CHAPTER 4

ヘルス モニタリングの設定

この章では、プローブを送信することでサーバの状態を追跡するよう、ACE 上でのヘルス モニタリングの設定方法を説明します。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 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 はサーバ応答に基づいて、サーバをイン オブ サービスまたはアウト オブ サービスにしたり、信頼性の高いロード バランシング判断を行ったりできます。

ヘルス モニタリングを使用すると、ハイ アベイラビリティ設定（冗長性）のゲートウェイまたはホストの障害を検出することもできます。詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

ACE 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返します。
- failed — サーバは ACE に有効な応答を返すことに失敗し、指定のリトライ回数でサーバに到達できません。

ACE にヘルス モニタリングを設定すると、ACE 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 は ICMP、TCP、HTTP、その他の定義済みヘルス プローブなど、1000 の一意なプローブ設定をサポートします。ACE が同時に実行できる並行スクリプト プローブは最大で 200 のみです。ACE は 2048 のソケットを同時に開くこともできます。

同じプローブを複数の実サーバまたはサーバ ファームに関連付けることができます。同じプローブを再使用するたびに、ACE は別のプローブ インスタンスとしてカウントします。最大で 4000 のプローブ インスタンスを割り当てることができます。

この章の主な内容は、次のとおりです。

アクティブ ヘルス プローブの設定

デフォルトでは、ACE にアクティブ ヘルス プローブは設定されていません。ACE にヘルス プローブを設定すると、接続をアクティブに確立したり、トラフィックをサーバに明示的に送信したりできます。プローブはサーバのヘルス状態が passed であるか、または failed であるかを、応答で判別します。

アクティブ プローブの設定プロセスは、3 つのステップで構成されます。

1. ヘルス プローブに名前、タイプ、およびアトリビュートを設定します。
2. プローブに次のいずれか 1 つを関連付けます。
   - 実サーバ
   - 実サーバ。その後、実サーバにサーバ ファームを関連付けます。サーバ ファーム内の実サーバには、プローブを 1 つまたは複数関連付けることができます。
   - サーバ ファーム。サーバ ファーム内のすべてのサーバは、関連付けられたプローブ タイプのプローブを受信します。
3. 実サーバまたはサーバ ファームをアクティブにします。

プローブに実サーバまたはサーバ ファームを関連付けて、処理する方法については、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。

ゲートウェイまたはホストを追跡するように、1 つまたは複数のプローブを設定することもできます。詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』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。

- HTTPS プローブの設定
- FTP プローブの設定
- Telnet プローブの設定
- DNS プローブの設定
- SMTP プローブの設定
- IMAP プローブの設定
- POP3 プローブの設定
- SIP プローブの設定
- RTSP プローブの設定
- RADIUS プローブの設定
- SNMP ベースのサーバ ロード プローブの設定
- スクリプト プローブの設定
- UDP プローブのロード バランシング設定例

アクティブ プローブの定義およびプローブ コンフィギュレーション モードへのアクセス

ヘルス プローブを最初に設定する場合は、プローブのタイプおよび名前を定義します。その後、CLI からプローブ コンフィギュレーション モードを開始し、プローブ タイプのアトリビュートを設定します。

プローブを定義し、プローブ コンフィギュレーション モードにアクセスするには、コンフィギュレーション モードで **probe** コマンドを使用します。このコマンドの構文は次のとおりです。

probe *probe_type probe_name*

引数は次のとおりです。

- *probe_type* — プローブからサーバに送信される内容を決定するプローブ タイプです。次のキーワードのいずれか 1 つを入力します。
  - **icmp** — Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）プローブ タイプを指定し、ICMP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「ICMP プローブの設定」を参照してください。

- **tcp** — TCP プローブ タイプを指定し、TCP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「TCP プローブの設定」を参照してください。
- **udp** — UDP プローブ タイプを指定し、UDP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「UDP プローブの設定」を参照してください。
- **echo** {**tcp** | **udp**} — ECHO TCP または UDP プローブ タイプを指定し、ECHO TCP または UDP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「Echo プローブの設定」を参照してください。
- **finger** — Finger プローブ タイプを指定し、Finger プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「Finger プローブの設定」を参照してください。
- **http** — HTTP プローブ タイプを指定し、HTTP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「HTTP プローブの設定」を参照してください。
- **https** — SSL に対応する HTTPS プローブ タイプを指定し、HTTPS コンフィギュレーション モードにアクセスします。設定の詳細については、「HTTPS プローブの設定」を参照してください。
- **ftp**— FTP プローブ タイプを指定し、FTP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「FTP プローブの設定」を参照してください。
- **telnet** — Telnet プローブ タイプを指定し、Telnet プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「Telnet プローブの設定」を参照してください。
- **dns** — DNS プローブ タイプを指定し、DNS コンフィギュレーション モードにアクセスします。設定の詳細については、「DNS プローブの設定」を参照してください。
- **smtp** — Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）プローブ タイプを指定し、SMTP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「SMTP プローブの設定」を参照してください。
- **icmp** — Internet Message Access Protocol（IMAP）プローブ タイプを指定し、IMAP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「IMAP プローブの設定」を参照してください。

- **pop** — POP プローブ タイプを指定し、POP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「POP3 プローブの設定」を参照してください。
- **sip** {**tcp** | **udp**} — SIP TCP または UDP プローブ タイプを指定し、SIP TCP または UDP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「SIP プローブの設定」を参照してください。
- **rtsp** — RTSP プローブ タイプを指定し、RTSP プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「RTSP プローブの設定」を参照してください。
- **radius** — RADIUS プローブ タイプを指定し、RADIUS プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「RADIUS プローブの設定」を参照してください。
- **snmp** — SNMP ベースのサーバ ロード プローブ タイプを指定し、SNMP ベースのサーバ ロード プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「SNMP ベースのサーバ ロード プローブの設定」を参照してください。
- **scripted** — スクリプト プローブ タイプを指定し、スクリプト プローブ コンフィギュレーション モードにアクセスします。設定の詳細については、「スクリプト プローブの設定」を参照してください。スクリプトの詳細については、付録 A「ACE での TCL スクリプトの使用」を参照してください。

- *probe_name* — プローブに割り当てる名前です。プローブを実サーバまたはサーバ ファームに関連付けるには、プローブ名を使用します。スペースを含まず引用符なしの英数字を入力します（最大 64 文字）。

たとえば、TCP プローブ PROBE1 を定義し、TCP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe tcp PROBE1
host1/Admin(config-probe-tcp)#
```

TCP プローブ PROBE1 を削除するには、次のように入力します。

```
host1/Admin(config)# no probe tcp PROBE1
```

プローブ アトリビュートおよび対応するコマンドの中には、すべてのプローブ タイプに適用されるものがあります。これらのアトリビュートの設定の詳細については、「一般的なプローブ アトリビュートの設定」を参照してください。

一般的なプローブ アトリビュートの設定

プローブ コンフィギュレーション モードにアクセスして、プローブのアトリビュートを設定する場合、ACE に用意されている一連のコマンドを使用すると、すべてのプローブ タイプ（指定されているものを除く）にアトリビュートを設定できます。次のトピックでは、プローブの一般的なアトリビュートの設定方法について説明します。

プローブの説明の設定

プローブの説明を設定するには、**description** コマンドを使用します。このコマンドは、すべてのプローブ タイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

description *text*

text 引数はプローブの説明です。最大 240 文字の英数字を入力します。

たとえば、説明として THIS PROBE IS FOR TCP SERVERS を設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# description THIS PROBE IS FOR TCP
SERVERS
```

プローブの説明を削除するには、**no description** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no description
```

宛先 IP アドレスの設定

デフォルトでは、プローブは実サーバまたはサーバ ファームに設定された IP アドレスを宛先 IP アドレスに使用します。プローブで使用される宛先アドレスを設定するには、**ip address** コマンドを使用します。このコマンドは、スクリプトを除くすべてのプローブタイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

ip address *ip_address* [**routed**]

引数およびオプションは、次のとおりです。

- *ip_address* — 宛先 IP アドレスです。ドット付き 10 進表記で一意の IPv4 アドレスを入力します（例：192.8.12.15）。
- **routed** —（任意）ACE が ACE 内部ルーティング テーブルに従ってルーティングするように指定します。ハードウェア起動型の SSL プローブでは、このオプションはサポートされません。

（注） HTTPS プローブの場合、非 ルーテッド モード（**routed** キーワードの指定なし）はルーテッド モードと同じ動作を行います。

たとえば、IP アドレス 192.8.12.15 を設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# ip address 192.8.12.15
```

実サーバまたはサーバ ファームに設定された IP アドレスを使用する、プローブのデフォルト動作にリセットするには、**no ip address** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no ip address
```

ポート番号の設定

デフォルトでは、プローブはプローブ タイプに基づいてポート番号を使用します。表 4-1 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。

表 4-1　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
HTTP	80
HTTPS	443
ICMP	適用されない
IMAP	143
POP3	110
RADIUS	1812
RTSP	554
SIP（TCP および UDP の両方）	5060
SNMP	161
SMTP	25
TCP	80
Telnet	23
UDP	53

プローブで使用されるポート番号を設定するには、**port** コマンドを使用します。このコマンドは、ICMP を除くすべてのプローブタイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

port *number*

number 引数はポート番号です。1 ～ 65535 の数値を入力します。

たとえば、HTTP プローブのポート番号に 88 を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# port 88
```

ポート番号をデフォルト値にリセットするには、**no port** コマンドを使用します。たとえば、HTTP プローブのポート番号 88 を削除し、この番号をデフォルト設定の 80 にリセットするには、次のように入力します。

```
host1/Admin(config-probe-http)# no port
```

プローブのポート番号の継承

プローブのポート番号を指定しない場合、ACE は以下によって指定されたポート番号を動的に継承できます。

- サーバ ファームで指定された実サーバ（「複数のヘルス プローブとサーバ ファームとの関連付け」を参照）。
- レイヤ 3 およびレイヤ 4 クラス マップで指定された VIP（「SLB 用レイヤ 3 およびレイヤ 4 SLB クラス マップの設定」を参照）。

このような柔軟性により、設定が容易になります。この場合、必要なのは 1 つのプローブ設定だけであり、その設定によって複数のポートやすべての VIP ポートで実サーバをプローブできます。同一のプローブが実サーバのポートや VIP ポートをすべて継承し、各ポートごとにプローブ インスタンスを作成します。

（注） プローブ ポートの継承は、サーバ ファームのプレディクタ方式（「サーバ ファーム プレディクタ方式の設定」を参照）、スタンドアロンの実サーバに割り当てられたプローブ（「実サーバのヘルス モニタリングの設定」を参照）、または冗長構成のアクティブな FT グループ メンバーに対して設定されたプローブ（『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照）の場合には適用されません。

レイヤ 3 およびレイヤ 4 クラス マップについては、**match** コマンドが 1 つのポートで構成されている場合にのみ、VIP ポートが継承されます。IP プロトコル値またはそのポートのポート範囲に対してワイルドカード値（**任意の**キーワード）を指定した場合、それらの match 文にはポートの継承は適用されません。

以下の設定では、match 文 2、3、4 だけがポートの継承を考慮されます。

```
class-map match-any l3class
  2 match virtual-address 11.0.0.10 tcp eq 201
  3 match virtual-address 11.0.0.10 tcp eq 202
  4 match virtual-address 11.0.0.10 tcp eq 203
  5 match virtual-address 11.0.0.10 204
  6 match virtual-address 1.1.1.1 10
  7 match virtual-address 1.1.1.1 tcp range 12 34
  9 match virtual-address 1.1.1.1 tcp eq 0
```

プローブのポート番号を継承する際の優先順序は次のとおりです。

1. プローブの設定済みポート
2. サーバ ファームの実サーバの設定済みポート
3. VIP の設定済みポート
4. プローブのデフォルト ポート

たとえば、設定されたプローブに指定のポート番号が含まれていない場合、ACE はサーバ ファームで指定された実サーバに関連付けられている設定済みポートを探します。そのポート番号が設定されていない場合、ACE はレイヤ 3 およびレイヤ 4 クラス マップで指定された VIP に関連付けられている設定済みポートを探します。そのポート番号も設定されていない場合、ACE はそのプローブのデフォルト ポートを使用して、バックエンドの実サーバに対するヘルス モニタリングを実行します。

設定の変更に基づき、プローブ インスタンスは ACE によって自動的に作成または削除されます。たとえば、プローブのポートや、サーバ ファーム内の実サーバのポートを指定しなかった場合、ACE は VIP のポート情報を使用してプローブ インスタンスを作成します。その後、プローブにポート番号を割り当てた場合、VIP のポートに対応する以前のプローブ インスタンスはすべて無効になります。ACE は、それらのプローブ インスタンスを自動的に削除して、プローブに割り当てられたポート番号に基づく新しいプローブ インスタンスと、新しいプローブを作成します。VIP が 1 つのポートではなくポートの範囲を保持している場合、ACE はデフォルトのプローブ ポートを使用したバックエンドの実サーバに対するプローブ インスタンスを作成します。

導入シナリオ 1 — 実サーバのポートを継承する

ポートが継承されない以下の例では、2 つの HTTP プローブに対して異なるポート番号（8001 および 8002）が割り当てられます。それがプローブの設定における唯一の相違点です。

```
probe http HTTP_PROBE_1
  port 8001
  request method get url /isalive.html

probe http HTTP_PROBE_2
  port 8002
 request method get url /isalive.html

rserver host RS1
  ip address 192.168.210.1
  inservice

serverfarm host SF1
    rserver RS1 8001
     probe HTTP_PROBE_1
     inservice
  rserver RS1 8002
     probe HTTP_PROBE_2
     inservice
```

ポートが継承される以下の例では、1 つの HTTP プローブが実サーバ RS1 用に指定されたポートを継承し、各ポートごとにプローブ インスタンスを作成します。

```
probe http HTTP_PROBE
   request method get url /isalive.html

rserver host RS1
  ip address 192.168.210.1
  inservice

serverfarm host SF1
  probe HTTP_PROBE
    rserver RS1 8001
      inservice
    rserver RS1 8002
      inservice
```

導入シナリオ 2 — VIP ポートをレイヤ 3 およびレイヤ 4 クラス マップから継承する

ポートが継承されない以下の例では、2 つの HTTP プローブに対して異なるポート番号（8001 および 8002）が割り当てられます。それがプローブの設定における唯一の相違点です。

```
class-map match-any HTTP_VIP
  match virtual-address 10.0.0.1 eq 8001
  match virtual-address 10.0.0.1 eq 8002

probe http HTTP_PROBE_1
  port 8001
  request method get url /isalive.html

probe http HTTP_PROBE_2
  port 8002
 request method get url /isalive.html

rserver host RS1
  ip address 192.168.210.1
  inservice

serverfarm host SF1
 probe HTTP_PROBE_1
 probe HTTP_PROBE_2
    rserver RS1
      inservice
```

ポートが継承される以下の例では、1 つの HTTP プローブが HTTP_VIP クラスマップから VIP ポートを継承し、各ポートごとにプローブ インスタンスを作成します。

```
class-map match-any HTTP_VIP
  match virtual-address 10.0.0.1 eq 8001
  match virtual-address 10.0.0.1 eq 8002

probe http HTTP_PROBE
  request method get url /isalive.html

rserver host RS1
  ip address 192.168.210.1
  inservice

serverfarm host SF1
  probe HTTP_PROBE
  rserver RS1
     inservice
```

プローブ間のインターバルの設定

プローブ間のインターバルは、ACE から passed とマークされたサーバにプローブが送信される頻度を示します。プローブ間のインターバルを変更するには、**interval** コマンドを使用します。このコマンドは、すべてのプローブ タイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

interval *seconds*

seconds 引数は秒単位で表したインターバルです。2 ～ 65535 の数値を入力します。デフォルトでは、インターバルは 15 です。

TCP または UDP ベースのプローブのオープン タイムアウト値および受信タイムアウト値はプローブの実行時間に影響を与えます。プローブ インターバルがこれらのタイムアウト値以下であり、サーバが応答するのに長い時間かかったり、タイムアウト値以内に応答できなかった場合、プローブはスキップされます。プローブがスキップされると、**show probe detail** コマンドにより、No. Probes skipped カウンタが増加します。

UDP プローブまたは UDP ベースのプローブの場合、インターバル値を 30 秒にすることを推奨します。この推奨の理由は、ACE のデータ プレーンにおける管理接続の上限が 100,000 であるためです。管理接続は、Telnet、SSH、SNMP などの管理アプリケーションと同様に、すべてのプローブによって使用されます。さらに、ACE における UDP 接続のデフォルト タイムアウトは 15 秒です。これは、UDP プローブが 2 分間中断しても、ACE は UDP 接続を削除しないことを意味します。30 秒未満にインターバルを設定すると、管理接続限界を超えることなく実行するよう設定できる UDP プローブの数を制限し、プローブはスキップされます。

たとえば、インターバルを 50 秒に設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# interval 50
```

インターバルをデフォルト設定の 15 にリセットするには、**no interval** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no interval
```

失敗したプローブのリトライ回数の設定

プローブの連続失敗回数が特定の値に達すると、ACE はサーバに failed とマークします。デフォルトでは、3 回のプローブに連続して失敗すると、ACE はサーバに failed とマークします。このプローブ失敗回数を設定するには、**faildetect** コマンドを使用します。このコマンドは、すべてのプローブ タイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

faildetect *retry_count*

retry_count 引数は、サーバが failed とマークされるまでに、プローブが連続して失敗する回数です。1 ～ 65535 の数値を入力します。デフォルトは 3 です。

たとえば、サーバが failed と宣言されるまでのプローブの失敗回数を 5 に設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# faildetect 5
```

プローブの失敗回数をデフォルト設定の 3 にリセットするには、**no faildetect** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no faildetect
```

プローブに成功するための待機期間およびしきい値の設定

サーバに failed とマークした ACE は、一定期間待機してから、failed 状態のサーバにプローブを送信します。ACE が成功プローブを特定の回数だけ連続して受信すると、サーバは passed とマークされます。デフォルトでは、ACE は 60 秒間待機したあとに、failed 状態のサーバにプローブを送信します。成功の応答を 3 回連続して受信すると、サーバは passed とマークされます。

ACE が failed 状態のサーバにプローブを送信するまでのインターバル、およびサーバに passed とマークするために必要な連続成功プローブ数を設定するには、**passdetect** コマンドを使用します。このコマンドは、すべてのプローブ タイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

passdetect {**interval** *seconds* | **count** *number*}

キーワードおよび引数は、次のとおりです。

- **interval** *seconds* — 待機インターバルを秒単位で指定します。2 ～ 65535 の数値を入力します。デフォルト値は 60 です。
- **count** *number* — サーバからの成功プローブ応答数を指定します。1 ～ 65535 の数値を入力します。デフォルトは 3 です。

（注） 受信タイムアウト値はプローブの実行時間に影響を与えます。プローブ　インターバルがこのタイムアウト値以下であり、サーバが応答するのに長時間かかったり、タイムアウト値以内に応答できなかった場合、プローブはスキップされます。プローブがスキップされると、**show probe detail** コマンドにより、No. Probes skipped カウンタが増加します。

たとえば、待機インターバルを 10 秒に設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# passdetect interval 10
```

たとえば、サーバが passed と宣言されるまでのサーバからの成功プローブ応答数を 5 に設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# passdetect count 5
```

待機インターバルをデフォルト設定にリセットするには、**no passdetect interval** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no passdetect interval
```

成功プローブ応答数をデフォルト設定にリセットするには、**no passdetect count** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no passdetect count
```

接続をオープニングするための待機インターバルの設定

プローブを送信した ACE は、SYN を送信して接続をオープンしたあとに、SYN-ACK を待機します。SYN-ACK を受信したら、ACK を送信して、サーバとの接続を確立します。接続を確立するためのインターバルを設定するには、**open** コマンドを使用します。このコマンドは Echo TCP、Finger、FTP、HTTP、HTTPS、IMAP、POP、スクリプト、SIP 、SMTP、TCP、および Telnet プローブ コンフィギュレーション モードで使用できます（すべて TCP ベース プローブ）。このコマンドの構文は次のとおりです。

open *timeout*

timeout 引数は、サーバとの接続をオープンするために待機する秒数です。1 ～ 65535 の整数を入力します。デフォルトの待機インターバルは 1 秒です。

（注）　TCP ベースのプローブのオープン タイムアウト値および受信タイムアウト値はプローブの実行時間に影響を与えます。プローブ インターバルがこれらのタイムアウト値以下であり、サーバが応答するのに長い時間かかったり、タイムアウト値以内に応答できなかった場合、プローブはスキップされます。プローブがスキップされると、**show probe detail** コマンドにより、No. Probes skipped カウンタが増加します。

たとえば、待機インターバルを 25 秒に設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# open 25
```

待機インターバルをデフォルト設定の 1 秒にリセットするには、**no open** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-type)# no open
```

プローブ応答のタイムアウト期間の設定

デフォルトでは、プローブを送信した ACE は、10 秒以内に応答があると予測します。たとえば、HTTP プローブの場合、タイムアウト期間は、GET または HEAD 要求に対する HTTP 応答の受信期間（秒数）です。サーバがプローブに応答しなかった場合、ACE はそのサーバに failed とマークします。

プローブに対するサーバ応答の受信期間を設定するには、**receive** コマンドを使用します。このコマンドは、すべてのプローブ タイプのコンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

receive *timeout*

timeout 引数は、秒単位で表したタイムアウト期間です。1 ～ 65535 の数値を入力します。デフォルトは 10 です。

（注）　TCP ベースのプローブのオープン タイムアウト値および受信タイムアウト値はプローブの実行時間に影響を与えます。プローブ インターバルがこれらのタイムアウト値以下であり、サーバが応答するのに長い時間かかったり、タイムアウト値以内に応答できなかった場合、プローブはスキップされます。プローブがスキップされると、**show probe detail** コマンドにより、No. Probes skipped カウンタが増加します。

たとえば、応答のタイムアウト期間を 5 秒に設定するには、次のように入力します。

```
host1/Admin(config-probe-type)# receive 5
```

サーバからの応答の受信期間をデフォルト設定の 10 秒にリセットするには、**no receive** コマンドを使用します。

次のように入力します。

```
host1/Admin(config-probe-type)# no receive
```

ICMP プローブの設定

ICMP プローブは ICMP エコー要求を送信し、応答を待機します。サーバが応答を返すと、ACE はサーバに passed とマークします。サーバが応答を送信しないためにプローブがタイムアウトした場合、またはサーバが予期せぬ ICMP エコー応答タイプを送信した場合、ACE はプローブを failed とマークします。

ICMP プローブを作成し、ICMP プローブ コンフィギュレーション モードにアクセスするには、コンフィギュレーション モードで **probe icmp** *name* コマンドを使用します。

たとえば、ICMP プローブ PROBE3 を定義して、ICMP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe icmp PROBE3
host1/Admin(config-probe-icmp)#
```

ICMP プローブを作成したあとに、「一般的なプローブ アトリビュートの設定」に記載されたアトリビュートを設定できます。

TCP プローブの設定

TCP プローブは TCP の 3 方向ハンドシェイクを開始して、サーバから応答が送信されるまで待機します。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。

また、RST または特定のデータを送信するようにプローブを設定したり、特定の応答を待機して、その応答を受信したらサーバに passed とマークするようにプローブを設定したりできます。特定のデータを送信して、サーバから特定の応答を受信するように、プローブを設定することもできます。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。

TCP プローブを作成し、TCP プローブ コンフィギュレーション モードにアクセスするには、コンフィギュレーション モードで **probe tcp** *name* コマンドを使用します。

たとえば、TCP プローブ PROBE1 を定義して、TCP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe tcp PROBE1
host1/Admin(config-probe-tcp)#
```

TCP プローブのアトリビュートを設定できます（次のトピックを参照）。

- TCP 接続の終了の設定
- サーバからの予測応答ストリングの設定
- 接続時にプローブからサーバに送信されるデータの設定

「一般的なプローブ アトリビュートの設定」に記載されたアトリビュートを設定することもできます。

TCP 接続の終了の設定

TCP プローブは接続を確立します。3 方向ハンドシェイク（SYN、SYN-ACK、および ACK）を通して接続が正常に確立されると、サーバは passed とマークされます。デフォルトでは、ACE はサーバに FIN を送信して、TCP 接続を通常どおりに終了します。

（注）　プローブにデフォルトの通常の接続終了（FIN）が設定されている場合に、ターゲット サーバが予測されるデータを送信しなければ、プローブはリセット（RST）を使用してサーバとの TCP 接続を終了します。返されたデータが予測されるデータでないかぎり、プローブは引き続き RST を送信してサーバ接続を終了します。サーバが再び正しいデータで応答した場合、プローブは FIN を使用して接続を終了するようになります。

RST を送信して TCP 接続を終了するように ACE を設定するには、**connection term** コマンドを使用します。このコマンドは、TCP ベースのコネクション型プローブ（ECHO TCP、Finger、FTP、HTTP、HTTPS、IMAP、POP、RTSP、SIP TCP、SMTP、TCP、および Telnet プローブ コンフィギュレーション モード）で使用できます。このコマンドの構文は次のとおりです。

connection term forced

たとえば、次のように入力します。

```
host1/Admin(config-probe-tcp)# connection term forced
```

終了方式をリセットして、接続を通常どおりに終了するよう設定するには、**no connection term** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-tcp)# no connection term forced
```

サーバからの予測応答ストリングの設定

サーバから送信される正規表現（regex）応答ストリングを待機するように設定されたプローブは、ストリングの応答を検索します。ACE が検出した場合、サーバは passed とマークされます。予測ストリングが設定されていない場合、ACE はサーバ応答を無視します。

（注）　HTTP または HTTPS プローブの場合、**expect regex** コマンドが機能するためには、サーバ応答に Content-Length ヘッダーが含まれている必要があります。含まれていないと、プローブは regex を解析しません。

ACE がプローブ宛先サーバからの応答ストリングとして予測するストリングを設定するには、**expect regex** コマンドを使用します。このコマンドは、Finger、HTTP、HTTPS、SIP、TCP、および UDP プローブ コンフィギュレーション モードで使用できます。

このコマンドの構文は次のとおりです。

expect regex *string* [**offset** *number*]

引数およびオプションは、次のとおりです。

- *string* — プローブ宛先から送信されると予測される正規表現の応答ストリングです。スペースを含まないテキスト ストリングを、引用符で囲まずに入力します。ストリングにスペースが含まれている場合は、引用符で囲みます。最大 255 文字の英数字を入力できます。
- **offset** *number* —（任意）ACE が定義された式の検出を開始する場所を、受信メッセージまたはバッファ内の文字数で設定します。1 ～ 4000 の数値を入力します。

たとえば、応答ストリング ack を待機するように ACE を設定するには、次のように入力します。

```
host1/Admin(config-probe-tcp)# expect regex ack
```

予測される応答ストリングを削除するには、**no expect regex** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-http)# no expect regex
```

接続時にプローブからサーバに送信されるデータの設定

ACE がサーバに接続した場合にプローブから送信される ASCII データを設定するには、**send-data** コマンドを使用します。このコマンドは Echo、Finger、TCP、および UDP プローブ コンフィギュレーション モードで使用できます。このコマンドの構文は次のとおりです。

send-data *expression*

expression 引数は、プローブから送信されるデータです。最大 255 文字のスペースを含む英数字を、引用符で囲まずに入力します。

（注） UDP プローブに **send-data** コマンドが設定されていない場合、このプローブは 1 バイト（0x00）を送信します。

たとえば、データとして TEST を送信するようにプローブを設定するには、次のように入力します。

```
host1/Admin(config-probe-tcp)# send-data test
```

データを削除するには、**no send-data** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-tcp)# no send-data
```

UDP プローブの設定

（注） UDP プローブを設定する場合は、管理ベース ポリシーを設定する必要があります。ポリシーの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

デフォルトでは、UDP プローブはサーバに UDP パケットを送信します。サーバから ICMP Host Unreachable または ICMP Port Unreachable メッセージが返された場合のみ、サーバは failed とマークされます。ACE が、送信された UDP 要求に対応する ICMP エラーを受信しなかった場合、サーバは passed とマークされます。また、特定のデータを送信するようにこのプローブを設定したり、特定の応答を待機して、その応答を受信したらサーバに passed とマークするようにプローブを設定したりできます。

実サーバが ACE に直接接続されておらず（たとえば、ゲートウェイ経由で接続）、サーバの IP インターフェイスがダウンしているか、切断されている場合、UDP プローブは UDP アプリケーションに到達できないことを自動的に認識しません。実サーバが ACE に直接接続されていて、サーバの IP インターフェイスがダウンしている場合、UDP プローブは失敗します。

UDP プローブを作成し、UDP プローブ コンフィギュレーション モードにアクセスするには、**probe udp** *name* コマンドを使用します。

たとえば、UDP プローブ PROBE2 を定義して、UDP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe udp PROBE2
host1/Admin(config-probe-udp)#
```

UDP プローブには次のアトリビュートを設定できます。

- ACE がプローブ宛先サーバからの応答として予測するストリングを設定するには、**expect regex** コマンドを使用します。このコマンドの詳細については、「サーバからの予測応答ストリングの設定」を参照してください。
- 接続時に送信されるデータを UDP プローブに設定するには、**send-data** *expression* コマンドを使用します。このコマンドの詳細については、「接続時にプローブからサーバに送信されるデータの設定」を参照してください。

「一般的なプローブ アトリビュートの設定」に記載されたアトリビュートを設定することもできます。

Echo プローブの設定

Echo プローブはサーバに指定のストリングを送信し、応答と元のストリングを比較します。エコーするストリングを設定する必要があります。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。ストリングを設定しない場合、プローブは TCP または UDP プローブと同様に動作します（「TCP プローブの設定」または「UDP プローブの設定」を参照）。

Echo プローブを作成し、Echo プローブ コンフィギュレーション モードにアクセスするには、**probe echo** コマンドを使用します。このコマンドの構文は次のとおりです。

probe echo {**tcp** | **udp**} *name*

キーワードおよび引数は、次のとおりです。

- *name* — プローブの ID です。最大 64 文字の英数字を、引用符で囲まずに入力します。
- **tcp** — TCP 接続に対応するようにプローブを設定します。
- **udp** — UDP 接続に対応するようにプローブを設定します。

たとえば、TCP Echo プローブ PROBE を定義して、TCP Echo プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe echo tcp PROBE
host1/Admin(config-probe-echo-tcp)#
```

たとえば、UDP Echo プローブ PROBE17 を定義して、UDP Echo プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe echo udp PROBE17
host1/Admin(config-probe-echo-udp)#
```

Echo TCP および Echo UDP プローブの場合は、「一般的なプローブ アトリビュートの設定」に記載されたアトリビュートを設定できます。

Echo TCP プローブ（**tcp** キーワードを使用して設定）の場合は、「TCP プローブの設定」に記載されたアトリビュートも設定できます。

Echo UDP プローブ（**udp** キーワードを使用して設定）の場合は、「UDP プローブの設定」に記載されたアトリビュートも設定できます。

Finger プローブの設定

Finger プローブは、予測される応答ストリングを求める Finger クエリーをサーバに実行します。ACE は応答内で、設定されたストリングを検索します。ACE が予測される応答ストリングを検出すると、サーバは passed とマークされます。予測される応答ストリングが設定されていない場合、ACE はサーバ応答を無視します。

Finger プローブを作成し、Finger プローブ コンフィギュレーション モードにアクセスするには、**probe finger** コマンドを使用します。このコマンドの構文は次のとおりです。

probe finger *name*

name 引数はプローブの ID です。スペースを含まず引用符なしの英数字を入力します（最大 64 文字）。

たとえば、Finger プローブ PROBE8 を定義して、Finger プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe finger PROBE8
host1/Admin(config-probe-finger)#
```

Finger プローブのアトリビュートを設定する方法については、「一般的なプローブ アトリビュートの設定」および「TCP プローブの設定」を参照してください。

HTTP プローブの設定

HTTP プローブは TCP 接続を確立し、予測ストリングおよびステータス コードを求める HTTP 要求をサーバに発行します。ACE は受信した応答と設定済みコードを比較し、受信した HTTP ページに設定済みコードが含まれているか検索したり、HTTP ページのハッシュを検証したりできます。これらのチェック処理のいずれかに失敗した場合、サーバは failed とマークされます。

たとえば、予測ストリングおよびステータス コードが設定されている場合に、ACE がサーバ応答内に両方を検出すると、サーバは passed とマークされます。ただし、ACE がサーバ応答ストリングと予測されるステータス コードのいずれかを受信しない場合、サーバは failed とマークされます。

（注）　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。

expect regex または **hash** コマンドが機能するためには、サーバ応答に Content-Length ヘッダーが含まれている必要があります。含まれていないと、プローブは regex またはハッシュ値を解析しません。

HTTP プローブを作成し、HTTP プローブ コンフィギュレーション モードにアクセスするには、**probe http** *name* コマンドを使用します。たとえば、HTTP プローブ PROBE4 を定義して、HTTP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe http PROBE4
host1/Admin(config-probe-http)#
```

HTTP プローブのアトリビュートを設定する方法については、次のトピックを参照してください。

- プローブの認定証の設定
- HTTP プローブのヘッダー フィールドの設定
- プローブの HTTP 方式の設定
- 宛先サーバから送信されるステータス コードの設定
- MD5 ハッシュ値の設定

HTTP プローブを作成したあとに、「一般的なプローブ アトリビュートの設定」に記載された一般的なプローブ アトリビュートを設定できます。予測される応答ストリングを含めて、「TCP プローブの設定」に記載された TCP プローブ アトリビュートを設定することもできます。

プローブの認定証の設定

プローブの認定証は、サーバで認証に使用されるユーザ名およびパスワードです。プローブの認定証を設定するには、**credentials** コマンドを使用します。このコマンドの構文は次のとおりです。

credentials *username* [*password*]

引数は次のとおりです。

- *username* — 認証に使用されるユーザ ID です。最大 64 文字の英数字を、引用符で囲まずに入力します。
- *password* —（任意）認証に使用されるパスワードです。最大 64 文字の英数字を、引用符で囲まずに入力します。

たとえば、ユーザ名 ENG1 およびパスワード TEST を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# credentials ENG1 TEST
```

プローブの認定証を削除するには、**no credentials** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-http)# no credentials
```

HTTP プローブのヘッダー フィールドの設定

HTTP プローブに 1 つまたは複数の HTTP ヘッダー フィールドを設定するには、**header** コマンドを使用します。このコマンドの構文は次のとおりです。

header *field_name* **header-value** *value*

キーワードおよび引数は、次のとおりです。

- *field_name* — 標準ヘッダー フィールドの ID です。テキスト ストリングを、スペースを含まない最大 64 文字の英数字で入力します。ヘッダー フィールドにスペースが含まれている場合は、ストリングを引用符で囲みます。次のいずれかのヘッダー キーワードを入力することもできます。
  - **Accept** — Accept 要求ヘッダー
  - **Accept-Charset** — Accept-Charset 要求ヘッダー
  - **Accept-Encoding** — Accept-Encoding 要求ヘッダー

- **Accept-Language** — Accept-Language 要求ヘッダー
- **Authorization** — Authorization 要求ヘッダー
- **Cache-Control** — Cache-Control 汎用ヘッダー
- **Connection** — Connection 汎用ヘッダー
- **Content-MD5** — Content-MD5 エンティティ ヘッダー
- **Accept** — Accept 要求ヘッダー
- **From** — From 要求ヘッダー
- **Host** — Host 要求ヘッダー
- **If-Match** — If-Match 要求ヘッダー
- **Pragma** — Pragma 汎用ヘッダー
- **Referer** — Referer 要求ヘッダー
- **Transfer-Encoding** — Transfer-Encoding 汎用ヘッダー
- **User-Agent** — User-Agent 要求ヘッダー
- **Via** — Via 汎用ヘッダー

• **header-value** *field_value* — ヘッダー フィールドに割り当てられる値を指定します。最大 255 文字の英数字を入力します。値を示すストリングにスペースが含まれている場合は、ストリングを引用符で囲みます。

たとえば、Accept-Encoding HTTP ヘッダーのフィールド値を IDENTITY に設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# header Accept-Encoding header-value
IDENTITY
```

プローブのヘッダー設定を削除するには、**header** コマンドの **no** 形式を使用します。たとえば、ヘッダーの Accept-Encoding フィールド名を削除するには、次のように入力します。

```
host1/Admin(config-probe-http)# no header Accept-Encoding
```

プローブの HTTP 方式の設定

デフォルトでは、HTTP 要求方式は GET、URL は「/」です。URL を設定しない場合、プローブは TCP プローブとして機能します。

プローブで使用される HTTP 方式および URL を設定するには、**request method** コマンドを使用します。このコマンドの構文は次のとおりです。

request method {**get** | **head**} **url** *path*

キーワードおよび引数は、次のとおりです。

- **get** | **head** — HTTP 要求方式を設定します。キーワードは次のとおりです。
  - **get** — HTTP GET 要求方式。ページを取得するようにサーバに指示します。これがデフォルトの方式です。
  - **head** — HTTP HEAD 要求方式。ページのヘッダーのみを取得するようにサーバに指示します。
- **url** *path* — URL パスを指定します。*path* 引数は最大 255 文字の英数字です。デフォルト パスは「/」です。

たとえば、HTTP プローブで使用される HEAD HTTP 方式および /digital/media/graphics.html URL を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# request method head url
/digital/media/graphics.html
```

プローブの HTTP 要求を GET にリセットするには、**no request method** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-http)# no request method head url
/digital/media/graphics.html
```

宛先サーバから送信されるステータス コードの設定

サーバから応答を受信した ACE 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 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。

ACE がプローブ宛先から送信されると予測する単一のステータス コード、または単一のコード応答範囲を設定するには、**expect status** コマンドを使用します。このコマンドで複数のステータス コード範囲を指定するには、各範囲を個別に指定したコマンドを入力します。このコマンドの構文は次のとおりです。

expect status *min_number max_number*

引数およびオプションは次のとおりです。

- *min_number* — 単一のステータス コードまたはステータス コード範囲の下限を示します。0 ～ 999 の整数を入力します。
- *max_number* — 単一のステータス コード範囲の上限です。0 ～ 999 の整数を入力します。単一コードを設定する場合は、*min_number* 値を再入力します。

たとえば、予測ステータス コードに、HTTP 要求に成功したことを示す値 200 を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# expect status 200 200
```

予測されるステータス コード範囲に 200 ～ 210 を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# expect status 200 210
```

予測されるステータス コード範囲を複数（200 ～ 202 および 204 ～ 205）を設定する場合は、各範囲を個別に設定する必要があります。次のように入力します。

```
host1/Admin(config-probe-http)# expect status 200 202
host1/Admin(config-probe-http)# expect status 204 205
```

単一の予測ステータス コードを削除するには、**no expect status** コマンドを使用します。たとえば、予測ステータス コード 200 を削除するには、次のように入力します。

```
host1/Admin(config-probe-http)# no expect status 200 200
```

予測される特定のステータス コード範囲を削除するには、**no expect status** コマンドを使用するときに、この範囲を入力します。たとえば、範囲 200 ～ 210 から範囲 200 ～ 202 を削除するには、次のように入力します。

```
host1/Admin(config-probe-http)# no expect status 200 202
```

予測されるステータス コード範囲を複数削除するには、各範囲を個別に削除する必要があります。たとえば、2 つの異なる範囲（200 ～ 202 および 204 ～ 205）が設定されている場合は、次のように入力します。

```
host1/Admin(config-probe-http)# no expect status 200 202
host1/Admin(config-probe-http)# no expect status 204 205
```

MD5 ハッシュ値の設定

デフォルトでは、ACE に MD5 ハッシュ値は設定されていません。ハッシュ値を動的に生成するように、またはハッシュ値を手動で設定するように、ACE を設定するには、**hash** コマンドを使用します。このコマンドを使用してハッシュ値が設定されていない場合、ACE はプローブから返される HTTP データに関するハッシュ値を計算しません。このコマンドの構文は次のとおりです。

hash [*value*]

引数を指定しないでこのコマンドを入力した場合、ACE は最初の成功プローブによって返された HTTP データに関するハッシュを生成します。後続の HTTP サーバ ハッシュ応答が、生成されたハッシュ値と一致した場合、ACE はサーバを passed とマークします。

HTTP データが変更されたためにハッシュ値が一致しなかった場合、プローブは失敗します。**show probe ... detail** コマンドを実行すると、[Last disconnect err] フィールドに MD5 不一致エラーが表示されます。参照ハッシュをクリアし、次の成功プローブのハッシュ値を ACE に再計算させるには、**request method** コマンドを使用して、URL または方式を変更します。詳細については、「プローブの HTTP 方式の設定」を参照してください。

オプションの *value* 引数は、手動で設定する MD5 ハッシュ値です。MD5 値は、正確に 32 文字（16 バイト）の 16 進数ストリングとして入力します。

（注）　**hash** コマンドが機能するためには、サーバ応答に Content-Length ヘッダーが含まれている必要があります。このヘッダーが含まれていない場合、プローブはハッシュ値を解析しようとしません。

HEAD 方式を使用してプローブに **hash** を設定できますが、ハッシュするデータは存在せず、プローブが常に成功するとはかぎりません。

たとえば、最初の成功プローブによって返された HTTP データに関するハッシュを生成するように ACE を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# hash
```

ハッシュ値を手動で設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# hash 0123456789abcdef0123456789abcdef
```

参照されたハッシュ値と計算されたハッシュ値を比較しないように ACE を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# no hash
```

手動で設定されたハッシュ値を使用しないように ACE を設定するには、次のように入力します。

```
host1/Admin(config-probe-http)# no hash
0123456789abcdef0123456789abcdef
```

HTTPS プローブの設定

HTTPS プローブは、SSL を使用して暗号化データを生成する点を除いて、HTTP プローブと類似しています。HTTPS プローブはハードウェア支援です。これにより、ACE はコントロール プレーンではなくデータ プレーンからプローブを送信できます。この機能により、ACE はルーティング テーブル（実サーバの IP アドレスをバイパスする）を使用して、**ip address** コマンドで **routed** オプションを指定しているかどうかに関係なく、HTTPS プローブを宛先に転送します。**ip address** コマンドの詳細については、「宛先 IP アドレスの設定」を参照してください。また、ACL を不適切に適用すると、ACL は HTTPS プローブに影響を与えることがあります。ACL の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

（注）　**expect regex** または **hash** コマンドが機能するためには、サーバ応答に Content-Length ヘッダーが含まれている必要があります。含まれていないと、プローブは regex またはハッシュ値を解析しません。

HTTPS プローブを作成し、HTTPS プローブ コンフィギュレーション モードにアクセスするには、**probe https** コマンドを使用します。このコマンドの構文は次のとおりです。

probe https *name*

name 引数には、HTTPS プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、HTTPS プローブ PROBE5 を定義して、HTTPS プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe https PROBE5
host1/Admin(config-probe-https)#
```

HTTPS プローブのアトリビュートを設定する方法については、次の項を参照してください。

- HTTPS プローブの暗号スイートの設定
- サポートされている SSL または TLS バージョンの設定

HTTPS プローブを作成したあとに、「一般的なプローブ アトリビュートの設定」に記載された一般的なプローブ アトリビュートを設定できます。「HTTP プローブの設定」に記載された HTTP プローブ アトリビュートを設定することもできます。

HTTPS プローブの暗号スイートの設定

デフォルトでは、HTTPS プローブは RSA で設定された暗号スイートをすべて受け入れます。バックエンド サーバから送信された特定タイプの RSA 暗号スイートを待機するようにプローブを設定するには、**ssl cipher** コマンドを使用します。このコマンドの構文は次のとおりです。

ssl cipher RSA_ANY | *cipher_suite*

キーワードおよび引数は、次のとおりです。

- **RSA_ANY** — ACE で許可されているすべての RSA 暗号スイートがサーバで許可されるように指定します。これは、デフォルト設定です。
- *cipher_suite* — プローブがバックエンド サーバから送信されると予測する RSA 暗号スイートです。次のキーワードのいずれか 1 つを入力します。

- **RSA_EXPORT1024_WITH_DES_CBC_SHA**
- **RSA_EXPORT1024_WITH_RC4_56_MD5**
- **RSA_EXPORT1024_WITH_RC4_56_SHA**
- **RSA_EXPORT_WITH_DES40_CBC_SHA**
- **RSA_EXPORT_WITH_RC4_40_MD5**
- **RSA_WITH_3DES_EDE_CBC_SHA**
- **RSA_WITH_AES_128_CBC_SHA**
- **RSA_WITH_AES_256_CBC_SHA**
- **RSA_WITH_DES_CBC_SHA**
- **RSA_WITH_RC4_128_MD5**
- **RSA_WITH_RC4_128_SHA**

たとえば、HTTPS プローブに RSA_WITH_RC4_128_SHA 暗号スイートを設定するには、次のように入力します。

```
host1/Admin(config-probe-https)# ssl cipher RSA_WITH_RC4_128_SHA
```

HTTPS プローブの動作をリセットして、任意の RSA 暗号スイートを受け入れるように設定するには、次のように入力します。

```
host1/Admin(config-probe-https)# no ssl cipher
```

サポートされている SSL または TLS バージョンの設定

サーバに送信される ClientHello メッセージのバージョンは、サポートされている最新バージョンを示します。デフォルトでは、プローブは **all**（すべて）を SSL バージョンとしてサポートします。プローブがサポートする SSL のバージョンを設定するには、プローブ HTTPS コンフィギュレーション モードで **ssl version** コマンドを使用します。このコマンドの構文は次のとおりです。

ssl version all | **SSLv3** | **TLSv1**

キーワードは次のとおりです。

- **all** — （デフォルト）すべての SSL バージョンを指定します。
- **SSLv3** — SSL バージョン 3 を指定します。
- **TLSv1** — TLS バージョン 1 を指定します。

たとえば、すべての SSL バージョンを設定するには、次のように入力します。

```
host1/Admin(config-probe-https)# ssl version all
```

デフォルト設定にリセットするには、次のように入力します。

```
host1/Admin(config-probe-https)# no ssl version
```

FTP プローブの設定

FTP プローブはサーバとの TCP 接続を確立します。ACE がサーバから service ready メッセージを受信すると、ACE は次のアクションを実行します。

- プローブが通常の終了に対応するよう設定されている場合、**quit** コマンドを発行します。
- 強制終了のため、接続をリセットします。

FTP プローブを作成し、FTP プローブ コンフィギュレーション モードにアクセスするには、**probe ftp** コマンドを使用します。このコマンドの構文は次のとおりです。

probe ftp *name*

name 引数には、FTP プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、FTP プローブ PROBE8 を定義して、FTP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe ftp PROBE8
host1/Admin(config-probe-ftp)#
```

「宛先サーバから送信されるステータス コードの設定」には、プローブのステータス コードの設定方法が記載されています。

「一般的なプローブ アトリビュートの設定」および「TCP プローブの設定」に記載されたアトリビュートを設定することもできます。

宛先サーバから送信されるステータス コードの設定

サーバから応答を受信した ACE 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 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。

ACE がプローブ宛先から送信されると予測する単一のステータス コード、または単一のコード応答範囲を設定するには、**expect status** コマンドを使用します。このコマンドで複数のステータス コード範囲を指定するには、各範囲を個別に指定したコマンドを入力します。このコマンドの構文は次のとおりです。

expect status *min_number max_number*

引数は次のとおりです。

- *min_number* — 単一のステータス コードまたはステータス コード範囲の下限を示します。0 ～ 999 の整数を入力します。
- *max_number* — 単一のステータス コード範囲の上限です。0 ～ 999 の整数を入力します。単一コードを設定する場合は、*min_number* 値を再入力します。

たとえば、予測ステータス コードに、要求に成功したことを示す値 200 を設定するには、次のように入力します。

```
host1/Admin(config-probe-ftp)# expect status 200 200
```

予測されるステータス コード範囲に 200 ～ 201 を設定するには、次のように入力します。

```
host1/Admin(config-probe-ftp)# expect status 200 201
```

予測されるステータス コード範囲を複数（200 ～ 201 および 230 ～ 250）を設定する場合は、各範囲を個別に設定する必要があります。次のように入力します。

```
host1/Admin(config-probe-ftp)# expect status 200 201
host1/Admin(config-probe-ftp)# expect status 230 250
```

単一の予測ステータス コードを削除するには、**no expect status** コマンドを使用します。たとえば、予測ステータス コード 200 を削除するには、次のように入力します。

```
host1/Admin(config-probe-ftp)# no expect status 200 200
```

予測される特定のステータス コード範囲を削除するには、**no expect status** コマンドを使用するときに、この範囲を入力します。たとえば、範囲 200 ～ 201 を削除するには、次のように入力します。

```
host1/Admin(config-probe-ftp)# no expect status 200 201
```

予測されるステータス コード範囲を複数削除するには、各範囲を個別に削除する必要があります。たとえば、2 つの異なる範囲（200 ～ 201 および 230 ～ 250）が設定されている場合は、次のように入力します。

```
host1/Admin(config-probe-ftp)# no expect status 200 201
host1/Admin(config-probe-ftp)# no expect status 230 250
```

Telnet プローブの設定

Telnet プローブは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。Telnet プローブを作成し、Telnet プローブ コンフィギュレーション モードにアクセスするには、**probe telnet** コマンドを使用します。このコマンドの構文は次のとおりです。

probe telnet *name*

name 引数には、Telnet プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、Telnet プローブ PROBE6 を定義して、Telnet プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe telnet PROBE6
host1/Admin(config-probe-telnet)#
```

「一般的なプローブ アトリビュートの設定」および「TCP プローブの設定」に記載されたアトリビュートを設定することもできます。

DNS プローブの設定

DNS プローブは DNS サーバに要求を送信し、設定されたドメインを指定します（デフォルトのドメインは www.cisco.com）。サーバが起動しているかどうかを判別するために、ACE はこのドメインに設定された IP アドレスを 1 つ受信する必要があります。DNS プローブを作成し、DNS プローブ コンフィギュレーション モードにアクセスするには、**probe dns** コマンドを使用します。このコマンドの構文は次のとおりです。

probe dns *name*

name 引数には、DNS プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、DNS プローブ PROBE7 を定義して、DNS プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe dns PROBE7
host1/Admin(config-probe-dns)#
```

DNS プローブのアトリビュートを設定する方法については、次のトピックを参照してください。

- ドメイン名の設定
- 予測 IP アドレスの設定

「一般的なプローブ アトリビュートの設定」に記載されたアトリビュートを設定することもできます。

ドメイン名の設定

DNS プローブは DNS サーバのドメイン名を送信して、解決します。デフォルトでは、プローブは www.cisco.com ドメインを使用します。プローブがサーバに送信するドメイン名を設定するには、**domain** コマンドを使用します。このコマンドの構文は次のとおりです。

domain *name*

name 引数は、プローブから DNS サーバに送信されるドメインです。最大 255 文字の英数字を、引用符で囲まずに入力します。

たとえば、support.cisco.com というドメイン名を設定するには、次のように入力します。

```
host1/Admin(config-probe-dns)# domain support.cisco.com
```

ドメインを www.cisco.com にリセットするには、**no domain** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-dns)# no domain
```

予測 IP 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 が DNS 要求に対するサーバ応答として予測する IP アドレスを設定するには、**expect address** コマンドを使用します。このコマンドの構文は次のとおりです。

expect address *ip_address*

ip_address 引数は、返されると予測される IP アドレスです。ドット付き 10 進表記で一意の IPv4 アドレスを入力します（例：192.8.12.15）。

このコマンドで複数の IP アドレスを指定するには、各アドレスを個別に指定したコマンドを入力します。たとえば、予測 IP アドレス 192.8.12.15 および 192.8.12.23 を設定するには、次のように入力します。

```
host1/Admin(config-probe-dns)# expect address 192.8.12.15
host1/Admin(config-probe-dns)# expect address 192.8.12.23
```

IP アドレスを削除するには、**no expect address** コマンドを入力します。次のように入力します。

```
host1/Admin(config-probe-dns)# no expect address 192.8.12.15
```

SMTP プローブの設定

SMTP プローブはサーバにログインして SMTP セッションを開始し、HELLO メッセージを送信してから、サーバとの接続を切断します。SMTP プローブを作成し、SMTP プローブ コンフィギュレーション モードにアクセスするには、**probe smtp** コマンドを使用します。このコマンドの構文は次のとおりです。

probe smtp *name*

name 引数には、SMTP プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、SMTP プローブ PROBE10 を定義して、SMTP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe smtp PROBE10
host1/Admin(config-probe-smtp)#
```

SMTP プローブを作成したあとに、「宛先サーバから送信されるステータス コードの設定」に記載されたステータス コードを設定できます。

「一般的なプローブ アトリビュートの設定」に記載されたアトリビュートや、「TCP 接続の終了の設定」に記載された接続終了も設定できます。

宛先サーバから送信されるステータス コードの設定

サーバから応答を受信した ACE 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 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。

ACE がプローブ宛先から送信されると予測する単一のステータス コード、または単一のコード応答範囲を設定するには、**expect status** コマンドを使用します。このコマンドで複数のステータス コード範囲を指定するには、各範囲を個別に指定したコマンドを入力します。このコマンドの構文は次のとおりです。

expect status *min_number max_number*

引数は次のとおりです。

- *min_number* — 単一のステータス コードまたはステータス コード範囲の下限を示します。0 ～ 999 の整数を入力します。
- *max_number* — 単一のステータス コード範囲の上限です。0 ～ 999 の整数を入力します。単一コードを設定する場合は、*min_number* 値を再入力します。

たとえば、単一の予測ステータス コード 211 を設定するには、次のように入力します。

```
host1/Admin(config-probe-smtp)# expect status 211 211
```

予測されるステータス コード範囲に 211 ～ 250 を設定するには、次のように入力します。

```
host1/Admin(config-probe-smtp)# expect status 211 250
```

予測されるステータス コード範囲を複数（211 ～ 250 および 252 ～ 254）を設定する場合は、各範囲を個別に次のように設定する必要があります。

```
host1/Admin(config-probe-smtp)# expect status 211 250
host1/Admin(config-probe-smtp)# expect status 252 254
```

単一の予測ステータス コードを削除するには、**no expect status** コマンドを使用します。たとえば、予測ステータス コード 211 を削除するには、次のように入力します。

```
host1/Admin(config-probe-smtp)# no expect status 211 211
```

予測される特定のステータス コード範囲を削除するには、**no expect status** コマンドを使用するときに、この範囲を入力します。たとえば、範囲 211 ～ 250 を削除するには、次のように入力します。

```
host1/Admin(config-probe-smtp)# no expect status 211 250
```

予測されるステータス コード範囲を複数削除するには、各範囲を個別に削除する必要があります。たとえば、2 つの異なる範囲（211 ～ 250 および 252 ～ 254）が設定されている場合は、次のように入力します。

```
host1/Admin(config-probe-smtp)# no expect status 211 250
host1/Admin(config-probe-smtp)# no expect status 252 254
```

IMAP プローブの設定

IMAP プローブはサーバ接続を確立し、ユーザ認定証（ログイン、パスワード、およびメールボックス）情報を送信します。ACE は設定済みコマンドを送信できます。ACE はサーバ応答に基づいて、プローブに passed または failed とマークします。

IMAP プローブを作成し、IMAP プローブ コンフィギュレーション モードにアクセスするには、**probe imap** コマンドを使用します。このコマンドの構文は次のとおりです。

probe imap *name*

name 引数には、IMAP プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、IMAP プローブ PROBE11 を定義して、IMAP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe imap PROBE11
host1/Admin(config-probe-imap)#
```

IMAP プローブのアトリビュートを設定できます（次のトピックを参照）。

- ユーザ名認定証の設定
- メールボックスの設定
- プローブの要求コマンドの設定

「一般的なプローブ アトリビュートの設定」に記載された一般的なアトリビュートや、「TCP 接続の終了の設定」に記載された接続終了も設定できます。

ユーザ名認定証の設定

IMAP プローブの認定証は、サーバで認証に使用されるユーザ名およびパスワードです。プローブの認定証を設定するには、**credentials** *username* コマンドを使用します。このコマンドの構文は次のとおりです。

credentials *username password*

引数は次のとおりです。

- *username* — 認証に使用されるユーザ ID です。最大 64 文字の英数字を、引用符で囲まずに入力します。
- *password* — 認証に使用されるパスワードです。最大 64 文字の英数字を、引用符で囲まずに入力します。

たとえば、ユーザ名 ENG1 およびパスワード TEST を設定するには、次のように入力します。

```
host1/Admin(config-probe-imap)# credentials ENG1 TEST
```

プローブのユーザ名認定証を削除するには、**no credentials** *username* コマンドを使用します。たとえば、ユーザ名 ENG1 を削除するには、次のように入力します。

```
host1/Admin(config-probe-imap)# no credentials ENG1
```

メールボックスの設定

プローブが E メールを取得するメールボックス名を設定するには、**credentials mailbox** コマンドを使用します。このコマンドの構文は次のとおりです。

credentials mailbox *name*

（注） メールボックスを設定する前に、**credentials** コマンドを使用して IMAP プローブの認定証を設定する必要があります。設定しないと、指定されたユーザ メールボックス名は ACE によって無視されます。「ユーザ名認定証の設定」を参照してください。

mailbox *name* キーワードおよび引数は、IMAP プローブの E メール取得元のユーザ メールボックス名を指定します。最大 64 文字の英数字を、引用符で囲まずに入力します。

たとえば、メールボックス LETTERS を設定するには、次のように入力します。

```
host1/Admin(config-probe-imap)# credentials mailbox LETTERS
```

プローブのメールボックスを削除するには、**no credentials mailbox** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-imap)# no credentials mailbox
```

プローブの要求コマンドの設定

IMAP プローブで使用される要求コマンドを設定するには、**request command** コマンドを使用します。このコマンドの構文は次のとおりです。

request command *command*

（注） IMAP プローブで使用される要求コマンドを設定する前に、**credentials mailbox** コマンドを使用してメールボックスの名前を設定する必要があります。設定しないと、指定された要求コマンドは ACE によって無視されます。「メールボックスの設定」を参照してください。

command 引数は、プローブに対する要求コマンドです。最大 32 文字の英数字を、スペースを含めないで入力します。

たとえば、IMAP プローブに対して直前の要求コマンドを設定するには、次のように入力します。

```
host1/Admin(config-probe-imap)# request command last
```

プローブの要求コマンドを削除するには、**no request** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-imap)# no request
```

POP3 プローブの設定

セッションを開始し、設定された認定証を送信するよう POP3 プローブを設定します。ACE は設定済みコマンドを送信することもできます。ACE はサーバ応答に基づいて、プローブに passed または failed とマークします。

POP プローブを作成し、POP プローブ コンフィギュレーション モードにアクセスするには、**probe pop** コマンドを使用します。このコマンドの構文は次のとおりです。

probe pop *name*

name 引数には、POP プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、POP プローブ PROBE12 を定義して、POP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe pop PROBE12
host1/Admin(config-probe-pop)#
```

POP プローブのアトリビュートを設定する方法については、次のトピックを参照してください。

- プローブの認定証の設定
- プローブの要求コマンドの設定

「一般的なプローブ アトリビュートの設定」に記載された一般的なアトリビュートや、「TCP 接続の終了の設定」に記載された接続終了も設定できます。

プローブの認定証の設定

プローブの認定証は、サーバで認証に使用されるユーザ名およびパスワードです。プローブの認定証を設定するには、**credentials** コマンドを使用します。このコマンドの構文は次のとおりです。

credentials *username* [*password*]

引数は次のとおりです。

- *username* — 認証に使用されるユーザ ID です。最大 64 文字の英数字を、引用符で囲まずに入力します。

- *password* —（任意）認証に使用されるパスワードです。最大 64 文字の英数字を、引用符で囲まずに入力します。

たとえば、ユーザ名 ENG1 およびパスワード TEST を設定するには、次のように入力します。

```
host1/Admin(config-probe-pop)# credentials ENG1 TEST
```

プローブの認定証を削除するには、**no credentials** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-pop)# no credentials
```

プローブの要求コマンドの設定

POP プローブで使用される要求方式を設定するには、**request command** コマンドを使用します。このコマンドの構文は次のとおりです。

request command *command*

command 引数は、プローブに対する要求方式コマンドです。最大 32 文字の英数字を、スペースを含めないで入力します。

たとえば、POP プローブに対して直前の要求コマンドを設定するには、次のように入力します。

```
host1/Admin(config-probe-pop)# request method last
```

プローブの要求コマンドを削除するには、**no request** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-pop)# no request
```

SIP プローブの設定

SIP プローブを使用して TCP または 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できます。ACE は応答と、設定された応答コード、予測ストリング、または両方を比較してプローブが成功したかを判別します。

たとえば、予測ストリングおよびステータス コードが設定されている場合に、ACE が応答内に両方を検出すると、サーバは passed とマークされます。ただし、ACE がサーバ応答ストリングと予測されるステータス コードのいずれかを受信しない場合、サーバは failed とマークされます。

（注） 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 プローブを作成し、SIP プローブ コンフィギュレーション モードにアクセスするには、**probe sip** {**tcp** | **udp**} *name* コマンドを使用します。このコマンドの構文は次のとおりです。

probe sip {**tcp** | **udp**} *name*

キーワードおよび引数は、次のとおりです。

- **tcp** — TCP 接続に対応するプローブを作成します。
- **udp** — UDP 接続に対応するプローブを作成します。
- *name* — プローブの ID です。最大 64 文字の英数字を、引用符で囲まずに入力します。

たとえば、TCP probe13 を使用して SIP プローブを定義し、SIP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe sip tcp probe13
host1/Admin(config-probe-sip-tcp)#
```

UDP probe14 を使用して SIP プローブを定義し、SIP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin# probe sip udp probe14
host1/Admin(config-probe-sip-udp)#
```

「一般的なプローブ アトリビュートの設定」に記載された最も一般的なプローブ アトリビュートを設定することもできます。プローブが、

- **tcp** キーワードで指定した TCP 接続を使用する場合、「TCP プローブの設定」の TCP アトリビュートを設定できます。

- **udp** キーワードで指定した UDP 接続を使用する場合、「UDP プローブの設定」の UDP アトリビュートを設定できます。

（注） UDP プローブの send data オプションは、SIP UDP プローブには適用できません。

追加のコマンドを使用して、SIP プローブのアトリビュートを設定することもできます。次に、追加のプローブ アトリビュートを設定する方法について説明します。

- プローブの要求方式の設定
- 宛先サーバから送信されるステータス コードの設定

プローブの要求方式の設定

デフォルトでは、SIP 要求方式は OPTIONS 方式です。現在、これは SIP プローブで使用できる唯一の方式です。プローブで使用される OPTIONS 方式 を設定するには、**request method options** コマンドを使用します。このコマンドの構文は次のとおりです。

request method options

たとえば、OPTIONS 方式を設定するには、次のように入力します。

```
host1/Admin(config-probe-sip-tcp)# request method options
```

プローブの方式を OPTIONS にリセットするには、**no request method** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-sip-tcp)# no request method
```

宛先サーバから送信されるステータス コードの設定

サーバから応答を受信した ACE 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 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。

ACE がプローブ宛先から送信されると予測する単一のステータス コード、または単一のコード応答範囲を設定するには、**expect status** コマンドを使用します。このコマンドで複数のステータス コード範囲を指定するには、各範囲を個別に指定したコマンドを入力します。このコマンドの構文は次のとおりです。

expect status *min_number max_number*

引数は次のとおりです。

- *min_number* — 単一のステータス コードまたはステータス コード範囲の下限を示します。0 ～ 999 の整数を入力します。
- *max_number* — 単一のステータス コード範囲の上限です。0 ～ 999 の整数を入力します。単一コードを設定する場合は、*min_number* 値を再入力します。

SIP の場合、予測ステータス コードは 200 で、成功プローブを示します。たとえば、予測ステータス コードに、要求に成功したことを示す値 200 を設定するには、次のように入力します。

```
host1/Admin(config-probe-sip-tcp)# expect status 200 200
```

RTSP プローブの設定

RTSP プローブを使用して 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。これらのプローブを設定する場合、**probe rtsp** *name* コマンドを使用してプローブを作成し、プローブ コンフィギュレーション モードにアクセスします。

たとえば、RTSP プローブ probe15 を定義して、RTSP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe rtsp probe15
host1/Admin(config-probe-rtsp)#
```

RTSP プローブを作成したあとに、「一般的なプローブ アトリビュートの設定」に記載された一般的なプローブ アトリビュートを設定できます。「TCP プローブの設定」に記載された RST および予測される応答ストリングを送信することで、TCP 接続を終了するよう ACE を設定することもできます。

追加のコマンドを使用して、RTSP プローブのアトリビュートを設定することもできます。次に、追加のプローブ アトリビュートを設定する方法について説明します。

- 要求方式の設定
- RTSP プローブのヘッダー フィールドの設定
- 宛先サーバから送信されるステータス コードの設定

要求方式の設定

デフォルトでは、RTSP 要求方式は OPTIONS 方式です。DESCRIBE 方式を設定することもできます。プローブで使用される要求方式 を設定するには、**request method** コマンドを使用します。このコマンドの構文は次のとおりです。

request method {**options** | **describe url** *url_string*}

キーワードおよび引数は、次のとおりです。

- **options** — OPTIONS 要求方式を設定します。これがデフォルトの方式です。ACE は、この方式のアスタリスク（*）要求 URL を使用します。
- **describe url** *url_string* — DESCRIBE 要求方式を設定します。*url_string* は、サーバの RTSP メディア ストリームの URL 要求です。最大 255 文字の英数字で URL ストリングを入力します。

たとえば、rtsp://media/video.smi に関する URL を使用するよう RTSP プローブを設定するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# request method describe url
rtsp://192.168.10.1/media/video.smi
```

たとえば、rtsp://media/video.smi に関する PATH を使用するよう RTSP プローブを設定するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# request method describe path
/media/video.smi
```

上記の例では、IP アドレスはプローブのターゲットの IP アドレスから取得されます。

デフォルトの OPTIONS 要求方式にリセットするには、**no request method** または **request method options** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-rtsp)# no request method
```

RTSP プローブのヘッダー フィールドの設定

プローブにヘッダー フィールド値を設定するには、**header** コマンドを使用します。このコマンドの構文は次のとおりです。

header {**require** | **proxy-require**} **header-value** *value*

キーワードおよび引数は、次のとおりです。

- **require** — Require ヘッダーを指定します。
- **proxy-require** — Proxy-Require ヘッダーを指定します。
- **header-value** *value* — ヘッダー値を指定します。この値には、最大 255 文字の英数字を、スペースを含めないで入力します。

たとえば、REQUIRE ヘッダーに implicit-play のフィールド値を設定するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# header require header-value
implicit-play
```

プローブのヘッダー設定を削除するには、**header** コマンドの **no** 形式を使用します。たとえば、Require ヘッダーを削除するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# no header require
```

Proxy-Require ヘッダーを削除するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# no header proxy-require
```

宛先サーバから送信されるステータス コードの設定

サーバから応答を受信した ACE 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 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。

ACE がプローブ宛先から送信されると予測する単一のステータス コード、または単一のコード応答範囲を設定するには、**expect status** コマンドを使用します。このコマンドで複数のステータス コード範囲を指定するには、各範囲を個別に指定したコマンドを入力します。このコマンドの構文は次のとおりです。

expect status *min_number max_number*

引数は次のとおりです。

- *min_number* — 単一のステータス コードまたはステータス コード範囲の下限を示します。0 ～ 999 の整数を入力します。
- *max_number* — 単一のステータス コード範囲の上限です。0 ～ 999 の整数を入力します。単一コードを設定する場合は、*min_number* 値を再入力します。

たとえば、予測ステータス コードに、要求に成功したことを示す値 200 を設定するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# expect status 200 200
```

予測されるステータス コード範囲に 100 ～ 200 を設定するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# expect status 100 200
```

予測されるステータス コード範囲を複数（100 ～ 200 および 250 ～ 305）を設定する場合は、各範囲を個別に設定する必要があります。次のように入力します。

```
host1/Admin(config-probe-rtsp)# expect status 100 200
host1/Admin(config-probe-rtsp)# expect status 250 305
```

単一の予測ステータス コードを削除するには、**no expect status** コマンドを使用します。たとえば、予測ステータス コード 200 を削除するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# no expect status 200 200
```

予測される特定のステータス コード範囲を削除するには、**no expect status** コマンドを使用して、この範囲を入力します。たとえば、範囲 250 ～ 305 から範囲 302 ～ 250 を削除するには、次のように入力します。

```
host1/Admin(config-probe-rtsp)# no expect status 250 305
```

予測されるステータス コード範囲を複数削除するには、各範囲を個別に削除する必要があります。たとえば、2 つの異なる範囲（200 ～ 100 および 250 ～ 305）が設定されている場合は、次のように入力します。

```
host1/Admin(config-probe-rtsp)# no expect status 100 200
host1/Admin(config-probe-rtsp)# no expect status 250 305
```

RADIUS プローブの設定

RADIUS プローブは、設定されたユーザ名、パスワード、および共有秘密を使用するクエリーを RADIUS サーバに送信します。サーバが起動している場合、サーバは passed とマークされます。ネットワーク アクセス サーバ（NAS）アドレスが設定されている場合、ACE は発信パケット内で NAS アドレスを使用します。NAS アドレスが設定されていない場合、ACE は発信インターフェイスに関連付けられた IP アドレスを NAS アドレスとして使用します。

RADIUS プローブを作成し、RADIUS プローブ コンフィギュレーション モードにアクセスするには、**probe radius** コマンドを使用します。このコマンドの構文は次のとおりです。

probe radius *name*

name 引数には、RADIUS プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、RADIUS プローブ PROBE を定義して、RADIUS プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe radius PROBE
host1/Admin(config-probe-radius)#
```

RADIUS プローブのプローブ アトリビュートを設定する方法については、次のトピックを参照してください。

- プローブの認定証および共有秘密の設定
- NAS IP アドレスの設定

「一般的なプローブ アトリビュートの設定」に記載された一般的なアトリビュートを設定することもできます。

プローブの認定証および共有秘密の設定

プローブの認定証は、サーバで認証に使用されるユーザ名およびパスワードと、RADIUS サーバにプローブがアクセスするためのオプションの共有秘密です。プローブの認定証を設定するには、**credentials** コマンドを使用します。このコマンドの構文は次のとおりです。

credentials *username password* [**secret** *shared_secret*]

キーワードおよび引数は、次のとおりです。

- *username* — 認証に使用されるユーザ ID です。最大 64 文字の英数字を、引用符で囲まずに入力します。
- *password* — 認証に使用されるパスワードです。最大 64 文字の英数字を、引用符で囲まずに入力します。
- **secret** *shared_secret* —（任意）共有秘密を指定します。共有秘密は、最大 64 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。

たとえば、ユーザ名 ENG1 およびパスワード TEST を設定するには、次のように入力します。

```
host1/Admin(config-probe-radius)# credentials ENG1 TEST
```

プローブの認定証を削除するには、**no credentials** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-radius)# no credentials
```

NAS IP アドレスの設定

RADIUS プローブに NAS アドレスが設定されていない場合、ACE は発信インターフェイスに関連付けられた IP アドレスを NAS アドレスとして使用します。NAS アドレスを設定するには、**nas ip address** コマンドを使用します。このコマンドの構文は次のとおりです。

nas ip address *ip_address*

ip_address 引数は、NAS IP アドレスです。ドット付き 10 進表記で一意の IPv4 アドレスを入力します（例：192.8.12.15）。

たとえば、NAS アドレス 192.8.12.15 を設定するには、次のように入力します。

```
host1/Admin(config-probe-radius)# nas ip address 192.8.12.15
```

NAS IP アドレスを削除するには、**no nas ip address** コマンドを入力します。次のように入力します。

```
host1/Admin(config-probe-radius)# no nas ip address
```

SNMP ベースのサーバ ロード プローブの設定

SNMP ベースのサーバ ロード プローブは UDP 接続を確立し、最大 8 つの SMNP OID クエリーを設定してサーバを検査できます。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。しきい値を越えた場合、サーバは failed とマークされます。

これらのプローブを設定する場合、**probe snmp** *name* コマンドを使用してプローブを作成し、プローブ コンフィギュレーション モードにアクセスします。

たとえば、SNMP プローブ probe18 を定義して、SNMP プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe snmp probe18
host1/Admin(config-probe-snmp)#
```

「一般的なプローブ アトリビュートの設定」に記載された一般的なアトリビュートを設定できます。追加のコマンドを使用して、SNMP プローブのアトリビュートを設定することもできます。次に、追加のプローブ アトリビュートを設定する方法について説明します。

- コミュニティ ストリングの設定
- SNMP バージョンの設定
- OID ストリングの設定
- OID 値タイプの設定
- OID しきい値の設定
- OID 重みの設定

コミュニティ ストリングの設定

ACE プローブはコミュニティ ストリング経由でサーバにアクセスします。デフォルトでは、コミュニティ ストリングは設定されていません。コミュニティ ストリングを設定するには、**community** コマンドを使用します。このコマンドの構文は次のとおりです。

community *text*

text 引数は、サーバの SNMP コミュニティ ストリングの名前です。最大 255 文字の英数字を入力します。

たとえば、プライベート コミュニティ ストリングを設定するには、次のように入力します。

```
host1/Admin(config-probe-snmp)# community private
```

コミュニティ ストリングを削除するには、次のように入力します。

```
host1/Admin(config-probe-snmp)# no community
```

SNMP バージョンの設定

サーバに送信される SNMP OID クエリーのバージョンは、サポートされている SNMP バージョンを示します。デフォルトでは、プローブは SNMP バージョン 1 をサポートします。

プローブがサポートする SNMP のバージョンを設定するには、**version** コマンドを使用します。このコマンドの構文は次のとおりです。

version {**1** | **2c**}

キーワードは次のとおりです。

- **1** — プローブが SNMP バージョン 1（デフォルト）をサポートするよう指定します。
- **2c** — プローブが SNMP バージョン 2c をサポートするよう指定します。

たとえば、SNMP バージョン 2c を設定するには、次のように入力します。

```
host1/Admin(config-probe-snmp)# version 2c
```

SNMP バージョン 1 のデフォルト設定にリセットするには、次のように入力します。

```
host1/Admin(config-probe-snmp)# no version
```

OID ストリングの設定

ACE が SNMP OID クエリーのあるプローブを送信する場合、ACE はロード 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取得した値を使用します。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。最大 8 つの OID を設定できます。

OID ストリングを設定し、プローブ SNMP OID コンフィギュレーション モードにアクセスするには、プローブ SNMP コンフィギュレーション モードで **oid** コマンドを使用します。このコマンドの構文は次のとおりです。

oid *string*

string 引数は、プローブがサーバに値について問い合わせるのに使用する OID です。ドット付き 10 進表記の最大 64 文字の英数字を、引用符で囲まずに入力します。OID ストリングはサーバ タイプに基づいています。文字列のドット（.）は、文字としてカウントされます。たとえば、OID ストリングが 10.0.0.1.1 の場合、文字カウントは 10 になります。

probe-snmp-oid コンフィギュレーション モードにアクセスすると、しきい値、OID 値のタイプ、OID に割り当てられた重みを次のように設定できます。

（注） 複数の OID を設定し、これらの OID をロード バランシング決定で使用する場合、重み値を設定する必要があります。

たとえば、OID ストリング .1.3.6.1.4.2021.10.1.3.1 を Linux サーバの CPU 負荷の 1 分平均に設定し、probe-snmp-oid コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config-probe-snmp)# oid .1.3.6.1.4.2021.10.1.3.1
host1/Admin(config-probe-snmp-oid)#
```

OID ストリング を削除するには、次のように入力します。

```
host1/Admin(config-probe-snmp)# no oid .1.3.6.1.4.2021.10.1.3.1
```

OID 値タイプの設定

デフォルトでは、取得した OID 値タイプはパーセント値です。OID 値タイプを絶対値として設定し、最大予測値を定義するには、プローブ SNMP OID コンフィギュレーション モードで **type absolute max** コマンドを使用します。このコマンドの構文は次のとおりです。

type absolute max *integer*

integer 引数は、OID の最大予測絶対値を指定します。1 ～ 4294967295 の整数を入力します。デフォルトでは、OID の値はパーセント値です。

（注）　**type absolute max** コマンドを設定する場合は、**threshold** コマンドの値も設定することを推奨します。デフォルトのしきい値は、**type absolute max** コマンドで指定された整数値に設定されるためです。

たとえば、絶対値タイプに最大予測値 65535 を設定するには、次のように入力します。

```
host1/Admin(config-probe-snmp-oid)# type absolute max 65535
```

OID 値タイプをパーセント値にリセットするには、次のように入力します。

```
host1/Admin(config-probe-snmp)# no type
```

（注）　**no type** コマンドを使用すると、OID タイプがパーセント値にリセットされ、**threshold** コマンドの値が 100 に設定されます。

OID しきい値の設定

OID のしきい値によって、サーバをアウト オブ サービスにする値が指定されます。

- OID の値がパーセントに基づく場合、デフォルトのしきい値は 100 となります。
- OID が絶対値に基づいている場合、しきい値の範囲は **type absolute max** コマンドで指定した値に基づきます（「OID しきい値の設定」を参照）。

しきい値を設定するには、プローブ SNMP OID コンフィギュレーション モードで **threshold** コマンドを使用します。このコマンドの構文は次のとおりです。

threshold *integer*

integer 引数は、サーバをアウト オブ サービスにするしきい値を指定します。

- OID 値がパーセントに基づいている場合、1 ～ 100 の整数を入力します。デフォルト値は 100 です。

- OID が絶対値に基づいている場合、しきい値範囲は 1 から **type absolute max** コマンドで指定した最大値になります。

たとえば、しきい値 50 を設定するには、次のように入力します。

```
host1/Admin(config-probe-snmp-oid)# threshold 50
```

OID しきい値をデフォルト値にリセットするには、次のように入力します。

```
host1/Admin(config-probe-snmp)# no threshold
```

OID 重みの設定

複数の OID を設定し、これらの OID をロード バランシング決定で使用する必要がある場合、OID 重みを指定する必要があります。OID に重みを設定するには、probe-snmp-oid コンフィギュレーション モードで **weight** コマンドを使用します。このコマンドの構文は次のとおりです。

weight *integer*

integer 引数は、OID の重みを指定します。1 ～ 16000 の整数を入力します。デフォルトでは、設定済みの各 OID に対して均等な重みが割り当てられます。

（注） 複数の OID を設定し、これらの OID をロード バランシング決定で使用する場合、重み値を設定する必要があります。

たとえば、重み 10000 を設定するには、次のように入力します。

```
host1/Admin(config-probe-snmp-oid)# weight 10000
```

デフォルト動作の、設定された OID それぞれに割り当てられた等しい重みにリセットするには、次のように入力します。

```
host1/Admin(config-probe-snmp)# no weight
```

スクリプト プローブの設定

スクリプト プローブを使用すると、ヘルス モニタリング用に作成されたプローブを実行するためのスクリプトを実行できます。標準ヘルス モニタリングに含まれない機能を持った特定のスクリプトを作成できます。スクリプト プローブを設定する手順は、次のとおりです。

- スクリプト ファイルを ACE disk0: ファイル システムにコピーします。
- スクリプト ファイルをロードします。
- スクリプト プローブにスクリプトを関連付けます。

ACE は 256 の一意なスクリプト ファイルを設定できます。

プローブにある（ACE のディレクトリ）、シスコが提供するスクリプトを使用することもできます。これらのスクリプトの詳細については、付録 A「ACE での TCL スクリプトの使用」の「スクリプトの概要」を参照してください。

（注） ACE で同時に実行できるスクリプト プローブ インスタンスは 200 だけです。この限度を超えると、**show probe detail** コマンドを実行したときに、Last disconnect err フィールドに「Out-of Resource: Max. script-instance limit reached」エラー メッセージが表示され、out-of-sockets カウンタが増加します。

ACE にスクリプト ファイルをコピーおよびロードする方法については、付録 A「ACE での TCL スクリプトの使用」を参照してください。

スクリプト プローブを作成し、スクリプト プローブ コンフィギュレーション モードにアクセスするには、**probe scripted** コマンドを使用します。このコマンドの構文は次のとおりです。

probe scripted *name*

name 引数には、スクリプト プローブの ID を入力します。この ID は、最大 64 文字のスペースを含まない英数字を、引用符で囲まずに入力します。

たとえば、スクリプト プローブ PROBE19 を定義して、スクリプト プローブ コンフィギュレーション モードにアクセスするには、次のように入力します。

```
host1/Admin(config)# probe scripted PROBE19
host1/Admin(config-probe-scrptd)#
```

スクリプト プローブ アトリビュートを設定する方法については、「スクリプトとプローブの関連付け」を参照してください。

「一般的なプローブ アトリビュートの設定」に記載された一般コマンドを設定することもできます。

スクリプトとプローブの関連付け

スクリプト プローブは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。スクリプトに渡される引数を設定することもできます。スクリプト ファイルをプローブに関連付ける前に、ACE にスクリプトをコピーして、ロードする必要があります。スクリプトのコピーおよびロードの詳細については、付録 A「ACE での TCL スクリプトの使用」を参照してください。

script コマンドを使用して、スクリプト ファイルの名前と、スクリプトに渡される引数を指定します。

このコマンドの構文は次のとおりです。

script *script_name* [*script_arguments*]

引数は次のとおりです。

- *script_name* — スクリプトの名前スペースを含まず引用符なしの英数字を入力します（最大 255 文字）。
- *script_arguments* — （任意）スクリプトに送信されるデータです。最大 255 文字の英数字を、スペースや引用符を含めて入力します。各引数はスペースで区切ります。1 つの引数にスペースが含まれている場合は、引数ストリングを引用符で囲みます。

たとえば、スクリプト名に PROBE-SCRIPT、引数に ?? を設定するには、次のように入力します。

```
host1/Admin(config-probe-scrptd)# script PROBE-SCRIPT ??
```

設定からスクリプトおよび引数を削除するには、**no script** コマンドを使用します。次のように入力します。

```
host1/Admin(config-probe-scrptd)# no script
```

UDP プローブのロード バランシング設定例

次に、複数の実サーバに DNS トラフィックのロード バランスを行い、複数のパケットにまたがる UDP データを送受信する実行コンフィギュレーションの例を示します。この設定では、UDP ヘルス プローブを使用します。この例では、UDP プローブ設定は太字で示されています。

```
access-list ACL1 line 10 extended permit ip any any

probe udp UDP
  interval 5
  passdetect interval 10
  description THIS PROBE IS INTENDED FOR LOAD BALANCING DNS TRAFFIC
  port 53
  send-data UDP_TEST

rserver host SERVER1
  ip address 192.168.252.245
  inservice
rserver host SERVER2
  ip address 192.168.252.246
  inservice
rserver host SERVER3
  ip address 192.168.252.247
  inservice

serverfarm host SFARM1
  probe UDP
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
  rserver SERVER3
    inservice

class-map match-all L4UDP-VIP_114:UDP_CLASS
   2 match virtual-address 192.168.120.114 udp eq 53
policy-map type loadbalance first-match L7PLBSF_UDP_POLICY
  class class-default
    serverfarm SFARM1
policy-map multi-match L4SH-Gold-VIPs_POLICY
    class L4UDP-VIP_114:UDP_CLASS
    loadbalance vip inservice
    loadbalance policy L7PLBSF_UDP_POLICY
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 120
    connection advanced-options 1SECOND-IDLE
```

```
interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.70 netmask 255.255.255.0 pat
  service-policy input L4SH-Gold-VIPs_POLICY
  no shutdown
ip route 10.1.0.0 255.255.255.0 192.168.120.254
```

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 VIP ベースおよび TAG ベースの KAL-AP プローブをサポートします。VIP ベースの KAL-AP の場合、ACE が kal-ap-by-vip 要求を受信すると、VIP アドレスで設定されたすべてのレイヤ 3 クラス マップで VIP アドレスがアクティブであるかどうかを確認します。ACE は VIP アドレスに関して、他のプロトコル固有の情報をすべて無視します。レイヤ 3 クラス マップごとに、ACE はサーバファームの関連したレイヤ 7 ポリシーおよび実サーバを配置します。ACE は、これらの VIP に関連付けられたサーバと動作状態であるサーバの合計数を判断します。

ACE は 0 ～ 255 の負荷数を計算し、VIP のサーバ アベイラビリティを KAL-AP デバイスに報告します。負荷値 0 は、VIP アドレスが使用できないことを示します。VIP 検索が失敗した場合にもこの値が送信されます。負荷値 1 は、VIP がオフラインで使用できないことを示すために予約されています。有効な負荷値は 2 ～ 255 です。負荷値 2 は VIP が最小の負荷であり、負荷値 255 は VIP が最大の負荷であることを示します。たとえば、サーバの合計数が 10 で 5 台のみが動作している場合、負荷値は 127 です。

（注） 同じ実サーバが複数のサーバ ファームに関連付けられている場合、ACE では計算上、重複した値が含まれます。

TAG ベースの KAL-AP の場合、VIP アドレスに関連付けられたドメインは ACE の TAG に対応します。ACE が kal-ap-by-tag 要求を受信した場合、プロセスは VIP ベースの KAL-AP プローブと似ています。負荷計算は、レイヤ 3 クラス マップ、サーバ ファーム、および実サーバのオブジェクトを考慮します。ドメインの他のオブジェクトはすべて、負荷計算中は無視されます。ドメインの計算は VIP ア

ドレスと類似しています。ただし、唯一の違いは、実サーバ オブジェクトとサーバ ファーム オブジェクトが計算中とみなされることです。ACE はドメイン内のレイヤ 3 VIP アドレスのサーバ アベイラビリティ情報を収集します。ACE は、すべてのサーバ ファームがドメインに関連付けられているものとみなします。実サーバがドメインに存在する場合、ACE は実サーバを現在の合計に加え、分割を実行し、TAG オブジェクトとしてのアベイラビリティを判断します。ACE は KAL-AP 応答でこの最終数を報告します。

ここでは、次の内容について説明します。

- ACE での KAL-AP のイネーブル化
- KAL-AP VIP アドレスの設定
- ドメインとしての KAL-AP TAG の設定
- セキュア KAL-AP の設定
- GSLB 情報の表示
- GSLB 統計情報の表示

ACE での KAL-AP のイネーブル化

ACE で KAL-AP をイネーブルにするには、管理クラス マップおよびポリシー マップを設定し、これを適切なインターフェイスに適用する必要があります。KAL-AP サーバは標準 5002 ポートですべての KAL-AP 要求を受信します。

KAL-AP over UDP 管理アクセスのためクラス マップを設定するには、クラス マップ管理コンフィギュレーション モードで **match protocol kalap-udp** コマンドを使用します。このコマンドの構文は次のとおりです。

match protocol kalap-udp any | [**source-address** *ip_address subnet_mask*]

キーワードおよび引数は、次のとおりです。

- **any** — 管理トラフィック分類にクライアント送信元アドレスを指定します。
- **source-address** — ネットワーク トラフィック一致基準として、クライアント送信元ホスト IP アドレスおよびサブネット マスクを指定します。分類の一部として、ACE はポリシー マップを適用するインターフェイスから宛先 IP アドレスを暗黙で取得します。
- *ip_address* — クライアントの送信元 IP アドレス。ドット付き 10 進表記で IP アドレスを入力します（例：192.168.11.1）。

- *mask* — ドット付き 10 進表記のクライアント エントリのサブネット マスク（例：255.255.255.0）

たとえば、送信元 IP アドレスから KAL-AP クラス マップを指定するには、次のように入力します。

```
host1/Admin(config)# class-map type management KALAP-CM
host1/Admin(config-cmap-mgmt)# match protocol kalap-udp any
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

クラス マップを削除するには、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no match protocol kalap-udp
source-address any
```

KAL-AP クラス マップを作成したあと、KAL-AP 管理ポリシー マップを作成し、クラス マップをこのポリシー マップに適用します。ポリシー マップを作成し、ポリシー マップ管理コンフィギュレーション モードにアクセスするには、コンフィギュレーション モードで **policy-map type management** コマンドを使用します。たとえば、KALAP-MGMT 管理ポリシー マップを作成し、KALAP-CM クラス マップをこのポリシー マップに適用するには、次のように入力します。

```
host1/Admin(config)# policy-map type management KALAP-MGMT
host1/Admin(config-pmap-mgmt)# class KALAP-CM
host1/Admin(config-cmap-mgmt)# permit
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

ポリシー マップをインターフェイスに適用するには、コンフィギュレーション モードで **interface vlan** コマンドを使用します。たとえば、KALAP-MGMT ポリシー マップを VLAN（仮想 LAN）インターフェイス 10 に適用するには、次のように入力します。

```
host1/Admin(config)# interface vlan 10
host1/Admin(config-if)# ip address 10.1.0.1 255.255.255.0
host1/Admin(config-if)# service-policy input KALAP-MGMT
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
host1/Admin(config)#
```

（注）　KAL-AP ポリシーを変更または削除する場合、既存の KAL-AP 接続を手動でクリアする必要があります。

KAL-AP VIP アドレスの設定

VIP ベースの KAL-AP を設定するには、VIP アドレス一致基準を含んだレイヤ 3/4 クラス マップを設定します。一致基準として VIP アドレス、プロトコル、およびポートからなる 3 タプル フローを定義するには、クラス マップ コンフィギュレーション モードで **match virtual-address** コマンドを使用します。複数の一致基準文を設定して、SLB 用の VIP を定義できます。このコマンドの構文は次のとおりです。

[*line_number*] **match virtual-address** *vip_address* {[*mask*] | **any** | {**tcp** | **udp** {**any** | **eq** *port_number* | **range** *port1 port2*}} | *protocol_number*}

キーワードおよび引数の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」の「VIP アドレス一致基準の定義」を参照してください。

（注）　KAL-AP の場合、ACE は、VIP アドレスで設定されたすべてのレイヤ 3 クラス マップで VIP アドレスがアクティブであるかどうかを確認します。これは VIP アドレスに関して、他のプロトコル固有の情報をすべて無視します。

たとえば、宛先が VIP アドレス 10.10.10.10 であり、IP プロトコル値のワイルドカード値を持ったトラフィックと一致するクラス マップ VIP-20（TCP または UDP）を作成するには、次のように入力します。

```
host1/Admin(config)# class-map VIP-20
host1/Admin(config-cmap)# match virtual-address 10.10.10.10 any
```

クラス マップから VIP match 文を削除するには、次のように入力します。

```
host1/Admin(config-cmap)# no match virtual-address 10.10.10.10 any
```

ドメインとしての KAL-AP TAG の設定

ドメインとして KAL-AP TAG を設定するには、コンフィギュレーション モードで **domain** コマンドを使用します。このコマンドの構文は次のとおりです。

domain *name*

name は KAL-AP TAG の名前です。

（注）　ドメインの負荷計算の場合、ACE はレイヤ 3 クラス マップ、サーバ ファーム、および実サーバのオブジェクトを考慮します。ドメインの他のオブジェクトはすべて、計算中は無視されます。

たとえば、ドメインとして KAL-AP-TAG1 を設定するには、次のように入力します。

```
host1/Admin(config)# domain KAL-AP-TAG1
```

ドメインを作成したあと、ドメイン コンフィギュレーション モードで **add-object class-map** コマンドを使用して、TAG ドメインに関連付けるクラス マップをそれぞれ追加します。たとえば、VIP-20 および VIP-71 クラス マップを TAG ドメインに追加するには、次のように入力します。

```
host1/Admin(config-domain)# add-object class-map VIP-20
host1/Admin(config-domain)# add-object class-map VIP-71
```

ドメインを削除するには、次のように入力します。

```
host1/Admin(config)# no domain KAL-AP-TAG1
```

クラス マップの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。ドメインの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

セキュア KAL-AP の設定

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。

ACE のセキュア KAL-AP を設定するには、コンフィギュレーション モードで **kalap udp** コマンドを使用して KAL-AP UDP コンフィギュレーション モードにアクセスします。このコマンドの構文は次のとおりです。

kalap udp

次のように入力します。

```
host1/Admin(config)# kalap udp
host1/Admin(config-kalap-udp)#
```

KAL-AP 設定およびすべての VIP エントリを削除するには、次のコマンドを入力します。

```
host1/Admin(config)# no kalap udp
```

このモードでセキュア KAL-AP をイネーブルにするには、**ip address** コマンドを使用して GSS および共有秘密に対して VIP アドレスを設定します。このコマンドの構文は次のとおりです。

ip address *ip_address* **encryption md5** *secret*

キーワードおよび引数は、次のとおりです。

- *ip_address* — GSS の VIP アドレス。ドット付き 10 進表記で IP アドレスを入力します（例：192.168.11.1）。
- **encryption** — 暗号化方式を指定します。
- **md5** — MD5 暗号化方式を指定します。
- *secret* — KAL-AP デバイスと ACE の間の共有秘密。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。

たとえば、セキュア KAL-AP をイネーブルにし、GSS および共有秘密の VIP アドレスを設定するには、次のように入力します。

```
host1/Admin(config-kalap-udp)# ip address 10.1.0.1 encryption md5
andromeda
```

セキュア KAL-AP をディセーブルにするには、**ip address** コマンドの **no** 形式を使用します。次のように入力します。

```
host1/Admin(config-kalap-udp)# no ip address 10.1.0.1
```

GSLB 情報の表示

KAL-AP 要求に提供された VIP アドレスまたはドメイン名の最新の負荷情報を表示するには、EXEC モードで **show kalap udp load** コマンドを使用します。このコマンドの構文は次のとおりです。

show kalap udp load {**all** | **vip** *ip_address*} | {**domain** *name*}

キーワードおよび引数は、次のとおりです。

- **all** — すべての VIP アドレスおよびドメインの最新の負荷情報を表示します。
- **vip** *ip_address* — 指定された VIP アドレスの最新の負荷情報を表示します。ドット付き 10 進表記で IP アドレスを入力します（例：192.168.11.1）。
- **domain** *name* — 指定されたドメイン名の最新の負荷情報を表示します。

show kalap udp load コマンドの出力フィールドでは、VIP アドレスまたはドメイン名、負荷値、およびタイムスタンプを表示します。

たとえば、すべての VIP アドレスおよびドメインの最新の負荷情報を表示するには、次のように入力します。

```
host1/Admin# show kalap udp load all
```

たとえば、KAL-AP 要求に対する VIP アドレス 10.10.10.10 の最新の負荷情報を表示するには、次のように入力します。

```
host1/Admin# show kalap udp load vip 10.10.10.10
```

KAL-AP 要求に対するドメイン KAL-AP-TAG1 の最新の負荷情報を表示するには、次のように入力します。

```
host1/Admin# show kalap udp load domain KAL-AP-TAG1
```

GSLB 統計情報の表示

コンテキストごとに GSLB 統計情報を表示するには、EXEC モードで **show stats kalap** コマンドを使用します。このコマンドの構文は次のとおりです。

show stats kalap

次のように入力します。

```
host1/Admin# show stats kalap
```

表 4-2 に、このコマンドが表示する出力フィールドを示します。

表 4-2　show stats kalap コマンドのフィールド

フィールド	説明
Total bytes received	受信されたバイトの総数
Total bytes sent	送信されたバイトの総数
Total requests received	受信された要求の総数
Total responses sent	送信された要求の総数
Total requests successfully received	正常に受信された要求の総数
Total responses successfully sent	正常に送信された要求の総数
Total secure requests received	受信されたセキュアな要求の総数
Total secure responses sent	送信されたセキュアな要求の総数
Total requests with errors	エラーが発生した要求の総数
Total requests with parse errors	解析エラーが発生した要求の総数
Total response transfer errors	応答転送エラーの総数

コンテキストごとの GSLB 統計情報を消去するには、EXEC モードで **clear stats kalap** コマンドを使用します。次のように入力します。

```
host1/Admin# clear stats kalap
```

プローブ情報の表示

プローブの設定情報および統計情報を表示するには、EXEC モードで **show probe** コマンドを使用します。このコマンドの構文は次のとおりです。

show probe [*probe_name*] [**detail**]

引数およびオプションは、次のとおりです。

- *probe_name* — （任意）指定されたプローブ名の情報です。
- **detail** — （任意）詳細なプローブ設定および統計情報を表示します。

プローブ名を入力しなかった場合、このコマンドは、設定されたすべてのプローブについて情報の要約を表示します。次のように入力します。

```
host1/Admin# show probe
```

show running-config probe コマンドを使用して、すべてのプローブの設定情報を表示することもできます。

次のように入力します。

```
host1/Admin# show running-config probe
```

表 4-3 に、**detail** オプションで指定された追加出力を含む、**show probe** コマンド出力のフィールドの説明を示します。

（注） 実サーバ、サーバ ファーム、サーバ ファーム内の実サーバ、プレディクタ、または実サーバがサービス外のときにアクティブな FT グループ メンバーに対して設定されたプローブなど、どのようなタイプのプローブでも、**show probe** コマンドの出力にはプローブ インスタンスは表示されません。この場合、show probe コマンドの出力には関連付けのみ一覧表示されます。これは、ポートが継承されないプローブ インスタンスと、ポートが継承されるプローブ インスタンスとの整合性を維持するためです（「プローブのポート番号の継承」を参照）。

表 4-3　show probe コマンドのフィールドの説明

フィールド	説明
Probe	プローブの名前
Type	プローブのタイプ
State	プローブがアクティブであるか、非アクティブであるか
Description	プローブに設定された説明（**detail** オプション出力）
Port	プローブによって使用されるポート番号。デフォルトでは、プローブはそのタイプに応じたポート番号を使用します。プローブのポート番号が継承される場合は（「プローブのポート番号の継承」を参照）、継承されるポート番号がこのフィールドに表示されます。
Address	プローブの宛先アドレス
Addr type	アドレス タイプ
Interval	passed とマーキングされたサーバに ACE がプローブを送信する時間間隔（秒）
Pass intvl	failed のサーバにプローブが送信される時間間隔（秒）
Pass count	サーバに passed とマークするまでのプローブの連続成功回数
Fail count	サーバが failed とマーキングされるまでに許容される連続した失敗プローブの数
Recv timeout	プローブに対するサーバの応答が受信される時間間隔（秒）
DNS domain	プローブに設定されたドメイン名（DNS プローブの **detail** オプション出力）
HTTP method	プローブで使用される HTTP 方式（GET または HEAD）、および URL（HTTP および HTTPS プローブの **detail** オプション出力）
HTTP URL	HTTP 方式の場合にプローブで使用される URL（HTTP および HTTPS プローブの **detail** オプション出力）
RTSP method	プローブで使用される RTSP 方式および URL（RTSP プローブの **detail** オプション出力）
RTSP URL	RTSP 方式でプローブが使用する URL（RTSP プローブの **detail** オプション出力）
IMAP mailbox	プローブが E メールを取得するメールボックスのユーザ名（IMAP プローブの **detail** オプション出力）

表 4-3　show probe コマンドのフィールドの説明（続き）

フィールド	説明
IMAP/POP Command	プローブの要求方式コマンド（IMAP および POP プローブの **detail** オプション出力）
NAS address	RADIUS サーバの NAS アドレス（RADIUS プローブの **detail** オプション出力）
Script filename	スクリプトのファイル名（スクリプト プローブの **detail** オプション出力）
Conn termination	GRACEFUL または FORCED を示す TCP 接続終了タイプ、（ECHO TCP、Finger、FTP、HTTP、HTTPS、IMAP、POP、SMTP、TCP、および Telnet プローブの **detail** オプション出力）
Expect/Search offset	expect regex 式の検索開始位置を示す、受信済みメッセージまたはバッファ内の文字数（HTTP、HTTPS、RTSP、SIP、TCP、および UDP プローブの **detail** オプション出力）
Request-method	**detail** オプション出力に表示される SIP プローブの要求方式。現在、OPTIONS 方式は SIP プローブで使用できる唯一の方式です。
Expect regex	プローブ宛先から送信されると予測される、設定済み応答データ（HTTP、HTTPS、RTSP、SIP、TCP、および UDP プローブの **detail** オプション出力）
Open timeout	サーバとの接続がオープンし、確立するまでプローブが待機する秒単位のインターバル（Finger、FTP、HTTP、HTTPS、IMAP、POP、スクリプト、RTSP、SMTP、TCP、および Telnet プローブの **detail** オプション出力）
Send data	プローブから送信される ASCII データ（ECHO、Finger、HTTP、HTTPS、RTSP、TCP、および UDP プローブの **detail** オプション出力）
Version	サポートされているバージョンを示す、サーバに送信される SNMP OID クエリーの SNMP バージョン（SNMP プローブの **detail** オプション出力）
Community	SNMP コミュニティ ストリング（SNMP プローブの **detail** オプション出力）
OID string	設定された OID（SNMP プローブの **detail** オプション出力）
Type	取得した OID 値に関する OID 値タイプ、絶対またはパーセント（SNMP プローブの **detail** オプション出力）

表 4-3　show probe コマンドのフィールドの説明（続き）

フィールド	説明
Max value	OID 負荷タイプの最大予測負荷値（SNMP プローブの **detail** オプション出力）
Weight	OID の負荷重み（SNMP プローブの **detail** オプション出力）
Threshold	OID のしきい値設定。しきい値を越えた場合、OID はアウト オブ サービスになります（SNMP プローブの **detail** オプション出力）。
プローブの結果	
associations	プローブの実サーバ アソシエーション
ip-address	プローブの宛先または送信元アドレス
port	プローブのポート番号
porttype	プローブのポート番号のソース。このフィールドは、プローブのポート番号が継承されるのかどうかを示します（「プローブのポート番号の継承」を参照）。可能な値は、PROBE、REAL、VIP、DEFAULT です。 **（注）** サーバ ファームのプレディクタ方式、スタンドアロンの実サーバに割り当てられたプローブ、または冗長構成のアクティブな FT グループ メンバーに対して設定されたプローブの場合は、“--” という値が表示されます。
probes	プローブの総数
failed	失敗したプローブの総数
passed	成功したプローブの総数
health	プローブのヘルス。有効値は PASSED または FAILED です。
スクリプト プローブの追加 **detail** オプション出力	
Socket state	ソケットの状態
No. Passed states	passed 状態の数
No. Failed states	failed 状態の数

表 4-3　show probe コマンドのフィールドの説明（続き）

フィールド	説明
No. Probes skipped	スキップされたプローブの数プローブがスキップされるのは、プローブを送信するための予定インターバルが、プローブ実行時間よりも短いために、ACE がプローブを送信しない場合です。オープン タイムアウトまたは受信タイムアウト インターバルよりも、送信インターバルが短いことです。 プローブがスキップされる、または **show probe detail** コマンドによって内部エラーが表示されると、プローブの状態は変更されません。失敗すると、failed のままです。
Last status code	直前の終了コード（表 A-7 を参照）
Last disconnect err	スクリプト プローブの終了コード（表 A-7）または内部エラーのメッセージ
Last probe time	直前のプローブのタイムスタンプ
Last fail time	直前の失敗プローブのタイムスタンプ
Last active time	直前のアクティブ時間のタイムスタンプ
Internal error	内部エラー発生回数のカウンタ

表 4-4 に、**show probe** 出力に表示される接続解除エラーを示します。スクリプト プローブの接続解除メッセージのリストについては、表 A-7 を参照してください。

表 4-4　ACE プローブの接続解除エラー

プローブ タイプ	エラー メッセージ
すべてのプローブ タイプ	Unrecognized or invalid probe request
	Connect error
	Connection reset by server
	Connection refused by server
	Authentication failed
	Unrecognized or invalid response
	Out of memory, packets discarded
	Server open timeout (no SYN ACK)
	Server reply timeout (no reply)
	Graceful disconnect timeout (no FIN ACK)
	Received Out-Of-Band data
	User defined Reg-Exp was not found in host response
	Expect status code mismatch
	Received invalid status code

表 4-4　ACE プローブの接続解除エラー（続き）

プローブ タイプ	エラー メッセージ
ICMP	ICMP Internal error
	ICMP Internal error: Write failure
	ICMP Internal error: Received bad FD
	Host Unreachable, no route found to destination
	ARP not resolved for dest-ip (destination IP address)
	Network down
	Egress interface has no ip addr (IP address)
	ICMP Internal error: Data entry being modified
	ICMP Internal error: No space, transmit path is full
	ICMP Host unreachable
	ICMP Dest unreachable
	ICMP Time exceeded
	ICMP Redirect
	Received ICMP Echo Request
	Received ICMP Stale pkt
	Unexpected ICMP pkt type received
	ICMP Pkt received is too short
	ICMP Pkt received is too long
HTTP/HTTPS	MD5 mismatch
HTTPS	Invalid server greeting
	Internal error: Failed to build a server query

表 4-4　ACE プローブの接続解除エラー（続き）

プローブ タイプ	エラー メッセージ
SNMP	Last Disconnect Error: Sum of weights don't add up to max weight value.
	Last Disconnect Error: ASN encoding failed for the configured SNMP OID.
	Last Disconnect Error: Server load hit max value for type percentile.
	Last Disconnect Error: Server load hit max value for type absolute.
	Last Disconnect Error: Server load hit the threshold value.
	Last Disconnect Error: Failed to parse the PDU reply sent by the server.
	Last Disconnect Error: Unrecognized or invalid response

プローブ タイプのグローバル統計情報を表示するには、EXEC モードで **show stats probe type** コマンドを使用します。このコマンドの構文は次のとおりです。

show stats probe type *probe_type*

プローブ タイプのリストを表示するには、次のように入力します。

```
host1/Admin# show stats probe type ?
```

たとえば、すべての DNS プローブのグローバル統計情報を表示するには、次のように入力します。

```
host1/Admin# show stats probe type dns
```

表 4-5 に、**show stats probe type** コマンド出力のフィールドの説明を示します。

表 4-5　show stats probe type コマンドのフィールドの説明

フィールド	説明
Total probes sent	送信されたプローブの総数
Total send failures	送信失敗の総数。失敗の原因は、内部エラーによるものです。
Total probes passed	成功したプローブの総数
Total probes failed	失敗したプローブの総数
Total connect errors	接続エラーの総数
Total conns refused	拒否された接続の総数
Total RST received	受信されたリセットの総数
Total open timeouts	指定されたプローブ タイプのオープン タイムアウトの総数
Total receive timeouts	受信されたタイムアウトの総数

プローブ統計情報の消去

ここでは、各プローブの、またはコンテキスト内のすべてのプローブの統計情報を消去するために使用されるコマンドについて説明します。具体的な内容は次のとおりです。

各プローブの統計情報の消去

特定のプローブに **show probe** コマンドを実行して表示された統計情報を消去するには、EXEC モードで **clear probe** コマンドを使用します。このコマンドの構文は次のとおりです。

clear probe *name*

name 引数は、設定されたプローブの名前です。

たとえば、DNS1 プローブの統計情報を消去するには、次のように入力します。

```
host1/Admin# clear probe DNS1
```

（注） 冗長構成の場合は、アクティブ状態とスタンバイ状態の両方の ACE で、ロードバランシング統計情報を明示的に消去する必要があります。アクティブ状態のアプライアンス上の統計情報を消去しても、スタンバイ状態のアプライアンスの統計情報は古い値のまま残ります。

コンテキスト内のすべてのプローブの統計情報の消去

現在のコンテキスト内のすべてのプローブの統計情報を消去するには、EXEC モードで **clear stats probe** コマンドを使用します。このコマンドの構文は次のとおりです。

clear stats probe

次のように入力します。

```
host1/Admin# clear stats probe
```

（注）　冗長構成の場合は、アクティブ状態とスタンバイ状態の両方の ACE で、ロードバランシング統計情報を明示的に消去する必要があります。アクティブ状態のアプライアンス上の統計情報を消去しても、スタンバイ状態のアプライアンスの統計情報は古い値のまま残ります。

次の作業

Toolkit Command Language（TCL）を使用して、プローブ スクリプトを記述する方法については、付録 A「ACE での TCL スクリプトの使用」を参照してください。スティッキ性（セッションの持続性）を設定する方法については、第 5 章「スティッキ機能の設定」を参照してください。ファイアウォール負荷分散を設定する場合は、第 6 章「ファイアウォール負荷分散の設定」を参照してください。