CHAPTER 6

# 実サーバおよびサーバ ファームの設定

この章では、サーバ ロード バランシングの概要および ACE アプライアンスでロード バランシングを実行するための実サーバおよびサーバ ファームの設定手順について説明します。

（注） ACE CLI を使用して名前付きオブジェクト（実サーバ、仮想サーバ、パラメータ マップ、クラス マップ、ヘルス プローブなど）を設定するとき、Device Manager（DM）でサポートされるのは、1 ～ 64 文字の英数字文字列を使用したオブジェクト名であることに注意してください。オブジェクト名には、下線（_）、ハイフン（-）、ドット（.）、およびアスタリスク（*）の特殊文字を含めることができます。スペースは使用できません。

ACE CLI を使用して、DM でサポートされていない特殊文字を含んだ名前付きオブジェクトを設定した場合、DM を使用して ACE を設定できない場合があります。

この章の内容は、次のとおりです。



## サーバ ロード バランシングの概要

サーバ ロード バランシング（SLB）とは、ロード バランシング デバイスが、サービスを求めるクライアント要求の送信先サーバを決定することです。たとえば、クライアント要求は、Web ページを求める HTTP GET またはファイルのダウンロードを求める FTP GET から構成することができます。ロード バランサのジョブは、クライアント要求に対応できるサーバを選択し、サーバにもサーバ ファーム全体にも過負荷を与えずに、できるだけ短時間に選択を行うことです。

設定するロード バランシング アルゴリズム、つまりプレディクタに応じて、ACE アプライアンスでは一連のチェックおよび計算を実行し、各クライアント要求に最良に対応できるサーバを決定します。ACE アプライアンスは、負荷に対して接続数が最小のサーバ、送信元または宛先アドレス、cookie、URL、HTTP ヘッダーなど、いくつかの要因に基づいてサーバを選択します。

ACE アプライアンス Device Manager では、次のものを使用してロード バランシングを設定できます。

- 仮想サーバ：「仮想サーバの設定」（P.5-2）を参照してください。
- 実サーバ：「実サーバの設定」（P.6-5）を参照してください。
- 動的ワークロード拡張：「動的ワークロード拡張の設定」（P.6-14）を参照してください。
- サーバ ファーム：「サーバ ファームの設定」（P.6-18）を参照してください。
- スティッキ グループ：「スティッキ グループの設定」（P.7-12）を参照してください。
- パラメータ マップ：「パラメータ マップの設定」（P.8-1）を参照してください。

ACE アプライアンスによって設定および実行される SLB の詳細については、次のトピックを参照してください。

- 「仮想サーバの設定」（P.5-2）
- 「ロード バランシング プレディクタ」（P.6-2）
- 「実サーバ」（P.6-3）
- 「動的ワークロード拡張の概要」（P.6-4）
- 「サーバ ファーム」（P.6-5）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「TCL スクリプト」（P.6-39）
- 「スティッキ機能の設定」（P.7-1）

# ロード バランシング プレディクタ

ACE アプライアンスは次のプレディクタを使用して、クライアント要求の対応に最適なサーバを選択します。

- ハッシュ アドレス：送信元または宛先のいずれかまたは両方の IP アドレスに基づくハッシュ値を使用して、サーバを選択します。ファイアウォール ロード バランシング（FWLB）のプレディクタを使用します。

**（注）** FWLB を設定すると、トラフィックを接続ごとに複数のファイアウォールに分散させることによって、ファイアウォール プロテクションを拡張できます。特定の接続に属するパケットは、すべて同じファイアウォールを通過します。ファイアウォールは、そのインターフェイスすべてにわたり、個々のパケットの伝送を許可または拒否します。ACE アプライアンスでの FWLB の設定に関する詳細は、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

- ハッシュ コンテンツ：HTTP パケット本体の指定したコンテンツ ストリングに基づくハッシュ値を使用して、サーバを選択します。
- ハッシュ Cookie：cookie 名に基づくハッシュ値を使用してサーバを選択します。
- ハッシュ セカンダリ Cookie：ACE は、cookie ヘッダーではなく、URL クエリー ストリングで指定された cookie 名に基づくハッシュ値を使用して、サーバを選択します。
- ハッシュ ヘッダー：HTTP ヘッダー名に基づくハッシュ値を使用してサーバを選択します。
- ハッシュ レイヤ 4：レイヤ 4 汎用プロトコル ロード バランシング方式を使用してサーバを選択します。

- ハッシュ URL：要求された URL に基づくハッシュ値を使用してサーバを選択します。URL で照合する開始パターンと終了パターンを指定できます。キャッシュ サーバのロード バランシングには、このプレディクタ方式を使用してください。URL ハッシュ方式ではキャッシュ サーバのパフォーマンスが向上します。トラフィックが十分にランダムな場合は、キャッシュのコンテンツを均一に分割することができるためです。冗長構成では、アクティブ ACE アプライアンスがスタンバイ ACE アプライアンスに切り替わった場合でも、キャッシュ サーバは引き続き動作します。冗長構成の詳細については、「ハイ アベイラビリティの設定」（P.11-1）を参照してください。
- 最小帯域幅：指定されたサンプル期間のネットワーク トラフィックが最小のサーバを選択します。ビデオ クリップのダウンロードなど、トラフィックの負荷が高いサーバ ファームにはこの方式を使用します。
- 最小接続：サーバの重みに基づいてアクティブ接続数が最小のサーバを選択します。最小接続プレディクタの場合、稼働させたばかりのサーバに対して高い割合で新規接続を送信することを避けるために、スロースタート メカニズムを設定できます。
- 最小負荷：SNMP プローブの情報から決定された最小負荷のサーバを選択します。
- 応答：特定の応答時間計測方法での最小応答時間のサーバを選択します。
- ラウンドロビン：サーバの重み（重み付けラウンドロビン）に基づいて実サーバのリストから次のサーバを選択します。大きい重み値を持つサーバは、受け取る接続の割合も大きくなります。これがデフォルトのプレディクタです。

（注）　異なるハッシュ プレディクタ方式では、実サーバに設定した重み値が認識されません。ユーザが実サーバに割り当てた重み値を ACE が使用するのは、ラウンドロビンと最小接続のプレディクタ方式の場合だけです。

### 関連項目

「ヘルス モニタリングの設定」（P.6-38）

## 実サーバ

クライアントにサービスを提供するためには、ACE アプライアンスに実サーバを設定する必要があります。実サーバとは専用物理サーバまたは VMware 仮想マシン（VM）のことで、サーバ ファームと呼ばれるグループに設定されます。

（注）　実サーバとして定義する VM は、動的ワークロード拡張用に設定されている場合に ACE が認識する VM です（「動的ワークロード拡張の設定」（P.6-14）を参照）。

これらのサーバは、HTTP や XML コンテンツ、Web サイトのホスティング、FTP ファイルのアップロードやダウンロード、別の場所に移された Web ページへのリダイレクションなどのクライアント サービスを提供します。実サーバは、名前で識別され、IP アドレス、接続制限、および重み値で特徴付けられます。ACE アプライアンス では、サーバが何らかの理由で稼働しなくなった場合に備えて、バックアップ サーバを設定することもできます。

ACE アプライアンス での実サーバの作成および名前の指定後、接続制限、ヘルス プローブ、重みなど、いくつかのパラメータを指定することができます。サーバ ファーム内の他のサーバとの相対重要度に基づいて、各実サーバに重みを割り当てることができます。ACE アプライアンス では、重み付きラウンドロビンのサーバの重み値、および最小接続ロード バランシング プレディクタを使用します。ロード バランシング プレディクタ アルゴリズム（ラウンドロビンや最小接続など）は、ACE アプライアンス の接続要求の送信先のサーバを決定します。ロード バランシング プレディクタのリストと説明については、「ロード バランシング プレディクタ」（P.6-2）を参照してください。

ACE アプライアンス では、ポリシー マップ内でトラフィック分類マップ（クラス マップ）を使用して対象のトラフィックをフィルタし、SLB（サーバ ロード バランシング）設定に基づいてこのトラフィックに特定のアクションを適用します。クラス マップを使用して、仮想サーバのアドレスおよび定義を設定します。

プライマリ実サーバで障害が発生すると、ACE アプライアンス はこのサーバを非稼働にし、ロード バランシングの対象から外します。障害が発生した実サーバに対してバックアップ サーバを設定していた場合は、ACE アプライアンス は、プライマリ実サーバの接続をバックアップ サーバにリダイレクトします。バックアップ サーバの設定に関する詳細は、「仮想サーバ レイヤ 7 のロード バランシングの設定」（P.5-31）を参照してください。

ACE アプライアンス は、次の理由で実サーバを非稼働にすることができます。

- プローブの失敗
- ARP タイムアウト
- ネイバー探索（ND）の失敗（IPv6 のみ）
- Retcode の失敗
- 最大接続数への到達
- 実サーバの管理ステートとして [Out Of Service] が指定された
- 実サーバの管理ステートとして [In Service Standby] が指定された

[Out Of Service] と [In Service Standby] のいずれを選択しても、サーバは正常にシャットダウンされます。

### 関連トピック

- 「実サーバの設定」（P.6-5）
- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）

## 動的ワークロード拡張の概要

ACE の動的ワークロード拡張機能では、リモート リソース（VM など）へのオンデマンド アクセスを許可します。このリモート リソースは、ユーザが所有しているもの、インターネット サービス プロバイダーまたはクラウド サービス プロバイダーからリースしているもののいずれでも構いません。この機能は、Overlay Transport Virtualization（OTV）テクノロジーを備えた Cisco Nexus 7000 シリーズ スイッチを使用して、地理的に分散したデータセンター間の既存 IP ネットワーク上のレイヤ 2 リンクに Data Center Interconnect（DCI）を作成します。ローカル データセンターの Nexus 7000 には、レイヤ 2 で拡張される Virtual Private Network (VPN) の MAC アドレスがリストされた OTV 転送テーブルが含まれ、ローカルまたはリモートのどちらのアドレスも識別されます。

この機能を使用するように ACE を設定すると、ACE は XML クエリーを使用して、Cisco Nexus 7000 シリーズ スイッチをポーリングし、ローカルまたはリモート VM の地域を決定するための OTV の転送テーブル情報を取得します。また ACE は、ローカルの VMware vCenter Server への送信を行うヘルス モニタリング プローブを使用して、CPU 使用率、メモリ使用率、またはその両方に基づいてローカル VM の負荷を監視します。ローカル VM の平均 CPU 使用率またはメモリ使用率が設定されている最大しきい値に達すると、ACE はリモート VM へのトラフィックをバーストさせます。ローカル VM の平均 CPU 使用率またはメモリ使用率が設定された最小しきい値未満まで低下すると、ACE はリモート VM へのトラフィックのバーストを停止します。

動的ワークロード拡張を使用するには、Data Center Interconnect デバイス（Cisco Nexus 7000 シリーズ スイッチ）とローカルおよびリモートの VM に関連する VMware コントローラに接続するように ACE を設定します。また、サーバ ファームのローカル VM の CPU 使用率とメモリの使用率を監視するよう、プローブ タイプの VM を使用して ACE を設定します。これにより、ACE がリモート VM にトラフィックをバーストさせるタイミングが決定されます。

この機能の詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

**関連項目**

- 「動的ワークロード拡張の設定」（P.6-14）

# サーバ ファーム

データセンターでは通常、サーバは、*サーバ ファーム*と呼ばれる関連グループに編成されています。多くの場合、サーバ ファーム内のサーバには同じコンテンツ（ミラー化されたコンテンツと呼ばれる）が格納されているため、1 つのサーバが動作しなくなると、別のサーバがただちに処理を引き継ぎます。また、ミラー コンテンツを使用すると、五輪などの重要な地元のイベントや国際的なイベント時に増加する要求の負荷を複数のサーバに分散できます。コンテンツに対するこの急激な要求の増加は、*フラッシュ クラウド*と呼ばれます。

サーバ ファームを作成して名前の付けた後で、サーバ ファームに既存の実サーバを追加したり、ロード バランシング プレディクタ、サーバの重み、バックアップ サーバ、ヘルス プローブなど、サーバ ファームの他のパラメータを指定したりすることができます。ロード バランシング プレディクタのリストと説明については、「ロード バランシング プレディクタ」（P.6-2）を参照してください。

**関連項目**

「サーバ ファームの設定」（P.6-18）

# 実サーバの設定

実サーバとは専用物理サーバのことで、通常はサーバ ファームと呼ばれるグループに構成されます。実サーバは、HTTP や XML コンテンツ、ストリーミング メディア（ビデオや音声）、TFTP や FTP サービスなどのサービスをクライアントに提供します。実サーバの設定時には、実サーバに名前、IP アドレス、接続制限、および重み値を指定します。

ACE アプライアンスは、ポリシー マップ内のトラフィック分類マップ（クラス マップ）を使用して指定トラフィックをフィルタリングし、ロード バランシングの設定に基づいてこのトラフィックに特定のアクションを適用します。ACE アプライアンスが接続要求を送信するサーバは、ロード バランシング プレディクタ アルゴリズム（ラウンドロビンや最小接続など）によって決まります。クラス マップの設定の詳細については、「仮想コンテキスト クラス マップの作成」（P.12-9）を参照してください。

実サーバにロード バランシングを設定するには、次の手順を行います。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Real Servers] を選択します。[Real Servers] テーブルが表示されます。

**ステップ 2**　[Add] をクリックして新しい実サーバを追加するか、変更する実サーバを選択してから [Edit] をクリックします。[Real Servers] 設定画面が表示されます。

**ステップ 3**　表 6-1 の情報を使用してサーバを設定します。

表 6-1　実サーバの属性

| フィールド | 説明 |
|---|---|
| Name | このフィールド内の自動増分値を受け入れるか、またはこのサーバ固有の名前を入力します。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。 |
| Type | サーバのタイプを選択します。<br>• [Host]：これがコンテンツおよびサービスをクライアントに提供する標準的な実サーバであることを示します。<br>• [Redirect]：このサーバは、トラフィックを新しい場所にリダイレクトするために使用されることを示します。 |
| State | この実サーバの状態を選択します。<br>• [In Service]：実サーバは稼働状態です。<br>• [Out Of Service]：実サーバは非稼働状態です。 |
| Description | この実サーバの簡単な説明を入力します。有効な値は、引用符で囲まずスペースを含まない 240 文字以下の英数字のテキスト文字列です。 |
| IP Address Type | このフィールドが表示されるのは、実サーバがホストとして指定された場合だけです。<br>この実サーバの IP アドレス タイプを選択します。<br>• IPv6：実サーバに IPv6 アドレスが設定されています。<br>• IPv4：実サーバに IPv4 アドレスが設定されています。 |
| IPv6/IPv4 Address | このフィールドが表示されるのは、実サーバがホストとして指定された場合だけです。<br>[IP Address Type] フィールドで指定されている一意の IP アドレスを入力します。IP アドレスには、既存の仮想 IP アドレス（VIP）、実サーバ、またはコンテキストのインターフェイスは設定できません。 |
| Fail-On-All | このフィールドは、ホスト サーバとして特定されている実サーバにだけ表示されます。<br>デフォルトでは、複数のプローブが設定された実サーバには、OR ロジックが関連付けられています。したがって、実サーバ プローブのいずれか 1 つがエラーになった場合、その実サーバはエラーとなり、PROBE-FAILED 状態になります。<br>このチェックボックスをオンにすると、関連付けられているプローブすべてでエラーが発生しない限り、実サーバは OPERATIONAL 状態のままになるように設定されます（AND ロジック）。<br>[Fail-On-All] 機能はすべてのプローブ タイプに適用できます。 |
| Min.Connections | [Max. Connections] の値を超えた後 ACE アプライアンスが再度接続を送信するまでに、サーバ上で許可される最小接続数を入力します。この値は [Max. Connections] の値以下である必要があります。デフォルトでは、この値は [Max. Connections] の値と同じです。有効な値は 1 ～ 4000000 の整数です。 |
| Max.Connections | このサーバに許可されるアクティブ接続の最大数を入力します。接続数がこの値を超えると、ACE アプライアンスは、接続数が [Min. Connections] の値未満になるまで、このサーバへの接続の送信を停止します。有効な値は 1 ～ 4000000 の整数で、デフォルトは 4000000 です。 |

表 6-1　実サーバの属性 （続き）

| フィールド | 説明 |
|---|---|
| Weight | このフィールドが表示されるのは、実サーバがホストとして指定された場合だけです。<br>サーバ ファーム内のこの実サーバに割り当てる重み値を入力します。有効な入力は 1 ～ 100 の整数で、デフォルトは 8 です。 |
| Web Host Redirection | 要求を別のサーバにリダイレクトする際に使用する URL 文字列。このフィールドが表示されるのは、実サーバがリダイレクト サーバとして指定された場合だけです。要求を別のサーバにリダイレクトする際に使用する URL とポートを入力します。<br>有効な値は、http://host.com:port の形式です（host はサーバの名前、*port* は使用されるポート）。有効なホスト エントリは、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 有効なポート番号は 1 ～ 65535 です。<br>リロケーション文字列は、次の特殊文字をサポートしています。<br>• %h：要求のホスト ヘッダーからホスト名を挿入します。<br>• %p：要求から URL パス文字列を挿入します。 |
| Redirection Code | このフィールドが表示されるのは、実サーバがリダイレクト サーバとして指定された場合だけです。<br>次のうちから適切なリダイレクション コードを選択します。<br>• [N/A]：Web ホスト リダイレクション コードは定義されていないことを示します。<br>• [301]：要求されたリソースは完全に移動されたことを示します。クライアントは、今後このリソースを参照する場合、返された URI のいずれかを使用する必要があります。<br>• [302]：要求されたリソースは検出されましたが、一時的に別の場所に移されていることを示します。リソースは別の場所に移されることもあるため、クライアントは、今後このリソースを参照する場合、引き続き、要求 URI を使用する必要があります。 |

表 6-1　実サーバの属性 （続き）

| フィールド | 説明 |
|---|---|
| Probes | [Probes] フィールドで、ヘルス モニタリングに使用するプローブを左側のリストから選択し、[Add] をクリックします。選択したプローブが右側のリストに表示されます。<br><br>（注）　プローブは実サーバと同じ IP アドレス タイプ（IPv6 または IPv4）であることが必要です。たとえば、IPv6 プローブを IPv4 実サーバには設定できません。<br><br>リダイレクト実サーバ プローブのリストに表示されるのは、タイプが Is Routed に設定されたプローブのみです。これは ACE が、ACE の内部ルーティング テーブルに従ってプローブのアドレスをルーティングすることを意味します（「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照）。<br><br>（注）　左側の [Probes] フィールドには、VM のプローブ タイプは表示されません。<br><br>ヘルス モニタリングに使用しないプローブを削除する場合は、右側のリストから該当するプローブを選択し、[Remove] をクリックします。選択したプローブが左側のリストに表示されます。 |
| Rate Bandwidth | 帯域幅レートは 1 秒当たりのバイト数で、ACE と実サーバ間で双方向に交換されるネットワーク トラフィックに適用されます。<br><br>実サーバの帯域幅制限値を 1 秒当たりのバイト数で指定します。有効な入力は 1 ～ 300000000 の整数です。 |
| Rate Connection | 接続レートは ACE が 1 秒間に受信する接続数のことで、実サーバへの新しい接続だけに適用されます。<br><br>1 秒当たりの接続数の制限値を指定します。有効な入力は 1 ～ 350000 の整数です。 |

**ステップ 4**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- エントリを保存せずに手順を終了し、[Real Servers] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別の実サーバを設定するには、[Add another] アイコンをクリックします。

**ステップ 5**　既存の実サーバの統計情報とステータス情報を表示するには、実サーバを [Real Servers] テーブルで選択し、[Details] をクリックします。**show rserver** *name* **detail** CLI コマンドの出力が表示されます。詳細については、「実サーバの統計情報およびステータス情報の表示」（P.6-9）を参照してください。

## 関連トピック

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「サーバ ファームの設定」（P.6-18）

- 「スティッキ グループの設定」（P.7-12）

## 実サーバの統計情報およびステータス情報の表示

特定の実サーバの統計情報とステータス情報を表示できます。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Real Servers] を選択します。

[Real Servers] テーブルが表示されます。

**ステップ 2**　[Real Servers] テーブルでは、実サーバを [Real Servers] テーブルで選択し、[Details] をクリックします。

**show rserver** *name* **detail** CLI コマンドの出力が表示されます。表示される出力フィールドの詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。

**ステップ 3**　[Update Details] をクリックして、**show rserver** *name* **detail** CLI コマンドの出力を更新します。新しい情報が新しいタイムスタンプの他のパネルに表示されます。新旧の実サーバの統計情報およびステータス情報が並べて表示され、最後に更新された情報が上書きされないようにしています。

**ステップ 4**　[Close] をクリックして、[Real Servers] テーブルに戻ります。

**関連トピック**

- 「実サーバの設定」（P.6-5）
- 「実サーバの管理」（P.6-9）
- 「すべての実サーバの表示」（P.6-12）

# 実サーバの管理

デフォルトの [Real Servers] テーブル（[Config] > [Operations] > [Real Servers]）には、各サーバについての次の情報が表示されます。

- サーバ名
- IP アドレス
- ポート
- 関連付けられている仮想サーバ
- 関連付けられている仮想コンテキスト
- 管理状態（[In Service]、[Out Of Service]、または [In Service Standby]）
- 動作状態（実サーバの動作状態については表 6-3 を参照してください）
- 現在の接続数
- 現在のサーバ重み値
- 地名
- Stat Age（SNMP 値のポーリング後、ページがロードされた時間）

- 関連付けられているサーバ ファーム

テーブル内の [Disabled] は、情報がデータベースから使用できないか、SNMP によって収集されていないことを示しています。SNMP 関連の問題点を明らかにするためには、オブジェクト セレクタから実サーバの仮想コンテキストを選択します。SNMP に問題があれば、コンテンツ ペインの右上に SNMP ステータスが表示されます。

[Real Servers] テーブルでは、次のオプションを使用できます。

- 「実サーバのアクティブ化」（P.6-10）
- 「実サーバの一時停止」（P.6-10）
- 「実サーバの変更」（P.6-11）
- 「すべての実サーバの表示」（P.6-12）

# 実サーバのアクティブ化

実サーバをアクティブにするには、次の手順を行います。

**手順**

**ステップ 1**　[Config] > [Operations] > [Real Servers] を選択します。[Real Servers] テーブルが表示されます。

**ステップ 2**　アクティブにするサーバを選択し、[Activate] をクリックします。[Activate Server] 画面が表示されます。

**ステップ 3**　[Task] フィールドで、これがアクティブにするサーバかどうかを確認します。

**ステップ 4**　[Reason] フィールドに、このアクションの理由を入力します。トラブル チケット、オーダー チケット、またはユーザ メッセージを入力できます。

**注意**　このフィールドにパスワードを入力しないでください。

**ステップ 5**　次の手順を実行します。

- この設定を適用して、[Real Servers] テーブルに戻るには、[Deploy Now] をクリックします。テーブル内のこのサーバの状態が [Inservice] になります。
- サーバをアクティブにせずにこの手順を終了し、[Real Servers] テーブルに戻るには、[Cancel] をクリックします。

**関連トピック**

- 「実サーバの管理」（P.6-9）
- 「実サーバの一時停止」（P.6-10）
- 「すべての実サーバの表示」（P.6-12）

# 実サーバの一時停止

実サーバを一時的に停止するには、次の手順を行います。

**手順**

**ステップ 1**　[Config] > [Operations] > [Real Servers] を選択します。[Real Servers] テーブルが表示されます。

**ステップ 2**　一時停止するサーバを選択し、[Suspend] をクリックします。[Suspend Server] 画面が表示されます。

**ステップ 3**　[Reason] フィールドに、このアクションの理由を入力します。トラブル チケット、オーダー チケット、またはユーザ メッセージを入力できます。**このフィールドにパスワードを入力しないでください。**

**ステップ 4**　[Type] ドロップ ダウン メニューから次のいずれかを選択します。

- Graceful
- Suspend
- シャットダウン プロセスの一部として、このサーバに対する既存の接続をクリアする場合は、[Suspend and Clear Connections]

**ステップ 5**　次の手順を実行します。

- この設定を適用して、[Real Servers] テーブルに戻るには、[Deploy Now] をクリックします。テーブル内のこのサーバの状態が [Out Of Service] になります。
- サーバを一時停止せずにこの手順を終了し、[Real Servers] テーブルに戻るには、[Cancel] をクリックします。

**関連トピック**

- 「実サーバの管理」（P.6-9）
- 「実サーバのアクティブ化」（P.6-10）
- 「すべての実サーバの表示」（P.6-12）

# 実サーバの変更

実サーバの重み値と接続制限を変更するには、次の手順を使用します。

**手順**

**ステップ 1**　設定を変更するサーバを選択してから、[Activate] と [Suspend] の右側のテーブルの下にある [Change Weight] をクリックします。[Change Weight Real Servers] ウィンドウが表示されます。

**ステップ 2**　選択したサーバに関する次の情報を入力します。

- [Reason for change]：トラブル チケット、オーダー チケット、またはユーザ メッセージなど。**このフィールドにパスワードを入力しないでください。**
- [Weight]：1 から 100 までの値を選択します。

**ステップ 3**　次の手順を実行します。

- エントリを確定して [Real Servers] テーブルに戻るには、[Deploy Now] をクリックします。テーブル内のこのサーバの情報が更新されます。
- エントリを保存せずに手順を終了し、[Real Servers] テーブルに戻るには、[Cancel] をクリックします。

**関連トピック**

- 「実サーバの管理」（P.6-9）
- 「実サーバのアクティブ化」（P.6-10）
- 「すべての実サーバの表示」（P.6-12）

# すべての実サーバの表示

すべての実サーバを表示するには、[Config ] > [Operations ] > [Real Servers] を選択します。デフォルトでは、[Real Servers] テーブルには表 6-2 に示す情報が表示されます。

**表 6-2　[Real Servers] テーブルのフィールド**

| 項目 | 説明 |
|---|---|
| Name | 実サーバ名。 |
| IP address | 実サーバの IP アドレス。 |
| Port | 実サーバが通信用に使用するポート。 |
| Vservers | 関連付けられている仮想サーバ。 |
| Context | 関連付けられている仮想コンテキスト。 |
| Admin | 実サーバの管理状態：[In Service]、[Out Of Service]、または [In Service Standby]。 |
| Oper | 実サーバの動作状態（実サーバの動作状態については表 6-3 を参照）。 |
| Conn | 現在の接続数。 |
| Wt | 現在のサーバ重み。 |
| Locality | [Locality] では ACE の動的ワークロード拡張を設定する必要があります（「動的ワークロード拡張の設定」（P.6-14）を参照）。<br>実サーバの場所。実サーバは、物理サーバではなく VM であることが必要です。地域の状態は次のとおりです。<br>• [N/A]：ACE は実サーバの場所（ローカルまたはリモート）を判断できません。この問題が生じる場合、動的ワークロード拡張が正しく設定されていない可能性があります。<br>• [Local]：実サーバはローカル ネットワーク内にあります。<br>• [Remote]：実サーバはリモート ネットワーク内にあります。ローカル実サーバの CPU 使用率またはメモリ使用率が指定された最大しきい値に達すると、ACE はこのサーバにトラフィックをバーストさせます。 |
| Stat Age | SNMP 値のポーリング後、ページがロードされた時間。 |
| Server Farm | 関連付けられているサーバ ファーム。 |

前述のテーブルで、[Disabled] は情報がデータベースから使用できないか、SNMP によって収集されていないことを示しています。SNMP 関連の問題点を明らかにするためには、オブジェクト セレクタから実サーバの仮想コンテキストを選択します。SNMP に問題があれば、コンテンツ ペインの右上に SNMP ステータスが表示されます。

表 6-3　実サーバの動作状態

| ステート | 説明 |
|---|---|
| ARP Failed | このサーバへの ARP 要求が失敗しました。 |
| Failed | サーバに障害が発生しました。リトライ タイマーでの指定時間のあいだ、再試行されません。 |
| Inactive | サーバは非アクティブ状態（実サーバがサーバ ファームに関連付けられていない場合など）のため使用できません。 |
| Inband probe failed | サーバのインバンド ヘルス プローブ エージェントが失敗しました。 |
| Inservice | このサーバは、サーバ ロード バランシングによるクライアント接続の宛先として使用されています。 |
| Inservice standby | このサーバはスタンバイ状態です。プライマリ サーバに障害が発生するまで、このサーバに接続は割り当てられません。 |
| Max.Load | サーバは最大負荷状態であり、これ以上接続を受け入れることはできません。 |
| ND Failed | IPv6 について、ネイバー探索（ND）は実サーバのアドレスを解決できませんでした。 |
| Operation wait | このサーバは稼働可能な状態ですが、関連付けられているリダイレクト仮想サーバが稼働状態になるまで待機しています。 |
| Out of service | このサーバは、サーバ ロード バランサでクライアント接続の宛先として使用されていません。 |
| Probe failed | このサーバへのサーバ ロード バランシング プローブが失敗しました。このサーバへのプローブが成功するまで、このサーバに新しい接続は割り当てられません。 |
| Probe testing | サーバは、サーバ ロード バランサからのテスト プローブを受信しました。 |
| Ready to test | サーバに障害が発生し、リトライ タイマーの時間が満了しました。このサーバへのテスト接続がすぐに開始されます。 |
| Return code failed | このサーバは、設定値と一致する HTTP コードを返したためディセーブルになりました。 |
| Test wait | サーバはテスト可能な状態です。この状態になるのは、サーバが HTTP リダイレクト ロード バランシングに使用されている場合だけです。 |
| Testing | サーバに障害が発生し、別のテスト接続が実行されました。この接続が成功したかどうかは不明です。 |
| Throttle: DFP | DFP が、サーバの重み値をスロットル レベルに下げました。DFP が重み値を上げるまで、このサーバには新しい接続は割り当てられません。 |
| Throttle: max clients | サーバは最大許容クライアント数に達しました。 |
| Throttle: max connections | サーバは最大接続数に達し、これ以上接続を受け入れることはできません。 |
| Unknown | サーバの状態は不明です。 |

## 関連トピック

- 「実サーバのアクティブ化」（P.6-10）
- 「実サーバの一時停止」（P.6-10）
- 「実サーバの変更」（P.6-11）

# 動的ワークロード拡張の設定

ここでは、ACE の動的ワークロード拡張（DWS）の設定方法を説明します。DWS により、ローカル VM の平均 CPU 使用率またはメモリ使用率が指定された最大しきい値に達すると、ACE は VM のリモート プールにトラフィックをバーストさせることができます。使用率が指定された最小しきい値を下回ると、ACE はリモート VM へのトラフィックのバーストを停止します。動的ワークロード拡張機能の詳細については、「動的ワークロード拡張の概要」（P.6-4）を参照してください。

DWS は次を備えた ACE を設定する必要があります。

- Nexus 7000 シリーズ スイッチ：VM のロケーション情報（ローカルまたはリモート）を取得するため ACE がポーリングするローカルの Cisco Nexus 7000 シリーズ スイッチの XML インターフェイスの IP アドレス。

（注）　Device Manager ソフトウェア バージョン A5(1.2) を使用して、ACE がポーリングする Nexus 7000 スイッチを最大 2 台指定できます。Device Manager ソフトウェア バージョン A5(1.1) を使用した場合は、Nexus 7000 スイッチを 1 台だけ指定できます。

- VM コントローラ：ACE がローカル VM の負荷を監視するためにヘルス プローブを送信する VM コントローラ（別名 VMware vCenter サーバ）の IP アドレス。
- VM プローブ：CPU 使用率、メモリ使用率、またはその両方に基づいてローカル VM の負荷を監視するよう、ACE が VM コントローラに送信するプローブ（「ヘルス モニタリングの設定」（P.6-38）を参照）。
- サーバ ファーム：コンテンツ配信を提供するネットワーク接続された実サーバのグループ（物理サーバと VM）。「サーバ ファームの設定」（P.6-18）を参照してください。

（注）　DWS に関連付けられたロード バランシング用の VM を ACE が使用できるようにするには、ACE で VM を実サーバとして設定する必要があります（「実サーバの設定」（P.6-5）を参照）。

### 前提条件

動的ワークロード拡張では次の設定要素が必要です。

- ローカル データセンターとリモート データセンターの DCI/OTV 用に設定された Cisco Nexus 7000 シリーズ スイッチ。DCI/OTV の Nexus 7000 の設定方法の詳細については、『*Cisco Nexus 7000 NX-OS OTV Configuration Guide, Release 5.x*』を参照してください。
- VMware vCenter Server 4.0 以降。
- 実サーバとして設定され、ACE で設定されたサーバ ファームに関連付けられた複数のローカルおよびリモート VM。
- DCI カプセル化および Don't Fragment（DF）ビットに対応するため 1430 以下に設定された ACE バックエンド インターフェイス MTU は、自動的に DCI リンク上で設定されます。ACE MTU の設定に関する詳細は、『*Routing and Bridging Guide, Cisco ACE Application Control Engine*』を参照してください。

ここでは、次の内容について説明します。

# Cisco Nexus 7000 接続の設定と検証

この手順では、ACE が SSH を使用して Cisco Nexus 7000 シリーズ スイッチと通信するために必要な Cisco Nexus 7000 シリーズ スイッチの属性を使用して ACE を設定する方法について説明します。ACE は、Cisco Nexus 7000 シリーズ スイッチを使用して VM のロケーション情報（ローカルまたはリモート）を取得します。

**（注）** Device Manager ソフトウェア バージョン A5(1.2) を使用して、ACE がポーリングする Cisco Nexus 7000 シリーズ スイッチを最大 2 台指定できます。Device Manager ソフトウェア バージョン A5(1.1) を使用した場合は、Cisco Nexus 7000 シリーズ スイッチを 1 台だけ指定できます。

またこの手順を使用して、既存の Cisco Nexus 7000 シリーズ スイッチ プロファイルの属性を編集したり、スイッチ プロファイルを削除できます。

### 注意事項および制約事項

管理コンテキストの ACE ごとに最大 2 台の Cisco Nexus 7000 シリーズ スイッチを設定します。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [Load Balancing] > [Dynamic Workload Scaling] > [Nexus 7000 Setup] を選択します。

[Nexus 7000 Setup] ペインが表示されます。

**（注）** 既存の Cisco Nexus 7000 シリーズ スイッチ プロファイルがすでにある場合は、[Name] フィールドの右側にあるドロップダウン リストにプロファイル名の表示されます。

**ステップ 2**　[Nexus 7000 Setup] ペインで、次のいずれかを実行します。

- 次のとおり、新しい Cisco Nexus 7000 シリーズ スイッチ プロファイルを定義します。

  **a.**[Name] フィールドで、まだ選択されていない場合はテキスト ボックスのオプション ボタンをクリックして、Nexus 7000 の名前を最大 64 文字で入力します。ACE オブジェクトの命名規則については、この章の冒頭の（注）を参照してください。

  **b.**[Primary IP] フィールドに、Cisco Nexus 7000 シリーズ XML インターフェイスの IP アドレスをドット付き 10 進表記で入力します（192.168.11.1 など）。

  **c.**[User Name] フィールドに、ACE が Nexus 7000 のアクセスおよび認証に使用するユーザ名を入力します。有効な値は、引用符で囲まずスペースを含まない 64 文字以下のテキスト文字列です。

  **（注）** ユーザが VM のロケーション情報に関する Nexus 7000 の出力を XML 形式で受信するには、vdc-admin または network-admin ロールが必要です。

  **d.**[Password] フィールドに、ACE が Nexus 7000 の認証に使用するパスワードを入力します。有効な値は、引用符で囲まずスペースを含まない 64 文字以下のテキスト文字列です。

  **e.**[Confirm] フィールドに、パスワードを再入力し、ステップ 3 に進みます。

- 次のとおり既存の Cisco Nexus 7000 シリーズ スイッチ プロファイルを編集します。

  **a.**[Name] フィールドで、既存のスイッチ プロファイル名のリストを含むドロップ ダウン リストのオプション ボタンをクリックします。

**b.** ドロップ ダウン リストから、編集するスイッチ プロファイルを選択します。現在のプロファイルの属性が表示されます。

**c.** 新しいプロファイルを作成するための前述の手順に従ってプロファイル フィールドを編集し、ステップ 3 に進みます。

**ステップ 3**　ACE でこの設定を展開し、実行コンフィギュレーションおよびスタートアップ コンフィギュレーション ファイルにエントリを保存するには、[Deploy Now] をクリックします。新しいスイッチ プロファイルを指定した場合は、[Name] フィールドにあるドロップ ダウン リストに追加されます。

**（注）**　動的ワークロード拡張を設定するには、ACE を VM コントローラ情報を使用して設定し（「VM コントローラ接続の設定と検証」（P.6-16）を参照）、VM ヘルス プローブを設定（「ヘルス モニタリングの設定」（P.6-38）を参照）する必要があります。

**ステップ 4**　（任意）このウィンドウで使用可能な機能ボタンを次のように使用します。

- ACE と選択した Nexus 7000 スイッチ プロファイル間の接続を確認するには、[Details] をクリックします。

  ポップアップ ウィンドウに、ACE の **show nexus-device** *device_name* **detail** CLI コマンドの出力が表示され、デバイス名、IP アドレス、および接続情報が含まれます。コマンド出力の詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。
- 現在選択されている Nexus 7000 スイッチ プロファイルを削除するには、[Delete] をクリックします。

**注意**　ACE が現在動的ワークロード拡張用に設定されている場合、スイッチ プロファイルが 1 つだけ定義されていれば Nexus 7000 スイッチ プロファイルを削除するとこの機能がディセーブルになります。

### 関連トピック

- 「VM コントローラ接続の設定と検証」（P.6-16）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「動的ワークロード拡張の設定」（P.6-14）
- 「動的ワークロード拡張の概要」（P.6-4）
- 「実サーバの設定」（P.6-5）
- 「サーバ ファームの設定」（P.6-18）

# VM コントローラ接続の設定と検証

この手順では、ACE が VM コントローラと通信するために必要な VM コントローラ（VMware vCenter Server）属性を使用して ACE を設定してローカル VM の負荷情報を取得する方法について説明します。

### 注意事項および制約事項

ACE の管理コンテキストあたり VM コントローラを 1 つだけ設定します。

### 前提条件

ACE がローカル Nexus 7000 と通信するように設定されていて、ACE が VM コントローラの VM の地域を検出できます（「Cisco Nexus 7000 接続の設定と検証」（P.6-15）を参照）。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [Load Balancing] > [Dynamic Workload Scaling] > [VM Controller Setup] を選択します。

[VM Controller Setup] ペインが表示されます。

**ステップ 2**　[VM Controller Setup] ペインで、表 6-4 の情報を使用して VM コントローラを定義します。

**表 6-4　VM コントローラの設定**

| フィールド | 説明 |
|---|---|
| Name | VM コントローラ名（ACE オブジェクトの命名規則については、この章の冒頭の（注）を参照してください）。 |
| URL | VM コントローラの Web サービス API エージェントの IP アドレスまたは URL。URL は VM コントローラ ソフトウェア開発キット（SDK）（https://1.2.3.4/sdk など）を指す必要があります。255 文字以内で入力します。 |
| User Name | ACE が VM コントローラのアクセスおよび認証に使用するユーザ名。ユーザは少なくとも読み取り専用ロールまたは読み取り特権を持つロールがなければなりません。有効な値は、引用符で囲まずスペースを含まない 64 文字以下のテキスト文字列です。 |
| Password | VM コントローラの認証に使用されるパスワード。有効な値は、引用符で囲まずスペースを含まない 64 文字以下のテキスト文字列です。<br>[Confirm] フィールドにパスワードを再入力します。 |

**ステップ 3**　[Deploy Now] をクリックして、ACE でこの設定を展開し、実行コンフィギュレーションおよびスタートアップ コンフィギュレーション ファイルにエントリを保存します。

**（注）**　動的ワークロード拡張を設定するには、ACE を Nexus 7000 情報を使用して設定し（「Cisco Nexus 7000 接続の設定と検証」（P.6-15）を参照）、VM ヘルス プローブを設定（「ヘルス モニタリングの設定」（P.6-38）を参照）する必要があります。

**ステップ 4**　（任意）ACE とリモートの VM コントローラ間の接続を確認するには、[Details] をクリックします。

ポップアップ ウィンドウに、ACE の **show vm-controller** *device_name* **detail** CLI コマンドの出力が表示され、VM コントローラのステータス、IP アドレス、および接続情報が含まれます。

**ステップ 5**　（任意）現在設定されている VM コントローラを削除するには、[Delete] をクリックします。

**（注）**　ACE が動的ワークロード拡張を使用するよう設定されている場合、VM コントローラを削除する前に、関連する VM のヘルス プローブを削除する必要があります（「ヘルス モニタリングの設定」（P.6-38）を参照）。

### 関連トピック

- 「Cisco Nexus 7000 接続の設定と検証」（P.6-15）

- 「ヘルス モニタリングの設定」（P.6-38）
- 「動的ワークロード拡張の設定」（P.6-14）
- 「動的ワークロード拡張の概要」（P.6-4）
- 「実サーバの設定」（P.6-5）
- 「サーバ ファームの設定」（P.6-18）

# サーバ ファームの設定

サーバ ファームとは、同じコンテンツを含み、データセンター内の同一の物理的な場所に位置する、ネットワーク接続された実サーバ（物理サーバと VM）のグループです。

（注）　ACE で動的ワークロード拡張が設定されている場合、VM である実サーバは、リモートのデータセンターにも存在できます（「動的ワークロード拡張の設定」（P.6-14）を参照）。

多くの場合 Web サイトは、サーバ ファーム内に設定されたサーバのグループから構成されています。ソフトウェアの負荷を分散すると、コンテンツまたはサービスを求めるクライアント要求は、設定済みポリシー、トラフィック分類、サーバ アベイラビリティ、負荷などの要因に基づいて実サーバに分散されます。1 つのサーバがダウンすると、別のサーバが処理を引き継ぎ、要求をしてきたクライアントに同じコンテンツを引き続き提供します。

（注）　サーバ ファームは、IPv6 および IPv4 実サーバの混在をサポートし、IPv6 および IPv4 の両方のプローブと関連付けることができます。

サーバ ファームにロード バランシングを設定するには、次の手順を行います。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Server Farms] を選択します。

[Server Farms] ウィンドウが表示されます。このウィンドウの詳細については、「すべてのサーバ ファームの表示」（P.6-37）を参照してください。

**ステップ 2**　[Add] をクリックして新しいサーバ ファームを追加するか、既存のサーバ ファームを選択してから [Edit] をクリックします。

[Server Farms] 設定画面が表示されます。

**ステップ 3**　サーバ ファームの属性を入力します（表 6-5 を参照）。

表 6-5　サーバ ファームの属性

| フィールド | 説明 |
|---|---|
| Name | このフィールド内の自動増分値を受け入れるか、またはこのサーバ ファームに固有の名前を入力します。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。 |
| Type | サーバ ファームのタイプを選択します。<br>• [Host]：これは、コンテンツおよびサービスをクライアントに提供する標準的な実サーバで構成されるサーバ ファームであることを示します。<br>• [Redirect]：これは、実サーバの設定で指定された代替の場所にクライアント要求をリダイレクトする実サーバだけで構成されるサーバ ファームであることを示します （「実サーバの設定」（P.6-5）を参照）。 |
| Description | このサーバ ファームの簡単な説明を入力します。有効な値は、引用符で囲まずスペースを含まない 240 文字以下の英数字のテキスト文字列です。 |
| Fail Action | サーバ ファーム内の実サーバに障害が発生した場合に、ACE アプライアンスが接続に対して実行するアクションを選択します。<br>• [N/A]：サーバ ファーム内のサーバに障害が発生しても、ACE アプライアンスはアクションを実行しません。<br>• [Purge]：サーバ ファーム内の実サーバに障害が発生した場合、ACE アプライアンスは実サーバへの接続を解除します。ACE アプライアンスは、リセット コマンドをクライアント、および障害が発生したサーバの両方に送信します。<br>• [Reassign]：このコマンドの入力後に実サーバで障害が発生した場合、バックアップ用の実サーバ（設定されている場合）に ACE はその既存サーバ接続を再割り当てします。障害が発生したサーバにバックアップ用の実サーバが設定されていない場合に [Reassign] を選択すると、既存の接続は障害が発生した実サーバに接続できない状態となります。 |

表 6-5　サーバ ファームの属性 （続き）

| フィールド | 説明 |
|---|---|
| Failaction Reassign Across Vlans | このフィールドは、[Fail Action] が [Reassign] に設定されている場合のみ表示されます。<br>実サーバで障害が発生した場合、ACE が別の VLAN インターフェイス（一般にバイパス VLAN と呼ばれます）のバックアップ用の実サーバに既存サーバ接続を再割り当てするよう指定する場合は、このチェックボックスをオンにします。障害が発生したサーバにバックアップ用の実サーバが設定されていない場合、このオプションを設定しても無効になり、既存の接続は障害が発生した実サーバに接続できない状態となります。<br>このオプションをイネーブルにする場合は、次の設定要件と制約事項に注意してください。<br>• ACE の VIP アドレスをサーバの IP アドレスに変換する際に NAT を使用しないよう ACE に指示するには、[Transport] オプションをイネーブルにします（次のフィールドを参照）。[Failaction Reassign Across Vlans] オプションは、ACE で処理状態を把握するファイアウォール ロード バランシング（FWLB）に使用することを目的としています。ここで、ACE への接続用の宛先 IP アドレスはエンドポイントの実サーバで、ACE は、別のネクスト ホップで転送されるように接続を割り当てます。<br>• フロー内の同じサーバから出入りするパケットが同じファイアウォールまたはステートフル デバイスを通過するようにするため、すべてのサーバ側インターフェイスで [MAC Sticky] オプションをイネーブルにします（「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）を参照）。<br>• [Predictor Hash Address] オプションを設定します。サポートされているプレディクタ方式、および各プレディクタ方式の設定可能な属性の詳細については、「サーバ ファームのプレディクタ方式の設定」（P.6-28）を参照してください。<br>• プライマリ インターフェイスとバックアップサーバのインターフェイスに対して同じポリシーを設定する必要があります。バックアップ インターフェイスは、プライマリ インターフェイスと同じ機能が設定されていることが必要です。<br>• プライマリサーバのインターフェイスのポリシーとは異なるポリシーをバックアップサーバのインターフェイスで設定した場合、そのポリシーは新しい接続に対してのみ有効になります。再割り当てされた接続には、プライマリサーバのインターフェイス ポリシーだけが常に設定されます。<br>• インターフェイス固有の機能（NAT、アプリケーション プロトコル インスペクション、アウトバウンド ACL、または SYN クッキーなど）はサポートされていません。<br>• 障害が発生した実サーバが復旧した後は、このサーバへの接続を再割り当てできません。この制約は、同じ VLAN バックアップ サーバにも適用されます。<br>• 実サーバは、ACE に直接接続する必要があります。この要件は、同じ VLAN バックアップ サーバにも適用されます。<br>• ファイアウォールのシーケンス番号のランダム化をディセーブルにする必要があります（「接続パラメータ マップの設定」（P.8-5）を参照）。<br>• プローブ設定は、両方の ACE で同一とする必要があり、インターバル値は低く設定する必要があります。たとえば、ACE-1 で高いインターバル値、ACE-2 で低いインターバル値を設定すると、再割り当てされた接続はプローブ設定の不一致により停止する場合があります。インターバル値が低い ACE-2 は、最初にプライマリ サーバの障害を検出し、着信接続をすべてバックアップサーバのインターフェイス VLAN に再割り当てします。インターバル値が高い ACE-1 は、プライマリ サーバが復旧する前に障害を検出しない場合があるので、プライマリ サーバを指し示し続けます。<br>パケット損失を最小限に抑えるために、両方の ACE で次に示すプローブ パラメータ値を推奨します。Interval：2、Faildetect：2、Passdetect interval：2、Passdetect count：5 |

表 6-5　サーバ ファームの属性 （続き）

| フィールド | 説明 |
|---|---|
| Dynamic Workload Scaling | このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。<br>ローカル VM の平均 CPU 使用率またはメモリ使用率が指定された最大しきい値に達すると、ACE はリモート VM にトラフィックをバーストさせることができます。ローカル VM の平均 CPU 使用率またはメモリ使用率が設定された最小しきい値未満まで低下すると、ACE はリモート VM へのトラフィックのバーストを停止します。このオプションは、Cisco Nexus 7000 シリーズ スイッチ、VM コントローラ、および VM プローブを使用して、ACE を動的ワークロード拡張用に設定する必要があります（「動的ワークロード拡張の設定」（P.6-14）を参照）。<br>次のオプション ボタンのオプションのいずれかをクリックします。<br>• [N/A]：適用しない（デフォルト）。<br>• [Local]：ACE がサーバのロード バランシング用だけにローカル VM を使用するよう制限します。<br>• [Burst]：必要に応じて ACE はリモート VM にトラフィックをバーストさせることができます。<br>[Burst] を選択すると、[VM Probe Name] フィールドが使用可能な VM プローブの一覧とともに表示されます。使用可能な VM のプローブを選択するか、または [Add] をクリックするとヘルス モニタリングのポップアップ ウィンドウが表示され、新しい VM プローブを作成するか、または既存の VM プローブを編集できます（「ヘルス モニタリングの設定」（P.6-38）を参照）。 |
| Fail-On-All | このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。<br>デフォルトでは、サーバ ファーム内に設定される実サーバは、そのサーバ ファーム上で直接設定されたプローブを継承します。1 つのサーバ ファームに複数のプローブを設定している場合、そのサーバ ファームの実サーバでは、これらのプローブに対して OR ロジックが使用されます。つまり、サーバ ファームに設定されているプローブの 1 つにエラーが発生した場合、このサーバ ファームにある実サーバすべてがエラーとなり、PROBE-FAILED 状態になります。AND ロジックを使用すると、あるサーバ ファーム プローブでエラーが発生した場合に、そのサーバ ファームにある実サーバは運用状態のままになります。そのサーバ ファームに関連付けられているすべてのプローブがエラーになると、そのサーバ ファームのすべての実サーバがエラーとなり、PROBE-FAILED 状態になります。<br>複数のサーバ ファーム プローブに対して AND ロジックを使用するよう、サーバ ファームにある実サーバを設定するには、このチェックボックスをクリックします。<br>[Fail-On-All] 機能はすべてのプローブ タイプに適用できます。 |

表 6-5　サーバ ファームの属性 （続き）

| フィールド | 説明 |
|---|---|
| Inband-Health Check | このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。<br>デフォルトでは、ACE は ARP およびヘルス プローブを使用して設定のすべての実サーバの状態を監視します。ただし、実サーバがダウンしたときと、ACE がその状態を認識したときとの間には遅延時間が生じます。インバンド ヘルス モニタリング機能では、ACE は次の接続障害からサーバ ファーム内の実サーバの状態を監視できます。<br>• TCP の場合、サーバまたは SYN タイムアウトからのリセット（RST）。<br>• UDP の場合、ICMP ホスト、ネットワーク、ポート、プロトコル、およびソース ルートの到達不能メッセージ。<br>障害カウントのしきい値を設定していて、障害の数がリセット時間内にしきい値を超えた場合、ACE はただちにそのサーバを [failed] のマークを付けて非稼働にし、ロード バランシングから除外します。サーバは、オプションの再開サービス期限が切れるまで、ロード バランシングの対象と見なされません。<br>次のいずれかを選択します。<br>• [Count] : TCP または UDP エラーの合計数を追跡し、**show serverfarm** *name* **inband** CLI コマンドで表示されるカウンタを増分します。<br>• [Log] : イベントの数が設定されている接続障害のしきい値に達すると、syslog エラー メッセージをログに記録します。<br>• [Remove] : ：イベントの数がしきい値に到達し、サーバをサービスから除外した場合、syslog エラー メッセージをログに記録します。<br>**（注）** サーバを監視するためにこの機能およびヘルス プローブを設定できます。設定を行う場合、サーバ ファーム内で実サーバを稼働状態に維持する必要があります。いずれかの機能がサーバが非稼働であることを検出した場合、ACE はこのサーバをロード バランシングの対象として選択しません。 |
| Connection Failure Threshold Count | このフィールドは、[Inband-Health Check] が [Log] または [Remove] に設定されている場合にだけ表示されます。<br>ACE が実サーバに [failed] のマークを付ける前に、実サーバがリセット時間間隔を示すことができる接続の最大数を入力します。有効な値は 1 ～ 4294967295 の整数です。 |
| Reset Timeout (Milliseconds) | このフィールドは、[Inband-Health Check] が [Log] または [Remove] に設定されている場合にだけ表示されます。<br>リセット時間間隔をミリ秒単位で入力します。有効な値は 100 ～ 300000 の整数です。デフォルトの間隔は、100 です。<br>この間隔は、ACE が接続障害を検出した時点で開始します。この間隔の間に接続障害のしきい値に到達すると、ACE は Syslog メッセージを生成します。[Inband-Health Check] が [Remove] に設定されている場合、ACE は、サービスからも実サーバを除外します。<br>このオプションの設定を変更すると、次の示すとおり実サーバの動作に影響します。<br>• 実サーバが OPERATIONAL 状態になると、一部の接続障害が発生していても、新しいリセット時間間隔は、次回接続エラーが発生したときに有効になります。<br>• 接続エラーが INBAND-HM-FAILED 状態の場合は、サーバが OPERATIONAL 状態に移行した後、次回接続エラーが発生したときに有効になります。 |

表 6-5　サーバ ファームの属性 （続き）

| フィールド | 説明 |
|---|---|
| Resume Service (Seconds) | このフィールドは、[Inband-Health Check] が [Remove] に設定されている場合にだけ表示されます。<br>[failed] とマークされたサーバが、アクティブな接続を送信することを再試行するまでの秒数を入力します。有効な値は 30 ～ 3600 の整数です。デフォルトでは、このフィールドは設定されていません。このオプションの設定は、次のとおり、インバンド障害状態の実サーバの動作に影響します。<br>• このフィールドが設定されていない場合、実サーバは、手動で一時停止され再びアクティブ化されるまで障害状態になります。<br>• このフィールドが設定されず、このオプションを 30 ～ 3,600 の整数で設定した場合、障害が発生した実サーバはただちに動作状態に移行します。<br>• このフィールドを設定しており、値が大きくなると、実サーバは、以前設定した値の期間中障害状態のままになります。新しい値は、次回実サーバが障害状態に移行したときに有効になります。<br>• このフィールドを設定しており、値が小さくなると、障害が発生した実サーバはただちに動作状態に移行します。<br>• 30 ～ 3,600 の整数でこのフィールドを設定し、フィールドから値を削除してリセットした場合、実サーバは、以前設定した値の期間中障害状態のままになります。未設定の設定は、次回実サーバが障害状態に移行したときに有効になります。その実サーバは、手動で一時停止され再びアクティブ化されるまで障害状態になります。<br>• リセット時間間隔内でこのフィールドを変更し、実サーバが複数の接続障害により OPERATIONAL 状態になると、新しいしきい値の間隔は、たとえ現在のリセット期間内にエラーが発生した場合でも、次回接続エラーが発生したときに有効になります。 |
| Transparent | このフィールドは、ホスト サーバとして特定されている実サーバにだけ表示されます。<br>VIP アドレスからサーバ IP アドレスへのネットワーク アドレス変換を指定するには、このチェックボックスをオンにします。VIP アドレスからサーバ IP アドレスへのネットワーク アドレス変換が行われないように指定するには、このチェックボックスをオフにします（デフォルト）。 |
| Partial-Threshold Percentage | このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。<br>プライマリ サーバ ファームが稼働状態を維持するために必要な、サーバ ファーム内にあるアクティブ状態の実サーバの最小パーセンテージを入力します。アクティブな実サーバのパーセンテージがこのしきい値を下回ると、ACE はそのサーバ ファームを非稼働状態にします。有効な入力は 0 ～ 99 の整数です。<br>このフィールドの値を設定した後、[Back Inservice] フィールドに値を入力して、プライマリ サーバ ファームを稼働状態にします。 |
| Back Inservice | このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。<br>ACE がプライマリ サーバ ファームを再稼働するために必要な、サーバ ファーム内のアクティブ状態の実サーバのパーセンテージを入力します。有効な入力は 0 ～ 99 の整数です。このフィールドの値は、[Partial Threshold Percentage] フィールドの値以上にする必要があります。 |

表 6-5　サーバ ファームの属性 （続き）

| フィールド | 説明 |
|---|---|
| Probes | [Available] リストで、ヘルス モニタリングに使用するプローブを選択し、[Add] をクリックします。選択したプローブが [Selected] リストに表示されます。<br>リダイレクト サーバ ファームのプローブ リストに表示されるのは、タイプが Is Routed に設定されたプローブのみです。これは ACE が、ACE の内部ルーティング テーブルに従ってプローブのアドレスをルーティングすることを意味します（「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照）。<br>（注）　サーバ ファームに IPv6 と IPv4 の両方のプローブを関連付けることができます。<br>（注）　使用可能なプローブのリストに VM プローブ タイプは表示されません。ローカル VM の使用率を監視するための VM プローブを選択するには、[Dynamic Workload Scaling] フィールドを参照してください。<br>ヘルス モニタリングに使用しないプローブを削除するには [Selected] リストで該当するプローブを選択し、[Remove] をクリックします。選択したプローブが [Available] リストに表示されます。 |

**ステップ 4**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。このファームに実サーバを追加し、サーバ ファームの属性を設定する場合は、次の各項を参照してください。
  - 「サーバ ファームへの実サーバの追加」（P.6-25）
  - 「ヘルス モニタリングの設定」（P.6-38）
  - 「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）
- エントリを保存せずに手順を終了し、[Server Farms] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別のサーバ ファームを設定するには、[Next] をクリックします。

**ステップ 5**　（任意）既存のサーバ ファームの統計情報とステータス情報を表示するには、サーバ ファームを [Server Farms] テーブルで選択し、[Details] をクリックします。

**show serverfarm** *name* **detail** CLI コマンドの出力が表示されます。詳細については、「サーバ ファームの統計情報およびステータス情報の表示」（P.6-38）を参照してください。

### 関連トピック

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「実サーバの設定」（P.6-5）
- 「スティッキ グループの設定」（P.7-12）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）
- 「動的ワークロード拡張の設定」（P.6-14）

# サーバ ファームへの実サーバの追加

サーバ ファームの追加後（「サーバ ファームの設定」（P.6-18）を参照）、そのサーバ ファームに実サーバを関連付けて、プレディクタと retcode マップを設定できます。これらの属性の設定画面は、[Server Farms] テーブルの下に表示されるか、または新しいサーバ ファームの追加が正常に終了した後で表示されます。

（注）　[Server Farms] テーブルの下にこれらのタブが表示されない場合は、[Switch between Configure and Browse Modes] ボタンをクリックしてください。

サーバ ファームの作成時または編集時に、追加される実サーバの名前が既存のグローバル実サーバと同一で、IP アドレスが異なる（または IP アドレスがない）場合、Device Manager は次のエラー メッセージを表示します。

```
IP address of pre-existing real sever cannot be changed: "<rs-name>" (ip-addr>).
```

このエラー メッセージが表示された場合は、既存の実サーバに、一致する IP アドレスを指定してください。

サーバ ファームに実サーバを追加するには、次の手順を行います。

### 前提

- ACE アプライアンス Device Manager にサーバ ファームが追加されている必要があります（「サーバ ファームの設定」（P.6-18）を参照）。
- 実サーバが 1 つ以上存在する必要があります。

### 考慮事項

サーバ ファームは、IPv6 と IPv4 実サーバの混在をサポートしています。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Server Farms] を選択します。[Server Farms] テーブルが表示されます。

**ステップ 2**　実サーバに関連付けるサーバ ファームを選択し、[Real Servers] タブを選択します。[Real Servers] テーブルが表示されます。

**ステップ 3**　[Add] をクリックして [Real Servers] テーブルに新しいエントリを追加するか、既存のサーバを選択してから [Edit] をクリックして、そのサーバを変更します。[Real Servers] 設定画面が表示されます。

**ステップ 4**　表 6-6 の情報を使用して実サーバを設定します。

**表 6-6　実サーバの設定属性**

| フィールド | 説明 |
|---|---|
| Name | そのサーバ ファームに関連付けるサーバを選択します。 |
| Port | サーバ ポート アドレス変換（PAT）に使用するポート番号を入力します。有効な入力は 1 ～ 65535 の整数です。 |
| Backup Server Name | サーバ ファームのバックアップ サーバとして機能するサーバを選択します。サーバ ファームにバックアップ サーバを指定しない場合は、このフィールドを空白のままにします。 |
| Backup Server Port | バックアップ サーバを選択した場合は、バックアップ サーバのポート番号を入力します。有効な入力は 1 ～ 65535 の整数です。 |

表 6-6　実サーバの設定属性 （続き）

| フィールド | 説明 |
|---|---|
| State | このサーバの状態を選択します。<br>• [In Service]：このサーバは稼働状態であることを示します。<br>• [In Service Standby]：このサーバはバックアップ サーバであり、プライマリ サーバに障害が発生するまでは非アクティブ状態であることを示します。プライマリ サーバに障害が発生すると、バックアップ サーバはアクティブになり、接続の受信を開始します。<br>• [Out Of Service]：このサーバは非稼働状態であることを示します。 |
| Buddy Real Group Name | バディ実サーバ グループを作成するか、既存のグループを選択して、複数のサーバ ファームにまたがる同じ実サーバまたはグループへの持続性をイネーブルにします（詳細については、「バディ スティッキ グループ」（P.7-6）を参照してください）。 |
| Fail-On-All | このフィールドは、ホスト サーバとして特定されている実サーバにだけ表示されます。<br>デフォルトでは、複数のプローブが設定された実サーバには、OR ロジックが関連付けられています。したがって、実サーバ プローブのいずれか 1 つがエラーになった場合、その実サーバはエラーとなり、PROBE-FAILED 状態になります。<br>このチェックボックスをオンにすると、関連付けられているプローブすべてでエラーが発生しない限り、実サーバは OPERATIONAL 状態のままになるように設定されます（AND ロジック）。<br>Fail On All 関数はすべてのプローブ タイプに適用できます。 |
| Min.Connections | [Max. Connections] フィールドの値を超えた後、ACE アプライアンス がサーバへの接続送信を再開するまでに、接続数がこの値未満でなければならない最小接続数を入力します。このフィールド内の数字は、[Max. Connections] フィールドの値以下である必要があります。1 ～ 4000000 です。デフォルト値は 4000000 です。 |
| Max.Connections | このサーバに送信できるアクティブ接続の最大数を入力します。接続数がこの数を超えると、ACE アプライアンスは、接続数が [Min. Connections] フィールドに指定された値を下回るまで、サーバへの接続の送信を停止します。有効な値は 1 ～ 4000000 の整数です。デフォルトは 4000000 です。 |
| Weight | このサーバに割り当てる重み値を入力します。有効な入力は 1 ～ 100 の整数で、デフォルトは 8 です。 |
| Cookie String | このフィールドが表示されるのは、実サーバがホストとして指定された場合だけです。<br>実サーバの cookie 文字列値を入力します。これは、スティッキ接続の確立時に HTTP cookie の挿入に使用されます。有効な入力は英数字ストリングで、最大 32 文字です。cookie 文字列値にはスペースや特殊文字を入力できます。<br>サーバが適切な cookie を設定しない場合にセッション cookie による固定を実行するには、cookie 挿入機能を使用します。この機能をイネーブルにすると、ACE によって、サーバからクライアントへの応答の Set-Cookie ヘッダーに cookie が挿入されます。HTTP cookie スティッキ接続の詳細については、第 7 章「スティッキ機能の設定」を参照してください。 |

表 6-6　実サーバの設定属性 （続き）

| フィールド | 説明 |
|---|---|
| Probes | このサーバに適用するプローブを [Available] リストから選択し、[Add] をクリックします。選択したプローブが [Selected] リストに表示されます。このサーバに適用しないプローブを削除する場合は、[Selected] リストから該当するプローブを選択し、[Remove] をクリックします。<br>（注）　[Available] リストに VM プローブ タイプは表示されません。 |
| Rate Bandwidth | 帯域幅レートは 1 秒当たりのバイト数で、ACE と実サーバ間で双方向に交換されるネットワーク トラフィックに適用されます。<br>帯域幅制限値を 1 秒当たりのバイト数で指定します。有効な入力は 1 ～ 300000000 の整数です。 |
| Rate Connection | 接続レートは ACE が 1 秒間に受信する接続数のことで、実サーバへの新しい接続だけに適用されます。<br>1 秒当たりの接続数の制限値を指定します。有効な入力は 1 ～ 350000 の整数です。 |

**ステップ 5**　このサーバ ファームのこのサーバの設定が完了したら、次のいずれかをクリックします。

- [Deploy Now]：ACE アプライアンスにこの設定を適用します。
- [Cancel]：エントリを保存しないで手順を終了し、[Real Servers] テーブルに戻ります。
- [Next]：エントリを保存し、このサーバ ファームの別の実サーバを追加します。

**関連トピック**

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「実サーバの設定」（P.6-5）
- 「スティッキ グループの設定」（P.7-12）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）
- 「動的ワークロード拡張の設定」（P.6-14）

# サーバ ファームのプレディクタ方式の設定

サーバ ファームの追加後（「サーバ ファームの設定」（P.6-18）を参照）、そのサーバ ファームに実サーバを関連付けて、プレディクタ方式と retcode マップを設定できます。これらの属性の設定画面は、[Server Farms] テーブルの下に表示されるか、または新しいサーバ ファームの追加が正常に終了した後で表示されます。

**（注）** [Server Farms] テーブルの下にこれらのタブが表示されない場合は、[Switch between Configure and Browse Modes] ボタンをクリックしてください。

サーバ ファームのプレディクタ方式を設定するには、次の手順を行います。サービスを求めるクライアント要求を受信した場合、ACE アプライアンスがサーバ ファーム内のサーバをどのように選択するかは、プレディクタ方式によって決まります。

**（注）** 各サーバ ファームに設定できるプレディクタ方式は 1 つだけです。

### 前提

- ACE アプライアンス Device Manager にサーバ ファームが追加されている必要があります（「サーバ ファームの設定」（P.6-18）を参照）。
- 実サーバが 1 つ以上存在する必要があります。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Server Farms] を選択します。[Server Farms] テーブルが表示されます。

**ステップ 2**　プレディクタ方式を設定するサーバ ファームを選択し、[Predictor] タブを選択します。[Predictor] 設定画面が表示されます。

**ステップ 3**　[Type] フィールドで、ACE アプライアンスがクライアント要求を受信した場合にこのサーバ ファームからサーバを選択するために使用する方式を選択します。表 6-7 に、使用できるオプションとその説明をリストします。

**ステップ 4**　選択したプレディクタ方式の必須情報を入力します。ラウンドロビンがデフォルトのプレディクタ方式です。表 6-7 を参照してください。

表 6-7　プレディクタ方式の属性

| プレディクタ方式 | 説明/処理 |
|---|---|
| Hash Address | ACE は、送信元または宛先 IP アドレスに基づいてハッシュ値を使用して、サーバを選択します。<br>ハッシュ アドレス プレディクタ方式を設定するには、次の手順を実行します。<br>1. [Mask Type] フィールドで、送信元 IP アドレスと宛先 IP アドレスのどちらを基にしてサーバを選択するかを指定します。<br>– [N/A]：このオプションは定義されていません。<br>– [Destination]：宛先 IP アドレスに基づいてサーバが選択されます。<br>– [Source]：送信元 IP アドレスに基づいてサーバが選択されます。<br>（注） IPv6 と IPv4 ハッシュ アドレス プレディクタを使用してサーバ ファームを同時に設定する場合、両方のプレディクタのマスク タイプは同じであることが必要です。<br>2. [IP Netmask] フィールドで、アドレスに適用するサブネット マスクを選択します。指定しない場合、デフォルトは 255.255.255.255 です。<br>3. [IPv6 Prefix-Length] フィールドに、IPv6 プレフィックスの長さを入力します。何も指定しない場合、デフォルトは 128 です。 |

表 6-7　プレディクタ方式の属性 （続き）

| プレディクタ方式 | 説明 / 処理 |
|---|---|
| Hash Content | ACE は、HTTP パケット本体の指定したコンテンツ ストリングに基づきハッシュ値を使用して、サーバを選択します。<br>**1.** [Begin Pattern] フィールドに、コンテンツ ストリングの開始パターン、およびハッシュ前に一致させるパターン ストリングを入力します。開始パターンを指定しないと、ACE はオフセット バイトの直後の HTTP ボディの解析を開始します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません<br>有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。<br>**2.** [End Pattern] フィールドに、ハッシュの終了を示すパターンを入力します。長さも終了パターンも指定しないと、ACE はフィールドの最後またはパケットの最後に到達するか、あるいは最大ボディ解析長に到達するまで、データを解析します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません<br>有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。<br>**3.** [Length] フィールドに、ACE がクライアントをサーバに固定するために使用するコンテンツ部分の長さ（オフセット値の後ろのバイトからの長さ）をバイト単位で入力します。有効な入力は 1 ～ 1000 の整数バイトです。<br>オフセットと長さは 0 ～ 1000 バイトまで変更できます。ペイロード値がオフセットよりも長く、オフセット + ペイロードの長さの値よりも短い場合、ACE は、オフセット値の後ろのバイトを始点とし、オフセット + 長さで指定されるバイトを終点とするペイロード部分に基づいて接続を固定します。オフセットと長さの合計は、1000 バイト以下にする必要があります。<br>ハッシュ コンテンツ プレディクタには、長さと終了パターン オプションの両方を指定することはできません。<br>**4.** [HTTP Content Offset] フィールドに、ペイロードの最初のバイトから無視するバイト数を示すことにより、ACE が特定のサーバにクライアントを固定するために使用するコンテンツ部分を入力します。有効な入力は 0 ～ 999 の整数バイトです。デフォルトは 0 です。デフォルトでは、ACE はコンテンツのどの部分も除外しません。 |
| Hash Cookie | ACE は、cookie 名に基づくハッシュ値を使用してサーバを選択します。<br>[Cookie Name] フィールドに、スペースを入れない引用符なしのテキスト ストリングの形式で、最大 64 文字で cookie 名を入力します。 |
| Hash Secondary Cookie | ACE は、cookie ヘッダーではなく、URL クエリー ストリングで指定された cookie 名に基づくハッシュ値を使用して、サーバを選択します。<br>[Cookie Name] フィールドに、スペースを入れない引用符なしのテキスト ストリングの形式で、最大 64 文字で cookie 名を入力します。 |

表 6-7　プレディクタ方式の属性 （続き）

| プレディクタ方式 | 説明/処理 |
|---|---|
| Hash Header | ACE は、ヘッダー名に基づくハッシュ値を使用してサーバを選択します。<br>[Header Name] フィールドで、サーバの選択に使用する HTTP ヘッダーを選択します。<br>• 標準 HTTP ヘッダーの 1 つではない HTTP ヘッダーを指定するには、1 番めのオプション ボタンを選択し、[Header Name] フィールドに HTTP ヘッダー名を入力します。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。<br>• 標準 HTTP ヘッダーの 1 つを指定するには、2 番めのオプション ボタンを選択し、リストから HTTP ヘッダーの 1 つを選択します。 |
| Hash Layer4 | ACE は、レイヤ 4 汎用プロトコル ロード バランシング方式を使用してサーバを選択します。ACE の正式なサポート対象ではないプロトコルからのパケットのロード バランシングを行う場合は、このプレディクタを使用します。<br>1. [Begin Pattern] フィールドに、レイヤ 4 ペイロードの開始パターン、およびハッシュ前に一致させるパターン ストリングを入力します。開始パターンを指定しないと、ACE はオフセット バイトの直後の HTTP ボディの解析を開始します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません<br>有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。<br>2. [End Pattern] フィールドに、ハッシュの終了を示すパターンを入力します。長さも終了パターンも指定しないと、ACE はフィールドの最後またはパケットの最後に到達するか、あるいは最大ボディ解析長に到達するまで、データを解析します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません<br>有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。<br>3. [Length] フィールドに、ACE がクライアントをサーバに固定するために使用するペイロード部分の長さ（オフセット値の後ろのバイトからの長さ）をバイト単位で入力します。有効な入力は 1 ～ 1000 の整数バイトです。<br>オフセットと長さは 0 ～ 1000 バイトまで変更できます。ペイロード値がオフセットよりも長く、オフセット + ペイロードの長さの値よりも短い場合、ACE は、オフセット値の後ろのバイトを始点とし、オフセット + 長さで指定されるバイトを終点とするペイロード部分に基づいて接続を固定します。オフセットと長さの合計は、1000 バイト以下にする必要があります。<br>ハッシュ レイヤ 4 プレディクタには、長さと終了パターン オプションの両方を指定することはできません。<br>4. [HTTP Content Offset] フィールドに、ペイロードの最初のバイトから無視するバイト数を示すことにより、ACE が特定のサーバにクライアントを固定するために使用するコンテンツ部分を入力します。有効な入力は 0 ～ 999 の整数バイトです。デフォルトは 0 です。デフォルトでは、ACE はコンテンツのどの部分も除外しません。 |

表 6-7　プレディクタ方式の属性 （続き）

| プレディクタ方式 | 説明 / 処理 |
|---|---|
| Hash URL | ACE は、URL に基づくハッシュ値を使用してサーバを選択します。ファイアウォールに対してロード バランシングを行うには、この方式を使用します。<br>パターン フィールドの一方または両方に値を入力します。<br>• [URL Begin Pattern] フィールドに、URL の開始パターン、および解析するパターン ストリングを入力します。<br>• [URL End Pattern] フィールドに、URL の終了パターン、および解析するパターン ストリングを入力します。<br>これらのフィールドには、設定するパターンごとに、引用符で囲まずにスペースを入れないで 255 文字以内で英数字を入力します。次の特殊文字も使用できます。@ # $ |
| Least Bandwidth | ACE は指定サンプル期間のネットワーク トラフィックが最小のサーバを選択します。<br>1. [Assess Time] フィールドに、ACE がトラフィック情報を収集する秒数を入力します。有効な入力は 1 ～ 10 の整数秒です。<br>2. [Least Bandwidth Samples] フィールドに、最終負荷値を計算するためにプローブ クエリーの結果を加重平均するサンプル数を入力します。有効な入力は 1、2、4、8、および 16（2 のべき乗でもある 1 ～ 16 の整数）です。 |
| Least Connections | ACE は接続数の最も少ないサーバを選択します。<br>[Slow Start Duration] フィールドに、このプレディクタ方式に適用する slow-start 値を入力します。有効な入力は 1 ～ 65535 の整数で、1 は最も遅い ramp-up 値です。<br>稼働させたばかりのサーバに高い割合で新規接続を送信することを避けるには、スロースタート メカニズムを使用します。 |

表 6-7　プレディクタ方式の属性 （続き）

| プレディクタ方式 | 説明/処理 |
|---|---|
| Least Loaded | ACE は SNMP プローブからの情報に基づいて、負荷が最小のサーバを選択します。<br>1. [SNMP Probe Name] フィールドで、使用する SNMP プローブの名前を選択します。<br>2. [Auto Adjust] フィールドで、負荷が 0 に達した実サーバに対して 16000 の最大負荷を適用するか、またはデフォルトの動作を上書きするよう ACE に指示する自動調整機能を設定します。デフォルトでは、ACE は負荷が 0 になった実サーバに、サーバ ファームの平均負荷を適用します。ACE は、サーバの SNMP プローブと設定されたその他のオプションからのフィードバックに基づいて、この負荷の値を定期的に調整します。<br>オプションは次のとおりです。<br>– [Average]：負荷が 0 になった実サーバに、サーバ ファームの平均負荷を適用します。この設定により、サーバがロード バランシングに参加できると同時に、そのサーバに新規の接続があふれるのを防ぎます。これがデフォルト設定です。<br>– [Maxload]：負荷が 0 になった実サーバに、16000 の最大負荷を適用するように ACE に指示します。<br>– [Off]：このサーバに対する次回の負荷更新が SNMP プローブから届くまで、負荷が 0 になったサーバにすべての新規接続を送信するよう ACE に指示します。2 つのサーバの負荷値が同一で、しかも最小（ゼロまたはゼロ以外）である場合、ACE は接続の負荷をラウンドロビン方式で 2 つのサーバに分散させます。<br>3. ACE で実サーバの最終負荷計算に現在の接続数が使用されるようにするには、[Weight Connection] フィールドで、このチェックボックスをオンにします。このオプションを設定した場合、ACE でサーバ ファームの個々の実サーバに対する総負荷計算に現在の接続数が含まれるようになります。ACE の動作をリセットして、負荷の計算から現在の接続数が除外されるようにする（デフォルト）には、このチェックボックスをオフにします。<br>負荷が最小のサーバを選択するよう ACE に指示するには、サーバ ファーム ホストまたはリダイレクト コンフィギュレーション モードで predictor least-loaded コマンドを使用します。このプレディクタにより、ACE では、SNMP プローブを使用して、実サーバへの負荷パラメータ値（たとえば、CPU 使用率やメモリ使用率）のクエリーを行います。実サーバの動作に基づいて、ACE によって、ロード バランシング アルゴリズムに連続してフィードバックが適用されるため、このプレディクタは適応型であると見なされます。<br>このプレディクタを使用するには、SNMP プローブをこれに関連付ける必要があります。ACE は、設定可能な時間間隔に基づいて、ユーザ指定の OID を定期的にクエリーします。ACE は、取得した SNMP 負荷値を使用して、負荷が最小のサーバを判別します。<br>このプレディクタ コマンドの構文は次のとおりです。<br>**predictor least-loaded probe** *name*<br>name 引数には、ACE にサーバのクエリーに使用させる既存の SNMP プローブの ID を指定します。最大 64 文字の英数字からなる、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。<br>たとえば、PROBE_SNMP という SNMP プローブからのフィードバックに基づいて、負荷が最小の実サーバを選択するよう ACE を設定するには、次のように入力します。<br>`host1/Admin(config)# serverfarm SF1`<br>`host1/Admin(config-sfarm-host)# predictor least-loaded probe PROBE_SNMP`<br>`host1/Admin(config-sfarm-host-predictor)#`<br>プレディクタ方式をデフォルトのラウンドロビンにリセットするには、次のように入力します。<br>`host1/Admin(config-sfarm-host)# no predictor` |

表 6-7　プレディクタ方式の属性 （続き）

| プレディクタ方式 | 説明 / 処理 |
|---|---|
| Response | ACE は、要求された応答時間の測定に対して、応答時間が最小のサーバを選択します。<br>1. [Response Type] フィールドで、使用する測定タイプを選択します。<br>– [App-Req-To-Resp] : ACE がサーバに HTTP 要求を送信してから、ACE がその要求に対する応答をサーバから受信するまでの応答時間です。<br>– [Syn-To-Close] : ACE がサーバに TCP SYN を送信してから、ACE がそのサーバから CLOSE を受信するまでの応答時間です。<br>– [Syn-To-Synack] : ACE がサーバに TCP SYN を送信してから、ACE がそのサーバから SYN-ACK を受信するまでの応答時間です。<br>2. [Response Samples] フィールドに、応答時間の測定結果を平均するサンプル数を入力します。有効な入力は 1、2、4、8、および 16（2 のべき乗でもある 1 ～ 16 の整数）です。<br>3. ACE で実サーバの最終負荷計算に現在の接続数が使用されるようにするには、[Weight Connection] フィールドで、このチェックボックスをオンにします。このオプションを設定した場合、ACE でサーバ ファームの個々の実サーバに対する総負荷計算に現在の接続数が含まれるようになります。ACE の動作をリセットして、負荷の計算から現在の接続数が除外されるようにする（デフォルト）には、このチェックボックスをオフにします。 |
| Round Robin | ACE はサーバの重みに基づいて、サーバのリストから次のサーバを選択します。これはデフォルトのプレディクタ方式です。 |

**ステップ 5**　次のいずれかをクリックします。

- [Deploy Now] : ACE アプライアンスにこの設定を適用します。
- [Cancel] : 入力した内容を保存せずにこの手順を終了して、[Connection] フィールド テーブルに戻ります。

---

**関連トピック**

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「実サーバの設定」（P.6-5）
- 「スティッキ グループの設定」（P.7-12）
- 「サーバ ファームへの実サーバの追加」（P.6-25）
- 「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）
- 「動的ワークロード拡張の設定」（P.6-14）

# サーバ ファームの HTTP リターン エラー コード チェックの設定

サーバ ファームの追加後（「サーバ ファームの設定」（P.6-18）を参照）、そのサーバ ファームに実サーバを関連付けて、プレディクタ方式と retcode マップを設定できます。これらの属性の設定画面は、[Server Farms] テーブルの下に表示されるか、または新しいサーバ ファームの追加が正常に終了した後で表示されます。

サーバ ファームの HTTP リターン コード チェック（retcode マップ）を設定するには、次の手順を行います。

（注）　この機能を使用できるのは、サーバ ファームがホストとして設定されている場合だけです。サーバ ファームが [Redirect] タイプに設定されている場合、この機能を使用できません。

### 前提

ACE アプライアンス Device Manager にホスト タイプのサーバ ファームを追加しておきます （「サーバ ファームの設定」（P.6-18）を参照）。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Server Farms] を選択します。[Server Farms] テーブルが表示されます。

**ステップ 2**　リターン エラー コード チェックを設定するサーバ ファームを選択し、[Retcode Map] タブを選択します。[Retcode Map] テーブルが表示されます。[Server Farms] テーブルの下にタブが表示されない場合は、[Switch Between Configure And Browse Modes] ボタンをクリックしてください。

**ステップ 3**　テーブルに新しいエントリを追加する場合は、[Add] をクリックします。[Retcode Map] 設定画面が表示されます。

（注）　[Retcode Map] テーブル内のエントリは変更できません。変更する代わりに、既存のエントリを削除してから新しいエントリを追加します。

**ステップ 4**　[Lowest Retcode] フィールドに、HTTP リターン エラー コードの最小値を入力します。有効な値は 100 ～ 599 の整数です。この数値は、[Highest Retcode] フィールドの数値以下にしなければなりません。

**ステップ 5**　[Lowest Retcode] フィールドに、HTTP リターン エラー コードの最大数を入力します。有効な値は 100 ～ 599 の整数です。この数値は、[Lowest Retcode] フィールドの数値以上にしなければなりません。

**ステップ 6**　表 6-8 の情報を使用して、[Type] フィールドで、行うアクションと関連オプションを指定します。

表 6-8　リターン コード タイプの設定オプション

| オプション | 説明 |
|---|---|
| Count | ACE は、指定されたリターン コード番号ごとに、受け取ったリターン コードの合計数を追跡します。 |
| Log | ACE は、イベント数が指定のしきい値に達すると、syslog エラー メッセージを生成します。<br>1. [Threshold] フィールドに、syslog エラー メッセージの生成前に ACE が受信するイベント数を入力します。有効な値は 1 ～ 4294967295 の整数です。<br>2. [Reset] フィールドに、ACE がリターン コードのチェックを行う間隔を秒単位で入力します。有効な値は 1 ～ 2147483647 の整数秒です。 |
| Remove | ACE は、イベント数が指定のしきい値に達すると、syslog エラー メッセージを生成し、そのサーバをサービスから削除します。<br>1. [Threshold] フィールドに、syslog エラー メッセージを生成し、サーバをサービスから削除する前に ACE が受信するイベント数を入力します。有効な値は 1 ～ 4294967295 の整数です。<br>2. [Reset] フィールドに、ACE がリターン コードのチェックを行う間隔を秒単位で入力します。有効な値は 1 ～ 2147483647 の整数秒です。<br>3. [Resume Service] フィールドには、ACE が実サーバを非稼働状態にした後で、自動的に実サーバが再稼働するまでの待機時間を秒数で入力します。有効な値は 30 ～ 3600 秒です。デフォルトでは、このフィールドは設定されていません。このフィールドの設定は、次のとおり、障害状態の実サーバの動作に影響します。<br>– このフィールドが設定されていない場合、手動でサービスからデータを削除して読み込むまで、実サーバは障害状態のままになります。<br>– このフィールドが設定されておらず、30～3,600 の整数で設定した場合、障害が発生した実サーバはただちに動作状態に移行します。<br>– このフィールドを設定しており、値が大きくなると、実サーバは、以前設定した値の期間中障害状態のままになります。新しい値は、次回実サーバが障害状態に移行したときに有効になります。<br>– このフィールドを設定しており、値が小さくなると、障害が発生した実サーバはただちに動作状態に移行します。<br>– 30 ～ 3,600 の整数でこのフィールドを設定し、フィールドから値を削除することで、パスワードをリセットする場合、実サーバは、以前設定した値の期間中障害状態のままになります。未設定の設定は、次回実サーバが障害状態に移行したときに有効になります。手動でサービスからデータを削除して読み込むまで、実サーバは障害状態のままになります。 |

**ステップ 7**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- エントリを保存せずに手順を終了し、[Retcode Map] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別の retcode マップを設定するには、[Next] をクリックします。

### 関連トピック

- 「仮想コンテキストの使用」（P.4-2）
- 「仮想コンテキスト クラス マップの作成」（P.12-9）
- 「仮想コンテキスト ポリシー マップの作成」（P.12-35）
- 「実サーバの設定」（P.6-5）

- 「スティッキ グループの設定」（P.7-12）
- 「動的ワークロード拡張の設定」（P.6-14）

# すべてのサーバ ファームの表示

特定の仮想コンテキストに関連付けられているすべてのサーバ ファームを表示するには、次の手順を行います。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] を選択します。

[All Virtual Contexts] テーブルが表示されます。

**ステップ 2**　表示するサーバ ファームを持つ仮想コンテキストを選択し、[Load Balancing] > [Server Farms] をクリックします。

[Server Farms] テーブルに次の情報が表示されます。

- サーバ ファーム名
- サーバ ファームのタイプ（[host] または [redirect] のいずれか）
- 説明

選択したサーバ ファームに応じて、[Server Farms] テーブルの下に追加テーブルが表示されます。これらのテーブルは次のとおりです。

- [Real Servers]：選択したサーバ ファームに関連付けられている実サーバが表示されます。
- [Predictor]：選択したサーバ ファームに選択されているプレディクタ方式が表示されます。
- [Retcode Map]：選択したサーバの使用に対して設定されている HTTP リターン エラーコード チェックが表示されます。

**ステップ 3**　（任意）次の手順を実行します。

- サーバ ファームの追加または編集します（「サーバ ファームの設定」（P.6-18）を参照）。
- サーバ ファームを選択して、[Buddy Group] をクリックすると、**show buddy group** コマンドの出力結果を表示するポップアップ ウィンドウが表示されます。ポップアップ ウィンドウには、仮想コンテキストで設定された関連グループのリストを表示します（詳細については、「バディ スティッキ グループ」（P.7-6）を参照してください）。
- 選択したサーバに関連付けられた実サーバを表示するには、[Real Servers] タブをクリックします。このタブからサーバ ファームの実サーバを管理できます（「サーバ ファームへの実サーバの追加」（P.6-25）を参照）。
- 選択したサーバ ファームに関連付けられたプレディクタ方式を表示するには、[Predictor] タブをクリックします。このタブからプレディクタ方式を選択できます（「サーバ ファームのプレディクタ方式の設定」（P.6-28）を参照）。
- 選択したサーバ ファームに設定されている HTTP リターン エラーコード チェックを表示するには、[Retcode Map] タブをクリックします。このタブからエラーコード チェックを管理できます（「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）を参照）。

**関連トピック**

- 「サーバ ファームの設定」（P.6-18）

- 「サーバ ファームへの実サーバの追加」（P.6-25）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）
- 「動的ワークロード拡張の設定」（P.6-14）

## サーバ ファームの統計情報およびステータス情報の表示

特定のサーバ ファームの統計情報とステータス情報を表示できます。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Server Farms] を選択します。

[Server Farms] テーブルが表示されます。

**ステップ 2**　[Server Farms] テーブルでサーバ ファームを選択し、[Details] をクリックします。

**show serverfarm** *name* **detail** CLI コマンドの出力が表示されます。表示される出力フィールドの詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。

**ステップ 3**　[Update Details] をクリックして、**show serverfarm** *name* **detail** CLI コマンドの出力を更新します。

新しい情報が新しいタイムスタンプの他のパネルに表示されます。新旧のサーバ ファームの統計情報およびステータス情報が並べて表示され、最後に更新された情報が上書きされないようにしています。

**ステップ 4**　[Close] をクリックして、[Server Farms] テーブルに戻ります。

**関連トピック**

- 「すべてのサーバ ファームの表示」（P.6-37）
- 「サーバ ファームの設定」（P.6-18）
- 「サーバ ファームへの実サーバの追加」（P.6-25）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「サーバ ファームの HTTP リターン エラー コード チェックの設定」（P.6-35）
- 「動的ワークロード拡張の設定」（P.6-14）

# ヘルス モニタリングの設定

ヘルス プローブ（*キープアライブ*とも呼ばれる）を設定することによって、サーバおよびサーバ ファームのヘルスをチェックするように ACE アプライアンス に指示することができます。プローブを作成したら、プローブを実サーバまたはサーバ ファームに割り当てます。プローブは、TCP、ICMP、Telnet、HTTP など、多くのタイプのいずれかにすることができます。TCL スクリプト言語を使用して、スクリプト化されたプローブを設定することもできます（「TCL スクリプト」（P.6-39）を参照）。

ACE アプライアンス は、プローブを定期的に送信してサーバのステータスを調べ、サーバの応答を確認し、クライアントがサーバにアクセスできなくなるようなネットワークの他の問題がないかどうかをチェックします。ACE アプライアンス は、サーバの応答に基づいてサーバの稼働と非稼働の切り替えを行うことができ、また、サーバ ファーム内のサーバのステータスに基づいて、ロード バランシングに関する信頼性の高い決定を行うことができます。

ACE アプライアンスのヘルス モニタリングでは、プローブの送出によってサーバの状態が追跡されます。この機能はアウトオブバンド ヘルス モニタリングともいいます。ACE アプライアンス はサーバ応答を検証したり、クライアントがサーバに到達できなくなるネットワーク問題が発生していないかを確認したりします。ACE アプライアンスは、サーバ応答に基づいて、サーバを稼働状態または非稼働状態にするほか、信頼性の高いロード バランシングの判断を行うことができます。

（注）　インバンド ヘルス モニタリング機能およびヘルス プローブを設定して、サーバ ファーム内の実サーバの状態を監視できます。インバンド ヘルス モニタリングの詳細については、「サーバ ファームの設定」（P.6-18）を参照してください。

ACE アプライアンス は、サーバのヘルスを次のカテゴリに分類して識別します。

- [Passed]：サーバは有効な応答を戻します。
- [Failed]：サーバは ACE に有効な応答を提供することに失敗したか、または ACE が指定のリトライ回数でサーバに到達できません。

ACE アプライアンス にヘルス モニタリングを設定すると、ACE アプライアンス はアクティブ プローブを定期的に送信して、サーバ状態を判別します。

ACE アプライアンスは ICMP、TCP、HTTP、その他の定義済みヘルス プローブなど、4000 の一意なプローブ設定をサポートします。ACE アプライアンスは 1000 のソケットを同時に開くこともできます。

### 関連トピック

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「TCL スクリプト」（P.6-39）

# TCL スクリプト

ACE アプライアンス は、さまざまなアプリケーションを使用するときに必要な複数のタイプのヘルス プローブ（たとえば、HTTP、TCP、または ICMP ヘルス プローブ）、およびネットワークを管理するためのヘルス プローブをサポートしています。現行の ACE アプライアンス ソフトウェア リリースでサポートされている基本的なヘルス プローブのタイプでは、ご使用のネットワークで要求される特定のプローブ動作がサポートされない場合もあります。より柔軟なヘルス プローブ機能をサポートするため、ACE アプライアンスでは、ACE アプライアンスで TCL スクリプトのアップロードと実行が可能です。

ACE アプライアンス の TCL インタープリタ コードは、標準の TCL ディストリビューションのリリース 8.44 に基づいています。ヘルス プローブを設定するためのスクリプトを作成できます。スクリプト プローブは、ACE アプライアンス ソフトウェアで利用できる他のヘルス プローブと同様に動作します。スクリプト プローブの一部として、ACE アプライアンス がスクリプトを定期的に実行し、実行スクリプトから返される終了コードによって、特定の実サーバの相対的な健全性と可用性が示されます。ヘルス プローブの詳細については、「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照してください。

TCL 機能をサポートするために使用できる ACE アプライアンス用のサンプル スクリプトを示します。Cisco TAC はこれらのスクリプトをサポートしています。

- ECHO_PROBE_SCRIPT
- FINGER_PROBE_SCRIPT
- FTP_PROBE_SCRIPT
- HTTP_PROBE_SCRIPT
- HTTPCONTENT_PROBE
- HTTPHEADER_PROBE
- HTTPPROXY_PROBE
- IMAP_PROBE
- LDAP_PROBE
- MAIL_PROBE
- POP3_PROBE
- PROBENOTICE_PROBE
- RTSP_PROBE
- SSL_PROBE_SCRIPT

これらのスクリプトは、probe: ディレクトリに置かれており、管理コンテキストおよびユーザ コンテキストの両方でアクセスできます。probe: ディレクトリのスクリプト ファイルは読み取り専用であるため、これをコピーしたり変更したりできません。ただし、probe: ディレクトリからファイルをコピーできます。詳細については、『*Administration Guide, Cisco ACE Application Control Engine*』を参照してください。

ACE アプライアンスのメモリにスクリプトをロードし使用できるようにするには、**script file** コマンドを使用します。ACE アプライアンスへの Toolkit Command Language（TCL）スクリプトのロードと実行に関する詳細は、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

# 実サーバに対するヘルス モニタリングの設定

実サーバのヘルスおよびアベイラビリティをチェックするために、ACE アプライアンスでは定期的にプローブを実サーバに送信します。サーバの応答に応じて、ACE アプライアンス は、サーバをロードバランシングの決定に含めるかどうかを判断します。

**（注）** インバンド ヘルス モニタリング機能およびヘルス プローブを設定して、サーバ ファーム内の実サーバの状態を監視できます。設定を行う場合、サーバ ファーム内で実サーバを稼働状態に維持する必要があります。いずれかの機能がサーバが非稼働であることを検出した場合、ACE はこのサーバをロードバランシングの対象として選択しません。インバンド ヘルス モニタリングの詳細については、「サーバ ファームの設定」（P.6-18）を参照してください。

ロード バランシングの決定に使用できるかどうかを判断するため、実サーバのモニタリングを確立するには、次の手順を行います。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring] を選択します。[Health Monitoring] テーブルが表示されます。

**ステップ 2**　[Add] をクリックして新しいヘルス モニタリング プローブを追加するか、既存のエントリを選択してから [Edit] をクリックして、そのエントリを変更します。[Health Monitoring] 画面が表示されます。

**ステップ 3**　[Name] フィールドに、プローブの名前を入力します。この名前によってプローブが特定され、実サーバに関連付けられます。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。

**ステップ 4**　[Type] フィールドで、使用するプローブのタイプを選択します。プローブのタイプによって、その実サーバにプローブとして何が送信されるのかが決まります。プローブのタイプと説明は、表 6-9 を参照してください。

**表 6-9　プローブ タイプ**

| プローブ タイプ | 説明 |
|---|---|
| DNS | DNS サーバに要求を送信し、設定済みのドメインを与えます。サーバが起動しているかどうかを判別するために、ACE アプライアンスはこのドメインに設定された IP アドレスを受信する必要があります。 |
| ECHO-TCP | サーバにストリングを送信し、応答を元のストリングと比較します。応答ストリングと元のストリングが一致する場合、サーバは [passed] とマークされます。一致しない場合、ACE アプライアンスは設定回数だけ再試行し、一致しなければサーバは [failed] とマークされます。 |
| ECHO-UDP | サーバにストリングを送信し、応答を元のストリングと比較します。応答ストリングと元のストリングが一致する場合、サーバは [passed] とマークされます。一致しない場合、ACE アプライアンスは設定回数だけ再試行し、一致しなければサーバは [failed] とマークされます。 |
| FINGER | 定義済みのユーザ名がサーバ上のユーザ名と同じであることを確認するためにサーバにプローブを送信します。 |
| FTP | FTP セッションを開始します。デフォルトでは、このプローブはユーザ ID とパスワードを設定するオプションを使用した匿名ログイン用です。ACE アプライアンスは問題の結果を判断するために FTP GET または LS を実行します。このプローブでサポートされるのはアクティブ接続だけです。 |
| HTTP | TCP 接続をセットアップし、HTTP 要求を送信します。HTTP 要求が有効であれば、実サーバは [passed] とマークされます。 |
| HTTPS | HTTP プローブと似ていますが、このプローブでは SSL を使用して暗号データが生成されます。<br>**（注）**　このオプションは、ACE NPE のソフトウェア バージョンに使用できません（「ACE No Payload Encryption ソフトウェア バージョン関する情報」（P.1-2）を参照）。 |
| ICMP | ICMP 要求を送信し、応答をリッスンします。サーバが応答を返すと、ACE アプライアンスはその実サーバに [passed] のマークを付けます。応答がなく、タイムアウトになった場合、または DESTINATION_UNREACHABLE などの ICMP 標準エラーが発生した場合、ACE アプライアンスはその実サーバに [failed] のマークを付けます。 |
| IMAP | 設定済みのユーザ ID とパスワードを使用して、IMAP セッションを開始します。その後、サーバからの E メールの取得を試行し、サーバから受信したリターン コードに基づいてプローブの結果を検証します。 |
| POP | 設定済みのユーザ ID とパスワードを使用して、POP セッションを開始します。その後、サーバからの E メールの取得を試行し、サーバから受信したリターン コードに基づいてプローブの結果を検証します。 |

表 6-9　プローブ タイプ （続き）

| プローブ タイプ | 説明 |
|---|---|
| RADIUS | RADIUS サーバに接続し、ログインして、サーバが起動しているかどうかを判断します。 |
| RTSP | TCP 接続を確立し、要求パケットをサーバに送信します。ACE は応答と設定された応答コードを比較して、プローブが成功したかどうかを判別します。 |
| Scripted | 設定されたスクリプトからプローブを実行して、ヘルス プローブを実行します。この方式では、標準プローブにない機能を持つ特定のスクリプトを作成できます。 |
| SIP-TCP | TCP 接続を確立し、OPTIONS 要求パケットをサーバのユーザ エージェントに送信します。ACE は応答と、設定されている応答コード、予期ストリング、またはその両方を比較してプローブが成功したかを判別します。予測されるステータス コードが設定されていない場合は、サーバからのすべての応答は failed とマークされます。 |
| SIP-UDP | UDP 接続を確立し、OPTIONS 要求パケットをサーバのユーザ エージェントに送信します。ACE は応答と、設定されている応答コード、予期ストリング、またはその両方を比較してプローブが成功したかを判別します。予測されるステータス コードが設定されていない場合は、サーバからのすべての応答は failed とマークされます。 |
| SMTP | サーバにログインすることにより SMTP セッションを開始します。 |
| SNMP | UDP 接続を確立し、サーバへのプローブとして最大 8 つの SMNP OID クエリーを送信します。ACE は取得した負荷情報を重み付けして平均化し、この情報をロード バランシング決定のため、最小負荷アルゴリズムへの入力として使用します。取得した値が設定したしきい値内である場合、サーバは passed とマークされます。しきい値を超えた場合、サーバは failed とマークされます。 |
| TCP | TCP ハンドシェイクを開始し、応答を待ちます。デフォルトでは、応答に 1 回成功すると、サーバは passed とマークされます。その後、プローブは FIN を送信して、セッションを終了します。応答が無効な場合、または応答がない場合、サーバは [failed] とマークされます。 |
| TELNET | 実サーバとの接続を確立し、アプリケーションからのグリーティングが受信されたか確認します。 |
| UDP | 実サーバに UDP パケットを送信します。サーバに [failed] のマークが付くのは、ICMP Port Unreachable メッセージが戻った場合だけです。 |
| VM | VMware VM コントローラにプローブを送信して、関連付けられているローカル VM の CPU 使用率とメモリ使用率両方の平均値を測定します。プローブ応答は ACE がローカル VM のみへのトラフィックのロード バランシングを行っているか、またはローカル VM の高い使用率によりリモート VM へのトラフィックのバーストを行っているかを判断します。<br><br>**（注）** ACE を動的ワークロード拡張用に設定している場合は、VM プローブを使用します（「動的ワークロード拡張の設定」（P.6-14）を参照）。 |

**ステップ 5**　ヘルス モニタリングの全般的な属性を入力します（表 6-10 を参照）。

**（注）** 選択したプローブ タイプの追加の全般属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、Device Manager は、デフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

**表 6-10　ヘルス モニタリングの全般属性**

| フィールド | アクション |
|---|---|
| Description | このプローブの説明を入力します。有効な値は、引用符で囲まずスペースを含まない 240 文字以下の英数字のテキスト文字列です。 |
| Probe Interval (Seconds) | [passed] とマークされたサーバに ACE が別のプローブを送信するまでの待機時間を秒数で入力します。有効な値は、VM プローブを除くすべてのプローブ タイプで 2 ～ 65535 です。VM プローブは 300 ～ 65535 です。<br>デフォルトは、VM プローブを除くすべてのプローブ タイプで 15 秒です。VM プローブのデフォルトは 300 秒です。 |
| Pass Detect Interval (Seconds) | [failed] とマークされたサーバに ACE が別のプローブを送信するまでの待機時間を秒数で入力します。有効な値は、2 ～ 65535 の整数です。デフォルト値は 60 です。<br>**（注）** このフィールドは、VM プローブ タイプには適用されません。 |
| Fail Detect | サーバに [failed] のマークを付けるために ACE が検出しなければならないサーバとの通信の連続失敗回数を入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 3 です。<br>**（注）** このフィールドは、VM プローブ タイプには適用されません。 |

表 6-10　ヘルス モニタリングの全般属性 （続き）

| フィールド | アクション |
|---|---|
| **[More Settings]（VM プローブ タイプには適用できません）** | |
| Pass Detect Count | サーバに [passed] のマークを付けるためにサーバから受信する必要のある有効なプローブ応答の数を入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 3 です。 |
| Receive Timeout (Seconds) | サーバに [failed] のマークを付けるまでの待機時間を秒数で入力します。ACE は、プローブが送信されたサーバからの応答を、この時間だけ待ちます。有効な値は、1 ～ 65535 の整数です。デフォルト値は 10 です。 |
| Destination IPv4/IPv6 Address[1] | デフォルトでは、プローブは実サーバまたは仮想サーバに設定された IP アドレスを宛先 IP アドレスに使用します。プローブが使用する宛先アドレスを上書きするには、このフィールドに目的の宛先 IP アドレスを入力します。<br>**（注）** 次のプローブは IPv6 の宛先アドレスをサポートします。DNS、HTTP、HTTPS、ICMP、TCP、および UDP<br>**（注）** プローブを実サーバに割り当てる場合、同じ IP アドレス タイプ（IPv6 または IPv4）で設定する必要があります。 |
| Is Routed[2] | 宛先 IP アドレスが ACE の内部ルーティング テーブルに従ってルーティングされることを示すには、このチェックボックスをオンにします。宛先 IP アドレスが ACE の内部ルーティング テーブルに基づいてルーティングされないことを示すには、このチェックボックスをクリアします。 |
| Port | デフォルトでは、プローブがポート番号を継承する優先順位は次のとおりです。<br>• プローブ用に設定するポート番号。<br>• サーバ ファーム内の実サーバから設定されたポート番号。<br>• レイヤ 3 およびレイヤ 4 クラス マップで VIP から設定されたポート番号。<br>• デフォルトのポート番号。表 6-11 に、各プローブ タイプのデフォルト ポート番号を示します。<br>明示的にデフォルト ポートを設定すると、ACE は常にデフォルト ポートにプローブを送信します。プローブは、サーバ ファームの実サーバまたはクラス マップで指定したまたは VIP からのポート番号を動的に継承しません。 |

1. Scripted プローブ タイプの場合、[Dest IP Address] フィールドは使用できません。
2. RTSP、Scripted、SIP-TCP、および SIP-UDP の各プローブ タイプの場合、[Is Routed] フィールドは使用できません。

表 6-11　各プローブ タイプのデフォルト ポート番号

| プローブ タイプ | デフォルト ポート番号 |
|---|---|
| DNS | 53 |
| Echo | 7 |
| Finger | 79 |
| FTP | 21 |

表 6-11　各プローブ タイプのデフォルト ポート番号 （続き）

| プローブ タイプ | デフォルト ポート番号 |
|---|---|
| HTTP | 80 |
| HTTPS | 443 |
| ICMP | N/A |
| IMAP | 143 |
| POP3 | 110 |
| RADIUS | 1812 |
| RTSP | 554 |
| Scripted | 1 |
| SIP（TCP および UDP の両方） | 5060 |
| SMTP | 25 |
| SNMP | 161 |
| Telnet | 23 |
| TCP | 80 |
| UDP | 53 |
| VM | 443 |

**ステップ 6**　選択した特定のプローブ タイプ用の属性を入力します。

- DNS プローブについては、表 6-12 を参照してください。
- Echo-TCP プローブについては、表 6-13 を参照してください。
- Echo-UDP プローブについては、表 6-14 を参照してください。
- Finger プローブについては、表 6-15 を参照してください。
- FTP プローブについては、表 6-16 を参照してください。
- HTTP プローブについては、表 6-17 を参照してください。
- HTTPS プローブについては、表 6-18 を参照してください。
- ICMP プローブには固有の属性はありません。
- IMAP プローブについては、表 6-19 を参照してください。
- POP プローブについては、表 6-20 を参照してください。
- RADIUS プローブについては、表 6-21 を参照してください。
- RTSP プローブについては、表 6-22 を参照してください。
- Scripted プローブについては、表 6-23 を参照してください。
- SIP-TCP プローブについては、表 6-24 を参照してください。
- SIP-UDP プローブについては、表 6-25 を参照してください。
- SMTP プローブについては、表 6-26 を参照してください。
- SNMP プローブについては、表 6-27 を参照してください。
- TCP プローブについては、表 6-28 を参照してください。
- Telnet プローブについては、表 6-29 を参照してください。
- UDP プローブについては、表 6-30 を参照してください。

- VM プローブについては、表 6-31 を参照してください。

**ステップ 7**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- エントリを保存せずに手順を終了し、[Health Monitoring] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別のプローブを設定するには、[Next] をクリックします。

**ステップ 8**　（任意）特定のプローブの統計情報およびステータス情報を表示するには、プローブを [Health Monitoring] テーブルから選択し、[Details] をクリックします。

**show probe** *name* **detail** CLI コマンドの出力が表示されます。詳細については、「ヘルス モニタリング統計情報およびステータス情報の表示」（P.6-67）を参照してください。

---

**関連トピック**

- 「DNS プローブの予期アドレスの設定」（P.6-64）
- 「HTTP プローブおよび HTTPS プローブのヘッダーの設定」（P.6-64）
- 「ヘルス モニタリングの予期ステータスの設定」（P.6-65）
- 「実サーバの設定」（P.6-5）
- 「サーバ ファームの設定」（P.6-18）
- 「スティッキ グループの設定」（P.7-12）

## プローブ属性の表

ヘルス モニタリング プローブ固有の属性を設定する際には、次の各項を参照してください。

- 「DNS プローブの属性」（P.6-47）
- 「Echo-TCP プローブの属性」（P.6-47）
- 「Echo-UDP プローブの属性」（P.6-48）
- 「Finger プローブの属性」（P.6-48）
- 「FTP プローブの属性」（P.6-49）
- 「HTTP プローブの属性」（P.6-49）
- 「HTTPS プローブの属性」（P.6-51）
- 「IMAP プローブの属性」（P.6-53）
- 「POP プローブの属性」（P.6-54）
- 「RADIUS プローブの属性」（P.6-55）
- 「RTSP プローブの属性」（P.6-56）
- 「Scripted プローブの属性」（P.6-56）
- 「SIP-TCP プローブの属性」（P.6-58）
- 「SIP-UDP プローブの属性」（P.6-58）
- 「SMTP プローブの属性」（P.6-59）
- 「SNMP プローブの属性」（P.6-60）
- 「TCP プローブの属性」（P.6-60）

- 「Telnet プローブの属性」（P.6-61）
- 「UDP プローブの属性」（P.6-61）
- 「VM プローブの属性」（P.6-63）

ヘルス モニタリング プローブのその他の設定オプションについては、次の各項を参照してください。

- 「DNS プローブの予期アドレスの設定」（P.6-64）
- 「HTTP プローブおよび HTTPS プローブのヘッダーの設定」（P.6-64）
- 「ヘルス モニタリングの予期ステータスの設定」（P.6-65）
- 「SNMP プローブの OID の設定」（P.6-66）

## DNS プローブの属性

（注）　DNS プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

**表 6-12　DNS プローブの属性**

| フィールド | アクション |
|---|---|
| Domain Name | プローブから DNS サーバに送信されるドメイン名を入力します。有効な値は、引用符で囲まない 255 文字以下のテキスト文字列です。 |
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |

DNS プローブの予期アドレスを設定する場合は、「DNS プローブの予期アドレスの設定」（P.6-64）を参照してください。

## Echo-TCP プローブの属性

（注）　Echo-TCP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

**表 6-13　Echo-TCP プローブの属性**

| フィールド | アクション |
|---|---|
| Send Data | プローブからサーバに送信される ASCII データを入力します。有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |

表 6-13　Echo-TCP プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| **More Settings** | |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

## Echo-UDP プローブの属性

（注）　Echo-UDP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-14　Echo-UDP プローブの属性

| フィールド | アクション |
|---|---|
| Send Data | プローブからサーバに送信される ASCII データを入力します。有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |

## Finger プローブの属性

（注）　Finger プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-15　Finger プローブの属性

| フィールド | アクション |
|---|---|
| Send Data | プローブからサーバに送信される ASCII データを入力します。有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |

表 6-15　Finger プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

## FTP プローブの属性

（注）　FTP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-16　FTP プローブの属性

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

FTP プローブのプローブ予期ステータスを設定する場合は、「ヘルス モニタリングの予期ステータスの設定」（P.6-65）を参照してください。

## HTTP プローブの属性

（注）　HTTP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-17　HTTP プローブの属性

| フィールド | アクション |
|---|---|
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| Request Method Type | このプローブに使用される HTTP 要求メソッドのタイプを選択します。<br>• [N/A]：このオプションは定義されていません。<br>• [Get]：HTTP 要求メソッドは GET（URL は「/」）です。この要求メソッドでは、サーバはページを取得し、ACE はページのコンテンツのハッシュ値を計算します。ページのコンテンツ情報が変化すると、ハッシュ値は元のハッシュ値と一致しなくなり、ACE はサービスが停止していると想定します。これがデフォルトの要求メソッドです。<br>• [Head]：サーバはページのヘッダーだけを取得します。このメソッドを使用すると、ACE はコンテンツが変更されたためにハッシュ値が変更されていても、サービスが停止されているとは判断しません。 |
| Request HTTP URL | このフィールドは、[Request Method Type] フィールドで [Head] または [Get] が選択された場合に表示されます。<br>リモート サーバの URL パスを入力します。有効な値は、URL パスを示す 255 文字以下の文字列です。デフォルト パスは「/」です。 |
| **More Settings** | |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Append Port Host Tag | HTTP プローブにデフォルト以外の宛先ポートを設定する場合、HTTP ホスト ヘッダーでポート情報を追加するには、このチェックボックスをオンにします。HTTP ホスト ヘッダーでポート情報を追加しない場合は、チェックボックスをオフにします。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |
| User Name | 実サーバに対する認証に使用されるユーザ ID を入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。 |
| Password | 実サーバに対する認証に使用されるパスワードを入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。<br>[Confirm] フィールドにパスワードを再入力します。 |
| Expect Regular Expression | プローブの宛先からの応答として予期するデータを入力します。有効な値は、255 文字以下のテキスト文字列（引用符使用可）です。 |
| Expect Regex Offset | ACE が [Expect Regular Expression] フィールドに指定された文字列の検索を開始する受信メッセージまたはバッファ位置までの文字数を入力します。有効な値は 1 ～ 4000 の整数です。 |

表 6-17　HTTP プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| Hash | ACE が HTTP GET プローブに MD5 ハッシュを使用するように指定する場合は [Hash] チェックボックスをオンにします。ACE が HTTP GET プローブに MD5 ハッシュを使用しないように指定する場合は [Hash] チェックボックスをクリアします。 |
| Hash String | [Hash] チェックボックスを選択すると、このフィールドが表示されます。<br>32 ビットのハッシュ値を入力します。ACE は、サーバが送信した HTTP ページから生成されたハッシュとこの値を比較します。値を入力しないと、ACE はサーバへの初回のクエリー時に値を生成し、その値を保存して、サーバからのその他の応答と照合します。照合の結果、一致すると、プローブは Alive 状態を維持します。<br>16 文字の 16 進文字列で MD 5 ハッシュ値を入力します（引用符で囲んでも囲まなくてもかまいません）。 |

HTTP プローブのヘッダーと予期ステータスを設定するには、次の項を参照してください。

- 「HTTP プローブおよび HTTPS プローブのヘッダーの設定」（P.6-64）
- 「ヘルス モニタリングの予期ステータスの設定」（P.6-65）

## HTTPS プローブの属性

（注）　HTTPS プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-18　HTTPS プローブの属性

| フィールド | アクション |
|---|---|
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| Request Method Type | このプローブに使用される HTTP 要求メソッドのタイプを選択します。<br>• [N/A]：このオプションは定義されていません。<br>• [Get]：HTTP 要求メソッドは GET（URL は「/」）です。この要求メソッドでは、サーバはページを取得し、ACE はページのコンテンツのハッシュ値を計算します。ページのコンテンツ情報が変化すると、ハッシュ値は元のハッシュ値と一致しなくなり、ACE はサービスが停止していると想定します。これがデフォルトの要求メソッドです。<br>• [Head]：サーバはページのヘッダーだけを取得します。このメソッドを使用すると、ACE はコンテンツが変更されたためにハッシュ値が変更されていても、サービスが停止されているとは判断しません。 |

表 6-18　HTTPS プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| Request HTTP URL | このフィールドは、[Request Method Type] フィールドで [Head] または [Get] が選択された場合に表示されます。<br>リモート サーバの URL パスを入力します。有効な値は、URL パスを示す 255 文字以下の文字列です。デフォルト パスは「/」です。 |
| Cipher | この HTTPS プローブに使用する暗号スイートを選択します。<br>• RSA_ANY：HTTPS プローブは RSA 設定のすべての暗号スイートを受け入れます。特定のスイートは設定しません。これがデフォルトのアクションになります。<br>• RSA_EXPORT1024_WITH_DES_CBC_SHA<br>• RSA_EXPORT1024_WITH_RC4_56_MD5<br>• RSA_EXPORT1024_WITH_RC4_56_SHA<br>• RSA_EXPORT_WITH_DES40_CBC_SHA<br>• RSA_EXPORT_WITH_RC4_40_MD5<br>• RSA_WITH_3DES_EDE_CBC_SHA<br>• RSA_WITH_AES_128_CBC_SHA<br>• RSA_WITH_AES_256_CBC_SHA<br>• RSA_WITH_DES_CBC_SHA<br>• RSA_WITH_RC4_128_MD5<br>• RSA_WITH_RC4_128_SHA |
| SSL Version | サーバに送信される ClientHello メッセージに使用される SSL または TLS のバージョンを選択します。<br>• [All]：このプローブはすべての SSL バージョンを使用します。<br>• [SSLv3]：このプローブは SSL バージョン 3 を使用します。<br>• [TLSv1]：このプローブは TLS バージョン 1 を使用します。<br>デフォルトでは、プローブは SSL バージョン 3 ヘッダーおよび TLS バージョン 1 メッセージで ClientHello メッセージを送信します。 |
| **More Settings** | |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Append Port Host Tag | HTTPS プローブにデフォルト以外の宛先ポートを設定する場合、HTTP ホスト ヘッダーでポート情報を追加するには、このチェックボックスをオンにします。HTTP ホスト ヘッダーでポート情報を追加しない場合は、チェックボックスをオフにします。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |
| User Name | 実サーバに対する認証に使用されるユーザ ID を入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。 |

表 6-18　HTTPS プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| Password | 実サーバに対する認証に使用されるパスワードを入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。<br>[Confirm] フィールドにパスワードを再入力します。 |
| Expect Regular Expression | プローブの宛先からの応答として予期するデータを入力します。有効な値は、255 文字以下のテキスト文字列（引用符使用可）です。 |
| Expect Regex Offset | ACE が [Expect Regular Expression] フィールドに指定された文字列の検索を開始する受信メッセージまたはバッファ位置までの文字数を入力します。入力値は 1 ～ 4000 の整数です。 |
| Hash | ACE が HTTP GET プローブに MD5 ハッシュを使用するように指定する場合は [Hash] チェックボックスをオンにします。ACE が HTTP GET プローブに MD5 ハッシュを使用しないように指定する場合は [Hash] チェックボックスをクリアします。 |
| Hash String | [Hash] チェックボックスを選択すると、このフィールドが表示されます。<br>32 ビットのハッシュ値を入力します。ACE は、サーバが送信した HTTP ページから生成されたハッシュとこの値を比較します。値を入力しないと、ACE はサーバへの初回のクエリー時に値を生成し、その値を保存して、サーバからのその他の応答と照合します。照合の結果、一致すると、プローブは Alive 状態を維持します。<br>16 文字の 16 進文字列で MD 5 ハッシュ値を入力します（引用符で囲んでも囲まなくてもかまいません）。 |
| Ignore Certificate Expiration | 証明書の有効期限を無視するようプローブを設定して、証明書の期限切れになった場合にプローブが ACE の機能に影響を与えないようにするには、このチェックボックスをオンにします。証明書の有効期限を無視しないように ACE を設定する場合は、このチェックボックスをオフにします。 |

HTTPS プローブのヘッダーと予期ステータスを設定するには、次の項を参照してください。

- 「HTTP プローブおよび HTTPS プローブのヘッダーの設定」（P.6-64）
- 「ヘルス モニタリングの予期ステータスの設定」（P.6-65）

## IMAP プローブの属性

（注）　IMAP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-19　IMAP プローブの属性

| フィールド | アクション |
|---|---|
| User Name | 実サーバに対する認証に使用されるユーザ ID を入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。 |
| Password | 実サーバに対する認証に使用されるパスワードを入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。<br>[Confirm] フィールドにパスワードを再入力します。 |
| Mailbox Name | この IMAP プローブの E メールを取得するユーザ メールボックスの名前を入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。 |
| Request Command | このプローブの要求メソッド コマンドを入力します。有効な値は、スペースを含まない 32 文字以下のテキスト文字列です。 |
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

## POP プローブの属性

（注）　POP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-20　POP プローブの属性

| フィールド | アクション |
|---|---|
| User Name | 実サーバに対する認証に使用されるユーザ ID を入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。 |
| Password | 実サーバに対する認証に使用されるパスワードを入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。<br>[Confirm] フィールドにパスワードを再入力します。 |
| Request Command | このプローブの要求メソッド コマンドを入力します。有効な値は、スペースを含まない 32 文字以下のテキスト文字列です。 |

表 6-20　POP プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

## RADIUS プローブの属性

（注）　RADIUS プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-21　RADIUS プローブの属性

| フィールド | アクション |
|---|---|
| User Secret | RADIUS サーバへのプローブ アクセスを許可するために使用する共有秘密を入力します。有効な値は、大文字と小文字を区別し、スペースを含まない 64 文字以下のテキスト文字列です。 |
| User Name | 実サーバに対する認証に使用されるユーザ ID を入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。 |
| Password | 実サーバに対する認証に使用されるパスワードを入力します。有効な値は、引用符で囲まない 64 文字以下のテキスト文字列です。<br>[Confirm] フィールドにパスワードを再入力します。 |
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| NAS IP Address | Network Access Server（NAS）の IP アドレスをドット付き 10 進表記で入力します（例：192.168.11.1）。 |

## RTSP プローブの属性

（注） RTSP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-22　RTSP プローブの属性

| フィールド | アクション |
|---|---|
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| RTSP Require Header Value | このプローブの Require ヘッダーを入力します。 |
| RTSP Proxy Require Header Value | このプローブの Proxy-Require ヘッダーを入力します。 |
| RTSP Request Method Type | 次のいずれかの要求メソッド タイプを選択します。<br>• [N/A]：要求メソッドは選択しません。<br>• [Describe]：このプローブは Describe 要求方式を使用します。 |
| Request HTTP URL | このフィールドは、[RTSP Request Method Type] フィールドで [Describe] が選択された場合に表示されます。<br>サーバの RTSP メディア ストリームの URL 要求の URL パスを入力します。有効な値は、255 文字以下の文字列です。 |
| **More Settings** | |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

RTSP プローブのプローブ予期ステータスを設定する場合は、「ヘルス モニタリングの予期ステータスの設定」（P.6-65）を参照してください。

## Scripted プローブの属性

（注） Scripted プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-23　Scripted プローブの属性

| フィールド | アクション |
|---|---|
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| Script Name | ACE でこのファイルに割り当てるローカル名を入力します。このファイルは、disk0: ディレクトリまたは probe: ディレクトリ（probe: ディレクトリが存在する場合）にあります。<br><br>（注）　最初に ACE デバイスでスクリプト ファイルを設定して、デバイスに表示されるとおりに正確に名前を入力する必要があります。詳細については、ACE のマニュアルを参照してください。<br><br>有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |
| Script Arguments | 有効な引数は、引用符で囲まず、スペースを含まないテキスト文字列です。複数の引数を指定する場合は、引数の間をスペースで区切ります。このフィールドの最大文字数は 255 です。 |
| **More Settings** | |
| Script Needs To Be Copied From Remote Location? | リモート サーバからファイルをコピーする必要があることを示すには、このチェックボックスをオンにします。スクリプトがローカル システムにあることを示すには、このチェックボックスをクリアします。 |
| Protocol | リモート サーバからスクリプトをコピーすると、このフィールドが表示されます。<br><br>スクリプトのコピーに使用するプロトコルを選択します。<br>• [FTP] : FTP を使用してスクリプトをコピーします。<br>• [TFTP] : TFTP を使用してスクリプトをコピーします。 |
| User Name | [Protocol] フィールドで FTP を選択すると、このフィールドが表示されます。<br><br>リモート サーバのユーザ アカウントの名前を入力します。 |
| Password | [Protocol] フィールドで FTP を選択すると、このフィールドが表示されます。<br><br>リモート サーバのユーザ アカウントのパスワードを入力します。<br><br>[Confirm] フィールドにパスワードを再入力します。 |
| Source File Name | リモート サーバからスクリプトをコピーすると、このフィールドが表示されます。<br><br>ホストの IP アドレス、リモート サーバ上のファイルのパスおよびファイル名を、*host-ip/path/filename* の形式で入力します。<br>• *host-ip* は、リモート サーバの IP アドレスを表します。<br>• *path* は、リモート サーバ上のファイルのディレクトリ パスを表します。<br>• *filename* は、リモート サーバ上のファイルのファイル名を表します。<br><br>たとえば、**192.168.11.2/usr/bin/my-script.ext** のように入力します。 |

## SIP-TCP プローブの属性

（注）　SIP-TCP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

**表 6-24　SIP-TCP プローブの属性**

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |
| Expect Regular Expression | プローブの宛先からの応答として予期するデータを入力します。有効な入力は、255 文字以下のテキスト文字列です。このフィールドでは、単一引用符と二重引用符の両方が使用できます。二重引用符は区切り文字と見なされるため、デバイスには表示されません。単一引用符はデバイスに表示されます。 |
| Expect Regex Offset | ACE が [Expect Regular Expression] フィールドに指定された文字列の検索を開始する受信メッセージまたはバッファ位置までの文字数を入力します。入力値は 1 ～ 4000 の整数です。 |

SIP-TCP プローブのプローブ予期ステータスを設定する場合は、「ヘルス モニタリングの予期ステータスの設定」（P.6-65）を参照してください。

## SIP-UDP プローブの属性

（注）　SIP-UDP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

**表 6-25　SIP-UDP プローブの属性**

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |

表 6-25　SIP-UDP プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| Enable Rport | 要求が受信されたポートと同じポートからサーバが強制的に応答を送信するようにする場合は、このチェックボックスをオンにします。サーバが要求を受信したポート以外のポートから応答を送信できるようにする場合は、このチェックボックスをオフにします。 |
| Expect Regular Expression | プローブの宛先からの応答として予期するデータを入力します。有効な入力は、255 文字以下のテキスト文字列です。このフィールドでは、単一引用符と二重引用符の両方が使用できます。二重引用符は区切り文字と見なされるため、デバイスには表示されません。単一引用符はデバイスに表示されます。 |
| Expect Regex Offset | ACE が [Expect Regular Expression] フィールドに指定された文字列の検索を開始する受信メッセージまたはバッファ位置までの文字数を入力します。入力値は 1 ～ 4000 の整数です。 |

SIP-UDP プローブのプローブ予期ステータスを設定する場合は、「ヘルス モニタリングの予期ステータスの設定」（P.6-65）を参照してください。

## SMTP プローブの属性

（注）　SMTP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-26　SMTP プローブの属性

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

SMTP プローブのプローブ予期ステータスを設定する場合は、「ヘルス モニタリングの予期ステータスの設定」（P.6-65）を参照してください。

## SNMP プローブの属性

（注）　SNMP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-27　SNMP プローブの属性

| フィールド | アクション |
|---|---|
| SNMP Community | SNMP コミュニティ ストリングを入力します。有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| SNMP Version | このプローブの SNMP バージョンを選択します。<br>• [N/A]：バージョンは選択しません。<br>• [SNMPv1]：このプローブは SNMPv1 を使用します。<br>• [SNMPv2c]：このプローブは SNMPv2c を使用します。 |

SNMP プローブの SNMP OID を設定する場合は、「SNMP プローブの OID の設定」（P.6-66）を参照してください。

## TCP プローブの属性

（注）　TCP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-28　TCP プローブの属性

| フィールド | アクション |
|---|---|
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| Send Data | プローブからサーバに送信される ASCII データを入力します。有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |
| **More Settings** | |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |

表 6-28　TCP プローブの属性 （続き）

| フィールド | アクション |
|---|---|
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |
| Expect Regular Expression | プローブの宛先からの応答として予期するデータを入力します。有効な値は、255 文字以下のテキスト文字列（引用符使用可）です。 |
| Expect Regex Offset | ACE が [Expect Regular Expression] フィールドに指定された文字列の検索を開始する受信メッセージまたはバッファ位置までの文字数を入力します。入力値は 1 ～ 4000 の整数です。 |

## Telnet プローブの属性

（注）　Telnet プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-29　Telnet プローブの属性

| フィールド | アクション |
|---|---|
| **More Settings** | |
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| TCP Connection Termination | このチェックボックスをオンにすると、ACE がサーバに FIN を送信することで、TCP 接続を通常どおりに終了するよう設定されます。このチェックボックスをオフにすると、ACE が RST を送信して TCP 接続を終了するよう設定されます。 |
| Open Timeout (Seconds) | 実サーバとの接続を開始する際の待機時間を秒数で入力します。有効な値は、1 ～ 65535 の整数です。デフォルト値は 1 です。 |

## UDP プローブの属性

（注）　UDP プローブ タイプの追加の属性にアクセスするには、[More Settings] をクリックします。デフォルトでは、ACE アプライアンス Device Manager はデフォルト値を持つプローブ属性と、あまり使用されないプローブ属性を非表示にします。

表 6-30　UDP プローブの属性

| フィールド | アクション |
|---|---|
| Port | プローブが使用するポート番号を入力します。デフォルトでは、プローブはポートを継承してポート番号を決定します。詳細については、全般属性の [Port] フィールドの説明を参照してください。 |
| Send Data | プローブからサーバに送信される ASCII データを入力します。有効な値は、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。 |
| **More Settings** | |
| Expect Regular Expression | プローブの宛先からの応答として予期するデータを入力します。有効な値は、255 文字以下のテキスト文字列（引用符使用可）です。 |
| Expect Regex Offset | ACE が [Expect Regular Expression] フィールドに指定された文字列の検索を開始する受信メッセージまたはバッファ位置までの文字数を入力します。入力値は 1 ～ 4000 の整数です。 |

## VM プローブの属性

（注）　ACE を動的ワークロード拡張用に設定している場合は、VM プローブを使用します（「動的ワークロード拡張の設定」（P.6-14）を参照）。

ACE がローカル VM の CPU 使用率、メモリ使用率、または両方の平均に基づいてリモート VM にトラフィックをバーストさせた場合、VM プローブが制御するよう設定します。ACE は、ローカル VM に関連付けられている指定された VM コントローラに VM プローブを送信することで、使用状況に関する情報を取得します。この VM コントローラは、すべてのローカル VM の平均的な集約付加の情報を、CPU 使用率またはメモリ使用率のパーセンテージとして計算し、どちらかまたは両方のパーセンテージを使用してリモート データセンターへトラフィックをバーストさせるタイミングを決定します。サーバ ファームが物理サーバと仮想マシンの両方で構成されている場合、ACE は VM からの負荷情報のみを考慮します。

デフォルトでは、VM プローブが最大しきい値に対する CPU またはメモリの使用率のパーセンテージを確認します。最大しきい値に達するとパーセンテージの値にかかわらず、まず ACE はリモート データセンターにトラフィックをバーストさせます。デフォルトの最大バーストしきい値 99 パーセントの場合、負荷値が 100 パーセントでないか、または VM が実行状態の場合、ACE が常にローカル VM へのトラフィックのロード バランシングを行うよう指示します。最大バーストしきい値が 1 パーセントに設定されいてる場合、ACE はリモート データセンターに常にトラフィックをバーストさせます。

使用率パーセンテージが最小しきい値未満の場合、ACE は、リモート データセンターへのトラフィックのバーストを停止し、ローカル VM へのトラフィックのロード バランスを続行します。リモート データセンターへのアクティブな接続は完了できます。

ACE がリモート VM へのトラフィックをバーストさせる時期の制御を可能にする VM のプローブ属性を、表 6-31 に示します。

**表 6-31　VM プローブの属性**

| フィールド | アクション |
|---|---|
| Probe Interval (seconds) | ACE がプローブを VM にコントローラを送信する頻度（秒）。300 ～ 65535 の整数を入力します。デフォルトは 300（5 分）です。 |
| Max CPU Burst Threshold | すべてのローカル VM の平均負荷情報に基づいた最大 CPU 使用率パーセンテージのしきい値。CPU 使用率パーセンテージがこのしきい値に達するか、または超過した場合、ACE はリモート VM へのトラフィックのバーストを開始します。1 ～ 99 の値を入力します。デフォルトは 99 です。 |
| Min CPU Burst Threshold | すべてのローカル VM の平均負荷情報に基づいた最小 CPU 使用率パーセンテージのしきい値。CPU 使用率パーセンテージがこのしきい値未満まで低下すると、ACE はリモート VM へのトラフィックのバーストを停止します。1～99 のパーセント値を入力します。デフォルトは 99 です。 |
| Max Memory Burst Threshold | すべてのローカル VM の平均負荷情報に基づいた最大メモリ使用率パーセンテージのしきい値。メモリ使用率パーセンテージがこのしきい値に達するか、または超過した場合、ACE はリモート VM へのトラフィックのバーストを開始します。1～99 のパーセント値を入力します。デフォルトは 99 です。 |
| Min Memory Burst Threshold | すべてのローカル VM の平均負荷情報に基づいた最小メモリ使用率パーセンテージのしきい値。メモリ使用率パーセンテージがこのしきい値未満まで低下すると、ACE はリモート VM へのトラフィックのバーストを停止します。1～99 のパーセント値を入力します。デフォルトは 99 です。 |
| VM Controller Name | ユーザが「VM コントローラ接続の設定と検証」（P.6-16）で設定した VM コントローラの ID。VM コントローラのオプション ボタンをクリックします。 |

**関連トピック**

- 「動的ワークロード拡張の設定」（P.6-14）

# DNS プローブの予期アドレスの設定

サーバにドメイン名解決要求を送信した DNS プローブは、受信した IP アドレスと設定済みアドレスを照合して、返された IP アドレスを検証します。

ACE アプライアンス が DNS 要求に対する応答として受信を予期する IP アドレスを指定するには、次の手順を行います。

**前提**

DNS プローブが設定されている必要があります。詳細については、「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照してください。

**手順**

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring] を選択します。[Health Monitoring] テーブルが表示されます。

**ステップ 2**　予期 IP アドレスを設定する DNS プローブを選択します。[Expect Addresses] サブテーブルが表示されます。

**ステップ 3**　[Expect Addresses] テーブルにエントリを追加するには、[Add] をクリックします。[Expect Address] 設定画面が表示されます。

**（注）**　[Expect Addresses] テーブル内のエントリは変更できません。変更する代わりに、既存のエントリを削除してから新しいエントリを追加します。

**ステップ 4**　[IPv4/IPv6 Address] フィールドに、ACE アプライアンスが DNS 要求へのサーバ応答として予期する IP アドレスを入力します。このフィールドに複数のアドレスを入力できます。ただし、IPv4 と IPv6 アドレスを混在させることはできません。

**ステップ 5**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- エントリを保存せずに手順を終了し、[Expect Addresses] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別の IP アドレスを [Expect Addresses] テーブルに追加するには、[Next] をクリックします。

**関連トピック**

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「DNS プローブの属性」（P.6-47）

# HTTP プローブおよび HTTPS プローブのヘッダーの設定

HTTP プローブおよび HTTPS プローブのヘッダー フィールドを指定するには、次の手順を行います。

### 前提

HTTP プローブまたは HTTPS プローブが設定されている必要があります。詳細については、「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照してください。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring] を選択します。[Health Monitoring] テーブルが表示されます。

**ステップ 2**　ヘッダーを設定するプローブとして [HTTP] または [HTTPS] を選択します。[Probe Headers] サブテーブルが表示されます。

**ステップ 3**　[Add] をクリックしてエントリを追加するか、または既存のエントリを選択して [Edit] をクリックし、そのエントリを変更します。[Probe Headers] 設定画面が表示されます。

**ステップ 4**　[Header Name] フィールドで、プローブが使用する HTTP ヘッダーを選択します。

**ステップ 5**　[Header Value] フィールドに、ヘッダー フィールドに割り当てる文字列を入力します。有効な入力は、255 文字以下のテキスト文字列です。文字列にスペースが含まれている場合は、文字列を引用符で囲みます。

**ステップ 6**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- エントリを保存せずに手順を終了し、[Probe Headers] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別のヘッダーを [Probe Headers] テーブルに追加するには、[Next] をクリックします。

### 関連トピック

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「HTTP プローブの属性」（P.6-49）
- 「HTTPS プローブの属性」（P.6-51）

## ヘルス モニタリングの予期ステータスの設定

サーバから応答を受信した ACE アプライアンス は、ステータス コードを待機します。このステータス コードを受信すると、サーバは passed とマークされます。デフォルトでは、ACE アプライアンスにステータス コードは設定されていません。ステータス コードが設定されていない場合は、サーバからのすべての応答コードは failed とマークされます。

予期ステータス コードを設定できるプローブは、FTP、HTTP、HTTPS、RTSP、SIP、TCP、SIP、UDP、SMTP です。

ACE アプライアンスがプローブの宛先からの応答として受信を予期する単一コードまたはコード範囲を設定するには、次の手順を行います。

### 前提

FTP、HTTP、HTTPS、RTSP、SIP-TCP、SIP-UDP、または SNMP のプローブが設定されている必要があります。詳細については、「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照してください。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring] を選択します。[Health Monitoring] テーブルが表示されます。

**ステップ 2**　予期ステータス コードを設定するプローブとして、[FTP]、[HTTP]、[HTTPS]、または [SMTP] を選択します。[Expect Status] サブテーブルが表示されます。

**ステップ 3**　[Add] をクリックしてエントリを追加するか、または既存のエントリを選択して [Edit] をクリックし、そのエントリを変更します。[Expect Status] 設定画面が表示されます。

**ステップ 4**　単一の予期ステータス コードを設定する場合

**a.** [Min. Expect Status Code] フィールドに、このプローブの予期ステータス コードを入力します。有効な入力は 0 ～ 999 の整数です。

**b.** [Max. Expect Status Code] フィールドに、[Min. Expect Status Code] フィールドで入力したのと同じ予期ステータス コードを入力します。

**ステップ 5**　予期ステータス コードの範囲を設定する場合

**a.** [Min. Expect Status Code] に、ステータス コードの範囲の下限を入力します。有効な入力は 0 ～ 999 の整数です。

**b.** [Max. Expect Status Code] に、ステータス コードの範囲の上限を入力します。有効な入力は 0 ～ 999 の整数です。このフィールドの値は、[Min. Expect Status Code] フィールドの値以上にする必要があります。

**ステップ 6**　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- エントリを保存せずに手順を終了し、[Expect Status] テーブルに戻るには、[Cancel] をクリックします。
- エントリを保存して、別の予期ステータス コードを [Expect Status] テーブルに追加するには、[Next] をクリックします。

### 関連トピック

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「FTP プローブの属性」（P.6-49）
- 「HTTP プローブの属性」（P.6-49）
- 「SNMP プローブの属性」（P.6-60）

# SNMP プローブの OID の設定

ACE が SNMP OID クエリーのプローブを送信する場合、ACE は取得した値を、ロード バランシング決定用の最小負荷アルゴリズムへの入力として使用します。最小ロードのロード バランシングは、最小負荷値を持ったサーバに基づいてサーバを選択します。取得した値が設定したしきい値内である場合、サーバは passed とマークされます。しきい値を超えた場合、サーバは failed とマークされます。

ACE では、サーバへのプローブとして最大 8 つの OID クエリーを使用できます。

### 前提

SNMP プローブが設定されている必要があります。詳細については、「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照してください。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring] を選択します。[Health Monitoring] テーブルが表示されます。

**ステップ 2**　OID を指定する SNMP プローブを選択します。[SNMP OID for Server Load Query] テーブルが表示されます。

**ステップ 3**　[Add] をクリックしてエントリを追加するか、または既存のエントリを選択して [Edit] をクリックし、そのエントリを変更します。[SNMP OID] 設定ペインが表示されます。

**ステップ 4**　[SNMP OID] フィールドに、プローブがサーバへの値のクエリーに使用する OID を入力します。有効な値は、引用符で囲まず、255 文字以下のドット付き 10 進表記の英数字です（例：1.3.6.1.4.2021.10.1.3.1）。OID ストリングはサーバ タイプに基づいています。

**ステップ 5**　[Maximum Absolute Server Load Value] フィールドに、整数の OID 値を入力して、取得した OID 値はパーセント値ではなく絶対値であることを示します。有効な値は 1 ～ 4294967295 の整数です。

ACE が SNMP OID クエリーのプローブを送信する場合、ACE は取得した値を、ロード バランシング決定用の最小負荷アルゴリズムへの入力として使用します。デフォルトでは、ACE は取得した OID 値をパーセント値であると見なします。取得される OID 値を絶対値にする場合は、このオプションを使用します。

**ステップ 6**　[Server Load Threshold Value] フィールドに、サーバを非稼働状態にするしきい値を指定します。

- OID 値がパーセント値の場合、有効な値は 1 ～ 100 の整数です。
- OID が絶対値の場合は、1 から [Maximum Absolute Server Load Value] フィールドに指定した値までが有効な値です。

**ステップ 7**　[Server Load Weighting] フィールドに、SNMP プローブのこの OID に割り当てる重み値を入力します。有効な値は 0 ～ 16000 の整数です。

**ステップ 8**　次の手順を実行します。

- この設定を展開するには、[Deploy Now] をクリックします。
- エントリを保存せずに手順を終了し、[SNMP OID] テーブルに戻るには、[Cancel] をクリックします。
- エントリを導入し、[SNMP OID] テーブルに別の項目を追加するには、[Next] をクリックします。

### 関連トピック

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）
- 「SNMP プローブの属性」（P.6-60）

# ヘルス モニタリング統計情報およびステータス情報の表示

特定のプローブの統計情報とステータス情報を表示できます。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring] を選択します。

[Health Monitoring] テーブルが表示されます。

**ステップ 2**　[Health Monitoring] テーブルでは、プローブを [Health Monitoring] テーブルから選択し、[Details] をクリックします。

**show probe** *name* **detail** CLI コマンドの出力が表示されます。表示される出力フィールドの詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』第 4 章「Configuring Health Monitoring」を参照してください。

**（注）**　DNS プローブの場合、詳細なプローブの結果には、デフォルトの DNS ドメイン www.Cisco.com が常に示されます。

**ステップ 3**　[Update Details] をクリックして、**show probe** *name* **detail** CLI コマンドの出力を更新します。

**ステップ 4**　[Close] をクリックして、[Health Monitoring] テーブルに戻りします。

### 関連項目

- 「実サーバに対するヘルス モニタリングの設定」（P.6-40）

# セキュア KAL-AP の設定

ACE の Keepalive-Appliance Protocol（KAL-AP）により、ACE と、KAL-AP 要求を送信する Global Site Selector（GSS）の間の通信を許可し、サーバの状態と Global-Server Load-Balancing（GSLB）決定のための負荷を報告します。ACE は UDP 接続を通じて KAL-AP を使用し、重みを計算してサーバのアベイラビリティに関する情報を KAL-AP デバイスに提供します。ACE はサーバとして機能し、KAL-AP 要求を受信します。KAL-AP が ACE で初期化されると、ACE は標準 5002 ポート上で KAL-AP 要求を受信します。他のポートは設定できません。

ACE は GSS との間のデータの MD5 暗号化のため、セキュア KAL-AP をサポートします。暗号化の場合、GSS と ACE コンテキストの間の認証用キーとして共有秘密を設定する必要があります。

KAL-AP を設定する場合、ワイルドカード KAL-AP GSS の IP アドレス（0.0.0.0）を使用して、同じ MD5 暗号化秘密を使用する複数の GSS デバイスと ACE 間で安全な通信チャネルを確立できます。

仮想コンテキストに関連付けられているセキュア KAL-AP を設定するには、この手順を使用します。

### 前提

- Keepalive Appliance Protocol over UDP を指定する仮想コンテキストを作成しておきます。
- 管理クラス マップおよびポリシー マップを設定することによって ACE で KAL-AP をイネーブルにしておき、これを適切なインターフェイスに適用します。

### 注意事項および制約事項

0.0.0.0 のワイルドカード KAL-AP GSS の IP アドレスを使用する場合、次のガイドラインと制約事項に従ってください。

- 次の条件がともに存在する場合は、ワイルドカードの IP アドレスを使用します。

- クラスタ内のすべての GSS デバイスが、ACE との KAL-AP のメッセージ交換用に安全なチャネルを使用します。クラスタ内の GSS が安全でないチャネルを使用している場合、ワイルドカードの IP アドレスは使用しません。
- クラスタ内のすべての GSS デバイスまたは一連の GSS デバイスが、同じ MD5 秘密を使用します。

（注）　ワイルドカード VIP アドレスは、同じ MD5 秘密を使用する 1 組の GSS デバイスに対してのみ使用できます。他の GSS デバイスはすべて、KAL-AP に対して個別に設定する必要があります。

- KAL-AP の IP アドレスを削除した場合、ワイルドカードの IP アドレスを使用すると、ワイルドカード値に関連付けられた秘密を使用するこれらの GSS の IP アドレスだけが削除されます。GSS 固有の IP アドレスを使用して定義された KAL-AP の IP アドレスは、個別に削除する必要があります。

### 手順

**ステップ 1**　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Secure KAL-AP] を選択します。

[Secure KAL-AP] テーブルが表示されます。

**ステップ 2**　[Add] をクリックし、MD5 データ暗号化用にセキュア KAL-AP を設定します。

[Secure KAL-AP] 設定画面が表示されます。

**ステップ 3**　[IP Address] フィールドで、GSS 用の IP アドレスを設定することによって、安全な KAL-AP をイネーブルにします。

クラスタ内のすべての GSS デバイスが同じ MD5 暗号化秘密を使用する場合、ドット付き 10 進表記（192.168.11.1 など）を使用して、特定の GSS デバイスの IP アドレスを入力するか、またはワイルドカード値（0.0.0.0）を入力します（「注意事項および制約事項」（P.6-68）を参照）。

[Hash Key] フィールドに、KAL-AP デバイスと ACE の間の MD5 暗号化方式の共有秘密を入力します。共有秘密は、最大 31 文字のスペースを含まない、大文字と小文字を区別する英数字で入力します。ACE は、共有秘密では次の特殊文字をサポートしています。

, ./ = + - ^ @ !% ~ # $ * ( )

**ステップ 4**　次のいずれかを実行します。

- エントリを保存するには、[Deploy Now] をクリックします。ACE アプライアンスによってセキュア KAL-AP 設定が確認され、配置されます。
- エントリを確定せずにこの手順を終了し、[Secure KAL-AP] テーブルに戻るには、[Cancel] をクリックします。
- エントリを確定するには、[Next] をクリックします。

### 関連トピック

- 「仮想コンテキストの作成」（P.4-2）
- 「レイヤ 3/4 管理トラフィックのクラス マップに関する一致条件の設定」（P.12-15）