

## Cisco ACE を使用した Oracle 10g Application Server の展開に関するガイド(バージョン 1.0)

この設計ガイドでは、Oracle 10g Application Server が展開されている環境にシスコの Cisco® Application Control Engine(Cisco ACE)を設定する手順について説明します。このガイドは、シスコと Oracle 社による市場への幅広いソリューション展開の一環として、両社の共同作業によって作成されました。他の製品を組み合わせる場合の設計ガイドおよびその他の関連マニュアルは、シスコおよび Oracle 社から入手できます。



Oracle Application Server 10g は、企業のアプリケーション、ポータル、および Web サービスの開発、統合、および展開向けの包括的なソリューションを提供します。Oracle Application Server 10g は強力な優れたスケーラビリティを持つ Java2 Platform, Enterprise Edition (J2EE) サーバをベースとして、包括的なビジネス統合スイート、ビジネス インテリジェンス スイート、および最適なポータル ソフトウェアを提供します。グリッド コンピューティングおよび Service-Oriented Architecture (SOA; サービス指向アーキテクチャ) のすべてのライフサイクルに対応した Oracle Application Server は、卓越したスケーラビリティ、アベイラビリティ、管理性、およびセキュリティを備えています。Oracle Application Server 10g は [Oracle Fusion Middleware](#) 製品ファミリの 1 つで、迅速な対応、適切な判断、コストの削減、および IT 環境の簡素化を可能にします。

Cisco ACE は、レイヤ 3 およびレイヤ 4 ~ 7 のパケット情報に基づいて、サーバ グループ、サーバ ファーム、ファイアウォール、およびその他のネットワーク デバイス間で高性能な Server Load Balancing (SLB; サーバ ロード バランシング) を実行します。Cisco ACE は Secure Sockets Layer (SSL) で暗号化されたトラフィックを処理することもできます。この機能を使用すると、セキュアなエンドツーエンドの暗号化を使用しながら、インテリジェントなロード バランシングを実行できます。このモジュールは、デフォルトで、4 Gbps の速度のネットワーク接続を実現します。アップグレード ライセンスを購入すれば、8 Gbps の速度を実現することも可能です。Cisco ACE は、高性能かつ豊富な機能を持つ製品として、レイヤ 4 ~ 7 のロード バランシング、TCP 最適化、SSL オフロードなどのアプリケーション アウェアな機能を提供します。

また、Oracle 10g Application Server と Cisco ACE を組み合わせて使用すると、優れたセキュリティ、スケーラビリティ、およびアベイラビリティを備えた企業向けソリューションを実現できます。

2006 年 5 月に、Oracle 社は Cisco ACE と Oracle Application Server 10g の相互運用性に関する検証を行い、シスコが本資料『Cisco ACE を使用した Oracle 10g Application Server の展開に関するガイド(バージョン 1.0)』で検証した内容のとおりであることを確認しました。

## この資料の目的

この資料では、Cisco ACE を使用した Oracle 10g Application Server を導入することによって、Oracle myPortal Enterprise Deployment Architecture を実現するための手順を説明しています。

Oracle myPortal Enterprise Deployment Architecture は、企業ポータルの開発、展開、および管理を行うための包括的な統合型フレームワークを提供します。このソリューションを使用すると、セキュアな情報アクセス、セルフサービス パブリッシング、オンライン コラボレーション、およびプロセスの自動化が可能になり、顧客、パートナー、およびサプライヤとのビジネスのさらなる効率化を実現できます。

この資料に記載されているネットワーク アーキテクチャは、『Oracle Application Server Enterprise Deployment Guide 10g Release 2 (10.1.2) for Windows or UNIX』(Part Number: B13998-03、Oracle 社の OTN サイトで提供)に記載されている Oracle 10g Application Server での myPortal アーキテクチャ構築に必要なすべての機能要件を満たしています。

この資料では、HTTP 圧縮やダイナミック キャッシングなどのアプリケーション最適化テクノロジーについては説明しませんが、これらの機能は、Cisco ACE やその他の製品に搭載された機能を使用すれば容易に統合できます。

## 概要

この資料で説明するアプリケーションおよびネットワーク アーキテクチャの概要は、次のとおりです。

- このネットワーク アーキテクチャは、Oracle myPortal Deployment Architecture に必要なすべての機能要件を満たしています。
- この資料で使用するルータベースのデータセンター ネットワーク アーキテクチャでは、ロード バランシングを行うトラフィックの送信元 Network Address Translation (NAT; ネットワーク アドレス変換) が不要なため、実装および管理が容易です。
- Cisco ACE のブリッジ モード(透過モード)を使用すると、アプリケーションの展開および管理が容易になります。
- Cisco ACE に搭載されたアプリケーション ヘルス チェック、持続性、および調整可能な接続タイムアウト機能を使用すると、ハイ アベイラビリティを実現し、アプリケーション リソースを最適に利用できるようになります。
- この資料では、主要なアプリケーション コンポーネントがそれぞれ個別の階層で使用されています。ただし、複数の階層を特定の展開方式に合わせて 1 つの階層に容易に統合できます。これは、アプリケーション展開における Cisco ACE の柔軟性を示しています。

シスコが検証した Cisco ACE と Oracle Application Server 10g の相互運用性は、2006 年 5 月に Oracle 社によって確認されています。

## 用語および定義

ここでは、この資料の内容に関連する Oracle Application Server および Cisco ACE の用語について説明します。

### Oracle 10g Application Server

この資料で使用される Oracle 10g Application Server の用語は次のとおりです。

APPHOST	ポータル、J2EE アプリケーション、およびキャッシング機能を提供する Oracle アプリケーションサーバ
IDMHOST	アイデンティティ管理(ログイン)機能を提供するアイデンティティ管理サーバ
OIDHOST	Lightweight Directory Access Protocol(LDAP)サービスを稼働する Oracle Internet Directory サーバ。Oracle Identity Management(IDM)ホストや他のコンポーネントと連携して、包括的なアイデンティティ管理機能を提供
APPDBHOST	2 ノード構成の Oracle Real Application Clusters データベースを搭載したアプリケーション データ用サーバ
INFRADBHOST	2 ノード構成の Oracle Real Application Clusters データベースを搭載した Security Metadata Repository 用サーバ
OHS	Oracle HTTP Server
SSO	Single Sign-On(SSO; シングル サインオン)。ユーザが何度もパスワードを入力しなくても、1 回の認証および許可でアクセス権限を持つすべてのアプリケーションにアクセスできるようにするメカニズム
JPDK	Java Portal Development Kit
サービス	HTTP サービスなどの特定の機能を提供する単一のマシン上で稼働するプロセス グループ
階層	複数のサービスをグループ化したもの(複数の物理マシンをまたがる場合もある)。階層は論理的なグループであり、複数のネットワーク セグメント(サブネット)で表される。セグメントでは、(複数の物理マシン上で稼働する)個別のアプリケーションがサブネット単位で使用される。複数のアプリケーションを単一のネットワーク セグメントに統合することも可能

### Cisco ACE

この資料で使用される Cisco ACE の用語は次のとおりです。

ブローブ	ロード バランサが送信するアプリケーション ヘルス チェック
Rserver	実サーバ。Cisco ACE の構成では、物理サーバを表す。
サーバファーム	同一のアプリケーションを実行し、同一のコンテンツを提供する実サーバグループ
スティッキー	「セッションの持続性」ともいう。セッションの期間中、クライアントを同一サーバに固定するメカニズム
VIP	ロード バランシングを行ったアプリケーションのフロントエンドで使用される仮想 IP アドレス

## アプリケーションおよびネットワーク アーキテクチャ

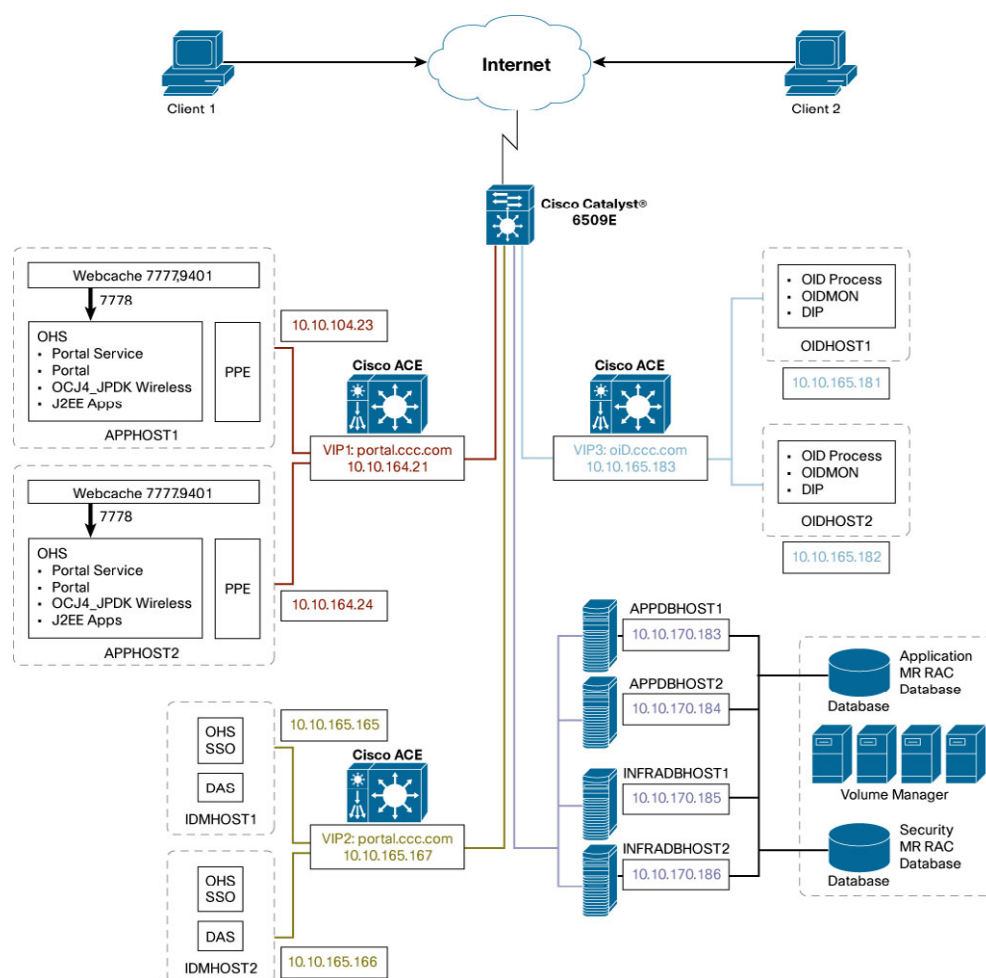
### アーキテクチャの概要

次に、この資料で説明するアプリケーションおよびネットワーク全体のアーキテクチャに関連する重要項目について説明します。

アプリケーション アーキテクチャは、次の 4 つの階層に分割されます。

- **デスクトップ階層** — この階層は、ポータル サイトにアクセスするインターネットまたはイントラネット上のクライアントを表します。クライアント インターフェイスは、Java 対応の Web ブラウザで提供されます。デスクトップ クライアントは、Java アプレットを必要に応じてダウンロードします。図 1 の Client1 および Client2 は、このアーキテクチャのデスクトップ階層です。

図 1 アプリケーションおよびネットワーク全体のアーキテクチャ



- Web 階層** — この階層は、外部（インターネット）および内部のクライアント（企業のクライアントやその他の Oracle アプリケーション製品）から直接アクセスするフロントエンド（Web）環境です。この階層へのアクセスに使用される主な方式は、プレーンテキストの HTTP または SHTTP です。このアーキテクチャでは、Web 階層はポータルおよびアイデンティティ管理（ログイン）の 2 つのネットワーク セグメントです。

ポータル サイト（portal.ccc.com）の機能は、図 1 の APPHOST1 と APPHOST2 によって提供されます。ポータル サイトへのトラフィックに対しては、仮想 IP アドレス 1（VIP1）を使用する Cisco ACE によってロード バランシングが行われます。APPHOST サーバ上では、Webcache サービスと Oracle HTTP Server（OHS）が稼働しています。ポータル サーバはデータベースサーバともコミュニケーションを行います。

アイデンティティ管理（ログイン）の機能は、図 1 の IDMHOST1 と IDMHOST2 によって提供されます。アイデンティティ管理サービスへのトラフィックに対しては、VIP2 を使用する Cisco ACE によってロード バランシングが行われます。IDM ホスト上では、OHS や Stateful Switchover などのアプリケーションレベルのサービスが実行されています。アイデンティティ管理サーバは、ログイン機能を実行するために、Oracle Internet Directory（OID）サービスやデータベースサーバともコミュニケーションを行います。

APPHOST(ポータル)および IDMHOST(ログイン)のフローの詳細については、この資料の後半で説明します。

**注:**この資料では、ポータル機能とログイン機能が異なるネットワーク セグメントに展開されていますが、これらの機能は必要に応じて単一のネットワーク セグメントに統合することもできます。また、Web 機能とアプリケーション機能を異なるセグメントに分離するアーキテクチャ構成もあります。

- **アプリケーション階層** — この階層には、OID サーバ(OIDHOST1 と OIDHOST2)があります。このアーキテクチャでは、OID サーバ上で LDAP サービスが稼働しています。デスクトップ階層のインターネット クライアントは、直接 OID サービスにアクセスすることはありません。OID サービスにアクセスするのは、Web 階層の IDMHOST やデータベース階層のデータベース サーバなどの他の階層にあるホストです。OID サービスへのトラフィックに対しては、VIP3 を使用する Cisco ACE によってロード バランシングが行われます。
- **データベース階層** — この階層には、myPortal アプリケーションで管理されるすべてのデータを格納するデータベース サーバがあります。一般的に、外部クライアントはデータベース サーバと直接コミュニケーションを行いませんが、アプリケーション階層や Web 階層のサーバは、特定のクライアント要求を処理するために、データベース サーバとのコミュニケーションを行います。この構成の場合、データベース サーバへのトラフィックには Cisco ACE によってロード バランシングが行われないため、データベース サーバは Cisco ACE の後方には配置されていません。データベースのハイ アベイラビリティとロード バランシングを実現するには、Oracle Resource Availability Confirmation(RAC)を実装します。この階層には、APPDBHOST1、APPDBHOST2、INFRADBHOST1、および INFRADBHOST2 のホストがあります。

## アプリケーションのフロー

### APPHOST(ポータル)のフロー

次のフローは、アプリケーション サーバスイートの APPHOST スイートに関連しています。

#### 1. クライアントからポータルの VIP へ

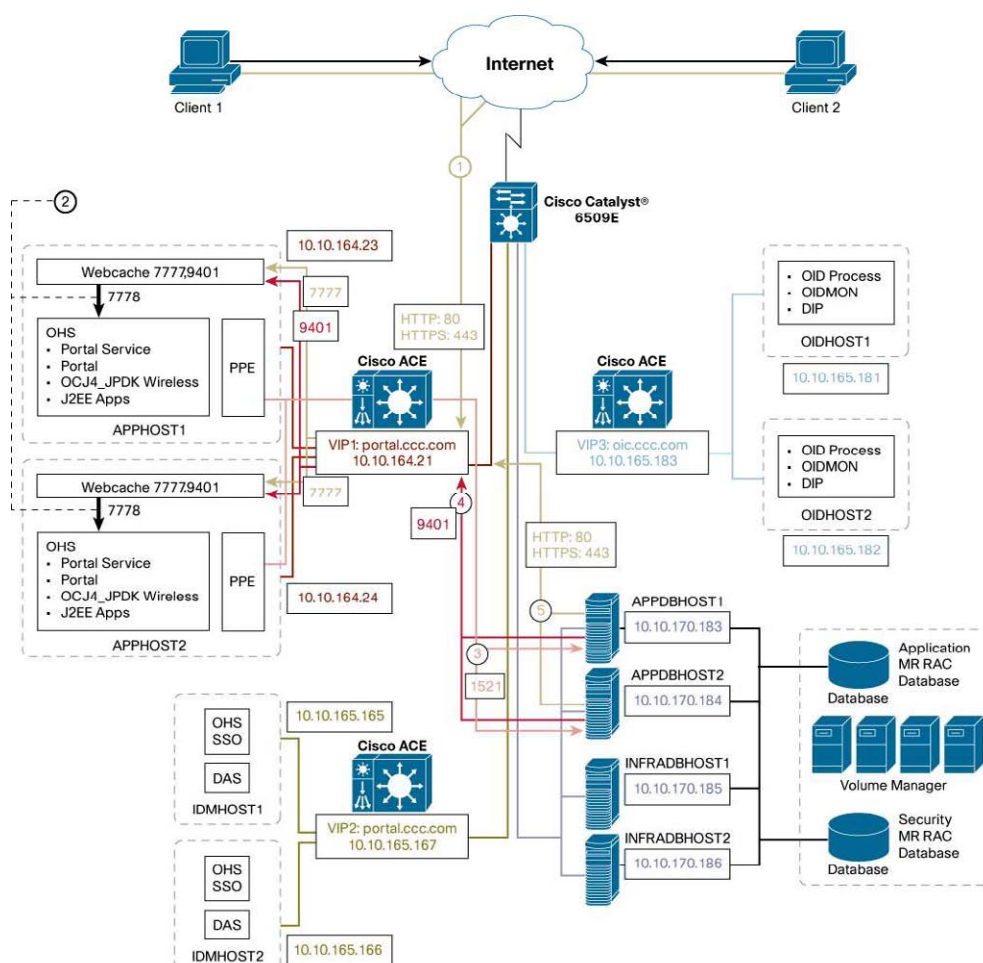
インターネット上のクライアントが、Cisco ACE で VIP1(10.10.164.21)として設定されている <http://portal.ccc.com>(ポート 80)または <https://portal.ccc.com>(ポート 443)にアクセスします。

Cisco ACE は、APPHOST1 または APPHOST2 のいずれかで稼働する有効な Webcache サーバの 1 つに対し、要求のロード バランシングを行います。Cisco ACE は要求のロード バランシングの際に、宛先 TCP ポート(80 または 443)をポート 7777(Webcache サーバのリスニング ポート)に変換します。

このフローでは、Cisco ACE 上でクライアントの送信元 IP アドレスまたは HTTP クッキーに基づくセッションの持続性(スティッキー)を設定することを推奨します。

このフローは、図 2 の①(ライト グリーン)で示されます。

図 2 APPHOST(ポータル)のフロー



## 2. Webcache サーバから OHS へ

このトポロジでは、Webcache サーバと OHS の両方が同じ APPHOST サーバ上で稼働しています。Webcache サーバは、TCP ポート 7778 で OHS と接続されます。

このフローは、ループバック アドレスを使用する一般的な Webcache サーバ構成では APPHOST サーバの内部で処理されるため、ネットワークを横断することはありません。

この構成の場合、このフローへのロード バランシングは行われません。

このフローは、図 2 の②(ブラック)で示されます。

## 3. APPHOST から APPDBHOST サーバへ

APPHOST1 と APPHOST2 は、データベース サーバ(APPDBHOST1 または APPDBHOST2) に対してデータベース クエリを実行します。このトポロジの場合、この接続はデータベース サーバ上で稼働する宛先 TCP ポート 1521(Oracle 社の SQL\*NET または NET8)を使って確立されます。構成によっては、このポートが別の TCP ポートにカスタマイズされます。

この要求はネットワークを横断し、Cisco ACE およびネットワーク上のルータを介してルーティングされます。

このフローは、図 2 の③(ピンク)で示されます。

#### 4. データベースから Webcache への失効メッセージ

Oracle Application Server Portal Repository(このトポロジでのデータベース サーバ)は、Oracle Application Server Webcache にキャッシュされているコンテンツの有効期限が切れると、Webcache サーバに失効メッセージを送信します。

Webcache サーバは、TCP ポート 9401 でこのメッセージを待ち受けます。

この要求は、APPDBHOST が TCP ポート 9401 を介して Cisco ACE 上の VIP アドレス (10.10.164.21)に実行する HTTP 要求です。

Cisco ACE は、APPHOST1 または APPHOST2 のいずれかで稼働する有効な Webcache サーバの 1 つに対し、要求のロード バランシングを行います。

このフローは、図 2 の④(レッド)で示されます。

#### 5. JPKD プロバイダー登録 (APPDBHOST からポータルへ)

このフローは、データベース ホスト APPDBHOST1 および APPDBHOST2 から開始されること以外は、フロー 1 と同じです。ロード バランサを使用する中間階層を複数持つ構成では、ロード バランサ ルータの URL を使用してすべての JPKD アプリケーションを登録する必要があります。

データベース ホスト (APPDBHOST 1 または APPDBHOST2)は、<http://portal.ccc.com/<webApp>/providers/<providername>> (ポート 80)としてポータルにアクセスできます。portal.ccc.com は、Cisco ACE 上の VIP1(10.10.164.21)として設定されます。

Cisco ACE は、有効なアプリケーション ホスト (APPHOST1 または APPHOST2)のいずれかに対し、要求のロード バランシングを行います。Cisco ACE は要求のロード バランシングの際に、宛先 TCP ポート(80 または 443)をポート 7777 (APPHOST のリスニング ポート)に変換します。

このフローでは、Cisco ACE 上でクライアントの送信元 IP アドレスまたは HTTP クッキーに基づく持続性(スティッキー)を設定することを推奨します。

このフローは、図 2 の⑤(ライト グリーン)で示されます。

#### IDMHOST(ログイン)のフロー

##### 6. クライアントからログインへ

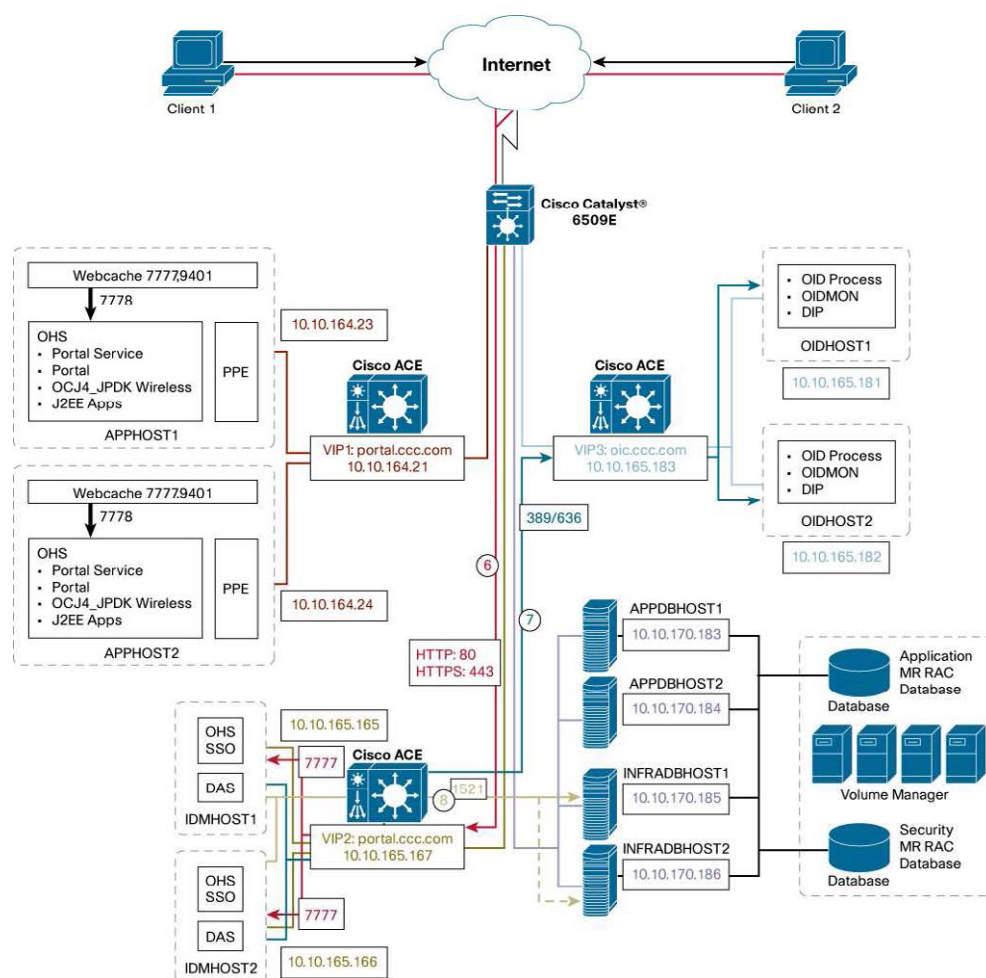
(インターネット上の)クライアントの認証が完了していない場合、クライアントは <http://login.ccc.com> (ポート 80)または <https://logic.ccc.com> (ポート 443)としてアイデンティティ管理サーバにリダイレクトされます。この接続は、Cisco ACE 上の VIP2(10.10.165.167)に対して確立されます。

Cisco ACE は、有効なアイデンティティ管理ホスト (IDMHOST1 または IDMHOST2)のいずれかに対し、要求のロード バランシングを行います。Cisco ACE は要求のロード バランシングの際に、宛先 TCP ポート(80 または 443)をポート 7777 (IDMHOST のリスニング ポート)に変換します。

このフローでは、Cisco ACE 上でクライアントの送信元 IP アドレスまたは HTTP クッキーに基づく持続性(スティッキー)を設定することを推奨します。

このフローは、図 3 の⑥(レッド)で示されます。

図 3 IDMHOST(ログイン)のフロー



## 7. アイデンティティ管理ホスト(IDMHOST)からOIDへ

アイデンティティ管理ホスト(IDMHOST1 または IDMHOST2)は、oid.ccc.com として OID サービスにアクセスします。oid.ccc.com は Cisco ACE 上で VIP3(10.10.165.183)として設定されています。この要求は、TCP ポート 389(セキュア LDAP を使用する場合は 636)を介した LDAP 要求です。

Cisco ACE は、有効な OID ホスト(OIDHOST1 または OIDHOST2)のいずれかに対し、要求のロード バランシングを行います。

このフローは、図 3 の⑦(シアン)で示されます。

## 8. アイデンティティ管理ホスト(IDMHOST)からデータベースサーバへ

IDMHOST1 と IDMHOST2 は、データベースサーバ(INFRADBHOST1 または INFRADBHOST2)に対してデータベース クエリーを実行します。このトポロジの場合、この接続はデータベースサーバ上で稼働する宛先 TCP ポート 1521(Oracle 社の SQL\*NET または NET8)を使って確立されます。構成によっては、このポートが別の TCP ポートにカスタマイズされます。

この要求はネットワークを横断し、Cisco ACE およびネットワーク上のルータを介してルーティングされます。

このフローは、図 3 の⑧(ライト グリーン)で示されます。

## OIDHOST(LDAP)のフロー

次のフローは、アプリケーション サーバサイトの APPHOST スイートに関連しています。

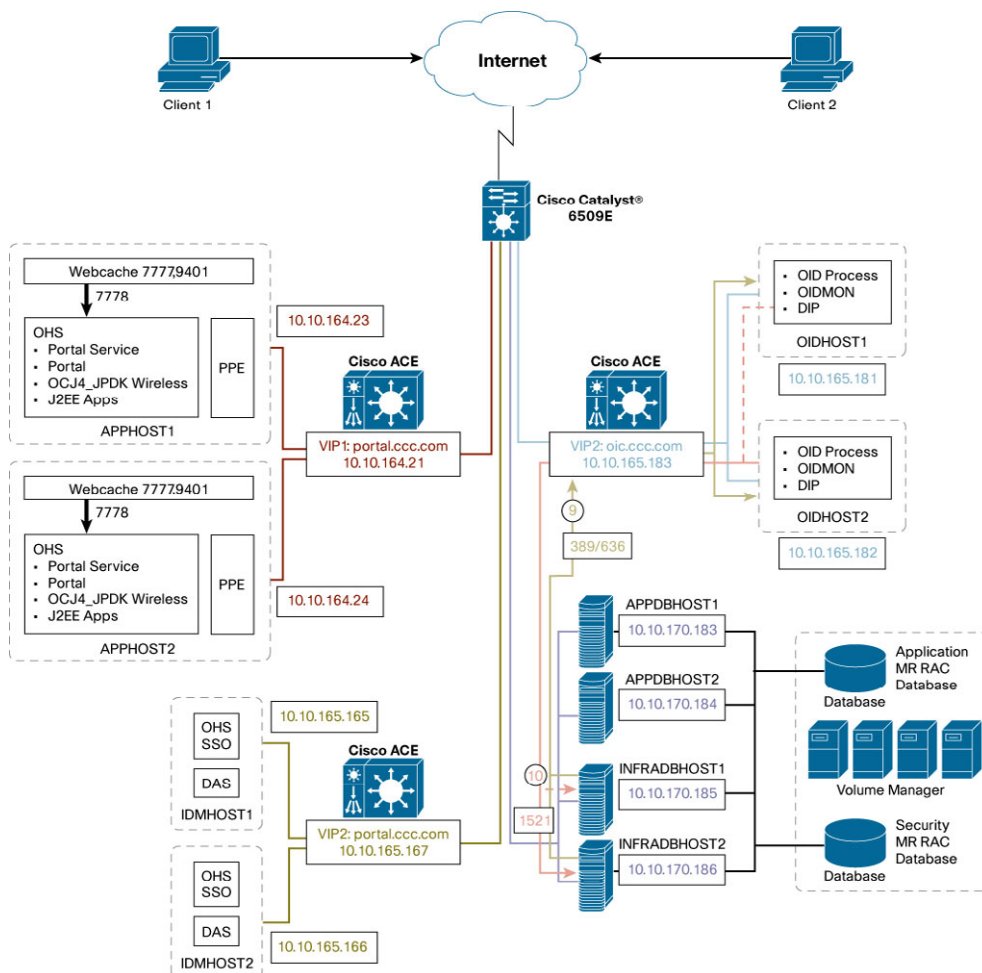
### 9. データベース ホスト(INFRADBHOST)から OID へ

データベース ホスト(INFRADBHOST1 または INFRADBHOST2)は、oid.ccc.com として OID サービスにアクセスします。oid.ccc.com は Cisco ACE 上で VIP3(10.10.165.183)として設定されています。この要求は、TCP ポート 389(セキュア LDAP を使用する場合は 636)を介した LDAP 要求です。

Cisco ACE は、有効な OID ホスト(OIDHOST1 または OIDHOST2)のいずれかに対し、要求のロード バランシングを行います。

このフローは、図 4 の⑨(ライト グリーン)で示されます。

図 4 OIDHOST(LDAP)のフロー



### 10. OIDHOST からデータベース サーバへ

OIDHOST1 と OIDHOST2 は、データベース サーバ(INFRADBHOST1 または INFRADBHOST2)に対してデータベース クエリーを実行します。このトポロジの場合、この接続はデータベース サーバ上で稼働する宛先 TCP ポート 1521(Oracle 社の SQL\*NET または NET8)を使って確立されます。構成によっては、このポートが別の TCP ポートにカスタマイズされます。

この要求はネットワークを横断し、Cisco ACE およびネットワーク上のルータを介してルーティングされます。

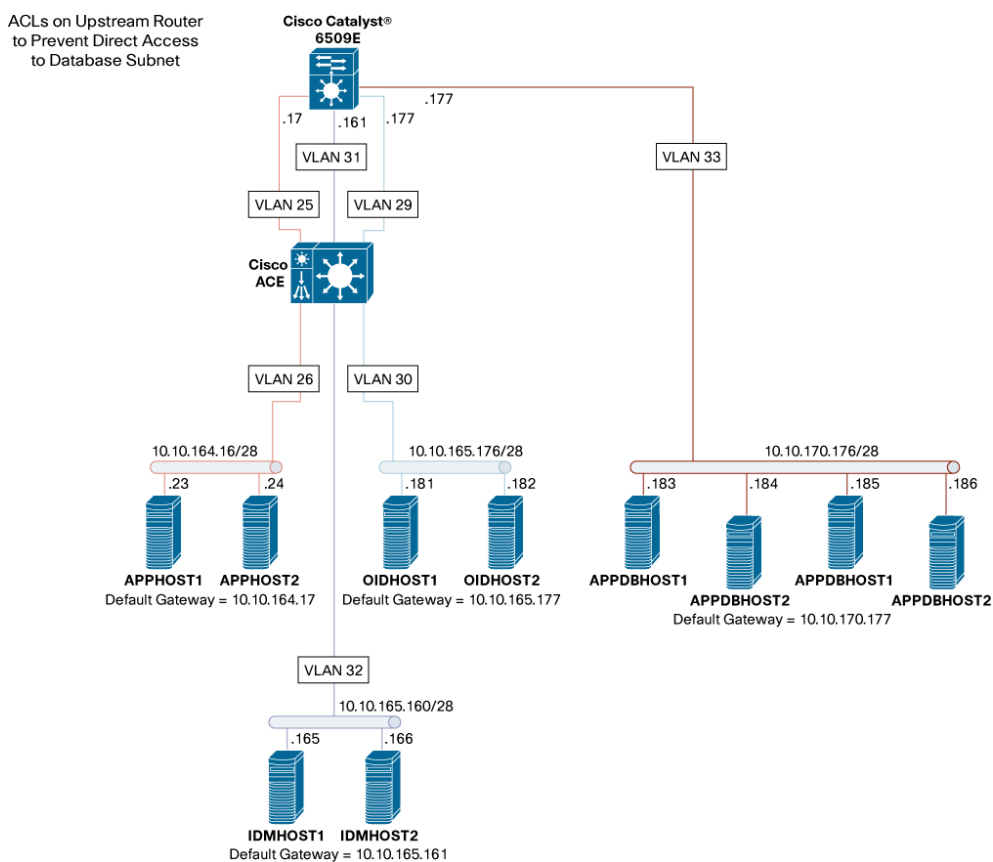
このフローは、図 4 の⑩(ピンク)で示されます。

## ネットワークの設計と構成

### ネットワークトポロジおよび設計上の機能

図 5 の論理ネットワークのトポロジ図は、Cisco ACE モジュールの導入例を示しています。Cisco ACE は、VLAN 間でトラフィックを単純にブリッジするブリッジド モードで動作しています。VLAN 間のルーティングは、上流のルータで実行されます。

図 5 詳細なネットワークトポロジ



以下に、ネットワーク設計の主な特徴の一部を示します。

1. Cisco ACE の内部 VLAN インターフェイスをルーテッド モードではなくブリッジド モードで設定
  - このネットワーク設計では、Cisco ACE モジュールはシンプルな構成モデルであるブリッジド モードで展開されています。
  - このモードの場合、Cisco ACE は 2 つの VLAN 間のブリッジとして動作し、VIP アドレス宛てのトラフィックに対するロード バランシングを実行します。
  - 各 VLAN のペアはスイッチ上に設定されていますが、クライアント側の VLAN だけが上流のルータ上に IP アドレスを持っています。

- サーバのデフォルト ゲートウェイは、各クライアント側 VLAN に対応した上流のルータ(Hot Standby Router Protocol [HSRP])の IP アドレスにアクセスするよう設定されています。
  - セキュリティ ポリシーで許可された場合は、サーバへの直接アクセスが可能です。
2. 複数のサブネットを使用したサーバのセグメント化
    - サーバは機能グループごとに専用の IP サブネット上に配置されています。
    - このセグメント化により、類似機能ごとに論理グループを構成し、将来的な拡張に容易に対応することができます。
  3. 上流のルータおよび Cisco ACE モジュールによるセキュリティの確保
    - 上流のルータ上のアクセス リストでは、Cisco ACE やサーバに直接到達させるべきトラフィックを許可します。
    - 上流のルータ上のアクセス リストでは、データベース サーバへの直接アクセスを禁止する設定になっています。
    - Cisco ACE モジュールのアクセス リストでは、アプリケーション ポート上の VIP へのアクセスを許可する設定になっています。
  4. Cisco ACE モジュールによるポート変換処理
    - Cisco ACE は、ポート 80 または 443 上の VIP1 および VIP2 宛てのトラフィックをアプリケーション ポート(7777)に変換します。
  5. Cisco ACE モジュール上での SSL ターミネーションの設定
    - SSL トラフィック(ポート 443)は Cisco ACE モジュールで終端します。Cisco ACE モジュールは Webcache サービス ポート(7777)上のアプリケーション サーバにクリアテキストのトラフィックを送信します。
    - このトランザクションでは、クライアントの送信元 IP アドレスが維持されます。
    - Cisco ACE は、最大で毎秒 1000 の SSL トランザクションをデフォルトで処理できます。さらに高いパフォーマンス要件に対応する場合は、Cisco ACE に追加ライセンスをインストールする必要があります。

## サーバの設定

表 1 は、このアーキテクチャで使用されるサーバの情報を示しています。

表 1 サーバ情報

サーバ名	IP アドレス	サブネット マスク	機能	外部リスニング ポート
APPHOST1	10.10.164.23	255.255.255.240	Webcache および OHS サーバ 1	7777 および 9401
APPHOST2	10.10.164.24	255.255.255.240	Webcache および OHS サーバ 1	7777 および 9401
IDMHOST1	10.10.165.165	255.255.255.240	アイデンティティ管理サーバ 1	7777
IDMHOST2	10.10.165.166	255.255.255.240	アイデンティティ管理サーバ 2	7777
OIDHOST1	10.10.165.181	255.255.255.240	Oracle Internet Directory Server 1	389/636
OIDHOST2	10.10.165.182	255.255.255.240	Oracle Internet Directory Server 2	389/636
APPDBHOST1	10.10.170.183	255.255.255.240	アプリケーション メタデータ リポジトリ用のデータベース サーバ 1	1521
APPDBHOST1	10.10.170.184	255.255.255.240	アプリケーション メタデータ リポジトリ用のデータベース サーバ 2	1521
INFRADBHOST1	10.10.170.185	255.255.255.240	セキュリティ メタデータ リポジトリ用のデータベース サーバ 1	1521
INFRADBHOST2	10.10.170.186	255.255.255.240	セキュリティ メタデータ リポジトリ用のデータベース サーバ 2	1521

**注:** 表 1 の外部リスニング ポートは、この資料で説明したフローで使用されるもののみ記載されています。また、各アプリケーション サーバでは、他のポートを管理者アクセス用に使用している場合もあります。アクセス リストの設定では、これらのポートも適切に許可する必要があります。詳細については、Oracle 社のマニュアルを参照してください。

### Oracle 10g Application Server の設定

外部のハードウェア ロード バランサおよび外部の SSL ターミネーション デバイスを使用して Oracle アプリケーション サーバを設定する手順については、『Oracle Application Server Enterprise Deployment Guide 10g Release 2 (10.1.2) for Windows or UNIX』(Part Number: B13998-03、Oracle 社の OTN サイトで提供)の Chapter 4「Configuring the Application Infrastructure for myPortalCompany.com」および Appendix A「Sample Configurations for Certified Load Balancers」を参照してください。

### ルータの設定

Cisco ACE は、ディストリビューション レイヤである Cisco Catalyst® 6509E スイッチ シャーシに搭載します。このシャーシに搭載された Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード)モジュールは、Cisco ACE に対する上流のルータとしても機能します。

#### 上流のルータ(MSFC)の設定手順

この構成で上流のルータを使用するには、次の設定手順を実行する必要があります。

#### ステップ 1 Cisco ACE VLAN とデータベース サーバ VLAN を追加します。

このトポロジの場合は、6 つの Cisco ACE VLAN と 1 つのデータベース サーバ VLAN (合計 7 つの VLAN)を MSFC に以下のように追加する必要があります。

```
vlan 25
  name ACE-APP-CLIENT:10.10.164.16/28
  !
vlan 26
  name ACE-APP-SERVER
  !
vlan 31
  name ACE-IDM-CLIENT:10.10.165.160/28
  !
vlan 32
  name ACE-IDM-SERVER
  !
vlan 29
  name ACE-OID-CLIENT:10.10.165.176/28
  !
vlan 30
  name ACE-OID-SERVER
  !
vlan 33
  name ACE-DB-SERVERIDM:10.10.170.176/28
  !
```

**注:** 定義された名前は説明目的でのみ使用されています。名前は組織の命名規則に従って設定してください。

**ステップ 2** Cisco ACE への VLAN トラフィックを許可します。

Cisco Catalyst 6509E スイッチで Cisco ACE への VLAN アクセスが明確に許可されている場合を除いて、Cisco ACE は VLAN トラフィックを受け入れません。この場合、すべての VLAN に対し ACE へのアクセスが許可されないため、ACE 以外の VLAN 上のブロードキャスト ストームが ACE に影響を与えることはありません。この構成では、Cisco ACE は Cisco Catalyst 6509E シャーシのスロット 4 に搭載されています。Cisco ACE 固有の VLAN トラフィックを Cisco ACE にリダイレクトできるようにするには、次の設定を追加する必要があります。

```
svclc multiple-vlan-interfaces
svclc module 4 vlan-group 11
svclc vlan-group 11 25,26,29,30,31,32,33
```

**ステップ 3** Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) (インターフェイス VLAN) を設定します。

SVI の設定では、ルータ (MSFC) 上のレイヤ 3 インスタンスを定義します。この構成では、Cisco ACE のクライアント側 VLAN に 3 つ、データベース サーバ側 VLAN に 1 つの、合計 4 つの SVI を設定する必要があります。

Cisco ACE のクライアント側 VLAN の SVI の設定は、次のとおりです。

```
interface Vlan25
description ACE-APPSRV-Client-Side
ip address 10.10.164.17 255.255.255.240
no ip redirects
no ip proxy-arp
!
```

**注:** この IP アドレスは、APPHOST サーバおよび Cisco ACE のデフォルト ゲートウェイとして使用されます。冗長構成の場合は、この IP アドレスを HSRP アドレスとして設定します。設定例については、次の URL から Cisco HSRP の設定ガイドを参照してください。

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies\\_tech\\_note09186a0080094afd.shtml#topic1](http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml#topic1)

自動翻訳:

<http://www.cisco.com/support/ja/473/62.shtml#topic1>

```
interface Vlan31
description ACE-IDMSRV-Client-Side
ip address 10.10.165.171 255.255.255.240
no ip redirects
no ip proxy-arp
!
```

**注:** この IP アドレスは、IDMHOST サーバおよび Cisco ACE のデフォルト ゲートウェイとして使用されます。冗長構成の場合は、この IP アドレスを HSRP アドレスとして設定します。設定例については、次の URL から Cisco HSRP の設定ガイドを参照してください。

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies\\_tech\\_note09186a0080094afd.shtml#topic1](http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml#topic1)

自動翻訳:

<http://www.cisco.com/support/ja/473/62.shtml#topic1>

```
interface Vlan29
  description ACE-OIDSRV-Client-Side
  ip address 10.10.165.177 255.255.255.240
  no ip redirects
  no ip proxy-arp
!
```

**注:** この IP アドレスは、OIDHOST サーバおよび Cisco ACE のデフォルト ゲートウェイとして使用されます。冗長構成の場合は、この IP アドレスを HSRP アドレスとして設定します。設定例については、次の URL から Cisco HSRP の設定ガイドを参照してください。

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies\\_tech\\_note09186a0080094afd.shtml#topic1](http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml#topic1)

自動翻訳:

<http://www.cisco.com/support/ja/473/62.shtml#topic1>

データベース サーバ VLAN の SVI の設定は、次のとおりです。

```
interface Vlan33
  description ACE-DBSRV-Client-Side
  ip address 10.10.170.177 255.255.255.240
  no ip redirects
  no ip proxy-arp
!
```

**注:** この IP アドレスは、データベース サーバのデフォルト ゲートウェイとして使用されます。冗長構成の場合は、この IP アドレスを HSRP アドレスとして設定します。設定例については、次の URL から Cisco HSRP の設定ガイドを参照してください。

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies\\_tech\\_note09186a0080094afd.shtml#topic1](http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml#topic1)

自動翻訳:

<http://www.cisco.com/support/ja/473/62.shtml#topic1>

## Cisco ACE の設定

表 2 は、このアーキテクチャで使用される Cisco ACE の情報を示しています。

表 2 Cisco ACE

ホスト	VIP アドレスおよびポート	関連付けられるサーバ	サーバポート	ヘルス チェックメカニズム	TCP 最適化の適用
portal.ccc.com:80	10.10.164.21:80	10.10.164.23 10.10.164.24	7777 7777	HTTP	可
portal.ccc.com:443	10.10.164.21:443	10.10.164.23 10.10.164.24	7777 7777	HTTP	可
portal.ccc.com:9401	10.10.164.21:9401	10.10.164.23 10.10.164.24	9401 9401	HTTP	可
login.ccc.com:80	10.10.165.167:80	10.10.165.165	7777	HTTP	可
login.ccc.com:443	10.10.165.167:443	10.10.165.166	7777	HTTP	可
oid.ccc.com:389/636	10.10.165.183:389/636	10.10.165.181 10.10.165.182	389/636 389/636	TCP TCP	不可

### Cisco ACE の設定手順

Cisco ACE の設定手順は、次のとおりです。トポロジと設定手順の関連性を確認する場合は、図 5 を参照してください。

#### ステップ 1 管理アクセスの設定

Telnet、Secure Shell (SSH; セキュア シェル) プロトコル、SNMP (簡易ネットワーク管理プロトコル)、HTTP、または HTTPS を使用して Cisco ACE モジュールにリモート アクセスする場合や、Cisco ACE モジュールへの Internet Control Management Protocol (ICMP) アクセスを実現する場合は、ポリシーを定義したうえでアクセス用インターフェイスに適用する必要があります。

次の設定手順を実行します。

1. *management* タイプのクラス マップを設定します。

```
class-map type management match-any remote-access
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any      Needed if Extensible Markup
Language (XML) interface access is
  50 match protocol https any      needed through HTTP(S)
```

2. *management* タイプのポリシー マップを設定します。

```
policy-map type management first-match everyone
  class remote-access
    permit
```

3. VLAN インターフェイスにポリシー マップを適用します。

```
interface vlan 25
  service-policy input everyone
```

```
interface vlan 26
  service-policy input everyone
```

```
interface vlan 29
  service-policy input everyone

interface vlan 30
  service-policy input everyone

interface vlan 31
  service-policy input everyone

interface vlan 32
  service-policy input everyone
```

## ステップ 2 プローブの設定

Cisco ACE は有効なキープアライブ方式の 1 つであるプローブを使用して、実サーバの可用性を確認します。Cisco ACE では異なるタイプのプローブを設定できます。この構成の HTTP ベースのアプリケーション (PORTAL [TCP ポート 7777 および 9401] および LOGIN) には、HTTP タイプのプローブを使用します。この構成の HTTP ベース以外のアプリケーション (OID) には、TCP タイプのプローブを使用します。

この構成では、次のプローブを使用します。

```
probe http ACECFG-http
  port 7777
  interval 30
  passdetect interval 10
  request method head url /test.html      This can be another URI
  based on the server configuration
  expect status 200 202

probe http ACEINV-http
  port 9401
  interval 30
  passdetect interval 10
  request method head url /test.html      This can be another URI
  based on the server configuration
  expect status 200 202
probe tcp OID-probe
  port 389
  interval 30
  passdetect interval 10
```

## ステップ 3 Rserver の設定

ロード バランサは、一定の基準に基づいて、目的のトラフィックを送信するための「実サーバ」 (Rserver) を選択します。Rserver を設定する際には、実サーバ名の大文字と小文字が区別されることに注意してください。Rserver を設定する場合は、少なくとも、IP アドレスを設定して Rserver をインサービスにする必要があります。

この構成では、次の Rserver を使用します。

```
rserver host aceapp1
  ip address 10.10.164.23
  inservice
rserver host aceapp2
  ip address 10.10.164.24
  inservice

rserver host aceidm1
  ip address 10.10.165.165
  inservice
rserver host aceidm2
  ip address 10.10.165.166
  inservice

rserver host aceoid1
  ip address 10.10.165.181
  inservice
rserver host aceoid2
  ip address 10.10.165.182
  inservice
```

#### ステップ 4 サーバファームの設定

サーバ ファームは、ロード バランサが一定の基準に基づいて選択する実サーバの論理的集合です。実サーバと同様に、サーバ ファームの名前も大文字と小文字が区別されます。基本的なサーバファームの設定では、サーバファームに実サーバとプローブを追加します。

この構成では、次のサーバファームを設定します。

```
serverfarm host aceapp
  probe ACECFG-http
  rserver aceapp1 7777
  inservice
  rserver aceapp2 7777
  inservice

serverfarm host aceinv
  probe ACEINV-http
  rserver aceapp1 9401
  inservice
  rserver aceapp2 9401
  inservice

serverfarm host aceidm
  probe ACECFG-http
  rserver aceidm1 7777
  inservice
  rserver aceidm2 7777
  inservice

serverfarm host aceoid
  probe OID-probe
```



3. CSR 要求を Certificate Authority (CA; 認証局) に転送して CA の署名を受けます。
4. CA によって署名された証明書を Cisco ACE にロードします。

Cisco ACE に証明書をインポートする場合の構文:

```
crypto import [non-exportable] [ ftp | sftp | tftp | terminal ]
[passphrase:passphrase] [ipaddr] [username] [password]
[remote_filename] [local_filename]
```

5. 必要に応じて、チェーン グループを使用して証明書をチェーン化します。  
証明書チェーンは、チェーン グループに含まれる証明書と設定済み証明書で構成されます。

```
crypto chaingroup CCCSSLCA-group
cert CCCSSLCA.PEM
cert DSTROOTCA.PEM
cert ACEAPP-CERT.PEM
```

6. SSL パラメータ マップを設定します。SSL パラメータ マップは、SSL 接続用パラメータの定義に使用されます。

```
parameter-map type ssl PARAMMAP_SSL
cipher RSA_WITH_AES_128_CBC_SHA priority 2
```

7. SSL プロキシ サービスを設定します。

```
ssl-proxy service PSERVICE_SERVER
key ACEKEY.PEM
cert ACEIDM-CERT.PEM
chaingroup CISCOSSLCA-group
ssl advanced-options PARAMMAP_SSL
```

## ステップ 6 セッションの持続性(スティッキー)の設定

セッションの持続性(スティッキー)を設定すると、Cisco ACE で同じクライアントからの複数の接続を同じ実サーバに送信できます。スティッキーは送信元 IP アドレス、HTTP クッキー、SSL セッション ID (SSL トラフィックのみ) などに基づいて設定できます。この構成では、送信元 IP アドレスに基づいたスティッキーが使用されています。また、この構成では、ポート 80/443 および 9401 上のアプリケーション サーバ、および ポート 80/433 上のアイデンティティ管理 (IDM) サーバへのトラフィックに対するロード バランシングを行う際にもスティッキーが必要になります。

スティッキーを設定するには、タイプ (送信元 IP アドレス、クッキーなど)、スティッキー グループ名、タイムアウト値、およびスティッキー グループに関連付けるサーバ ファームを指定します。この構成では、次のスティッキーの設定を使用します。

```
sticky ip-netmask 255.255.255.255 address both ACEAPP-sticky
timeout 720
serverfarm aceapp
```

```
sticky ip-netmask 255.255.255.255 address both ACEIDM-sticky
timeout 720
serverfarm aceidm
```

ACEAPP-sticky および ACEIDM-sticky は、この構成で設定されるスティッキー グループ名です。

## ステップ 7 SLB の設定

Cisco ACE 製品は、レイヤ 3 とレイヤ 4 の接続情報およびレイヤ 7 のプロトコル情報に基づく SLB をサポートしています。Cisco ACE は、クラス マップ、ポリシー マップ、およびサービス ポリシーを使用して、着信トラフィックの分類と処理を行います。レイヤ 3 およびレイヤ 4 のトラフィックを分類する場合のクラス マップの一致基準には、VIP アドレス、プロトコル、および ACE のポートが含まれます。

次の 4 つの設定手順を実行します。

1. *match all* タイプのクラス マップを使用して、VIP を設定します。

```
class-map match-all VIP-aceapp-http
  2 match virtual-address 10.10.164.21 tcp eq www
class-map match-all VIP-aceapp-https
  3 match virtual-address 10.10.164.21 tcp eq https
class-map match-all VIP-aceinv-9401
  2 match virtual-address 10.10.165.21 tcp eq 9401
```

```
class-map match-all VIP-aceidm-http
  2 match virtual-address 10.10.165.167 tcp eq www
class-map match-all VIP-aceidm-https
  3 match virtual-address 10.10.165.167 tcp eq https
```

```
class-map match-all VIP-aceoid
  2 match virtual-address 10.10.165.183 tcp eq 389
```

2. *load balance* タイプのポリシー マップを設定して、スティッキー サーバファームに関連付けます。

```
policy-map type loadbalance first-match vip-lb-ACEAPP
  class class-default
    sticky-serverfarm ACEAPP-sticky
policy-map type loadbalance first-match vip-lb-ACEINV
  class class-default
    serverfarm aceinv
```

```
policy-map type loadbalance first-match vip-lb-ACEIDM
  class class-default
    sticky-serverfarm ACEIDM-sticky
```

```
policy-map type loadbalance first-match vip-lb-ACEOID
  class class-default
    serverfarm aceoid
```

3. *multimatch* タイプのポリシー マップを設定して、ステップ 1 で設定したクラス マップを関連付けます。また、HTTPS トラフィックのクラス マップで、SSL プロキシ サーバを適用します。

```
policy-map multi-match lb-vip
  class VIP-aceapp-https
    loadbalance vip inservice
    loadbalance vip-lb-ACEAPP
    ssl-proxy server PSERVICE_SERVER
  class VIP-aceapp-http
```

```
        loadbalance vip inservice
        loadbalance vip-lb-ACEAPP
class VIP-aceinv-9401
        loadbalance vip inservice
        loadbalance vip-lb-ACEINV
class VIP-aceidm-https
        loadbalance vip inservice
        loadbalance vip-lb-ACEIDM
        ssl-proxy server PSERVICE_SERVER
class VIP-aceidm-http
        loadbalance vip inservice
        loadbalance vip-lb-ACEIDM
class VIP-aceoid
        loadbalance vip inservice
        loadbalance vip-lb-ACEOID

policy-map multi-match lb-vip-server
class VIP-aceoid
        loadbalance vip inservice
        loadbalance vip-lb-ACEOID
class VIP-aceidm-http
        loadbalance vip inservice
        loadbalance vip-lb-ACEIDM
```

#### 4. インターフェイス VLAN にポリシー マップを適用します。

```
interface vlan 25
    service-policy input lb-vip

interface vlan 26
    service-policy input lb-vip-server

interface vlan 29
    service-policy input lb-vip

interface vlan 30
    service-policy input lb-vip-server

interface vlan 31
    service-policy input lb-vip

interface vlan 32
    service-policy input lb-vip-server
```

### ステップ 8 ブリッジ モードの設定

Cisco ACE モジュールには外部用の物理インターフェイスは搭載されていません。代わりに、Cisco ACE は内部 VLAN インターフェイスを使用します。Cisco ACE のインターフェイスは、ルーテッド モードまたはブリッジド モードのいずれかに設定できます。ブリッジ モードの設定を使用すると、Cisco ACE の構成を簡素化できます。この構成では、VLAN 25 がクライアント側に配置され、VLAN 26 が実サーバ側に配置されています。

Cisco ACE でブリッジ モードを設定するには、次の手順を実行します。

#### 1. アクセス リストの設定

接続を許可するには、すべてのインターフェイスで Access Control List (ACL; アクセス コントロール リスト) を設定する必要があります。ACL を設定しない場合、Cisco ACE はインターフェイス上のすべてのトラフィックを拒否します。この構成の場合、PERMIT\_ALL というアクセス リストが 2 つ設定されており、インターフェイス VLAN 上で IP および ICMP トラフィックを許可しています。PERMIT\_ALL というアクセス リストは、インターフェイス VLAN 25、VLAN 29、および VLAN 31 のセキュリティ ポリシー用に割り当てられ、実サーバへの直接アクセスを許可します。同じアクセス リストは、インターフェイス VLAN 26、VLAN 30、および VLAN 32 のセキュリティ ポリシー用にも割り当てられています。これは、実サーバ間のトラフィックを許可し、実サーバから他のネットワークへのアクセスを可能にするためです。次の設定では、目的のインターフェイス VLAN 上のすべての IP および ICMP トラフィックを許可します。ただし、Cisco ACE では、送信元アドレス、宛先アドレス、プロトコル、およびプロトコル固有のパラメータなどの基準に基づいて、インターフェイス VLAN 上の着信/発信トラフィックをフィルタリングするように設定することもできます。これは、必要に応じて容易に行えます。

```
access-list PERMIT_ALL line 5 extended permit ip any any
access-list PERMIT_ALL line 6 extended permit icmp any any
```

#### 2. VLAN インターフェイスの設定

ブリッジ モードを設定する場合は、クライアント側 VLAN およびサーバ側 VLAN の両方を設定する必要があります。これらの VLAN インターフェイスは共通のブリッジ グループを共有します。また、インターフェイス VLAN では、アクセス リストとロード バランシング サービス ポリシーも適用されます。

次の設定は、この構成のインターフェイス VLAN 設定を示しています(図 5 を参照)。

```
interface vlan 25
  bridge-group 1
  access-group input PERMIT_ALL
  service-policy input everyone
  service-policy input lb-vip
  no shutdown
interface vlan 26
  bridge-group 1
  access-group input PERMIT_ALL
  service-policy input everyone
  service-policy input lb-vip-server
  no shutdown

interface vlan 29
  bridge-group 2
  access-group input PERMIT_ALL
  service-policy input everyone
  service-policy input lb-vip
  no shutdown
interface vlan 30
  bridge-group 2
  access-group input PERMIT_ALL
  service-policy input everyone
```

```
service-policy input lb-vip-server
no shutdown

interface vlan 31
bridge-group 3
access-group input PERMIT_ALL
service-policy input everyone
service-policy input lb-vip
no shutdown
interface vlan 32
bridge-group 3
access-group input PERMIT_ALL
service-policy input everyone
service-policy input lb-vip-server
no shutdown
```

### 3. Bridge Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス) の設定

BVI の設定では、ブリッジ グループのレイヤ 3 インスタンスを定義します。この設定を使用すると、2 つの VLAN 間でのトラフィックのブリッジングが可能になります。インターフェイス番号はステップ 2 で定義したブリッジ グループと同じです。次の設定は、この構成での BVI の設定を示しています。

```
interface bvi 1
ip address 10.10.164.20 255.255.255.240
no shutdown
interface bvi 2
ip address 10.10.165.180 255.255.255.240
no shutdown

interface bvi 3
ip address 10.10.165.164 255.255.255.240
no shutdown
```

#### ステップ 9 デフォルト ゲートウェイの設定

リモート マシンにアクセスする場合や、他のネットワーク上にあるクライアントの要求に応答するには、ロード バランシングを必要とするレイヤ 3 VLAN インターフェイスに対してデフォルト ルートを設定する必要があります。Cisco ACE のデフォルト ゲートウェイは、上流のルータ上にあるレイヤ 3 インターフェイスの IP アドレスにアクセスします。冗長構成の場合、このインターフェイス アドレスの代わりに HSRP アドレスを使用します。以下に、この構成での Cisco ACE のデフォルト ゲートウェイの設定を示します。

```
ip route 0.0.0.0 0.0.0.0 10.10.164.17
ip route 0.0.0.0 0.0.0.0 10.10.165.177
ip route 0.0.0.0 0.0.0.0 10.10.165.161
```

ロード バランシングが必要なインターフェイスを追加する場合は、インターフェイスごとに個別のゲートウェイを設定する必要があります。たとえば、インターフェイス VLAN 31 (VLAN 31 と 32 をペアで使用) には個別のゲートウェイを設定する必要があります。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)  
この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ株式会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

#### お問い合わせ先