



GEO

製品概要

バージョン : 7.0

更新 : 2016 年 7 月

著作権

Copyright © 2002-2016 KEMP Technologies, Inc. 著作権は KEMP Technologies Inc.が所有しています。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は、Frank Denis（2004-2006 年）、Michael Shalayeff（2002 年）、Ryan McBride（2003 年）が著作権を保有し、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、配布時に提供されるドキュメント、および/またはその他の資料に、上記の著作権表示、本条件、以下の免責事項を複製して提示する必要があります。

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、明示的または暗示的を問わず、商品性や特定の目的への適合性などの保証は一切行いません。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報告を受けていたとしても、責任の法理、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失かどうかは関係なく）において、いかなる直接的、間接的、偶発的、特殊的、懲戒的、結果的損害（代替製品やサービスの調達費用、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など）に関する責め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、明示的または暗示的を問わず、上記著作権者の公式方針を表すものではありません。

ロードマスターのソフトウェアの一部分は、1989、1991 年に、51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA にある Free Software Foundation, Inc.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を変更せずそのまま複製して頒布することは誰もが許可されていますが、それを変更することは許されません。



このソフトウェアの一部は、マサチューセッツ工科大学のリージェンツが 1988 年に著作権を保有しています。

ソース形式およびバイナリ形式での再配布と使用は、上記の著作権表示および本パラグラフが、それらの全ての形式において複製され、それらの再配布と使用に関するすべての文書、広告素材その他の資料において、本ソフトウェアがカリフォルニア大学バークレー校により開発されたことを認知させる場合に許可します。大学の名前は、書面による事前の許可なしに、本ソフトウェアより派生した製品の保証または販売促進のために使用することはできません。

本ソフトウェアは“現状有姿”で提供され、明示的または黙示的を問わず、商品性や特定の目的への適合性などの保証は一切行いません。

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。

以下に定める条件に従い、本ソフトウェアおよび関連文書のファイル（以下“ソフトウェア”）の複製を取得するすべての人に対し、ソフトウェアを無制限に扱うことを無償で許可します。これには、ソフトウェアの複製を使用、複写、変更、結合、掲載、頒布、サブライセンス、および/または販売する権利、およびソフトウェアを提供する相手に同じことを許可する権利も無制限に含まれます。

上記の著作権表示および本許諾表示を、ソフトウェアのすべての複製または重要な部分に記載するものとします。

本ソフトウェアは“現状有姿”で提供され、明示的または黙示的を問わず、商品性や特定の目的への適合性、権利非侵害などの保証は一切行いません。作者または著作権者は、契約行為、不法行為、またはそれ以外であろうと、ソフトウェアに起因または関連し、あるいはソフトウェアの使用またはその他の扱いによって生じる一切の請求、損害、その他の義務について何らの責任も負わないものとします。

このソフトウェアの一部（1995 年に発行、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。

本ソフトウェアは“現状有姿”で提供され、明示的または黙示的を問わず、何らの保証もなく提供されます。いかなる場合であっても、本ソフトウェアの使用に起因する損害に関して作者は一切責任を負わないものとします。

以下に定める制限に従う限り、本ソフトウェアを商用アプリケーションを含む任意の目的に使用し、自由に変更、再配布することをすべての人に許可します。

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なりません。本ソフトウェアを製品にて使用する場合、製品の文書に謝辞を入れて頂ければ幸いです、必須ではありません。
2. ソースを変更した場合、その旨を明示しなければなりません。そのソースがオリジナルであるという虚偽の表示をしてはなりません。
3. いかなる場合であっても、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してはなりません。

このソフトウェアの一部は、インターネットシステムズコンソーシアム 2003 年に著作権を保有しています。

手数料の有無にかかわらず、本ソフトウェアの使用、複製、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すべてのコピーに表示されている限り許可されます。

本ソフトウェアは、“現状有姿”で提供され、作書は、市場への適合性や適切性へのすべての黙示的保証を含め、本ソフトウェアに関して一切の保証をいたしません。作者は、いかなる場合においても、本ソフトウェアの性能、使用または不使



用によって生じるいかなるデータまたは利益の損失、契約、過失、またはその他の不法行為から生じる特別、直接的、間接的は損害、または結果的損害に対して一切の責任を負いません。

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



目次

1	はじめに.....	7
1.1	ドキュメントの目的.....	8
1.2	対象読者.....	8
2	GEO の概要	9
2.1	高可用性 (HA) /信頼性	9
2.2	Fail Over (フェイルオーバー)	9
2.3	Failure Delay (障害遅延) と Site Recovery (サイト復旧) モード	10
2.4	Unanimous Cluster Health Checks (全部一致方式のクラスターヘルスチェック)	11
2.5	パブリックリクエスト/プライベートリクエスト	12
2.6	Speed (速度)	13
2.7	拡張性 (スケーラビリティ)	13
2.8	管理容易性.....	14
2.9	Selection Criteria (選択条件)	14
2.9.1	ラウンドロビン.....	14
2.9.2	重み付けラウンドロビン.....	15
2.9.3	固定重み.....	15
2.9.4	実サーバー負荷.....	15
2.9.5	近接性.....	16
2.9.6	ロケーションベース.....	16
2.9.7	All Available (利用可能なものすべて)	17
2.9.8	IP 範囲の選択条件.....	17
2.10	クラスター.....	18
2.10.1	クラスタータイプ.....	19
2.11	実サーバー/クラスターのヘルスチェック	19
2.12	IP Blacklist (IP ブラックリスト)	22
2.13	リモート管理.....	22
2.14	GEO の応答およびリクエストに使用するインターフェイスの指定.....	22



2.15	代替ゲートウェイのサポートの有効化.....	23
2.16	GEO の例	23
	参考ドキュメント.....	25
	ドキュメント履歴.....	26

1 はじめに

GEO は、パフォーマンスが最も高く地理的に最も近いデータセンターに、シームレスなフェイルオーバーとフェイルバックを確実に行います。これにより、Microsoft Exchange などの Web ベースのアプリケーションを最大限活用することが可能になります。サービスが停止した場合、設定されたポリシーに基づきトラフィックが自動的に制御されるため、サービス停止による影響や、人手による作業を最小限に抑えることができます。

GEO は 2 つの形態で提供されます。

- スタンドアロン GEO 製品
- KEMP ロードマスターの一部であるグローバルサーバーロードバランシング (GSLB) 機能パック

本ドキュメントで「ロードマスター」というときは、GEO ロードマスターまたは GSLB 機能パックが有効なロードマスターのいずれかのことをいいます。GEO は、KEMP のサーバーロードマスターのハードウェアと同じ管理インターフェイスを持ち、syslog の記録や E メール通知、インターフェイスのボンディング、ギガビットのサポートといったすべての基本技術を備えています。GEO には高度なアプリケーションヘルスチェック機能が用意されており、利用できないサービスやデータセンターがクライアントから見えないようになっています。ヘルスチェックはサービスレベルまたはサイトレベルで実行可能で、完全修飾ドメイン名 (FQDN) に基づいていつトラフィックを迂回すべきかを柔軟に決定できます。

GEO には、**ラウンドロビン、重み付けラウンドロビン、固定重み、実サーバー負荷、ロケーションベース、近接性**など、数多くの負荷分散アルゴリズムが用意されています。「ラウンドロビン」負荷分散は、すべてのアクティブなデータセンターに対して使用可能で、災害復旧のための重みおよび連鎖フェイルオーバーオプションを備えています。**ロケーションベース**の負荷分散は、作成したポリシーの定義に従って、クライアントが位置する国や大陸、IP アドレス範囲に基づき決定されたデータセンターにクライアントを誘導します。近接性は、**ロケーションベース**より一歩進んだ方式で、緯度経度の単位で近接性を定義できます。GEO はロードマスターと安全かつシームレスに統合され、ロードマスターから提供されるローカルデータセンターの測定基準を使用して「実サーバー負荷」の負荷分散を実現しています。この機能により、最も処理能力に余裕があるデータセンターにクライアントを接続できます。

GEO は分散型 (アクティブ/アクティブ) 高可用性構成として展開することが可能であり、複数の機器で情報が安全に同期されます。既存の権威ドメイン名サービス (DNS) に GEO を導入する際の統合作業やリスクは必要最小限に抑えられており、既存の DNS 資源を最大限活用できます。



1.1 ドキュメントの目的

本ドキュメントでは、GEO 製品とその機能についての概要を説明することを目的としています。

1.2 対象読者

本ドキュメントは、KEMP の GEO およびその機能について知りたい方を対象としています。

2 GEO の概要

GEO 製品とその機能の概要については、以下のセクションを参照してください。

2.1 高可用性 (HA) / 信頼性

GEO はクライアントリクエスト配信機能によってデータセンター機能を最適化するとともに、データセンターリソースの障害を迅速に検出して必要に応じてトラフィックをリダイレクトする機能によってサービス停止を防ぎます。監視と負荷分散は、開放型システム間相互接続 (OSI) 基本参照モデルのレイヤー3 および 4 に基づいています。HA に採用されたのは、複数のロードマスターによってハードウェアまたはネットワーク接続の単一障害点を保護する機能です。それぞれの KEMP ロードマスターを個別に構成して、ネットワークリンクレイヤーの冗長性を確保することも可能です。

2.2 Fail Over (フェイルオーバー)

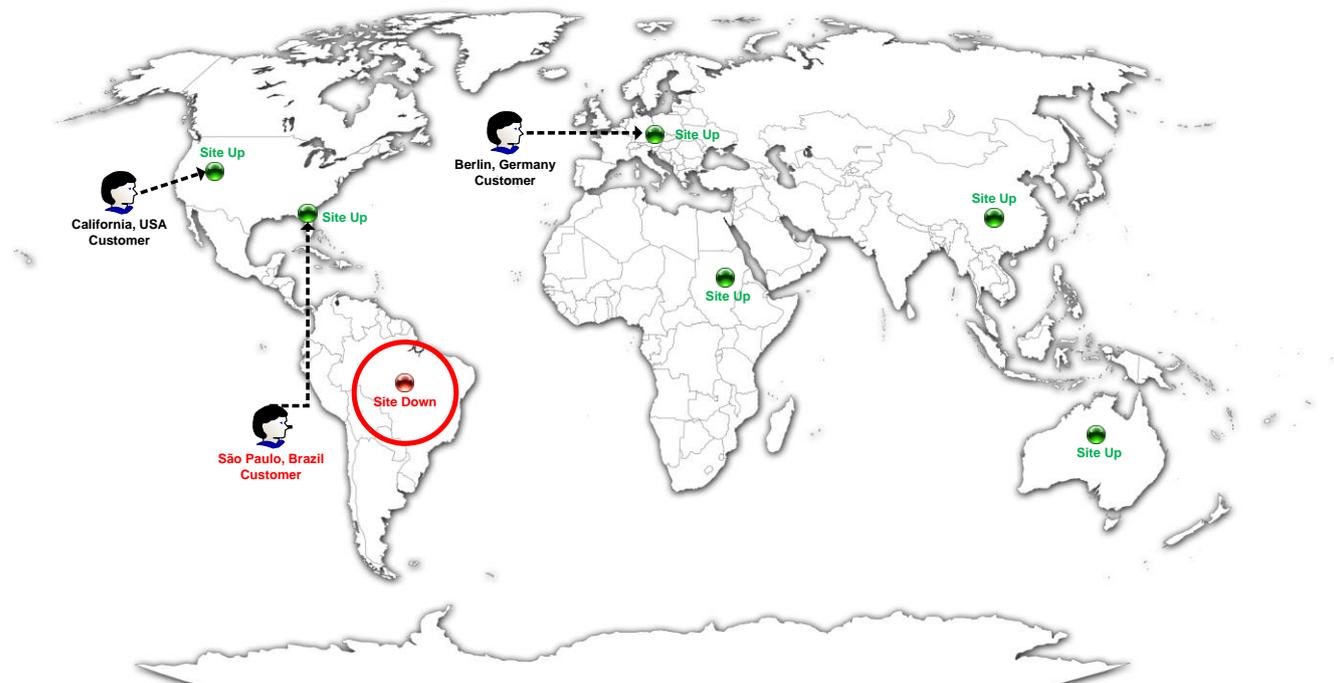


図 2-1: グローバルマルチデータセンターの負荷分散の例

フェイルオーバーによって、ロケーションベースの FQDN で最適な一致が得られない場合でも、リクエストに最も適したサイトを選択できます。""Fail Over"オプションが有効な場合に、特定の地域からリクエストが送信されてそのターゲットが停止していると、その接続はフェイルオーバーされ、階層の次のレベルにて応答が行われます。それが不可能な場合は、最も近い（近接の）ターゲットが応答が行います。それが不可能な場合は、最も少ないリクエストを持つターゲットが選択されます。例えば、アイルランドからリクエストが送信された場合に、"Ireland"（アイルランド）に割り当てたサイトが利用できないと、"Europe"（ヨーロッパ）に割り当てたサイトが選択されます。ヨーロッパに割り当てたサイトが利用できない場合には、"Everywhere"（全地域）に割り当てたサイトが選択されます。このサイトも利用できない場合は、利用可能なサイトのうち最もリクエストが少ないサイトが選択されます。""Fail Over"の設定はすべてのターゲットに影響を与えます"Fail Over"オプションは、"Selection Criteria"が"Location Based"に設定されている場合に限り利用できます。

"Failover"は各 GEO ノードで設定されます。パートナーの GEO ユニットが設定されている場合、すべてのノードが同じ設定で動作しているとみなして構いません。ある 1 つの GEO で行った設定は、他のすべての GEO ノードに同期されます。

2.3 Failure Delay（障害遅延）と Site Recovery（サイト復旧）モード

デフォルトでは、ターゲット（リクエストの通常のリダイレクト先） - すなわち、サーバーが停止している場合、 - を利用できない場合、利用可能な次善のターゲット候補にリクエストがリダイレクトされます。元のターゲットは利用可能になった時点で、指定されたタイムアウトまたはフェイルオーバー後にローテーションに組み込まれます。ただし、必要に応じて、"Failure Delay"（障害遅延）を設定できます。"Failure Delay"は、Exchange データセンターで特に重要です。

フェイルオーバーに短時間の遅延を持たせると、軽微な障害や一時的な障害の発生時にフェイルオーバーを発生させないように設定することが可能です。フェイルオーバーの遅延を設定することで、セカンダリサイトが必要なレベルのサービスを提供できる状態であることを管理者が確認する時間も確保できます。

ロードマスターには"Failure Delay"オプションが用意されており、このオプションを有効にすると、サイトの障害を検出した際に設定された時間だけフェイルオーバーの発生を遅らせることが可能です。遅延時間経過後にサイトが復旧している場合には、フェイルオーバーは開始されません。サイトがまだ復旧していない場合は、通常どおりフェイルオーバーが開始されます。

"Failure Delay"を設定すると、その下に"Site Recovery Mode"という別のオプションが利用可能になります。2 つのモードが用意されています。

- **Automatic（自動）**: 復旧すると直ちにサイトの動作が開始されます。



- **Manual (手動)** :サイトに障害が発生するとそのサイトは無効になります。通常動作に復旧するには手動の作業が必要になります。

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

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

例えば、**example.com** が、クラスター **cl58** に属するアドレスとして、172.21.58.101、172.21.58.102、172.21.58.103 を持っていたとします。

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

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

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

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

"Unanimous Cluster Health Checks"を有効にすると、設定によっては、FQDN のアドレスが強制的に停止させられたり、バックアップ状態になったりする場合があります。例えば、アドレスが強制的に停止させられ、全部一致の方針が適用されている間にそのアドレスをクラスターから外すと、そのアドレスはバックアップ状態になります。同様に、全部一致の方針が適用されているクラスターにアドレスを追加し、そのクラスターのいずれかのアドレスが停止している場合、新たに追加したアドレスが強制的に停止させられます。この状態変化は直ちに発生しない場合がありますが、次のヘルスチェック実行時には発生します。



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

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

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

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

2.5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 7.1-29 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
----	---	-----------	-------------



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 1:パブリック/プライベートリクエストの設定

2.6Speed (速度)

GEO によって、ミッションクリティカルなサーバーが継続的に利用可能になり、処理が確実に実行されます。GEO では、サーバーとアプリケーションの負荷を監視できます。この情報に基づいて、ユーザーリクエストは最も処理能力に余裕があるクラスターにリダイレクトされます。このトラフィックのインテリジェントなリダイレクトによって、ロードマスターはパフォーマンスの低下を招く可能性があるサーバーの過負荷状況とラウンドトリップの伝達遅延を排除し、エンドユーザーアプリケーションの処理速度の向上を可能にします。

2.7拡張性 (スケーラビリティ)

GEO は、巷間よく語られるスケーラビリティのジレンマを解決します。「規模拡大は難しい。スケーラビリティが鍵を握る」GEO は、ネットワークサーバーの負荷増加に継続して対処しながら、優れた信頼性をもたらすことで、この考え方に見られる拡張性のジレンマを解決します。具体的なポイントは、次のとおりです。GEO:



- サーバーアレイやデータセンター全体にまたがってトラフィックをインテリジェントに分配する
- ネットワークトラフィックの増加に対処する目的で、規模やコストが増加し続けているサーバーを導入する必要性を低減する
- 複数の分散型アプリケーションサーバーを単一の仮想サーバーとして機能可能にする
- アプリケーションリソースを単一の場所に配置した場合のリスクを低減する
- エンドユーザーへのサービス提供を中断せずに、新しいリソースの追加や、データセンターの定期的なメンテナンスを可能にする
- 複数の異種ハードウェアプラットフォームで使用可能であり、組織による従来のハードウェアインストールへの投資の保護と同時に、将来的なハードウェア投資との統合を可能にする

2.8 管理容易性

GEO はセットアップしやすく、管理も容易です。ネットワーク管理も簡素化され、管理者はエンドユーザーへのサービス提供を中断せずに、新しいサーバーを展開することも、定期的なメンテナンス中に個別のデータセンターをオフラインに移行することもできます。サービスに影響を及ぼすことなく、GEO を既存の DNS インフラストラクチャーに統合して、分散型の管理を実現できます。

2.9 Selection Criteria (選択条件)

選択した選択基準によって、GEO で受信されたリクエストが FQDN の IP アドレスエンドポイントにまたがってどのように分配されるかが決定されます。

選択基準は、リアルタイムで変更できます。事前に設定した情報は、変更中も保持されます。FQDN ごとに許可される選択基準は 1 つだけです。各 FQDN には、固有の選択基準を設定できます。次のセクションでは、ロードマスターで利用可能な選択基準の概要について説明します。

2.9.1 ラウンドロビン

ラウンドロビン方式では、受信されたリクエストは順番に IP アドレスエンドポイントにまたがって分配されます。

FQDN の IP アドレスエンドポイントに該当するのは実サーバー、ロードマスター、データセンターであり、FQDN の設定に応じて異なります。

この方式を選択した場合、FQDN に割り当てられるすべての IP アドレスエンドポイントについて、リソース容量が同程度であり、同じアプリケーションをホスティングするこ



とが求められます。この前提条件によって、ラウンドロビンシステムはシンプルかつ効果的な分配方法であると位置付けられます。

ただし、各 IP アドレスエンドポイントの処理容量が異なる場合、ラウンドロビンシステムを使用すると、現在の処理に対応できない性能の低い IP アドレスエンドポイントにも照会の順番がくることとなります。このため、性能の低い IP アドレスエンドポイントが過負荷状態になる可能性があります。

この選択基準は、地理的な IP データベースには依存しません。

2.9.2 重み付けラウンドロビン

この方式では、受信されたリクエストを順番にクラスターにまたがって分配できるようにするとともに、IP アドレスエンドポイントに事前に割り当てられた静的な重みも考慮することで、シンプルなラウンドロビン方式の機能を拡張します。

管理者は IP アドレスエンドポイントの重みを設定することで、IP アドレスエンドポイントの利用可能な処理容量をシンプルに定義します。たとえば、処理効率が最も高いデータセンター A に重み 100、その次に高いデータセンター B に重み 50 を設定するとします。この場合、データセンター B が最初のリクエストを受けるまでに、データセンター A は 2 つ連続でリクエストを受けることとなります。

この選択基準は、地理的な IP データベースには依存しません。

2.9.3 固定重み

他の IP アドレスエンドポイントとの比較で、最も高い重みの IP アドレスエンドポイントが必ず使用されます。ただし、最も高い重みのサーバーで障害が発生した場合、次に高い重みの IP アドレスエンドポイントが利用可能になり、クライアントの処理に対応します。各 IP アドレスエンドポイントの重みは、IP アドレスエンドポイント間の優先度に基づいて割り当てられます。障害が発生した IP アドレスエンドポイントは再び利用可能になった時点で、自動的にリクエストの受信を開始します。

この選択基準は、地理的な IP データベースには依存しません。

2.9.4 実サーバー負荷

ロードマスターとの統合によって、ロードマスターからデータセンターレベルのメトリックスが取得可能になります。ロードマスターはリアルタイムで使用され、最も処理能力に余裕があるクラスターにクライアントをリダイレクトします。ロードマスターはロードマスターの接続統計情報をポーリングして、利用可能なデータの一部またはすべてを使用して、関連する仮想サービスのビジューレベル全般を判定します。リクエストを受信するのは、最も低い値のクラスターです。各 IP アドレスエンドポイントはクラスターに接続している状態で、"Checker"オプションが"Cluster Checks"であることが必須です。



ポーリング対象のロードマスターでは、クラスターのビジーレベルを判定するため、Adaptive Agent をセットアップする必要があります。Adaptive Agent の詳細については、**Adaptive Agent のインストール - Windows**、**テクニカルノート**を参照してください。

この選択基準は地理的な IP データベースには依存しませんが、ロードマスタークラスターを必要とします。

2.9.5 近接性

"Proximity" (近接) スケジューリングを使用する場合、GEO データベースに基づき新しいパブリックサイトが地理的座標に自動的にマッピングされます。新しいプライベートサイトは 0°0'0" にマッピングされ、期待どおりに機能します。負荷分散を正しく行うには、この座標を正確な値で上書きする必要があります。

クライアントソース IP アドレスは、ロードマスターによりリアルタイムでジオコード化されてから、クラスターまたは FQDN 実サーバー定義のジオコードの経度および緯度と照合されます。クライアントに提供される IP アドレスは、クライアントに最も近い位置にあるクラスターまたは IP アドレスエンドポイントのものです。クラスターまたは IP アドレスエンドポイントの経度および緯度は自動的に事前設定され、手動で上書きすることもできます。

この選択基準は、地理的な IP データベースに依存します。

プライベート IP アドレスで選択基準 "Proximity" (近接) を使用するには、すべてのプライベートサブネットに対して "IP Range Selection Criteria" (IP 範囲選択基準) を設定する必要があります。さらに、座標と国を設定する必要があります。これらが設定されていない場合、プライベート IP アドレスからのリクエストは拒否されます。

IP 範囲選択基準に関する詳細は、**セクション 2.9.7** を参照してください。

2.9.6 ロケーションベース

クライアントのソース IP アドレスは、定義済みのロケーションにリアルタイムでジオコード化されます。たとえば、国または大陸を使用して、各地域を特定の IP アドレスエンドポイントに割り当てて、ロケーション定義に一致するクライアントリクエストを対応するデータセンターにリダイレクトするように設定できます。

同じ IP アドレスエンドポイントへの割り当ての場合、国による限定は大陸による限定よりも優先されます。ターゲットが国に設定されていて、異なるターゲットがその国を含む大陸に設定されている場合、国によってターゲットが選択されるのは、リクエスト元がその国である場合に限定されます。つまり、階層で最も高い位置のターゲットが優先されます。この階層は、次のとおりです。

"Everywhere" (全地域) > "Continent" (大陸) > "Country" (国)



クライアントの場所は、IP アドレスエンドポイントの順序付きリストと照合されます。Web ユーザーインターフェイスに表示される IP アドレスエンドポイントの順序は、照合基準に関連します。同じ国コードを持つ複数のサイトがある場合、リクエストは各サイトにラウンドロビン方式で配信されます。

この選択基準は、地理的な IP データベースに依存します。

2.9.7 All Available (利用可能なものすべて)

"All Available"の選択基準は、A、AAAA、ANY クエリリクエストに対し、健全と思われるすべてのターゲットを返します。返されるリストの内容は、"Public Requests"および"Private Requests"の設定によっても制御されます。

- "Public Sites Only"を選択すると、パブリックアドレスのみリストに含まれます。同様に、"Private Sites Only"を選択すると、プライベートアドレスのみリストに含まれます。
- "Prefer Public"を選択すると、利用できるパブリックアドレスが存在しない場合を除き、パブリックアドレスのみリストに含まれます。利用できるパブリックアドレスが存在しない場合、利用可能なプライベートアドレスが存在すれば、そのプライベートアドレスがリストに含まれます。同様に、"Prefer Private"を選択すると、利用できるプライベートアドレスが存在しない場合を除き、プライベートアドレスのみリストに含まれます。利用できるプライベートアドレスが存在しない場合、利用可能なパブリックアドレスが存在すれば、そのパブリックアドレスがリストに含まれます。
- "All Sites"を選択すると、利用可能なすべてのアドレスがリストに含まれます。

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

2.9.8 IP 範囲の選択条件

"IP Range Selection Criteria" (IP 範囲の選択基準) メニューオプションでは、IP アドレスまたは IP アドレス範囲に当てはまる座標や場所を指定できます。また、カスタムロケーションも追加できます。独自の場所を追加して、手動で定義した内部 IP アドレス/範囲に基づいてユーザーをサービスにルーティングすることもできます。データセンターごとに最大 64 個の IP 範囲を定義できます。その範囲は、IPv4 または IPv6 のネイティブな範囲により制限されます。IP アドレスまたはネットワークを指定できます。ここで有効なエントリーは、単一の IP (たとえば、**192.168.0.1**) または Classless Inter-Domain Routing (CIDR) フォーマットのネットワーク (たとえば、**192.168.0.0/24**) です。

GEO では、"IP Range Selection Criteria"でのカスタム定義 IP アドレスのサブネット優先準備をサポートしています。例：



- 172.16.0.0/12 – アメリカ
- 172.16.100.0/21 – イギリス
- 172.16.200.0/21 – ドイツ

GEO では、複数のエントリが一致した場合、最も長いプレフィックスが解決に使用されます。したがって、上記の例では、172.16.100.1 は/21 イギリスの解決ルールと一致することになります。

2.10 クラスタ

クラスターはデバイスの論理グループであり、可用性のチェックに使用できる任意の IP アドレスとして物理的に定義できます。クラスターによって、一元的なヘルスチェックに加えて、実サーバー、ロードマスター、または FQDN で定義されたその他のリソースのグループ化が可能になり、サイトまたはデータセンターレベルのデバイス管理が実現します。次の図は、エッジルーター、ファイアウォール、ロードバランサーなど、一般的なクラスターデバイスをわかりやすく示しています。これらのデバイスのヘルスチェックによって、各サービスの背後にあるデバイスの可用性に関する情報を集約できます。

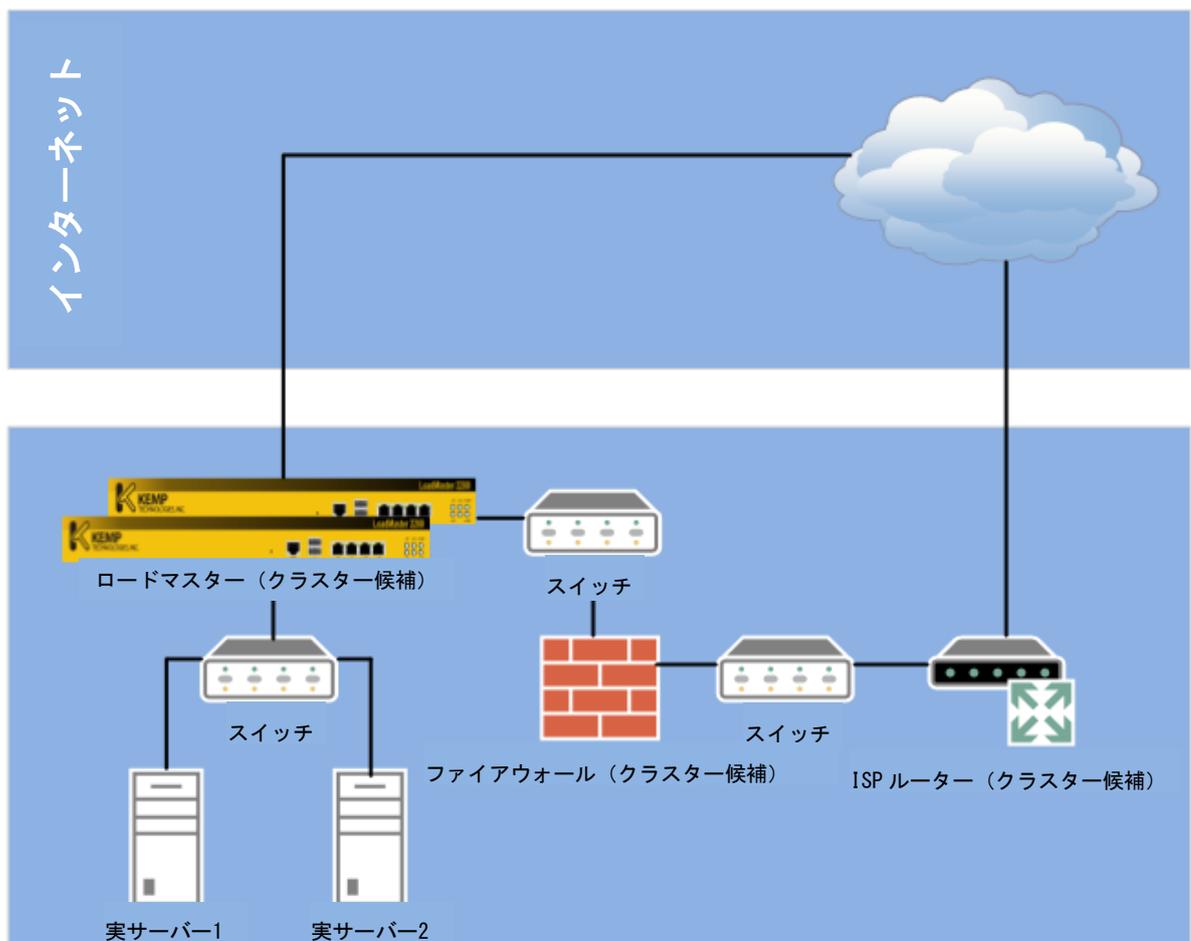


図 2-2: クラスタ候補のデバイスの例

- **ISP ルーター:**ISP のエッジルーターのチェックによって、ISP ネットワーク接続ロスの迅速な検出が可能
- **ファイアウォール:**ファイアウォールのチェックによって、ISP ネットワークが利用可能であることを確認して、データセンターに配置されている機器のアプリケーション応答測定 (ARM) を可視化
- **ロードマスター:**ロードバランサーのチェックによって、ISP が利用可能かどうか、ネットワークインフラストラクチャーが利用可能かどうか、実サーバーの応答が想定どおりかどうかを確認

2.10.1 クラスタータイプ

クラスタの定義時には、そのタイプを設定できます。利用可能なクラスタタイプについて、以下で説明します

- **Default (デフォルト)** :クラスタタイプを"Default"に設定すると、利用可能な以下の3つのヘルスチェックのいずれかを使用して、クラスタに対するヘルスチェックが行われます。
 - **None (なし)** :ヘルスチェックは行われません。そのため、マシンは常に稼働中であるように見えます。
 - **ICMP Ping:**クラスタの IP アドレスに Ping を送信することでヘルスチェックが行われます。
 - **TCP Connect (TCP 接続)** :指定したポートにてクラスタの IP アドレスに接続することでヘルスチェックが行われます。

ヘルスチェックの頻度は、"Miscellaneous Params"画面で指定できます。

- **Local LM (ローカル LM)** : "Type"として"Local LM"を選択すると、"Checkers"フィールドは自動的に"Not Needed"に設定されます。これは、クラスタがローカルマシンであるため、ヘルスチェックが必要ないためです。
- **Remote LM (リモート LM)** :このタイプのクラスタのヘルスチェックは"Implicit" (暗黙) です (ヘルスチェックはSSHにより行われます)。

2.11 実サーバー/クラスタのヘルスチェック

GEO では、レイヤー3、レイヤー4、およびレイヤー7のヘルスチェックによって、IP アドレスエンドポイントとクラスタの可用性を監視します。いずれかのサーバーが既定の時間内にヘルスチェックに応答しない場合、該当するサーバーの重みはゼロに減らされます。このゼロの重みには、実サーバーがオンラインに戻るまで、仮想サービス構成から実サーバーを除外する効果があります。



ヘルスチェックは、ロードマスターから実行されます。このため、ロードマスターが各クラスターおよび IP アドレスにアクセスできる状態であることが重要です。すべてのチェックに失敗した場合、デフォルトのゲートウェイが正しく動作していることを確認します。

レイヤー	種類	説明
None (なし)	None (なし)	チェックは実行されません。
Layer 3 (レイヤー7)	ICMP	ロードマスターが ICMP エコーリクエスト (ping) を実サーバーに送信します。IP アドレスエンドポイントがこのチェックに失敗したとみなされるのは、既定の回数の再試行で既定の応答時間内に ICMP エコー応答で応答しなかった場合です。このヘルスチェックが関連するのは、エンドポイントがロードマスターと異なる場合に限定されます。
Layer 4 (レイヤー7)	TCP	ロードマスターが既定のサービスポートで IP アドレスエンドポイントへの TCP 接続を確立しようと試みます。サーバーがチェックに合格したとみなされるのは、応答時間内に TCP SYN ACK で応答した場合です。この場合、ロードマスターは TCP RESET を送信して、接続を終了します。サーバーが既定の回数の再試行で既定の応答時間内に応答しなかった場合、停止状態であるとみなされます。

レイヤー	種類	説明
Layer 7 (レイヤー7)	Cluster Check (クラスターチェック)	<p>クラスターの IP アドレスに対してヘルスチェックが実行されます。異なるタイプのクラスターを定義できません。ヘルスチェックは、タイプごとに異なります。</p> <p>Default Cluster Type (デフォルトクラスタータイプ) :Default Cluster Type (デフォルトクラスタータイプ) : ICMP Ping または TCP Connect ヘルスチェック ("Manage Cluster" (クラスターの管理) オプションで選択した内容に応じて異なる) が実行されます。</p> <p>Remote LM Cluster Type (リモート LM クラスタータイプ) :SSH 接続を試みますロードマスター固有の統計情報が取得されて、FQDN 実サーバーと照合されます。一致する仮想サービス IP アドレスが見つからなかった場合、実サーバークラスターのリストでダウン状態としてマークされます。接続許可をロードマスターに付与する必要があります。</p> <p>Local LM (ローカル LM) :この方式が必要になるのは、ヘルスチェックが正しく機能するように、ロードマスターが GSLB 機能パックとともに導入されている場合です。</p>

"Slection Criteria"として"Real Server Load"が設定されており、"Checker"が"Cluster Checks"に設定されており、クラスターの"Type"が"Local LM"または"Remote LM"に設定されている場合、関連付けられている仮想サービスを"Mapping Menu"ドロップダウンリストで選択する必要があります。

"Mapping Menu"ドロップダウンリストには、そのロードマスターからの仮想サービスの IP アドレスのリストが表示されます。ここには、ポートを持たない各仮想サービスの IP アドレス、および仮想 IP アドレスとポートのすべての組み合わせがリストされます。このマッピングに割り当てられている仮想 IP アドレスを選択してください。

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

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



2.12 IP Blacklist (IP ブラックリスト)

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

この機能に関する詳細 (IP ブラックリストの設定方法など) は、**GEO 機能説明**を参照してください。

2.13 リモート管理

フルリモート管理は、デフォルトの SSL ポート 443 を使用して HTTPS 上で実行されます。制限付きリモート管理は、デフォルトのポート 22 を使用して SSH 上で実行できます。この内容には、システムレベルの設定、デバッグ/高度なトラブルシューティングが含まれますが、DNS 管理は含まれません。リモート管理用に推奨されるグラフィカルユーザーインターフェイスは HTTPS です。

ロードマスターとの HTTPS 接続のネゴシエーション時に、ホスト名と IP または証明書の署名者の不一致の確認など、セキュリティ警告を確認するように求められる場合があります。このような警告に関係なく、ロードマスターの処理はすべてセキュアなチャンネル上で実行されるので、警告の無視を承認/許可しても安全です。署名機関に関する警告を完全に除外するには、メインメニューで"**Download Root Cert**" (ルート証明書のダウンロード) をクリックしてルート証明書をダウンロードします。

2.14 GEO の応答およびリクエストに使用するインターフェイスの指定

デフォルトでは、デフォルトゲートウェイを使用して DNS 要求をリッスンして応答を返します。

"Use for GEO Responses and Requests" というフィールドがあり、これを使用するとリッスンを行うインターフェイスを追加できます。このオプションを有効にすると、GEO はそのインターフェイスで設定された "**Additional addresses**" でもリッスンします。このオプションにアクセスするには、"**System Configuration > Network Setup**" を選択して関連するインターフェイス番号を選択します。

このオプションは、デフォルトゲートウェイを含むインターフェイスでは無効にできません。デフォルトでは eth0 に設定されています。

2.15 代替ゲートウェイのサポートの有効化

複数のインターフェイスが有効になっている場合、デフォルトゲートウェイを他のインターフェイスに移動するオプションを使用できます。

このオプションを有効にすると、"Interfaces"画面に"Use for Default Gateway"オプションが追加されます。

GEO のみのロードマスターの場合、"Enable Alternate GW support"オプションは"Certificates & Security" > "Remote Access"で表示されます。

ロードマスター + GEO の製品の場合、"Enable Alternate GW support"オプションは"System Configuration" > "Miscellaneous Options" > "Network Options"で表示されます。

2.16 GEO の例

このセクションでは、GEO が通常どのように機能するか説明します。なお、この構成では、ロードマスターはデータセンターの外にあるものとして説明します。このような構成も可能ですが、ロードマスターは、データセンター内に置いて運用するのが一般的です。

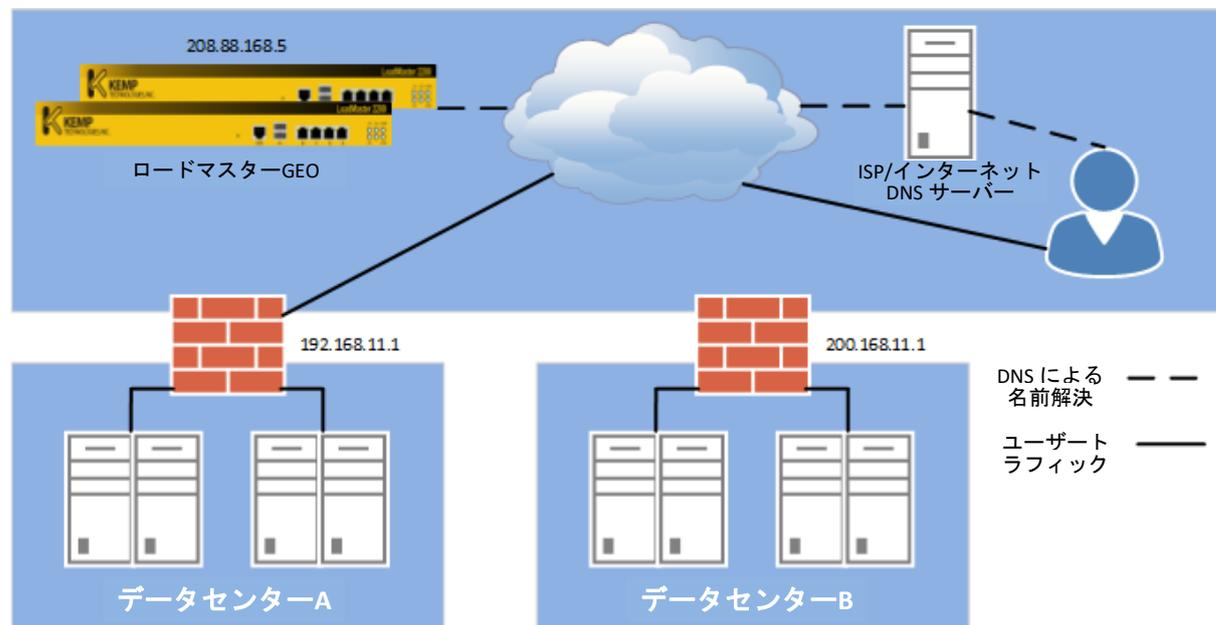


図 2-3:ロードマスター概要

1. クライアントが、Web ブラウザーのアドレスバーに Web サイトのアドレスを入力します (例: `www.web.example.com`)。
2. 名前解決要求がそのドメインの権威 DNS サーバーに渡されます。

3. 通常、リクエストは権威 DNS サーバーで解決されますが、この場合、権限はロードマスターに委譲されています。
4. 権威 DNS サーバーには、ロードマスターをポイントする A レコードと、対応する IP による逆引き参照用の PTR レコードが保持されています。
ロードマスターに委譲されたホスト名ごとに NS レコードが作成されて、たとえば、次のように、ロードマスター用に作成された A レコードに対して設定されます。

レコードタイプ (A および PTR)

lm1.example.com = 208.88.168.5

レコードタイプ (NS)

www.example.com = lm1.example.com

5. 権威 DNS サーバーにより名前解決要求がロードマスターに渡されます。
6. ロードマスターは、設定された FQDN のリストを参照し、FQDN をどの IP に解決するかを判断します。この例では、FQDN をデータセンターA (192.168.11.1) またはデータセンターB (200.168.11.1) のいずれかの IP に解決します。
7. ロードマスターは、定期的にヘルスチェックを行っているため、データセンターが2つとも健全かどうか把握しています。
8. ロードマスターは、選択基準に基づいて、リクエストをどの IP アドレスに解決するか決定します。
この例では、リクエストをデータセンターA (192.168.11.1) に解決するものとします。
何らかの理由によりデータセンターA のヘルスチェックに失敗した場合は、リクエストはデータセンターB に解決されます。
9. ロードマスターは、IP アドレスを DNS サーバーに返し、DNS サーバーはそのアドレスをクライアントに返します。
10. クライアントは、データセンターA (192.168.11.1) に直接接続します。

参考ドキュメント

特に明記されていない限り、以下のドキュメントは
<http://kemptechnologies.com/documentation>から入手できます。

ウェブユーザーインターフェイス (WUI) 設定ガイド

Adaptive Agent のインストール - Windows、テクニカルノート

GEO 機能説明

ドキュメント履歴

日付	変更	変更理由	バージョン	回答者
2014年10月	リリース更新	7.1-22/2.1-22 のリリースにともなう更新	1.10	LB
2015年1月	リリース更新	7.1-24/2.1-24 のリリースにともなう更新	1.11	LB
2015年1月	小規模な変更	誤記訂正	1.12	LB
2015年9月	リリース更新	7.1-30 のリリースにともなう更新	3.0	KG
2015年10月	小規模な変更	ヘッダーとフッターの更新	4.0	LB
2016年1月	小規模な変更	「著作権表示」の更新	5.0	LB
2016年3月	リリース更新	7.1-34 のリリースにともなう更新	6.0	LB
2016年7月	リリース更新	7.1-35 のリリースにともなう更新	7.0	LB