CHAPTER 3

DM によるガイド付きセットアップの使用

この章では、Cisco Device Manager（DM）によるガイド付きセットアップを使用する方法について説明します。

（注） ACE 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）の名前を付ける際は、1 ～ 64 文字の英数字文字列を入力します。次の特殊文字を含めることができます。下線（_）、ハイフン（-）、ドット（.）、およびアスタリスク（*）。スペースは使用できません。

ACE のアプライアンスで DM を使用しており、ACE CLI で名前付きオブジェクトを設定する場合は、名前付きオブジェクトを設定する際に ACE CLI が使用可能にする特殊文字すべてを DM がサポートするわけではないことに注意してください。DM がサポートしない特殊文字を使用すると、DM を使用して ACE をインポートまたは管理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。

- 「ガイド付きセットアップに関する情報」（P.3-1）
- 「注意事項と制約事項」（P.3-3）
- 「ACE Hardware Setup の使用」（P.3-3）
- 「Virtual Context Setup の使用」（P.3-7）
- 「Application Setup の使用」（P.3-9）

ガイド付きセットアップに関する情報

DM ガイド付きセットアップは、DM と DM が管理するネットワーク デバイスの設定を単純化するために GUI ウィンドウによるガイダンスとネットワーク図によるセットアップ シーケンスを提供します。

ガイド付きセットアップにより、次のタスクをすばやく実行できます。

- スタンドアロンまたはハイ アベイラビリティ（HA）環境のいずれかにネットワーク接続を確立することにより、ネットワークに新しい ACE デバイスを設定します。
- ACE 仮想コンテキストを作成し接続します。
- ACE からバック エンド サーバ グループへのロード バランシング アプリケーションを設定します。

ガイド付きセットアップにアクセスするには、ウィンドウ最上部の [Config] タブをクリックし、次に [Guided Setup] をクリックします。

（注）　ガイド付きセットアップのタスクで使用可能なメニューとオプションは、[Role-Based Access Control (RBAC)] に表示されます。ログイン ユーザに対する正しい権限が管理者によって許可されていない場合は、メニューおよびボタン オプションはグレー表示されます。DM の RBAC の詳細については、「Cisco ACE アプライアンスへのアクセスの制御」（P.15-3）を参照してください。

表 3-1 に、ガイド付きセットアップの個々のタスクと関連トピックを示します。

表 3-1　ガイド付きセットアップのタスクと関連トピック

ガイド付きセットアップのタスク	目的	関連トピック
ACE Hardware Setup	[ACE Hardware Setup] タスクを起動すると、スタンドアロンまたはハイアベイラビリティ（HA）環境のいずれかにネットワーク接続を確立することにより、ネットワークに新しい ACE デバイスを設定できます。	• 「ACE Hardware Setup の使用」（P.3-3） • 「ACE アプライアンス ライセンスの管理」（P.4-29） • 「仮想コンテキストの SNMP 設定」（P.4-19） • 「ポート チャネル インターフェイスの設定」（P.10-2） • 「ギガビット イーサネット インターフェイスの設定」（P.10-5） • 「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10） • 「ハイ アベイラビリティ ピアの設定」（P.11-8）
Virtual Context Setup	[Virtual Context Setup] タスクを起動すると、ACE 仮想コンテキストを作成して接続できます。	• 「Virtual Context Setup の使用」（P.3-7） • 「リソース クラスの管理」（P.4-36） • 「仮想コンテキストの作成」（P.4-2） • 「仮想コンテキストの設定」（P.4-7）
Application Setup	[Application Setup] タスクを起動すると、アプリケーションに適したロードバランシングを設定できます。このタスクでは、サーバのロードバランシングに関して共通する多くの状況に対して、ACE の詳細な設定全体をガイドします。	• 「Application Setup の使用」（P.3-9） • 「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10） • 「仮想コンテキスト BVI インターフェイスの設定」（P.10-24） • 「VLAN インターフェイス NAT プールの設定および NAT 使用率の表示」（P.10-32） • 「ACL を使用したセキュリティの設定」（P.4-60） • 「SSL セットアップ シーケンス」（P.9-5） • 「仮想サーバの設定」（P.5-2）

注意事項と制約事項

ガイド付きセットアップ タスクを実行する際は、次の操作規則を使用してください。

- ステップ間を移動するには、左のメニューの手順の名前をクリックします。
- 各タスクのステップは、後の手順で問題を防止するために設計された順序で示されています。ただし、お使いのアプリケーションに該当しないことがわかっている場合は、手順を省略できます。
- ユーザ権限によっては、DM では、特定の手順で変更を行えないことがあります。
- 各ページを終了する前に保持する変更を保存して導入する必要があります。
- 各タスクは必要な回数だけ実行できます。

ACE Hardware Setup の使用

[ACE Hardware Setup] タスクを使用して、スタンドアロンまたはハイ アベイラビリティ（HA）環境のいずれかにネットワーク接続を確立することにより、ネットワークに新しい ACE デバイスを設定できます。

前提

- ライセンスをインストールすることで、ACE の機能を拡張できます。ACE の機能を拡張する場合は、ACE 用の適切なソフトウェア ライセンス キーを受領していること、ACE のライセンスが ACE にインポートするためにリモート サーバで使用可能であること、またはソフトウェア ライセンス キーを受領していて、ACE の disk0: ファイルシステムに **copy** *path/]filename1* **disk0:** CLI コマンドを使用してライセンス ファイルをコピーしたことを確認してください。

（注）　**copy** *path/]filename1* **disk0:** CLI コマンドの詳細については、『*Administration Guide, Cisco ACE Application Control Engine*』を参照してください。

- ネットワークに新しい ACE デバイスを設定するには、ACE アプライアンスの管理仮想コンテキストに入る必要があります。
- ACE HA ペアを DM にインポートする際、DM が ACE HA ペアを一意に識別できるように、次の設定要件のいずれか 1 つに従う必要があります。
  - DM にインポートされたすべての ACE HA ペアに FT インターフェイス VLAN と FT の IP アドレス/ピア IP アドレスの一意の組み合わせを使用します。HA の場合、FT インターフェイス VLAN と IP アドレス/ピア IP アドレスの組み合わせは、ACE ピア デバイスのすべてのペアに対して常に一意であることが必要です。
  - ピア ACE（モジュールまたはアプライアンス）の管理 IP アドレスを使用して、管理インターフェイスでピア IP アドレスを定義します。管理 IP アドレスと、この定義に使用する管理ピア IP アドレスは、DM に両方の ACE デバイスをインポートするための管理 IP アドレスにする必要があります。

（注）　DM にインポートする HA ペアの使用方法の詳細については、「ACE の冗長性の概要」（P.11-2）を参照してください。

- ACE を設定する際、物理インターフェイス（ギガビット イーサネット ポートまたはポート チャネルなど）を変更すると、DM と ACE 間の接続が失われる可能性があります。管理トラフィックが通過するインターフェイスを変更する場合に、ACE Hardware Setup タスクに従う際は注意してください。

手順

ステップ 1　[Config] > [Guided Setup] > [ACE Hardware Setup] を選択します。

[ACE Hardware Setup] ウィンドウに [Configuration Type] ドロップダウン リストが表示されます。

ステップ 2　[Configuration Type] ドロップダウン リストから、スタンドアロン デバイスまたはハイ アベイラビリティ（HA）ACE ペアのメンバのどちらとして ACE を設定するかを選択します。

- [Standalone] : ACE は、HA 設定で使用されません。
- [HA Secondary] : ACE は、HA 設定のセカンダリ ピアとなります。
- [HA Secondary] : ACE は、HA 設定のプライマリ ピアとなります。

（注）　プライマリ デバイスをセット アップする*前に*、セカンダリ デバイスの ACE Hardware Setup タスクを完了していることを確認します。

ステップ 3　[Start Setup] をクリックします。

[License] ウィンドウが表示されます（[Config] > [Guided Setup] > [ACE Hardware Setup] > [Licenses]）。シスコは、デフォルト コンテキストの数、帯域幅、および SSL TPS（トランザクション / 秒）を向上させる ACE アプライアンスにライセンスを提供します。詳細については、cisco.com の『*Administration Guide, Cisco ACE Application Control Engine*』を参照してください。

この時点でライセンスをインストールする必要がある場合は、ステップ 4 に進みます。

この時点でライセンスをインストールする必要がない場合は、ステップ 5 に進みます。

ステップ 4　1 つまたは複数の ACE ライセンスをインストールします（「ACE アプライアンス ライセンスの管理」（P.4-29）を参照）。

（注）　ACE のプライマリおよびセカンダリ HA ペアに対しては、各 ACE ライセンスは、単一のハードウェア・デバイスに対してのみ有効なため、ライセンスは HA ピア デバイス間で同期されません。プライマリおよびセカンダリ ACE デバイスで各ライセンスの適切なバージョンを個別にインストールする必要があります。

ステップ 5　[ACE Hardware Setup] の [SNMP v2c Read-Only Community String] をクリックします（[Config] > [Guided Setup] > [ACE Hardware Setup] > [SNMP v2c Read-Only Community String]）。

[SNMP v2c Read-Only Community String] ウィンドウが表示されます。

SNMP コミュニティ ストリング（DM によって監視される ACE の要件）を設定するには、次の操作を実行します。

a.　SNMP v2c Read-Only Community String テーブルの最上部にある [Add]（+）をクリックして、SNMP コミュニティ ストリングを作成します。[New SNMP v2c Community] ウィンドウが表示されます。

（注）　DM が ACE を監視するには、管理仮想コンテキストで SNMPv2c コミュニティ ストリングを設定する必要があります。

b. [Read-Only Community] フィールドに、SNMP 読み取り専用コミュニティ ストリングの名前を入力します。有効な入力は、引用符で囲まずスペースを含まない 32 文字以下のテキスト文字列です。

追加の SNMP 設定は、[Config] > [Virtual Contexts] > [context] > [System] > [SNMP] で選択できます。「仮想コンテキストの SNMP 設定」（P.4-19）を参照してください。

ステップ 6　ACE アプライアンスを設定する場合で、ACE アプライアンス で物理ポートをまとめて、ポートチャネルと呼ばれる論理レイヤ 2 インターフェイス（EtherChannels とも呼ばれる）を形成するには、[ACE Hardware Setup] の [Port Channel Interfaces] をクリックします。

[Port Channel Interfaces] ウィンドウが表示されます（[Config] > [Guided Setup] > [ACE Hardware Setup] > [Port Channel Interfaces]）。

（注）　ACE が接続されている ACE アプライアンスとスイッチの両方でポート チャネルを設定する必要があります。

ポート チャネル インターフェイスを設定するには、次の操作を実行します。

a. [Port Channel Interfaces] テーブルの上部にある [Add]（+）をクリックして、ポート チャネル インターフェイスを追加するか、または既存のポート チャネル インターフェイスを選択し [Edit] をクリックして変更します。[New Port Channel Interface] ウィンドウが表示されます。

（注）　[Edit] をクリックしても、すべてのフィールドを変更できるわけではありません。

b. 「ポート チャネル インターフェイスの設定」（P.10-2）の説明に従って、ポート チャネル インターフェイスの属性を入力します。

c. [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。

d. ポートチャネル インターフェイスの統計情報とステータス情報を表示するには、[Port Channel Interfaces] テーブルからインターフェイスを選択して、[Details] をクリックします。**show interface port-channel** CLI コマンドの出力が表示されます。詳細については、「ポート チャネル インターフェイス統計情報およびステータス情報の表示」（P.10-5）を参照してください。

ステップ 7　ACE アプライアンスを設定する場合で、アプライアンスでギガビットイーサネット ポートを 1 つ以上設定するには、[ACE Hardware Setup] で [GigabitEthernet Interfaces] をクリックします。[GigabitEthernet Interfaces] ウィンドウが表示されます（[Config] > [Guided Setup] > [ACE Hardware Setup] > [GigabitEthernet Interfaces]）。

a. 既存のギガビット イーサネット インターフェイスを選択し、[Edit] をクリックして変更します。

b. 「ギガビット イーサネット インターフェイスの設定」（P.10-5）の説明に従って、ギガビット イーサネット物理インターフェイスの属性を入力します。

c. 入力後 [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。

d. 設定する各ギガビット イーサネット インターフェイスについて、ステップ a ～ c を繰り返します。

e. 特定のギガビットイーサネット インターフェイスの統計情報とステータス情報を表示するには、[Gigabit Ethernet Interfaces] テーブルからインターフェイスを選択し、[Details] をクリックします。**show interface gigabitEthernet** CLI コマンドの出力が表示されます。詳細については、「ギガビット イーサネット インターフェイスの統計情報およびステータス情報の表示」（P.10-9）を参照してください。

ステップ 8　ACE が HA ACE ペアのメンバの場合は、[ACE Hardware Setup] で [VLAN Interfaces] をクリックします。

[VLAN Interfaces] ウィンドウが表示されます（[Config] > [Guided Setup] > [ACE Hardware Setup] > [VLAN Interfaces]）。

（注）　HA の設定中、管理接続の損失を防ぐため、管理 VLAN インターフェイスの IP アドレスを HA セットアップ用に正しく設定する必要があります。この手順では、管理 VLAN インターフェイスを選択し、([Edit] ボタンをクリックして)、IP アドレス、エイリアス IP アドレス、およびピア IP アドレスがすべて正しく設定されていることを確認してください。必要な VLAN インターフェイスに対してこのプロセスを繰り返すことができます。HA を確立する前に、管理 VLAN が適切に設定されている場合は、後で他の VLAN を再設定できます。

a. [Add] をクリックして新しい VLAN インターフェイスを追加するか、または既存の VLAN インターフェイスを選択し、[Edit] をクリックして変更します。

（注）　[Edit] をクリックしても、すべてのフィールドを変更できるわけではありません。

b. 「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）の説明に従って、VLAN インターフェイスの属性を入力します。その他の VLAN インターフェイス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、DM は、デフォルトの VLAN インターフェイス属性およびあまり使用されない VLAN インターフェイス属性を非表示にします。

c. [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。

d. VLAN インターフェイスの統計情報とステータス情報を表示するには、[VLAN Interface] テーブルから VLAN インターフェイスを選択し、[Details] をクリックします。**show interface vlan**、**show ipv6 interface vlan**、および **show ipv6 neighbors** CLI コマンドが表示されます。出力を表示するコマンドをクリックします。詳細については、「VLAN インターフェイスの統計情報およびステータス情報の表示」（P.10-23）を参照してください。

ステップ 9　ACE がハイ アベイラビリティ（HA）設定のプライマリ ピアの場合、[ACE Hardware Setup] の [HA Peering] をクリックします（[Config] > [Guided Setup] > [ACE Hardware Setup] > [HA Peering]）。

a. 「ハイ アベイラビリティ ピアの設定」（P.11-8）の説明に従って、[HA Management] セクションの [Edit] をクリックしてプライマリ ACE およびセカンダリ ACE を設定します。2 列あり、1 つは選択した ACE 用、もう 1 つはピア ACE 用です。

次の情報を指定できます。

- HA ペアの 2 つのメンバを特定します。
- ピア ACE に IP アドレスを割り当てます。
- HA ピアに HA VLAN を割り当て、FT VLAN に物理ギガビット イーサネット インターフェイスをバインドします。
- FT VLAN の ACE 上で、ハート ビートの間隔および回数を設定します。

入力後、[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。

b. [ACE HA Group] テーブルの下の [Add] をクリックして、新しいハイ アベイラビリティ グループを追加します。「ハイ アベイラビリティ ピアの設定」（P.11-8）の説明に従って、設定可能なフィールドに情報を入力します。入力後、[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。

HA セットアップが正常に完了した後、[HA State] フィールドに FT VLAN Compatible が表示されます。

（注）　特定の HA グループの統計情報とステータス情報を表示するには、[ACE HA Groups] テーブルからグループを選択して、[Details] をクリックします。**show ft group** *group_id* **detail** CLI コマンドの出力が表示されます。詳細については、「ハイ アベイラビリティ グループの統計情報およびステータス情報の表示」（P.11-16）を参照してください。

ステップ 10　[ACE HA Groups] テーブルの [HA State] フィールドに正常な状態であることが表示されると、ACE はさらに次に示す設定を行う準備ができています。

- 追加の仮想コンテキストを設定するには、引き続き [Virtual Context Setup] タスクを実行し、ACE 仮想コンテキストを作成して接続します。「Virtual Context Setup の使用」（P.3-7）を参照してください。
- 既存の仮想コンテキストでアプリケーションを設定するには、引き続き [Application Setup] タスクを実行し、ACE からバック エンド サーバ グループへのアプリケーションのロードバランシングを設定します。「Application Setup の使用」（P.3-9）を参照してください。

関連トピック

- 「ACE アプライアンス ライセンスの管理」（P.4-29）
- 「仮想コンテキストの SNMP 設定」（P.4-19）
- 「ポート チャネル インターフェイスの設定」（P.10-2）
- 「ギガビット イーサネット インターフェイスの設定」（P.10-5）
- 「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）
- 「ハイ アベイラビリティ ピアの設定」（P.11-8）

Virtual Context Setup の使用

[Virtual Context Setup] タスクを使用して、ACE 仮想コンテキストを作成し接続できます。仮想コンテキストは、仮想化を使用して ACE を複数の仮想デバイスまたはコンテキストに分割します。各コンテキストには、それぞれ独自のポリシー、インターフェイス、リソース、および管理者のセットが含まれています。

はじめる前に

新しいユーザ コンテキストを作成するには、ACE の管理コンテキストに入る必要があります。

手順

ステップ 1　[Config] > [Guided Setup] > [Virtual Context Setup] を選択します。

[Virtual Context Setup] ウィンドウが表示されます。

ステップ 2　[ACE Device] ドロップダウン リストから、ACE を選択します。

ステップ 3　[Start Setup] をクリックします。

[Resource Classes] ウィンドウが表示されます（[Config] > [Guided Setup] > [Virtual Context Setup] > [Resource Classes]）。

リソース クラスを作成または変更するには、次のタスクを実行します。

a. リソース クラスを作成する場合は、[Add]（+）をクリックします。[New Resource Class] 設定ウィンドウが表示されます。「リソース クラスの管理」（P.4-36）の説明に従ってリソース情報を入力します。

b. 既存のリソースを変更する場合は、変更するリソース クラスを選択し、[Edit] をクリックします。[Edit Resource Class] 設定ウィンドウが表示されます。「リソース クラスの管理」（P.4-36）の説明に従ってリソース情報を入力します。

c. エントリを保存して、[Resource Classes] テーブルに戻るには、[OK] をクリックします。

ステップ 5 で必要になるため、使用するリソース クラスを書き留めておきます。

ステップ 4　[Virtual Context Setup] の [Virtual Context Management] をクリックします。

[Virtual Context] ウィンドウが表示されます（[Config] > [Guided Setup] > [Virtual Context Setup] > [Virtual Context Management]）。

仮想コンテキストを作成または変更するには、次の操作を実行します。

a. 仮想コンテキストを作成する場合は、[Add]（+）をクリックします。[New Virtual Context] ウィンドウが表示されます。「仮想コンテキストの設定」（P.4-7）の説明に従って、仮想コンテキストを設定します。

b. 既存の仮想コンテキストを変更する場合は、変更する仮想コンテキストを選択し、[Edit] をクリックします。[Primary Attributes] 設定画面が表示されます。「仮想コンテキスト プライマリ属性の設定」（P.4-11）の説明に従って、この仮想コンテキストのプライマリ属性を入力します。

ステップ 5　入力後、[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。仮想コンテキストを作成または変更する場合は、次の注意事項に従ってください。

- 使用可能な VLAN に仮想コンテキストを接続するには、[Allocated VLANs] フィールドに 1 つ以上の VLAN を指定します。複数の VLAN 値と範囲（「10、14、70-79」など）を指定できます。
- ACE に設定された仮想コンテキストの場合は、このステップで使用されているすべての VLAN をトランクとして設定するか、ポート チャネルまたはギガビット イーサネット インターフェイス上の VLAN にアクセスする必要があります。ACE Hardware Setup タスク中にこれらの VLAN を設定しなかった場合、[ACE Hardware Setup] ウィンドウに戻って、必要な VLAN を設定できます。「ACE Hardware Setup の使用」（P.3-3）を参照してください。
- リソース クラスを仮想コンテキストに指定する場合は、ステップ 3 で作成または指定したリソース クラスを選択します。

（注）　この仮想コンテキスト用に使用するリソース クラスが不明な場合は、[default] を選択します。設定するリソース クラスを後で変更できます。

- HA がこの ACE デバイス用に正しく設定されている場合、[High Availability] チェックボックスがオンになっています。このチェックボックスがオフになっている場合は、チェックボックスをオンにして、DM にこの仮想コンテキストの自動的に同期を設定するよう指示します。

（注）　[High Availability] チェックボックスは、HA のピアリングが ACE のハードウェアについて前に完了している場合にだけ使用できます。

- [Management Settings] で仮想コンテキスト用に個別の管理 VLAN インターフェイスを設定する場合は、この仮想コンテキストの管理インターフェイスを設定し、管理ユーザを作成します。各コンテキストにも、DM GUI を使用してアクセスできる専用の管理 VLAN があります。この場合、管理トラフィックが仮想コンテキストにアクセスできるように、独立した VLAN および IP アドレスを割り当てます。

ステップ 6　仮想コンテキスト用のロードバランシング設定を編集するには、[Application Setup] タスクに進みます。「Application Setup の使用」（P.3-9）を参照してください。

関連トピック

- 「ACE Hardware Setup の使用」（P.3-3）
- 「仮想コンテキストの使用」（P.4-2）
- 「リソース クラスの管理」（P.4-36）
- 「仮想コンテキストの作成」（P.4-2）
- 「仮想コンテキストの設定」（P.4-7）
- 「Application Setup の使用」（P.3-9）

Application Setup の使用

ここでは、次の内容について説明します。

- 「ACE ネットワーク トポロジの概要」（P.3-9）
- 「Application Setup の使用」（P.3-10）

ACE ネットワーク トポロジの概要

ACE の設定に関して、ネットワーク トポロジは、クライアント トラフィックがどの VLAN またはサブネットを通じて ACE に入り、実サーバへ送信されるかを記述しています。ACE ロード バランシング用のネットワーク設定は周囲のトポロジによって異なります。DM にネットワーキング アプリケーションに適したトポロジを指定することで、DM は関連するオプションおよびガイダンスを提示できます。

ネットワーク トポロジは、しばしば既存のネットワーク単独で判断されます。ただし、ACE の展開に向けた目標も関与しています。たとえば、ACE では、クライアントとサーバ間のルータとして機能する場合、クライアントからサーバを効果的に非表示にすることで、あるレベルの保護を提供します。一方、ルーティングしたトポロジが動作するには、これらのサーバをそれぞれ設定して ACE 経由でルーティングを行う必要があり、これはネットワーク ルーティングに対する大幅な変更となることがあります。

また ACE は、クライアントおよびサーバ VLAN をブリッジすることもでき、これはサーバのルーティングに影響を与えません。ただし、ネットワークに VLAN が適切に設定されていることが必要です。

使用するトポロジが不明な場合、またはトポロジをすぐに決定したくない場合は、「ワンアーム」トポロジを使用します。ワンアーム トポロジは通常、既存のネットワークの変更を必要とせず、ネットワークの最小限の情報で設定できます。これにより、ネットワーキング要件に適合するように、ACE ネットワーク トポロジをルーテッド モードまたはブリッジ モードに拡大できます。

図 3-1 に、ワンアーム ネットワーク トポロジを示します。

図 3-1　ワンアーム ネットワーク トポロジの例

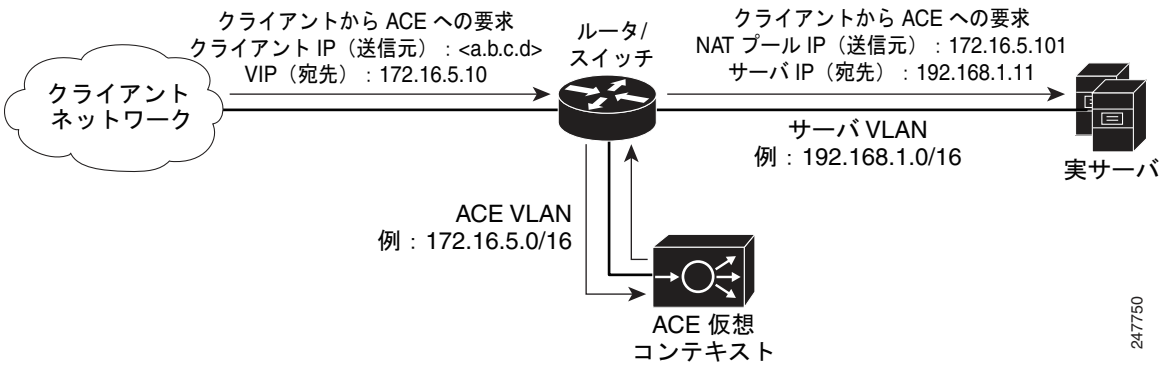
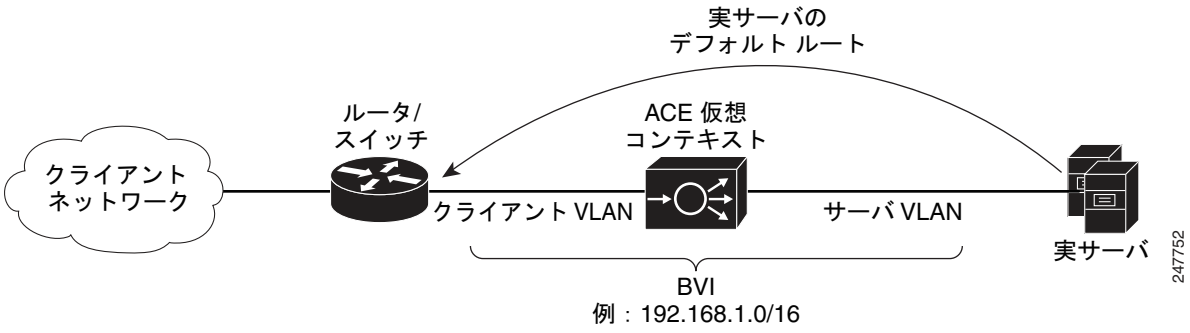


図 3-2 に、ルーテッド モードのネットワーク トポロジを示します。

図 3-2　ルーテッド モードのネットワーク トポロジの例

図 3-3 に、ブリッジ モードのネットワーク トポロジを示します。

図 3-3　ブリッジ モードのネットワーク トポロジの例



Application Setup の使用

[Application Setup] タスクを使用して、アプリケーションのロード バランシングを設定できます。

手順

ステップ 1　[Config] > [Guided Setup] > [Application Setup] を選択します。

[Application Setup] ウィンドウが表示されます。

ステップ 2　[Select Virtual Context] ドロップダウン リストから、既存の ACE 仮想コンテキストを選択します。

ステップ 3　ACE がクライアントまたは実サーバとの通信に HTTPS を使用する場合、[Use HTTPS (SSL)] フィールドで [Yes] を選択して、ACE がセキュア（SSL）ハイパーテキスト転送プロトコル（HTTP）向けに設定する必要があることを指定します。

（注）　HTTPS オプションは ACE NPE ソフトウェア バージョンには適用されません。オプション ボタンは [No] に設定されていて変更できません。詳細については、「ACE No Payload Encryption ソフトウェア バージョン関する情報」（P.1-2）を参照してください。

ステップ 4　ネットワークで選択されている ACE 仮想コンテキストの実サーバに対する関係を反映したネットワーク トポロジを選択します。

トポロジの選択項目には、ワンアーム、ルーテッド、またはブリッジドがあります。ネットワーキング トポロジの背景の詳細については「ACE ネットワーク トポロジの概要」（P.3-9）を参照してください。

ステップ 5　[Start Setup] をクリックします。

ステップ 6　ワンアームまたはルーテッド トポロジを選択した場合は、[VLAN Interfaces] ウィンドウが表示されます（[Config] > [Guided Setup] > [Application Setup] > [VLAN Interfaces]）。

クライアントおよび実サーバと通信するには、VLAN インターフェイスを、送受信が行われるクライアントおよびサーバ トラフィック用に指定する必要があります。

VLAN インターフェイスを設定するには、次の操作を実行します。

a.　[Add] をクリックして新しい VLAN インターフェイスを追加するか、または既存の VLAN インターフェイスを選択し、[Edit] をクリックして変更します。

b.　「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）の説明に従って、VLAN インターフェイスの属性を入力します。その他の VLAN インターフェイス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、DM は、デフォルトの VLAN インターフェイス属性およびあまり使用されない VLAN インターフェイス属性を非表示にします。

（注）　VLAN を定義したら、VLAN 番号を書き留めておきます。この手順の ACL および仮想サーバのステップ（ステップ 9 および 11）でこの VLAN 番号が必要になります。

c.　[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。

d.　VLAN インターフェイスの統計情報とステータス情報を表示するには、[VLAN Interface] テーブルから VLAN インターフェイスを選択し、[Details] をクリックします。**show interface vlan**、**show ipv6 interface vlan**、および **show ipv6 neighbors** CLI コマンドが表示されます。出力を表示するコマンドをクリックします。詳細については、「VLAN インターフェイスの統計情報およびステータス情報の表示」（P.10-23）を参照してください。

ステップ 7　ブリッジド トポロジを選択した場合、[BVI Interfaces] ウィンドウが表示されます（[Config] > [Guided Setup] > [Application Setup] > [BVI Interfaces]）。

BVI インターフェイスを設定するには、次の操作を実行します。

a.　[Add] をクリックして新しい BVI インターフェイスを追加するか、または既存の BVI インターフェイスを選択し、[Edit] をクリックして変更します。

b.　「仮想コンテキスト BVI インターフェイスの設定」（P.10-24）の説明に従って、BVI インターフェイスの属性を入力します。

（注）　BVI を定義したら、クライアント側の VLAN の番号を書き留めておきます。この手順の ACL および仮想サーバのステップ（ステップ 9 および 11）でこの BVI 番号が必要になります。

c. [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。

d. BVI インターフェイスの統計情報とステータス情報を表示するには、[BVI Interface] テーブルから BVI インターフェイスを選択し、[Details] をクリックします。**show interface bvi**、**show ipv6 interface bvi** および **show ipv6 neighbors** CLI コマンドが表示されます。出力を表示するコマンドをクリックします。詳細については、「BVI インターフェイスの統計情報およびステータス情報の表示」（P.10-32）を参照してください。

ステップ 8　ワンアーム トポロジを選択した場合、[Application Setup] の [NAT Pools] をクリックします。

[NAT Pool] ウィンドウが表示されます（[Config] > [Guided Setup] > [Application Setup] > [NAT Pools]）。ワンアーム トポロジを設定するには、実サーバに要求を送信する際に ACE が送信元アドレスとして使用できる IP アドレスのセットを提供する NAT プールが必要です。

（注）　ステップ 6 で設定した VLAN インターフェイスで NAT プールを設定する必要があります。

VLAN 用の NAT プールを作成または変更するには、次の操作を実行します。

a. [Add] をクリックして新しい NAT プール エントリを追加するか、または既存の NAT プール エントリを選択し、[Edit] をクリックして変更します。[NAT Pool] 設定ウィンドウが表示されます。

b. 「VLAN インターフェイス NAT プールの設定および NAT 使用率の表示」（P.10-32）の説明に従って、NAT プール属性を設定します。

（注）　NAT プールを定義したら、NAT プール ID を書き留めておきます。この手順の仮想サーバのステップ（ステップ 11）で NAT プール ID を指定します。

c. [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。

ステップ 9　[Application Setup] で [ACLs] をクリックします。

[ACLs] ウィンドウが表示されます（[Config] > [Guided Setup] > [Application Setup] > [ACLs]）。ACL は、1 つ以上の VLAN インターフェイスに適用されます。各 ACL はエントリのリストで構成され、各リストでは送信元、宛先、送信先と宛先間でのトラフィックを許可または拒否するかを定義しています。

ACL を作成または変更するには、次の操作を実行します。

a. [Add] をクリックして新しい ACL エントリを追加するか、または既存の ACL エントリを選択し、[Edit] をクリックして変更します。[Access List] 設定ウィンドウが表示されます。

b. 「ACL を使用したセキュリティの設定」（P.4-60）の説明に従って、必須フィールドを追加または編集します。

c. [Deploy] をクリックして、この設定を保存します。

d. ACL の統計情報とステータス情報を表示するには、[ACLs] テーブルから ACL を選択し、[Details] をクリックします。**show access-list** *access-list* **detail** CLI コマンドの出力が表示されます。詳細については、「ACL 情報および統計情報の表示」（P.4-72）を参照してください。

ステップ 10　[Application Setup] で [SSL Proxy] をクリックします。

この選択項目は、ACE がクライアントまたは実サーバとの通信に HTTPS を使用することをステップ 3 で指定した場合にだけ表示されます。

[SSL Proxy] ウィンドウが表示されます（[Config] > [Guided Setup] > [Application Setup] > [SSL Proxy]）。

（注） ACE との HTTPS 接続を終了または開始するには、仮想コンテキストに少なくとも 1 つの SSL プロキシ サービスが設定されていることが必要です。SSL プロキシには、クライアントからの HTTPS 接続を終了したり、サーバへの HTTPS 接続の開始に必要な証明書およびキー情報が含まれます。

SSL プロキシ サービスを作成または変更するには、次の操作を実行します。

a. SSL プロキシ サービスを作成するには、[SSL Proxy Setup] をクリックします。

（注） 既存の SSL プロキシ サービスを編集するには、[SSL Proxy] テーブルからサービスを選択し、[Edit] をクリックして SSL プロキシ サービスを変更します。[SSL Proxy Service] 設定ウィンドウが表示されます。「SSL プロキシ サービスの設定」（P.9-28）の説明に従って、必須フィールドを編集します。

b. 「SSL プロキシ サービスの設定」（P.9-28）の説明に従って、必須フィールドを追加します。

c. [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。

ステップ 11　[Application Setup] で [Virtual Server] をクリックします。

[Virtual Servers] ウィンドウが表示されます（[Config] > [Guided Setup] > [Application Setup] > [Virtual Server]）。仮想サーバは、アプリケーションのロードバランシング設定を定義します。

仮想サーバを作成または変更するには、次の操作を実行します。

a. [Add] をクリックして新しい仮想サーバを追加するか、または既存の仮想サーバを選択し、[Edit] をクリックして変更します。[Virtual Server] 設定ウィンドウが表示され、数多くの設定サブセットが表示されます。表示されるサブセットは、[Basic View] または [Advanced View] のいずれを使用しているか、また [Properties] サブセットで行っているエントリによって異なります。設定ペインの上部にある View オブジェクト セレクタを使用して、ビューを変更します。

b. 「仮想サーバの設定手順」（P.5-7）の説明に従って、必要なフィールドを追加または編集します。表 5-1 に、設定情報用の関連項目へのリンクが設定されている、仮想サーバの設定サブセットを示します。

仮想サーバには多数の設定オプションがあります。少なくとも、次の属性を設定する必要があります。

- アプリケーションに VIP、ポート番号（TCP または UDP）、およびアプリケーション プロトコルを設定します。

（注） ACE がクライアント HTTPS 接続を終了する場合は、アプリケーション プロトコルとして [HTTPS] を選択します。

- （ワンアーム トポロジ）VLAN には、ステップ 6 の VLAN を選択します。
- （ルーテッド トポロジ）VLAN には、ステップ 6 のクライアント側 VLAN を選択します。
- （ブリッジド トポロジ）VLAN には、ステップ 6 からクライアント側 VLAN を選択します。

- ACE がクライアント HTTPS 接続を終了する場合は、[SSL Termination] ヘッダーで、ステップ 10 で定義された SSL プロキシを指定します。
- [Default L7 Loadbalancing Action] で、[Loadbalance] に [Primary Action] を設定します。
- このアプリケーションに 1 つまたは複数の実サーバを含むサーバ ファームを作成します（サーバ ファーム属性の設定方法の詳細については、「仮想サーバ レイヤ 7 のロード バランシングの設定」の表 5-10 を参照してください）。
- ACE が実サーバへの HTTPS 接続を開始する場合は、このアプリケーションに対する、開始するための適切な SSL プロキシを [SSL Initiation] の横のメニューから選択します。
- （ワンアーム トポロジ）[NAT] で、ステップ 8 の NAT プール ID を入力します。

基本仮想サーバを設定した後、サーバをテストして設定を検証し、ネットワーキング アプリケーションの問題を切り分けることができます。その後、次のより高度なロード バランシング オプションをネットワーキング アプリケーションに追加できます。

- サーバ ファームへの実サーバの追加。詳細については、「仮想サーバ レイヤ 7 のロード バランシングの設定」セクションの表 5-10 を参照してください。
- 特定のプローブ タイプに対するヘルス モニタリング プローブおよび属性。詳細については、「仮想サーバ レイヤ 7 のロード バランシングの設定」セクションの表 5-11 を参照してください。
- スティッキ機能。この機能により、一致条件が満たされると、コンテンツに対するクライアント要求がスティッキ グループによって処理されます。詳細については、「仮想サーバ レイヤ 7 のロード バランシングの設定」セクションの表 5-13 を参照してください。
- アプリケーション プロトコル インスペクション。この機能により、ACE は、仮想サーバがプロトコル動作を確認し、ACE を通過する不要なまたは悪意のあるトラフィックを特定できるようにします。詳細は「仮想サーバのプロトコル インスペクションの設定」を参照してください。

c. [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。

d. 既存の仮想サーバの統計情報とステータス情報を表示するには、[Virtual Servers] テーブルから仮想サーバを選択し、[Details] をクリックします。**show service-policy global detail** CLI コマンドの出力が表示されます。詳細については、「すべての仮想サーバの表示」（P.5-67）を参照してください。

関連トピック

- 「ACE Hardware Setup の使用」（P.3-3）
- 「Virtual Context Setup の使用」（P.3-7）
- 「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）
- 「仮想コンテキスト BVI インターフェイスの設定」（P.10-24）
- 「仮想コンテキスト スタティック ルートの設定」（P.10-34）
- 「ACL を使用したセキュリティの設定」（P.4-60）
- 「SSL セットアップ シーケンス」（P.9-5）