仮想サービスに関するブラック/ホワイトリストの表示:

`https://<LoadMaster IP Address>/access/aclcontrol?listvs=<ListType>&vsip=<Virtual Server IP Address>&vsprot=<Virtual Server Protocol>&vsport=<Virtual Server Port>`

仮想サーバーのプロトコル
tcp
udp

表3-44: 仮想サーバーのプロトコル

CIDRが指定されていない場合、システムは独自のデフォルト値（/32）を使用します。

仮想サービスのブラック/ホワイトリストへの（またはブラック/ホワイトリストからの）アドレスの追加/削除:

`https://<LoadMaster IP Address>/access/aclcontrol?addvs=<ListType>&vsip=<Virtual Server IP Address>&vsprot=<Virtual Server Protocol>&vsport=<Virtual Server Port>&addr=<IP Address To Add/CIDR>`

`https://<LoadMaster IP Address>/access/aclcontrol?delvs=<ListType>&vsip=<Virtual Server IP Address>&vsprot=<Virtual Server Protocol>&vsport=<Virtual Server Port>&addr=<IP Address To Remove/CIDR>`

接続がブラックリスト上にあるとき、その接続がドロップまたはリジェクトされたかどうかのチェック:

`https://<LoadMaster IP Address>/access/aclcontrol?isdrop`

ブラックリストエントリのドロップの有効化:

`https://<LoadMaster IP Address>/access/aclcontrol?drop=1`

ブラックリストエントリのドロップの無効化:

`https://<LoadMaster IP Address>/access/aclcontrol?drop=0`

接続がブラックリスト上にあるとき、その接続がブロックされたかどうかのチェック:

`https://<LoadMaster IP Address>/access/aclcontrol?isifblock`



ブラックリストエントリのブロックの有効化:

```
https://<LoadMasterIPAddress>/access/aclcontrol?ifblock=1
```

ブラックリストエントリのブロックの無効化:

```
https://<LoadMasterIPAddress>/access/aclcontrol?ifblock=0
```

3.16 Cluster Control (クラスターの制御)

クラスタリングはAPIコマンドで設定できます。使用可能な各コマンドの詳細は、以下のセクションを参照してください。

クラスタリングに関するAPIコマンドは、クラスタリングのライセンスが設定されているロードマスターでのみ利用できます。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。

3.16.1 クラスタリングに関するAPI コマンド

以下のセクションでは、クラスタリングに関する各RESTful APIコマンドについて詳しく説明します。RESTful APIを使用してクラスタリングを設定するステップバイステップの手順については、**セクション3.16.2**を参照してください。

3.16.1.1 クラスターの状態取得

クラスターの状態を取得するには、以下のコマンドを実行します。

```
https://<LoadMasterIPAddress>/access/cluster/status
```

クラスター内にある各ノードの詳細が返されます。これは、クラスター内にある有効なノードの一覧をXML形式で返します。

そのロードマスターがクラスターにない場合、WUIを介してエラーメッセージが返されます。

状態は、以下のように値で示されます。

- 0 - このノードは停止しています。
- 1 - このノードは稼働しています。
- 2 - このノードは無効です（このノードには接続は送信されません）。ノード内に仮想サービスが存在しない場合、そのノードは「無効」状態になります。
- 3 - 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。



- 4 - このノードは起動中です。
- 5 - このノードはプライマリ制御ノードです。

3.16.1.2 クラスターの作成

ロードマスターがクラスターモードでない場合、次のコマンドを実行してクラスターモードにすることができます。

```
https://<LoadMaster IPAddress>/access/cluster/create?SharedAddress=<SharedIPAdress>
```

3.16.1.3 クラスターへのノード参加の開始

クラスターへのノード参加を開始するには、次のコマンドを実行します。

```
https://<LoadMaster IPAddress>/access/cluster/joincluster
```

このコマンドを実行すると、ロードマスターをクラスターに追加できるようになります。ノードの追加を完了するには、**addnode**コマンドを実行してください。詳細はSection 3.16.1.4を参照してください。

3.16.1.4 クラスターへのノードの追加

このコマンドを実行する前に、ノードロードマスターを追加できるようにしなければなりません。ノードロードマスターを追加できるようにするには、そのノードロードマスター上で**joincluster**コマンドを実行します。**joincluster**コマンドの詳細については、**セクション3.16.1.3**を参照してください。

ノードロードマスターが追加できるようになっていない状態で**addnode**コマンドを実行すると、そのマシンにコンタクトできないことを表すエラーが返されます。

(ノードロードマスターが追加できるようになっている状態で) クラスターにノードを追加するには、共有IPアドレス上で次のコマンドを実行します。

```
https://<LoadMaster IPAddress>/access/cluster/addnode?Address=<NodeIPAdress>
```

3.16.1.5 ノードの有効化

クラスターにはじめてノードを追加する場合、そのノードはデフォルトで無効になっています。ノードを有効にするには、次のコマンドを実行します。

```
https://<LoadMaster IPAddress>/access/cluster/enablenode?nodeid=<NodeID>
```



ノードのIDを調べるには、ロードマスターWUIの“Cluster Control”画面の“ID”列を見るか、`status`コマンド（セクション3.16.1.1）を実行します。

3.16.1.6 ノードの無効化

ノードを無効にするには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/cluster/disablenode?nodeid=<NodeID>
```

ノードのIDを調べるには、ロードマスターWUIの“Cluster Control”画面の“ID”列を見るか、`status`コマンド（セクション3.16.1.1）を実行します。

3.16.1.7 ノードの削除

クラスターからノードを削除するには、次のコマンドを実行します。

```
https://<LoadMaster IP Address>/access/cluster/deletenode?NodeID=<NodeID>
```

ノードのIDを調べるには、ロードマスターWUIの“Cluster Control”画面の“ID”列を見るか、`status`コマンド（セクション3.16.1.1）を実行します。

3.16.2 RESTful APIを用いたクラスタリングの例

先のセクションでは、クラスタリングに関する各RESTful APIコマンドについて説明しました。このセクションでは、それらのAPIコマンドを用いてクラスターの作成とノードの追加を行う方法について、具体的な手順を説明します。コマンド例で使用するサンプルのIPアドレスは以下のとおりです。

- ロードマスター1: 10.154.11.10
- ロードマスター2: 10.154.11.20
- 共有IPアドレス: 10.154.11.30
- ノードID: 2

クラスターを作成してそのクラスターにノードを追加するには、以下の手順を順番に行います。

1. クラスターを作成します。ロードマスター1にて次のコマンドを実行します:

```
https://10.154.11.10/access/cluster/create?SharedAddress=10.154.11.30
```

2. ノード（ロードマスター2）のクラスターへの参加を開始します。ロードマスター2で次のコマンドを実行します:

```
https://10.154.11.20/access/cluster/joincluster
```

3. ノード（ロードマスター2）をクラスターに追加します。ロードマスター1で次のコマンドを実行します:



<https://10.154.11.10/access/cluster/addnode?Address=10.154.11.20>

ノードロードマスターがクラスターに参加できるようになっている状態で、**addnode**コマンドを実行しなければなりません。このコマンドは、**joincluster**コマンドに続けて実行します。

ノードロードマスターが追加できるようになっていない状態で**addnode**コマンドを実行すると、そのマシンにコンタクトできないことを表すエラーが返されます。

4. ノードを有効にします。ロードマスター1にて次のコマンドを実行します:

<https://10.154.11.10/access/cluster/enablenode?nodeid=2>

3.17 System Administration (システム管理)

各種のシステム管理タスクは、RESTful APIで管理できます。

3.17.1 ユーザの管理

3.17.1.1 システムパスワードの変更

デフォルトの**bal**ユーザーのパスワードを変更するには、以下のコマンドを実行します。

<https://<LoadMaster IP Address>/access/usersetsyspassword?currpassword=<Current Password>&password=<New Password>>

3.17.1.2 すべてのローカルユーザーの表示

すべてのローカルユーザーおよびその権限を表示するには、以下のコマンドを実行します。

<https://<LoadMaster IP Address>/access/userlist>

3.17.1.3 特定のローカルユーザーの権限表示

特定のローカルユーザーの権限を表示するには、以下のコマンドを実行します。

<https://<LoadMaster IP Address>/access/usershow?user=<Username>>

3.17.1.4 ローカルユーザーの新規追加

ローカルユーザーを新規に追加するには、以下のコマンドを実行します。

<https://<LoadMaster IP Address>/access/useraddlocal?user=<Username>&password=<User Password>>



名前	種類	説明	必須
user	String	新規ユーザーのユーザー名	Yes
password	String	新規ユーザーのパスワード	Yes - nopassまたはradiusがyesに設定されている場合を除く
radius	Boolean	ユーザがロードマスターにログインするときにRADIUSサーバによる認証を行うかどうかを決定します。このオプションを有効にする前に、RADIUSサーバの詳細を設定する必要があります。	No
nopass	Boolean	このオプションは、セッション管理が有効な場合のみ有効です。パスワードなしでユーザーを作成するには、このオプションをyesに設定します。このパラメーターを使用すると、証明書を用いたアクセスを許可することができます。詳細はセクション3.17.1.8を参照してください。	No

表3-45: UserAddLocalパラメーター

3.17.1.5 ローカルユーザーの削除

ローカルユーザーを削除するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/userdellocal?user=<Username>`

3.17.1.6 ローカルユーザーのパスワードの変更

ローカルユーザーのパスワードを変更するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/userchange locpass?user=<Username>&password=<New Password>&radius=<0/1>`

ユーザー名は大文字と小文字が区別されます。設定したとおりにユーザー名を入力してください。

すべてのパラメーターが必要です。radiusパラメーターは、ユーザがロードマスターにログインするときにRADIUSサーバによる認証を行うかどうかを決定します。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。

3.17.1.7 ローカルユーザーの権限の設定

ローカルユーザーの権限を設定するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/usersetperms?user=<Username>&perms=<Comma Separated List Of Permissions>`



値をカンマで区切ることで、複数の権限を同時に設定できます。例：

`https://<LoadMaster IP Address>/access/usersetperms?user=<Username>&perms=real,vs`

このコマンドを実行すると、そのユーザーに設定されていた以前の権限が上書きされます。例えば、あるユーザーがrules権限を持っているときに上記のコマンドを実行すると、このユーザーはrulesの権限を失い、realおよびvsの権限を持つようになります。

permsパラメーターの有効な値とその説明を以下に示します。

値	説明
real	このロールは、実サーバーを有効/無効にする権限を持ちません。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。
vs	このロールは、仮想サービスの管理権限を持ちます。これはサブVSを含みます。仮想サービスの変更では、すべてのサブネットに対する追加、削除、変更が可能です。
rules	このロールは、ルールの管理権限を持ちます。ルールの変更では、追加、削除、変更が可能です。
backup	このロールは、システムバックアップを行う権限を持ちません。
certs	このロールは、SSL証明書の管理権限を持ちます。証明書の管理では、SSL証明書の追加、削除、変更が可能です。
cert3	このロールは、インターミディエート証明書（中間証明書）の管理権限を持ちます。証明書の管理では、インターミディエート証明書の追加および削除が可能です。
certbackup	このロールは、証明書をエクスポート/インポートする権限を持ちます。
users	このロールは、“System Configuration > System Administration > User Management”のWUI画面における全ての機能を使う権限を持ちます。
root	このロールを設定すると、ユーザーは、balパスワードの変更権限および他のユーザーの作成/削除権限を除く、すべての権限を持ちます。
geo	このロールは、ロードマスターのGEO製品でのみ使用されます。GEOおよびグローバルサーバーロードバランシング（GSLB）機能パックの詳細は、 GEO Sticky DNS 機能説明 を参照してください。
	権限を何も設定しない場合は、パラメーターを空にしてください（例：&perms=）。

表3-46:権限に関するパラメーター - 有効な値



3.17.1.8 ローカル証明書の管理

あるユーザーに対して過去に作成した証明書を返すには、以下の書式で`userreadcert`コマンドを実行します。

```
https://<LoadMaster IPAddress>/access/userreadcert?user=<Username>
```

あるユーザーに対して過去に作成した証明書をダウンロードするには、以下の書式で`userdownloadcert`コマンドを実行します。

```
https://<LoadMaster IPAddress>/access/userdownloadcert?user=<Username>
```

あるユーザーに対して新しい証明書を作成するには、以下の書式で`usernewcert`コマンドを実行します。

```
https://<LoadMaster IPAddress>/access/usernewcert?user=<Username>&passphrase=<Passphrase>
```

パスフレーズは任意です。パスフレーズを入力した場合、そのパスフレーズは秘密鍵の暗号化に使用されます。

既存のユーザー証明書を削除するには、以下の書式で`userdelcert`コマンドを実行します。

```
https://<LoadMaster IPAddress>/access/userdelcert?user=<Username>
```

3.17.2 ライセンス設定

ロードマスターにライセンスを初めて設定するときと同様に、オンライン方式またはオフライン方式でライセンスの更新が行えます。

オフラインでライセンスを設定するには、KEMPから提供されるバイナリラージオブジェクト (BLOB) が必要です。

オンラインで更新する場合、KEMP IDとパスワードが必要です。

ライセンス設定についての詳細は、[ライセンス 機能説明](#)を参照してください。

3.17.2.1 ライセンス

ロードマスターのライセンスは、`license`コマンドを使用してオフラインで更新できます。

BLOBは、要求に応じてユーザーに送信されます。ライセンスを更新するたびに、新しいBLOBが必要になります。



以下に、BLOBの例を示します。



License Block (copy and paste from begin to end):

```
begin 0 /dev/null
hYE4t3iNKfk-YA42oB46lNGpZMq7Y9HEnBX6hCKNZBGomAaBYMaMpMXVYBnA+
h+++++
h+++++
h+-Y0+++++fpOF+PYKtU-ZGWF1cbXK-SOvXSyZahlABq2jVm1e7CEUOYBx
h2NZ3bEH2mpiPUoBAaSB7Enog+NYNn+cT-S204NIieVyYf5fx11pHh1kU8yg0
h326f1WZpBuflkT8tYwvFT2F9RjtYa9z4W9O9bRvTZKmN+1Thvbcgo-IiLsH
hA57Nbb5cWmLbagFWu63rbUSHZwVgVZ-gsTR0HZqMPCH2Q4oM0A1t0qRo97io
hegKgNv3mrWqQ7k9xuCJjQ+S8maYokFhthEMZrv9bCKSuxAP97EaYxXP9Ycm2
h1A5KNkO9j8B89DpN19jxFgYrIKSJrfz6981e9WD8K3ob6d5uwcc8JxqkeLXX
hIkI49ijAI9J7rpgoeheNrZaFwO2gK54w60WHdTMO2y58JC3SNs69Fj24mLtN
hyiGSNZV6XoMkXBzrP9vPEAA9YjHuRy4srTiEiGm4V97Q6C0AwM7W9asJI3fs
hPfyYt0LjY6CwAn+N0hI3Phjfu6kbbFkPNkVu4PMigBSDCtKKwfoL5ftQhTKE
hE6PRw1dzotz9C1ZGPKglehdeA5kIQf5PiRo9yElQAWbaG3F-Yx8D2A1oTRbx
hnC8RZXI2zpkwQNiCdZByQ85XK1wOM6ataWKSiwMz50ttiVToXypB-HHRZqTN
h-aqA6wbSjNoD-vEO5FWnr4dPMFUsddv8UCgQfwbuTfFkCBipTFHk8yBWuSMV
CLFxaR0WUbggw1X9mmS++
+
end
```

Legacy License Key: OBG6Adv-idO9Pek-ufZPqan-PZN0tae

It has been issued a **Single Perm** license.

図 3-4: BLOB

BLOBは、図 3-4: BLOBの例で反転表示されているように、beginで始まりendで終わるテキストの塊です。BLOBをテキストファイル（以下の例ではlicense.txt）にコピーアンドペーストする必要があります。ライセンス設定に関する詳細（BLOBを取得する方法など）は、[ライセンス 機能説明](#)を参照してください。

ライセンスコマンドはさまざまな方法で使用できます。例えば、LinuxでCURLコマンドを使用する場合は以下ようになります。

```
curl -X POST --data-binary "@license.txt" -k https://<LoadMaster IP Address>/access/li
cense
```

このコマンドは、ロードマスターにBLOBファイルをアップロードします。上記のコマンド例では、license.txtがカレントディレクトリにあるものと仮定しています。license.



txtが他の場所に保存されている場合は、@記号の後にファイルのパスを指定してください。

3.17.2.2 *AlsiLicense*

AlsiLicenseコマンドは、ロードマスターのライセンスをオンラインで更新します。ロードマスターがKEMPのライセンスシステムを参照して最新のライセンスを確認し、最新版があった場合に更新するようにするには、以下のコマンドを実行します。

`https://<LoadMaster IPAddress>/access/alsi license?kempid=<KEMPID>&password=<KEMPIDPassword>`

名前	種類	説明	必須
kempid	String	KEMP IDを登録する際に使用するEメールアドレス	Yes
password	String	KEMP IDアカウントのパスワード	Yes
http_proxy	String	<プロキシアドレス>:<ポート>の形式でHTTP(S)のプロキシサーバーとポートを指定します。	No

表3-47:AlsiLicenseパラメーター

3.17.2.3 *アクセスキー*

アクセスキーは、以下のコマンドで取得できます。

`https://<LoadMaster IPAddress>/access/accesskey?`

3.17.2.4 *KillASLInstance*

アクティベーションサーバーライト (ASL) 機能を用いてロードマスターにライセンスを設定した場合、**KillASLInstance**コマンドを実行してクライアントのロードマスターのライセンスを無効にできます。

`https://<LoadMaster IPAddress>/access/KillASLInstance`

3.17.3 *System Reboot (システムリブート)*

ロードマスターは、以下のコマンドでシャットダウンまたは再起動できます。

`https://<LoadMaster IPAddress>/access/shutdown?`

`https://<LoadMaster IPAddress>/access/reboot?`



3.17.4 Update Software (ファームウェア更新)

3.17.4.1 新しいバージョンのソフトウェアへのアップグレード

installpatchコマンドを実行することで、ロードマスターのソフトウェアを新しいバージョンにアップグレードできます。このコマンドには、いくつかの使用方法があります。このコマンドには、いくつかの使用方法があります。たとえば、LinuxでCURLコマンドを使用する場合は、以下のようになります。

```
curl -X POST --data-binary "@<LM Patch File>" -k https://<LoadMasterIPAddress>/access/installpatch
```

このcURLコマンドは、パッチ (<LM Patch File>) をシステムにインストールします。

アップロードするファイルは有効なパッチファイルでなければなりません。WUIにてファイルが機能しない場合、そのファイルはRESTful APIコマンドでも機能しません。

3.17.4.2 以前にインストールしたバージョンのソフトウェアの復元

ロードマスターの以前のバージョンのファームウェアは、以下のコマンドで復元できます。

```
https://<LoadMasterIPAddress>/access/restorepatch
```

変更内容を反映するには、マシンを再起動する必要があります。

3.17.4.3 インストールされているアドオンパックのリスト表示

ロードマスターにインストールされているアドオンパッケージは、以下のコマンドでリスト表示できます。

```
https://<LoadMasterIPAddress>/access/listaddon
```

3.17.4.4 アドオンパックのアップロードまたは更新

アドオンパックは以下のPOSTコマンドでアップロードできます。

```
curl -X POST --data-binary "@<Path To Add-On Pack File>" -k https://<LoadMasterIPAddress>/access/addaddon
```

アドオンパックが既に存在する場合、そのアドオンパックはアップロードされるバージョンに更新されます。



3.17.4.5 アドオンパックの削除

アドオンパックは以下のコマンドで削除できます。

```
https://<LoadMaster IP Address>/access/deladdon?name=<AddOnPackName>
```

既存のアドオンパックの名前を表示するには、listaddonコマンドを実行します。

3.17.5 バックアップ/復元

ロードマスターの設定は、以下のコマンドでバックアップまたは復元できます。

```
https://<LoadMaster IP Address>/access/backup
```

cURLを使用してこのコマンドを実行すると、Linuxの作業ディレクトリにファイルがダウンロードされます。

以下に、ロードマスターの設定を復元するcURLコマンドの例を示します。

```
curl -X POST --data-binary "@<Path To Backup File>" -k https://<LoadMaster IP Address>/access/restore?type=<1, 2 or 3>
```

type takes the integer range from 1 to 3:

名前	種類	範囲	追加情報
種類	整数	1-3	1 = ロードマスターの基本設定 2 = VSの設定 3 = GGeoの設定

表3-48:バックアップのパラメータ

3.17.5.1 自動バックアップ

getコマンドとsetコマンドで管理可能な自動バックアップに関するパラメーターの詳細を以下の表3-49に示します。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	デフォルト	範囲	追加情報
----	----	-------	----	------



名前	種類	デフォルト	範囲	追加情報
backupday	整数	Daily (毎日)	0-7	自動バックアップを何曜日に行うか（または毎日実行するか）を指定します。 0 = Daily (毎日) 1 = Monday (月曜日) 2 = Tuesday (火曜日) 3 = Wednesday (水曜日) 4 = Thursday (木曜日) 5 = Friday (金曜日) 6 = Saturday (土曜日) 7 = Sunday (日曜日)
backupenable	Boolean	N		自動定期バックアップを有効にします (FTP経由)。
backuphost	String			リモートホスト
backuphour	整数	0	0-23	自動バックアップ実行時刻 (時) 0 = Midnight (真夜中) 23 = 11pm
backupminute	整数	0	0-59	自動バックアップ実行時刻 (分) なお、範囲値は1分単位です。
backuppassword	String			リモートユーザーのパスワード
backuppath	String			リモートパス名を指定します。
backupuser	String			リモートユーザー名を指定します。

表3-49:バックアップのパラメータ

3.17.6 Date/Time (日付/時間)

`get`および`set`コマンドで管理できる日付と時刻のパラメータの詳細については、表3-50を参照してください。`get`および`set`コマンドについてはセクション2.4を参照してください。

名前	種類	追加情報
ntphost	S	ロードマスターが時刻を設定するのに使用するホストを指定します。スペース区切りのリストを使用して複数のホストを指定できません。%20を使用して空白文字をエスケープしてください。時刻は、有効な値を返した最初のホストを使用して設定されます。
time	I	時分秒で表された時刻



名前	種類	追加情報
timezone	S	ロードマスターが位置するタイムゾーン
ntpkeyid	I	NTP鍵IDです。有効な値の範囲は1~99です。
ntpkeysecret	S	NTP共有秘密鍵の文字列です。NTP秘密鍵には最大40文字まで使用できます。秘密鍵が20文字より長い場合、16進文字列として扱われます。この値に空の文字列を設定すると、NTPv4機能が無効になります。

表3-50:Date/Time (日付/時間)

RESTful APIコマンドを使用して時刻を設定することはできません。

3.18 Logging Options (ログオプション)

3.18.1 システムログの管理

システムログファイルをダウンロードするには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/logging/downloadlogs`

システムログファイルをリセットするには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/logging/resetlogs`

3.18.2 Ping Host (pingホスト)

pingを実行するには、次のコマンドを実行します。

`https://<LoadMaster IP Address>/access/logging/ping?addr=<IP Address>&intf=<Interface ID>`

パラメーター	パラメーターの種類	パラメーターの説明	必須
addr	アドレス	pingを実行するホストを指定します。	Yes
intf	整数	ping送信元インターフェイスのIDを指定します。ここでインターフェイスを指定しない場合、特定のネットワーク上のアドレスにpingを実行するインターフェイスが自動的に選択されます。	No

表3-51:pingのパラメーター

3.18.3 tracerouteの実行

tracerouteを実行するには、次のコマンドを実行します。



<https://<LoadMaster IP Address>/access/logging/traceroute?addr=<IP Address>>

3.18.4 Debug Options (デバッグオプション)

3.18.4.1 デバッグオプションの取得/設定

getおよびsetコマンドで管理できるデバッグオプション関連のパラメータの詳細については、下記の表を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	パラメーターの説明
irqbalance	B	IRQBalanceは、マルチプロセッサシステムにおいてハードウェア割り込みをプロセッサ全体に分散させることを目的としています。このオプションを有効にする場合は、必ずKEMPの技術サポートにご相談ください。
linearesplogs	B	デフォルトでは、ロードマスターは古いログファイルを削除します。このパラメーターを有効にすると、古いログファイルは削除されなくなります。ファイルシステムが一杯になると、ロードマスターからのアクセスはブロックされます。
netconsole	A	Netconsoleは、カーネルのprintkメッセージをUDP経由で記録するカーネルモジュールで、これを使用すると、ディスクがログ作成に失敗する問題をデバッグすることができます。このパラメーターを設定すると、特定のホストで動作する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。これにより、ロードマスターが再起動する原因を突き止めることができます。
netconsoleinterface	I	Netconsoleをホストするインターフェイス

表3-52: デバッグオプション

3.18.4.2 その他のデバッグオプションの実行

その他のデバッグオプションのコマンドをAPIから実行できます。

- ps

psコマンドは、ブラウザで実行しても機能しません。psコマンドを実行するには、cURLコマンドを使用してください。

- meminfo
- ifconfig
- netstat
- interrupts



- partitions
- cpuinfo
- df
- lspci
- lsmod
- slabinfo

例 :

`https://<LoadMaster IPAddress>/access/logging/meminfo`

3.18.4.3 統計情報のリセット

統計情報をリセットするには、次のコマンドを実行します。

`https://<LoadMaster IPAddress>/access/logging/resetstats`

3.18.4.4 Flush SSO Authentication Cache (SSO認証のキャッシュの消去)

ssoflushコマンドを実行すると、SSO認証キャッシュを消去できます。

`https://<LoadMaster IPAddress>/access/logging/debug/ssoflush`

3.18.5 Extended Log Files (拡張ログファイル)

3.18.5.1 WAF監査ファイルのリスト表示

WAF監査ファイルのリストを表示するには、listwafauditfilesコマンドを実行します。

`https://<LoadMaster IPAddress>/access/listwafauditfiles`

3.18.5.2 WAF監査ファイルのダウンロード

WAF監査ファイルをダウンロードするには、downloadwafauditlogコマンドを実行します。

`https://<LoadMaster IPAddress>/access/downloadwafauditlog?file=wafaudit.1`

AFPのログはリアルタイムでは作成されません。このログは、AFP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。

名前	種類	パラメーターの説明	必須
----	----	-----------	----



名前	種類	パラメーターの説明	必須
file	S	ダウンロードされるWAF監査ファイル。このファイルは<wafaudit>. <number>という形式になっています。WAF監査ファイルのリストを取得するには、listwafauditfilesコマンドを実行します。コマンドごとにファイル名のみ指定します。	Y
filter	S	フィルター文字列。正規表現を使用できます。	N

表3-53: DownloadWafAuditLogパラメーター

3.18.6 Syslog Options (シスログ・オプション)

getおよびsetコマンドで管理できるSyslogオプション関連のパラメータの詳細については、表3-54を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	パラメーターの説明
syslogemergency	A	Emergency (緊急) のイベントのみ受信するようにホストを設定するには、このオプションを使用します。入力値はスペースで区切る必要があります。最大10個の値まで入力できます。
syslogcritical	A	Emergency (緊急) および Critical (重大) のイベントを受信するようにホストを設定するには、このオプションを使用します。入力値はスペースで区切る必要があります。最大10個の値まで入力できます。
syslogerror	A	Emergency (緊急) 、 Critical (重大) 、および Error (エラー) のイベントを受信するようにホストを設定するには、このオプションを使用します。入力値はスペースで区切る必要があります。最大10個の値まで入力できます。
syslogwarn	A	Emergency (緊急) 、 Critical (重大) 、 Error (エラー) 、および Warning (警告) のイベントを受信するようにホストを設定するには、このオプションを使用します。入力値はスペースで区切る必要があります。最大10個の値まで入力できます。
syslognotice	A	Emergency (緊急) 、 Critical (重大) 、 Error (エラー) 、 Warning (警告) 、 Notice (通知) のイベントを受信するようにホストを設定するには、このオプションを使用します。入力値はスペースで区切る必要があります。最大10個の値まで入力できます。



名前	種類	パラメーターの説明
sysloginfo	A	All (すべて) のイベントを受信するようにホストを設定するには、このオプションを使用します。入力値はスペースで区切る必要があります。最大10個の値まで入力できます。

表3-54:Syslog Options (シスログ・オプション)

各Syslogフィールドでは、最大10個までのIPアドレスおよびホスト名を指定できます。複数のIPアドレス/ホスト名を指定する場合は、カンマ区切りリストを使用しなければなりません。

3.18.7 SNMPオプション

`get`および`set`コマンドで管理できるSNMPログオプション関連のパラメータの詳細については、表3-55を参照してください。`get`および`set`コマンドについてはセクション2.4を参照してください。

名前	種類	追加情報
snmpcommunity	S	SNMPのコミュニティ文字列を指定します。
snmpcontact	S	SNMPのレスポンスにて送信された問い合わせアドレスを指定します。
snmpenable	B	0 = 無効 1 = 有効
snmptrapenable	B	重大なイベントが発生したとき、常にSNMPイベントを生成します。
snmpv1sink	A	SNMPタイプ1トラップのシンクアドレスを指定します。
snmpv2sink	A	SNMPタイプ2トラップのシンクアドレスを指定します。
snmpV3enable	B	SNMP V3の有効化/無効化 0 = 無効 1 = 有効
snmpv3user	A	ユーザー名を指定します。
snmpv3userpasswd	A	ユーザーパスワードを指定します。
snmplocation	S	SNMPのレスポンスにて送信されたロケーションを指定します。
snmpclient	S	SNMPサブシステムにアクセスできるマシンのリストを指定します。クライアントを指定しない場合、誰でもSNMPにアクセスできます。



名前	種類	追加情報
snmpHATrap	B	共有IPアドレスからSNMPトラップを送信します。このオプションは、ロードマスターがHAモードにあるときのみ利用できます。
snmpAuthProt	S	目的の認証プロトコルを指定します。 MD5 SHA SHAの方がより安全なプロトコルです。 注: これらの値は大文字と小文字が区別されます。大文字で入力してください。
snmpPrivProt	S	目的のプライバシープロトコルを指定します。 DES AES AESの方がより安全なプロトコルです。 注: これらの値は大文字と小文字が区別されます。大文字で入力してください。

表3-55:SNMPログオプション

3.18.8 Email Options (E-Mail オプション)

getおよびsetコマンドで管理できるEmailログオプション関連のパラメータの詳細については、表3-56を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	範囲	追加情報
emailcritical	S		重大なメッセージを受信するためのEメールアドレス
emaildomain	S		ユーザーアカウントを認証するためのドメイン (必要な場合)
emailemergency	S		緊急のメッセージを受信するためのEメールアドレス
emailenable	B		Eメールのログ作成オプションを有効/無効にします。
emailerror	S		エラーメッセージを受信するためのEメールアドレス
emailinfo	S		情報メッセージを受信するためのEメールアドレス
emailnotice	S		通知を受信するためのEメールアドレス
emailpassword	S		Eメールユーザーのパスワード
emailport	I	0-65535	お使いのEメールサーバーが接続を受け入れるTCPポート (通常は25)



名前	種類	範囲	追加情報
emailserver	S		SMTPサーバーがEメールメッセージの送信に使用するホスト名またはアドレス
emailsslmode	I	0-3	接続で使用するセキュリティプロトコルの種類を指定します。 0 = なし 1 = STARTTLS (利用可能な場合) 2 = STARTTLS 3 = SSL/TLS
emailuser	S		Eメールメッセージの送信権限を持つユーザーアカウント
emailwarn	S		警告を受信するためのEメールアドレス

表3-56:Emailログオプション

3.18.9 SDN Log Files (SDNログファイル)

3.18.9.1 Debug Options (デバッグオプション)

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。

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。

SDNの統計モードは、`get`コマンドおよび`set`コマンドを使用し、パラメーター`sdnstatsmode`を1または2に設定することで管理できます。例:

```
https://<LoadMaster IP Address>/access/set?param=sdnstatsmode&value=2
```

3.19 その他のオプション

3.19.1 WUI Settings (WUIの設定)

`get`および`set`コマンドで管理できるWUI設定関連のパラメータの詳細については、表3-57を参照してください。`get`および`set`コマンドについてはセクション2.4を参照してください。

名前	種類	範囲	説明
----	----	----	----



名前	種類	範囲	説明
hoverhelp	B	0 - 無効 1 = 有効	このオプションを使用すると、WUI画面にてクリック可能なオプションにマウスカーソルを置いたときにその説明を表示することができます。
motd	S		これはMessage of the Day (MOTD) です。プレーンテキストまたはテキストファイルを使用できます。 最大5,000文字 MOTDが5,000文字を超えるとエラーが表示されます。
wuidisplaylines	I	10-100	1つの統計情報ページで表示可能な最大行数を設定します。

表3-57:WUI設定のパラメータ

上記のように“set”コマンドを使用してMessage Of The Day (MOTD) を指定する場合、最大5,000文字まで入力できます。5,000文字を超えるMOTDを入力したい場合は、プレーンテキスト形式でMOTDを保存し、下記のコマンドにてKEMPロードマスターにそのMOTDをポストしてください。

```
curl -d @<filename> -k https://bal:<Bal Password>@<IPAddress>/access/setmotd
```

3.19.2 WUIの認証および承認オプション

getおよびsetコマンドで管理できるWUIの認証および承認オプション関連のパラメータの詳細については、表3-58を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	範囲	説明
ldapbackupserver	A		認証用のバックアップLDAPサーバーを指定します。
ldapsecurity	I	0 = 暗号化しない 1 = StartTLS 2 = LDAPS	LDAP認証のセキュリティモードを指定します。
ldapserver	A		認証用のLDAPサーバーを指定します。
ldaprevalidateinterval	B		LDAPサーバーへの認証を再度行う頻度を指定します。
radiusbackupport	I	3-65535	バックアップRADIUSサーバーのTCPポートを指定します。



名前	種類	範囲	説明
radiusbackupsecret	S		バックアップRADIUSサーバーのパスワード（秘密鍵）を指定します。
radiusbackupserver	A		認証用のバックアップRADIUSサーバーを指定します。
radiusport	I	3-65535	RADIUSサーバーへの通信に使用するTCPポートを指定します。
radiusrevalidateinterval	I	10-86400	RADIUSサーバーへの認証を再度行うタイミングを指定します。
radiussecret	S		RADIUSサーバーのパスワード（秘密鍵）を指定します。
radiusserver	A		認証用のRADIUSサーバーを指定します。
sessionlocalauth	B		ローカル認証を有効/無効にします。
sessionauthmode	I	表3-59: セッション認証モードの値を参照してください。	ロードバランサーの認証モードを指定します。

表3-58: WUIの認証および承認オプション

表3-59は、`sessionauthmode`パラメータに与えられた値に応じて選択される、Radius、LDAP、およびローカルユーザーのオプションについて説明しています。

値	Radius		LDAP	ローカル	
	認証	承認	認証	認証	承認
7	No	No	No	No	No
263	Yes	No	No	Yes	Yes
775	Yes	Yes	No	Yes	Yes
23	No	No	Yes	Yes	Yes
22	No	No	Yes	No	Yes
788	Yes	Yes	Yes	No	No
790	Yes	Yes	Yes	No	Yes
791	Yes	Yes	Yes	Yes	Yes
789	Yes	Yes	Yes	Yes	No
773	Yes	Yes	No	Yes	No
262	Yes	No	No	No	Yes
774	Yes	Yes	No	No	Yes
772	Yes	Yes	No	No	No



	Radius	LDAP	ローカル
278	Yes	No	No
279	Yes	No	Yes

表3-59: セッション認証モードの値

3.19.3 レイヤ7設定

getおよびsetコマンドで管理できるL7関連のパラメータの詳細については、表3-60を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	範囲	説明
addcookieport	B	0 = 無効 1 = 有効	NAT変換を行うゲートウェイの内側でロードマスターを使用する場合、クライアントのアドレスはすべて同じになります。クッキーを個別に作成する場合、リモートポートをクッキーに追加できます。必要がないときにこのオプションを有効にすると、リソースが浪費されます。
addvia	B	0 = 無効 1 = 有効	このオプションを有効にすると、すべてのキャッシュ応答にVIAヘッダーフィールドが追加されます。仮想サービスアドレスは、使用されているアドレスになります。
allowemptyposts	B	0 = 無効 1 = 有効	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。このパラメータをtrueに設定すると、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。



名前	種類	範囲	説明
alwayspersist	S	0 = HTTP/1.1接続の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 1 = 全てのリクエストに対してパーシステンスをチェック 2 = 接続の途中であってもパーシステンスの全ての変更を保存	このパラメーターはnoとyesも有効な値として受け付けます。noとyesはそれぞれ0と1に対応します。
closeonerror	B	0 = 無効 1 = 有効	このオプションを有効にすると、クライアントからエラー応答が返されたときにクライアントとの接続が必ずクローズされます。例えば、このオプションにより、If-Modified-Since HTTPヘッダー受信後に「304 ファイルが変更されませんでした」のメッセージを返信する際のロードマスターの動作が変わります。
dropatdrainend	B	0 = 無効 1 = 有効	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）。
droponfail	B	0 = 無効 1 = 有効	デフォルトでは、実サーバーに障害が発生しても既存の接続はクローズされません。この機能を有効にすると、実サーバーの障害発生時にすべての接続が直ちにドロップされます。



名前	種類	範囲	説明
expect100	I	0 = RFC準拠 1 = 常にExpect-100 2 = Continue-100を無視	デフォルトでは、L7モジュールはExpect-100ヘッダーを検出したときのみ100-Continueの応答を待ちます (RFC-2616 Compliant)。システムが常に100 Continueのメッセージを待つようにするには、 Require 100-Continue を使用します。100 Continueのメッセージが送信されない場合でも、クライアントが常にPOSTデータを送信するようにするには、 RFC-7231 Compliant を使用します。
rfcconform	B	0 = 無効 1 = 有効	デフォルトでは、ロードマスターはHTTPヘッダーの構文解析時にRFCを確認します。このオプションを無効にすると、規格に準拠していないブラウザとデータをやり取りできます。
rsarelocal	B	0 = 無効 1 = 有効	クライアントがローカルサブネット上にあるかどうかを確認する際、クライアントが実際の実サーバーかどうかを確認します。
localbind	B	0 = 無効 1 = 有効	非常に負荷が高い状況では、ローカルポートの枯渇が発生します。このオプションを有効にすると、代替ソースアドレスを設定できます。これを使用すると、利用可能なローカルポートの数を増やすことができます。
transparent	B	0 = 無効 1 = 有効	L7サブシステムによる接続の透過処理をグローバルに有効/無効にします。L4接続は「常に」透過処理されます。
slowstart	I	0-600	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、オンラインになった実サーバーへの負荷を徐々に増やす時間を指定します。
addforwardheader	I	0 = X-クライアントサイド 1 = X-フォワーディングされる 2 = なし	このオプションを使用すると、HTTPヘッダーにX-ClientSideまたはX-Forwarded Forを追加できます (このオプションはL7 Transparencyが無効な場合に限り利用可能)。
logsplitinterval	I	1-100	Log Insight Scheduling を使用している場合、この値は、ある接続においてストリームが再スケジュールされるまでに受信するメッセージの数を表します。デフォルト値は10です。



名前	種類	範囲	説明
authtimeout	I	30 - 300	認証進行中に接続をオープンのままにする期間（単位：秒）この値は30～300の範囲で設定できます。

表3-60: レイヤ7設定

3.19.4 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

getおよびsetコマンドで管理できるネットワークオプション関連のパラメータの詳細については、表3-61を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	範囲	追加情報
snat	B	0 = 無効 1 = 有効	このオプションを有効にすると、ロードマスターによる実サーバーからインターネットへのNAT接続が可能になります。
allowupload	B	0 = 無効 1 = 有効	なお、ロードマスターはHTTPの負荷に対して最適化されていることに注意してください。このオプションを有効にすると、非HTMLのアップロードが正しく機能するようになります。
conntimeout	I	0-86400	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、デフォルト値の660秒にリセットされます。
keepalive	B	0 = 無効 1 = 有効	デフォルトでは、クライアントに障害が発生しているかどうかはTCPのキープアライブを用いてチェックされます。このオプションを有効にすると、古いTCP接続（SSHセッション）の信頼性が向上します。普通は、通常のHTTP/HTTPSサービスではこれは必要ありません。



名前	種類	範囲	追加情報
multigw	B	0 = 無効 1 = 有効	このオプションを有効にすると、デフォルトゲートウェイを別のインターフェイスに移行することができます。
nonlocalrs	B	0 = 無効 1 = 有効	このオプションを有効にすると、ローカルで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。
onlydefaultroutes	B	0 = 無効 1 = 有効	このオプションを有効にすると、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。
resetclose	B	0 = 無効 1 = 有効	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TCP RESETを使用して実サーバーとの接続を終了します。
subnetorigin	B	0 = 無効 1 = 有効	仮想サービスの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。このオプションを有効にすると、送信元IPアドレスはロードマスターのローカルアドレスになります。実サーバーがサブネット上にある場合、ロードマスターのサブネットアドレスが使用されます。
subnetoriginating	B	0 = 無効 1 = 有効	仮想サービスの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。このオプションを有効にすると、送信元IPアドレスはロードマスターのローカルアドレスになります。実サーバーがサブネット上にある場合、ロードマスターのサブネットアドレスが使用されます。



名前	種類	範囲	追加情報
tcptimestamp	B	0 = 無効 1 = 有効	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、0n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。KEMPのサポートから要求された場合のみ有効にしてください。
routefilter	B	0 = 無効 1 = 有効	このオプションを有効にすると、ホストからのIPフレームは、そのホストにフレームを転送するようルーティングアルゴリズムが設定されたインターフェイスを経由したもののみ受け付けられます。これは、厳格な送信元検証として知られています。
dhkeysize	I	512、1024、 または2048	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。
http_proxy	S		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。

表3-61: 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

3.19.5 アプリケーションフロントエンド (AFE) の設定

侵入検出パラメータは、以下のコマンドで更新できます。

`https://<LoadMaster IP Address>/access/updatedetect`



このコマンドには、いくつかの使用方法があります。たとえば、LinuxでCURLコマンドを使用する場合は、以下ようになります。

```
curl -X POST --data-binary "@<Detection Rules File>" -k https://<LoadMasterIPAddress>/access/updatedetect
```

上記の例では、新しい検出ルール（<Detection Rules File>）がシステムにインストールされます。

ファイル拡張子は、キャッシュ対象外のファイル拡張子のリストから以下のコマンドで追加または削除できます。

```
https://<LoadMasterIPAddress>/access/addnocache?param=<FileExtension>
```

```
https://<LoadMasterIPAddress>/access/delnocache?param=<FileExtension>
```

<FileExtension>文字列は、"."で始める必要があります。例：

```
https://<LoadMasterIPAddress>/access/addnocache?param=.jpg
```

ファイル拡張子は、圧縮対象外のファイル拡張子のリストから以下のコマンドで追加または削除できます。

```
https://<LoadMasterIPAddress>/access/addnocompress?param=<.FileExtension>
```

```
https://<LoadMasterIPAddress>/access/delnocompress?param=<.FileExtension>
```

<FileExtension>文字列は、"."で始める必要があります。

getおよび**set**コマンドで管理できるAFE設定関連のパラメータの詳細については、表3-62を参照してください。**get**および**set**コマンドについてはセクション2.4を参照してください。

名前	種類	範囲	説明
cache size	I	1-409	キャッシュサイズを指定します。
host cache	B	0 = 無効 1 = 有効	ホストのキャッシュを有効/無効にします。
paranoia	I	0 = 低 1 = デフォルト 2 = 高 3 = 非常に敏感	侵入検出システム（IDS）の検出感度を設定します。
limit input	I	0-10000	接続数を制限します。

表3-62: AFE設定パラメータ



クライアントの制限を使用すると、指定したホストからの（1秒当たりの）接続試行回数を制限できます。この制限値はsetコマンドで設定できます。例：

```
https://<LoadMaster IPAddress>/access/set?param=l7limitinput&value=25
```

制限値を0に設定すると、このオプションが無効になります。

複数のアドレスまたはネットワークに制限をかけることができます。アドレスを追加するには、以下のコマンドを実行します。

```
https://<LoadMaster IPAddress>/access/afeclientlimitadd?l7addr=<L7Address>&l7limit=<L7Limit>
```

アドレスを削除するには、以下のコマンドを実行します。

```
https://<LoadMaster IPAddress>/access/afeclientlimitdel?l7addr=<L7Address>
```

アドレスおよびその制限値の一覧を表示するには、以下のコマンドを実行します。

```
https://<LoadMaster IPAddress>/access/afeclientlimitlist?
```

3.19.6 HA管理

ロードマスターfor Azureを使用する場合は次のセクションを参照してください。

getおよびsetコマンドで管理できるHAパラメータ関連のパラメータの詳細については、表3-63を参照してください。getおよびsetコマンドについてはセクション2.4を参照してください。

名前	種類	範囲	説明
haif	I		HAクラスタのメンバー間で設定を同期する際に使用するネットワークインターフェイス
hainitial	B	0 - 無効 1 - 有効	起動時に追加のネットワークチェックを行います。これは不安定な動作を引き起こす可能性があるため、使用しないでください。
haprefered	I	0 = 優先ホストなし 1 = 最初のHAを優先 2 = 2番目のHAを優先	デフォルトでは、HAクラスタのいずれのパートナーも優先権を持っていません。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ります。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。



名前	種類	範囲	説明
hastyle	B	0 = レガシーハート 1 = carp	デフォルトでは、VRRP (carp) のバージョンを用いてパートナーの状態がチェックされます。また、本システムは従来のハートビートプログラムもサポートします。このオプションは、両方のマシンが再起動された場合のみ有効になります。
hatimeout	I	1 = 3秒 2 = 6秒 3 = 9秒 4 = 12秒 5 = 15秒	スイッチオーバーが発生する前にマスターを利用できなくする時間です。
havhid	I	1-255	同じネットワーク上で複数のHAロードマスターを使用する場合、この値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。
hawait	I	0-200	これは、初回起動後にロードマスターがアクティブになるまでの時間 (単位: 秒) 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。
mcast	I		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。
vmac	B		このオプションは、2つのユニットの共有MACアドレスを作成します。フェイルオーバーが発生すると、ロードマスターによりMACアドレスも引き渡されます。これにより、スイッチのMACアドレスが維持されるため、ARPのキャッシュや古いレコードを気にする必要がなくなります。
Tcpfailover	B	0 - 無効 1 - 有効	L4サービス使用時、更新を有効にすると、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。このパラメーターは廃止され、hal4updateパラメーターに置き換えられました。
hal4update	B	0 - 無効 1 - 有効	L4サービス使用時、更新を有効にすると、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。



名前	種類	範囲	説明
cookieupdate	B	0 - 無効 1 - 有効	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のスイッチ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。 このパラメーターは廃止され、hal7updateパラメーターに置き換えられました。
hal7update	B	0 - 無効 1 - 有効	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のスイッチ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。
finalpersist	I	0, 60-86400	実サーバーを無効にすると、その実サーバーで継続されていたセッションは、ドレイン時間が経過するか、実サーバーによりこれ以上セッションが処理されなくなるまで維持されます。新たなセッションは実サーバーにより処理されません。
hamode	I	0 = HAモードオフ 1 = HA 1モード 2 = HA 2モード	HAモードを指定します。ロードマスターを1台のみ使用する場合は、非HAモードを使用します。HAモードでは、1台のロードマスターを1次マシンとして指定し、もう1台のロードマスターを2次マシンとして指定する必要があります。2台のロードマスターを同じモードに指定した場合、HAは機能しません。
hacheck	B	0 = 無効 1 = 有効	HAのヘルスチェックを有効にします。少なくとも1つのインターフェイスを有効にする必要があります。

表3-63:HAのパラメータ

HAモードを変更しただけでは、非HAとHAは切り替わりません。システムを完全にスイッチオーバーさせるには、パートナーと仮想IP (V IP) アドレスも設定して再起動する必要があります。RESTful APIを使用してHAを設定する方法については、[セクション3.19.7](#)。

hastyleまたはhamodeの変更内容を有効にするには再起動する必要があります。



3.19.7 AzureのHAパラメータ

このコマンドはロードマスター for Azureにのみ関係します。

AzureのHAモードは、以下のコマンドで設定できます。

```
https://<LoadMaster IP Address>/access/azurehamode?hamode=<master/slave/single>
```

AzureのHAパラメータは、以下のコマンドで設定できます。

```
https://<LoadMaster IP Address>/access/azurehaparam?partner=<PartnerHostNameOr IP Address>&hcp=<HealthCheckPort>
```

名前	種類	範囲	追加情報
partner	S	有効なIPアドレスでなければなりません。	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。
hcp	I	有効なポート値でなければなりません。	ヘルスチェックを行うポートを設定します。HAが正しく機能するには、マスターとスレーブでポートが同じでなければなりません。

表3-64: AzureのHAパラメータ

AzureのHAパラメータは、以下のコマンドで取得できます。

```
https://<LoadMaster IP Address>/access/getazurehaparams?
```

3.19.8 AWSのHAパラメーター

このコマンドはロードマスター for AWSにのみ関係します。

AWSのHAモードは、以下のコマンドで設定できます。

```
https://<LoadMaster IP Address>/access/awshamode?hamode=<master/slave/single>
```

AWSのHAパラメーターは、以下のコマンドで設定できます。

```
https://<LoadMaster IP Address>/access/awshaparam?partner=<PartnerHostNameOr IP Address>&hcp=<HealthCheckPort>
```

名前	種類	範囲	追加情報
partner	S	有効なIPアドレスでなければなりません。	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。
hcp	I	有効なポート値でなければなりません。	ヘルスチェックを行うポートを設定します。HAが正しく機能するには、マスターとスレーブでポートが同じでなければなりません。

表3-65: AWSのHAパラメーター



AWSのHAパラメータは、以下のコマンドで取得できます。

`https://<LoadMaster IP Address>/access/getawshaparams?`

`getawshaparams`コマンドの出力例を以下に示します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="200" code="ok">
<Success><Data><AwsHA>
<HaMode>slave</HaMode>
<Partner>172.31.12.48</Partner>
<Port>5000</Port>
</AwsHA>
</Data>
</Success>
</Response>
```

3.19.9 SDNの設定

3.19.9.1 SDNコントローラーの追加

ロードマスターにSDNコントローラーを新規に追加するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/addsdncontroller?ipv4=<IPv4 Address>&port=<SDN Controller Port>&https=<0/1>&user=<User To Access SDN Controller API>&password=<Password For SDN User>&clid=<Cluster ID>`

このコマンドで使用するパラメーターを以下に示します。

名前	必須	種類	デフォルト	範囲	追加情報
ipv4	Yes	S	<未設定>	有効なIPv4アドレス範囲	SDNコントローラーのIPv4アドレス。
port	Yes	I	<未設定>	有効なポート範囲	SDNコントローラーのポート。
https	No	B	0 - HTTP	0 - HTTP 1 - HTTPS	使用するHTTPメソッド。
user	No	S	<未設定>		SDNコントローラーのRESTful APIにアクセスするためのユーザー名。
password	No	S	<未設定>		SDNコントローラーのRESTful APIにアクセスするためのパスワード。



名前	必須	種類	デフォルト	範囲	追加情報
clid	No	I	<未設定>	1 - 6	新規SDNコントローラーのクラスターID。番号を指定すると、該当するID番号を持つクラスターにSDNコントローラーが追加されます。指定したID番号を持つクラスターが存在している必要があります。番号を指定しない場合、新規クラスターにSDNコントローラーが追加されます。

期待される出力

```
<Response stat="200" code="ok">
<Success>Command completed ok</Success>
</Response>
```

3.19.9.2 SDNコントローラーの変更

既存のSDNコントローラーを変更するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/modsdncontroller?エラー! ハイパーリンクの参照に誤りがあります。>`

このコマンドで使用するパラメーターを以下に示します。

名前	必須	種類	デフォルト	範囲	追加情報
cid	Yes	I	番号の自動 インクリメント		変更するコントローラーのID。コントローラーのIDを取得するには、 <code>getsdncontroller</code> コマンドを実行します。
ipv4	No	S	<未設定>	有効なIPv4アドレス範囲	SDNコントローラーのIPv4アドレス。
port	No	I	<未設定>	有効なポート範囲	SDNコントローラーのポート。
https	No	B	0 - HTTP	0 - HTTP 1 - HTTPS	使用するHTTPメソッド。
user	No	S	<未設定>		SDNコントローラーのRESTful APIにアクセスするためのユーザー名。
password	No	S	<未設定>		SDNコントローラーのRESTful APIにアクセスするためのパスワード。
clid	No	I	<未設定>	1 - 6	新規SDNコントローラーのクラスターID。番号を指定すると、該当するID番号を持つクラスターにSDNコントローラーが追加されます。指定したID番号を持つクラスターが存在している必要があります。番号を指定しない場合、新規クラスターにSDNコントローラーが追加されます。

期待される出力



```
<Response stat="200" code="ok">
<Success>
<Data>
<controllers>
<cluster id="2"/>
<cluster id="3"/>
<cluster id="5"/>
<cluster id="6"/>
<cluster id="7"/>
<cluster id="8"/>
<cluster id="9"/>
<cluster id="10"/>
<cluster id="11"/>
<cluster id="12"/>
<cluster id="13"/>
<cluster id="14"/>
<cluster id="15"/>
<cluster id="16"/>
<cluster id="17"/>
<cluster id="18">
<controller id="30">
<ipv4>172.16.0.6</ipv4>
<port>8443</port>
<https>yes</https>
<user>sdn</user>
<password>****</password>
</controller>
</cluster>
<cluster id="19">
<controller id="31">
<ipv4>172.16.0.8</ipv4>
<port>8443</port>
<https>yes</https>
<user>sdn</user>
<password>****</password>
</controller>
</cluster>
<cluster id="20">
<controller id="32">
<ipv4>172.16.0.8</ipv4>
<port>8443</port>
<https>no</https>
<user/>
<password/>
</controller>
</cluster>
</controllers>
</Data>
</Success>
</Response>
```



3.19.9.3 SDNコントローラーの削除

SDNコントローラーを削除するには、以下のコマンドを実行します。

エラー! ハイパーリンクの参照に誤りがあります。>

コントローラーIDまたはクラスターIDを指定する必要があります。コントローラーIDとクラスターIDを調べるには、`getsdncontroller`コマンドを実行します。詳細はセクション3.19.9.4を参照してください。

期待される出力

```
<Response stat="200" code="ok">
<Success>Command completed ok</Success>
</Response>
```

3.19.9.4 既存のSDNコントローラーの表示

ロードマスター上に存在するSDNコントローラーのリストを表示するには、以下のコマンドを実行します。

`https://<LoadMaster IP Address>/access/getsdncontroller`

返送される出力の例を以下に示します。

```
<Response stat="200" code="ok">
<Success>
<Data>
<controllers>
<cluster id="2">
<controller id="29">
<ipv4>172.16.0.6</ipv4>
<port>8443</port>
<https>yes</https>
<user>sdn</user>
<password>****</password>
</controller>
</cluster>
<cluster id="3"/>
<cluster id="5"/>
<cluster id="6"/>
<cluster id="7"/>
<cluster id="8"/>
<cluster id="9"/>
<cluster id="10"/>
<cluster id="11"/>
<cluster id="12"/>
<cluster id="13"/>
<cluster id="14"/>
<cluster id="15"/>
<cluster id="16"/>
<cluster id="17"/>
```



```
</controllers>  
</Data>  
</Success>  
</Response>
```

出力に現れるパラメーターを以下に説明します。

- **Cluster ID (クラスターID)** :SDNコントローラーが属するクラスターの一意的IDです。

空のクラスターパラメーターのセクションは、過去に追加されたがその後削除されたクラスターに関係します。クラスターを新たに追加するたびに、新たなID番号が割り当てられます。

- **Controller ID (コントローラーID)** :SDNコントローラーのIDです。
- **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。
- **HTTPS**:SDNコントローラーへのアクセスにおいてHTTPS (yes) とHTTP (no) のどちらを使用するかが表示されます。
- **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。

3.20 RESTful APIによるHAの設定

以下の2つのセクションでは、RESTful APIを使用して通常のロードマスターおよびロードマスターfor AzureにHAを設定する方法について、ステップバイステップで説明します。

3.20.1 RESTful APIを使用して通常のロードマスターにHAを設定する

RESTful APIを使用して通常のロードマスターにHAを設定するのに必要なコマンド例を以下に示します。

1. 機器1をHA1に設定する:
`https://192.168.1.1/access/set?param=hamode&value=1`
2. HA1を再起動する:
`https://192.168.1.1/access/reboot?`
3. HA1のパートナーのアドレス (HA2のアドレス) を設定する:
`https://192.168.1.1/access/modiface?interface=0&PartnerIPAddress=192.168.1.2`



4. HAペアに共通のIPアドレスを設定する：
`https://192.168.1.1/access/modiface?interface=0&SharedIPAddress=192.168.1.10`
5. HA2をセカンダリに設定する：
`https://192.168.1.2/access/set?param=hamode&value=2`
6. HA2を再起動する：
`https://192.168.1.2/access/reboot?`
7. HA2のパートナーのアドレス（HA1のアドレス）を設定する：
`https://192.168.1.2/access/modiface?interface=0&partner=192.168.1.1`
8. HAペアに共通のIPアドレスを設定する：
`https://192.168.1.2/access/modiface?interface=0&shared=192.168.1.10`

LoadMasterでは、**reboot**などのコマンドが完了するまで数秒かかります。処理を記述する際は、**reboot**コマンドの後に適切な遅延を入れるよう考慮してください。

HAを削除するには以下のコマンドを使用します。

1. 非HAに設定する：
`https://192.168.1.1/access/set?param=hamode&value=0`
2. Reboot（再起動）：
`https://192.168.1.1/access/reboot?`

3.20.2 RESTful APIを使用してロードマスターfor AzureにHAを設定する

RESTful APIを使用してロードマスターfor AzureにHAを設定するのに必要なコマンド例を以下に示します。

1. マスターユニットをマスターHAモードに設定する：
`https://192.168.1.1/access/azurehamode?hamode=master`
2. マスターのHAパラメータ（パートナーアドレスおよびヘルスチェックポート）
`https://192.168.1.1/access/azurehaparam?partner=192.168.1.2&hcp=8444`
3. スレーブユニットをスレーブHAモードに設定する：
`https://192.168.1.2/access/azurehamode?hamode=slave`
4. スレーブのHAパラメータ（パートナーアドレスおよびヘルスチェックポート）を設定する：
`https://192.168.1.2/access/azurehaparam?partner=192.168.1.1&hcp=8444`



HAを削除するには以下のコマンドを使用します。

`https://192.168.1.1/access/azurehamode?hamode=single`

`https://192.168.1.2/access/azurehamode?hamode=single`



4. ロードマスターRESTful APIのスキプト例文

ロードマスターRESTful API は、ユーザーもしくはアプリケーションがロードマスターへ直接アクセスするのを許すための、多種のスキプトとアプリケーションの組み合わせが使用可能です。

RESTful APIの詳しい使用例については、[RESTful APIプログラマーズガイド](#) [テクニカルノート](#)を参照してください。



5. 付録A - パラメータの取得と設定

getコマンドとsetコマンドを使用して、さまざまなパラメータの取得と設定が行えます。以下に、そのパラメータのリストを示します。各パラメータの内容に関する説明は、前記のセクションを参照してください。

これは完全なリストではありません。

- dfltgw
- dfltgwv6
- admingw
- snat
- hatimeout
- hawait
- haprefered
- hamode
- haif
- havhid
- hastyle
- hainitial
- tcpfailover
- cookieupdate
- vmac
- sshaccess
- sshport
- wuiaccess
- mcast
- wuiiface
- wuiport
- sshiface
- hoverhelp
- routefilter
- transparent
- alwayspersist
- expect100
- localbind



- addcookieport
- subnetoriginating
- nonlocalrs
- multigw
- addforwardheader
- conntimeout
- authtimeout
- finalpersist
- tcptimestamp
- paranoia
- cachesize
- hostcache
- resetclose
- rfconform
- keepalive
- backupday
- backupenable
- backuphost
- backuphour
- backupminute
- backuppassword
- backuppath
- backupuser
- backupuser
- emailuser
- emaildomain
- emailpassword
- emailserver
- emailsslmode
- emailport
- emailcritical
- emailemergency
- emailerror
- emailinfo
- emailnotice
- emailwarn
- addvia



- allowupload
- dropatdrainend
- droponfail
- closeonerror
- limitinput
- rsarelocal
- slowstart
- subnetorigin
- syslogcritical
- syslogemergency
- syslogerror
- sysloginfo
- syslognotice
- syslogwarn
- sslrenegotiate
- emailenable
- irqbalance
- snmpenable
- snmpV3enable
- snmpv3user
- snmpv3userpasswd
- snmpcontact
- snmpcommunity
- snmplocation
- snmpHaTrap
- snmpv1sink
- snmpv2sink
- snmpclient
- snmptrapenable
- motd
- wuidisplaylines
- linearesplogs
- onlydefaultroutes
- sessionauthmode
- sessionidletime
- sessionmaxfailattempts
- sessioncontrol



- sessionlocalauth
- ntphost
- netconsole
- netconsoleinterface
- namserver
- radiusbackupport
- radiusbackupsecret
- radiusbackupserver
- radiusport
- radiussecret
- radiusserver
- radiusrevalidateinterval
- ldapserver
- ldapbackupserver
- ldapsecurity
- ldaprevalidateinterval
- geoclients
- geopartners
- geosshport
- ha1hostname
- ha2hostname
- hostname
- searchlist
- timezone
- admincert
- localcert
- time
- ntphost
- version
- Tethering
- multihomedwui
- logsplitinterval
- allowemptyposts
- OCSPPort
- OCSPUseSSL
- OCSPOnServerFail
- OCSPServer



- OCSPUrl
- L7LimitInput
- sdnstatsmode



6. 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。

WUI 設定ガイド

KEMPロードマスター 製品概要

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

GEO 機能説明

GEO Sticky DNS 機能説明

RESTful APIプログラマーズガイド テクニカルノート

ライセンス 機能説明

CLI インターフェイス説明

ロードマスターのクラスタリング 機能説明

ポートフォローウィング 機能説明



Document History

Date	Change	Reason for Change	Version	Resp.
Sep 2015	Release Updates	Updates for 7.1-30	6.0	KG
Oct 2015	Minor changes	Updated header and footer	7.0	LB
Oct 2015	Release updates	Updates for 7.1-30a	8.0	LB
Nov 2015	Minor changes	Enhancements made	9.0	LB
Dec 2015	Release updates	Updates for 7.1-32	10.0	LB
Jan 2016	Release updates	Updated for 7.1-32a	11.0	LB
Mar 2016	Minor changes	Enhancements made	12.0	LB
May 2016	Minor changes	Enhancements made	13.0	LB

