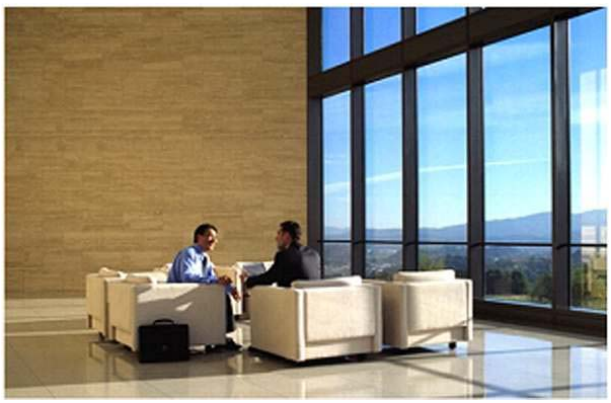
Oracle E-Business Suite 11i と Cisco ACE シリーズ Application Control Engineの導入ガイド、バージョン 1.0

この設計ガイドでは、シスコシステムズの Cisco® Application Control Engine（Cisco ACE）を Oracle E-Business Suite 11i（Oracle 11i）とともに導入する方法について説明します。このガイドは、シスコとOracleによるソリューションを業界に広めるための大規模な取り組みの一環として、シスコとOracleの協力の下で作成されました。シスコとOracleは、他の製品の組み合わせに関する設計ガイドおよび関連ドキュメントも提供しています。



Oracle E-Business Suite 11i（Oracle 11i）は、完全に統合された包括的なビジネス アプリケーション スイートです。このスイートによって企業は、効果的な意思決定のための良質なビジネス情報を入手し、最適な対処を実行するために必要な順応性を高め、変化に対応し競争に打ち勝つためのベスト プラクティスと業界固有の機能を活用できるようになります。Oracle 11i は、ビジネス プロセスを改善し、カスタマイゼーションを軽減し、統合コストを減らし、事例を集約することにより、IT と事業に必要なコストを劇的に低減します。

Cisco ACE は、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 デバイスの間に、レイヤ 3 とレイヤ 4 ～ 7 のパケット情報に基づいて高性能なサーバ ロード バランシング（SLB）を実現します。ACE はまた、SSL 暗号化トラフィックの終端および始端となることもできるため、セキュアなエンドツーエンドの暗号化を確保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することができます。このモジュールは、インターネットワーキングにおいてデフォルトでも 4 Gbps の速度を実現でき、アップグレード ライセンスを購入した場合の速度は 16 Gbps に達します。これは、レイヤ 4 ～ 7 のロード バランシング、TCP 最適化、SSL（Secure Sockets Layer）オフロードといったアプリケーション認識型の機能をネットワークに提供する、高性能で機能豊富な製品です。

Oracle 11i を Cisco ACE とともに導入すると、企業はセキュリティ、スケーラビリティ、アベイラビリティを兼ね備えたソリューションを得ることができます。

このドキュメントは、多層アーキテクチャに対して Oracle 11i と Cisco ACE を導入するためのガイドです。

このドキュメントで紹介するネットワーク アーキテクチャは、Oracle 11i の機能要件を満たしています。このドキュメントでは、HTTP 圧縮やダイナミック キャッシングといった他のアプリケーション最適化テクノロジーについては触れていませんが、Cisco ACE と他の製品の機能を使えばこれらも簡単に統合できます。

概要

このドキュメントでは、アプリケーションとネットワーク アーキテクチャの次の特徴について説明しています。

- このネットワーク アーキテクチャは、Oracle 11i 導入アーキテクチャのすべての機能要件を満たしています。
- この導入例では、Oracle 11i（Oracle9i Application Server、Concurrent Manager、およびOracle Forms Server）が複数のアプリケーション フロントエンド サーバ上で実行されます。
- このドキュメントで取り上げているデータセンター ネットワーク アーキテクチャ（Cisco ACE モジュールを Cisco Catalyst® 6509-E Multilayer Switch Feature Card [MSFC] ルータ シャーシにインストール）では、どのロード バランシング トラフィックに関しても送信元 NAT（Network Address Translation）が不要なので、実装と管理が容易です。
- Cisco ACE をブリッジ モード（透過モード）で実装することにより、アプリケーションの展開と管理が容易になります。
- Cisco ACE のアプリケーション健全性チェック、持続性、調整可能な接続タイムアウト機能により、ハイアベイラビリティが実現し、アプリケーション リソースの使用も最適化されます。
- 説明を簡単にするために、このドキュメントでは単一デバイスの導入のみを紹介します。実際の現場では、ハイアベイラビリティを提供するために冗長設計が展開されます。

用語と定義

ここでは、本ドキュメントで使用する Oracle 11i および Cisco ACE 関連の用語を説明します。

Oracle 11i E-Business Suite

本ドキュメントで使用する Oracle 11i E-Business Suite 関連の用語は次のとおりです。

APPHost	Oracle 11i （Oracle9i Application Server 、Concurrent Manager 、Oracle Forms Server、および Oracle HTTP Server [OHS]）を実行するサーバ。フロントエンドの接続性を提供します。
DBHost	アプリケーション データ用に、2 ノードの Oracle Database 10g Enterprise Edition および Oracle Real Application Clusters（RAC）を持つサーバ。
OHS	Oracle HTTP Server
サービス（Service）	HTTP サービスなど、特定の 1 つの機能を提供するために 1 台のマシンで実行されているプロセスのグループ。
層（Tier）	サービスのグループ。複数の物理マシンにまたがることもあります。層は論理グループを表し、複数のネットワーク セグメント（サブネット）で構成されることもあります。複数の物理マシン上で実行される特定の 1 つのアプリケーションを各サブネットに展開することも、複数のアプリケーションを 1 つのネットワーク セグメントにマージすることもあります。

Cisco ACE

本ドキュメントで使用する Cisco ACE シリーズ Application Control Engine 関連の用語は次のとおりです。

プローブ（Probe）	ロード バランサによって送信される、アプリケーションの健全性チェック。
リアル サーバ（Rserver）	リアル サーバ。Cisco ACE の構成では物理サーバのこと。
サーバ ファーム（Server farm）	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リアル サーバのグループ。
スティッキ（Sticky）	セッション期間の最後までクライアントを同じサーバにバインドするメカニズム。セッション持続性とも呼ばれます。
仮想アドレス（Virtual address）	ロード バランシングされたアプリケーションのフロントエンドとなる仮想 IP アドレス。

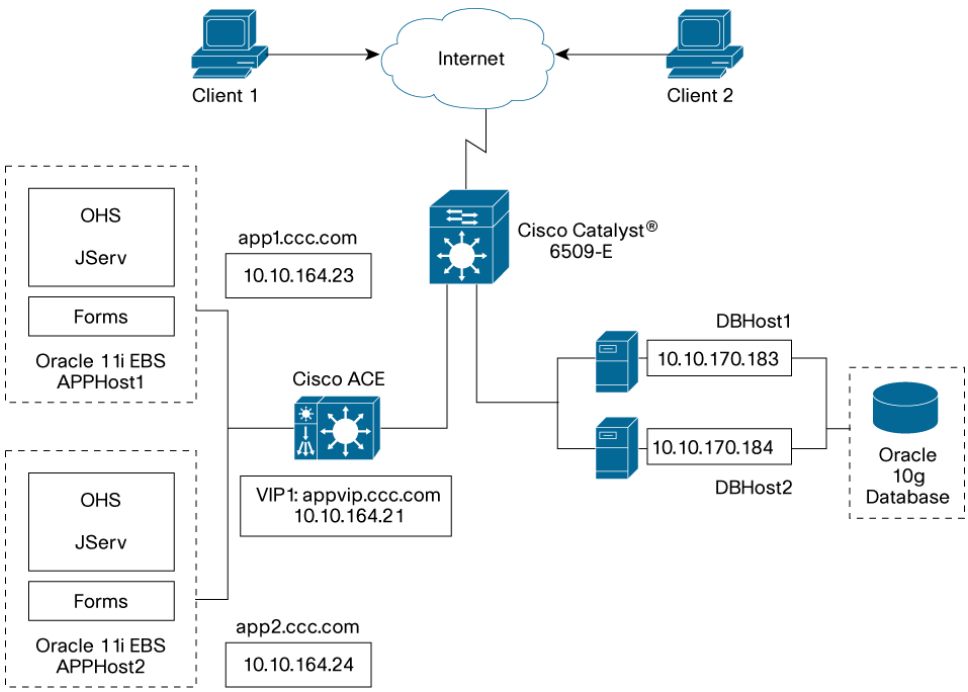
アプリケーションとネットワーク アーキテクチャ

アーキテクチャの概要

アプリケーションの観点から見ると、このアーキテクチャは、デスクトップ層、アプリケーション層、データベース層という3つの層に分けられます。

- **デスクトップ層**：この層は、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。このクライアント インターフェイスは、Java 対応の Web ブラウザを通じて提供されます。デスクトップ クライアントは、必要に応じて Java アプレットをダウンロードします。図 1 では、クライアント 1 とクライアント 2 がこのアーキテクチャのデスクトップ層を表しています。

図 1　アプリケーションとネットワーク アーキテクチャの全体図



- **アプリケーション層**：この層は、外部（インターネット）クライアントと内部クライアント（社内クライアントまたは他の Oracle アプリケーション製品）から直接アクセスされるフロントエンド（Web）環境を表します。この層にアクセスするために使われる主な手段は、プレーンテキスト HTTP または HTTPS です。このアーキテクチャでは、アプリケーション層は 1 つのネットワーク セグメントから構成されます。
  - 図 1では、Oracle 11i APPHost1 と Oracle 11i APPHost2 がフロントエンドの接続機能を提供しています。これら 2 つの APPHost サーバに向かうトラフィックは、Cisco ACE により、VIP1 を使ってロードバランシングされます。OHS、JServ、Forms Server は、それぞれのAPPHost サーバで実行されています。APPHost サーバはデータベース サーバとも通信します。
  - APPHost サーバへのフローについては、このドキュメントでこの後詳しく説明します。
- **データベース層**：この層には、Oracle E-Business Suite 11i で管理されるすべてのデータを保管するデータベース サーバが含まれます。通常、デスクトップ層がデータベース サーバと直接通信することはありません。一方、アプリケーション層のサーバは、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 サーバと通信します。データベース サーバに向かうトラフィックは、この導入例の場合、ロードバランシングされません。このため、図 1 には Cisco ACE の背後にあるデータベース サーバを示していません。この層に含まれるホストは、DBHost1 と DBHost2 です。データベース サーバのハイアベイラビリティとロード バランシングは、Oracle RAC によって提供されます。

アプリケーションのフロー

ここでは Oracle 11i APPHost アプリケーション サーバ スイートのフローについて説明します。

Oracle 11i E-Business Suite のクライアント

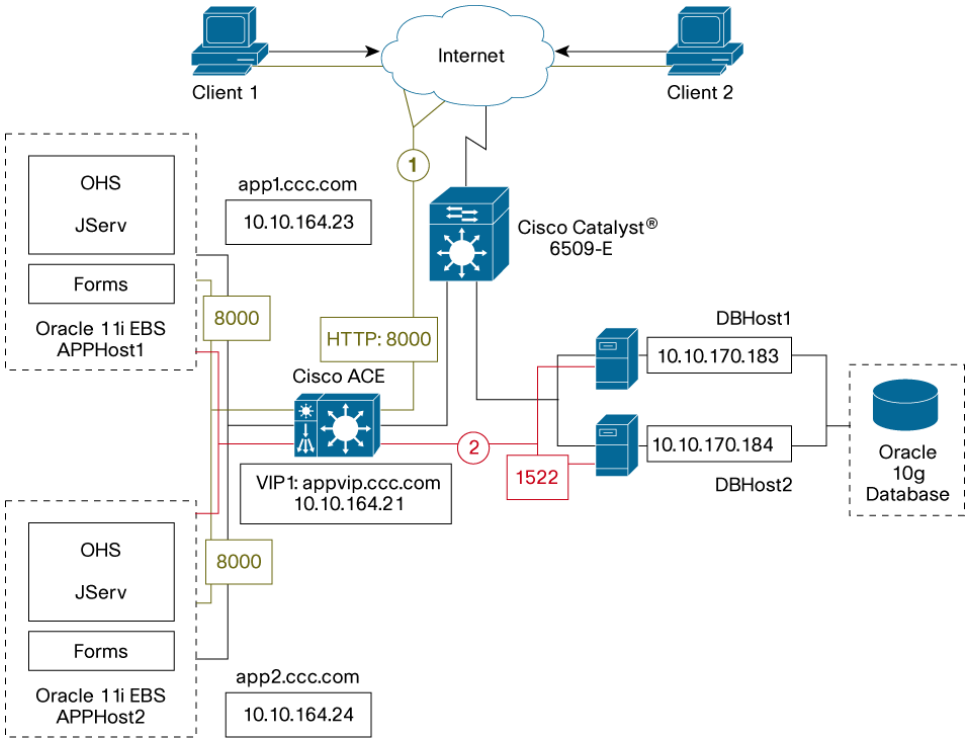
イントラネットのクライアントが http://appvip.ccc.com:8000 にアクセスします。この場所は、Cisco ACE 上で VIP1: 10.10.164.21 と設定されています。この導入例では、必要に応じて HTTPS ポート 443 向けの設定を簡単に行うことができます。

Cisco ACE はクライアントからの要求をロード バランシングして、Oracle 11i の APPHost1 または APPHost2 上で稼働中の利用可能な Web（OHS）サーバの 1 つに送信します。

このフローでは、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持続性を Cisco ACE で設定する必要があります。

図 2 の緑色の 1 は、このフローを示しています。

図 2　APPHost（ポータル）のフロー



Oracle E-Business Suite 11i APPHost から Oracle Database 10g Server へ

Oracle 11i の APPHost1 と APPHost2は、データベース サーバ DBHost1 および DBHost2 へのデータベース クエリを実行します。デフォルトの TCP ポートは 1521 ですが、このトポロジの場合、この接続は、データベース サーバで実行される宛先 TCP ポート 1522（Oracle では SQL*NET または NET8 として参照可能）上に確立されます。

この要求はネットワーク内を移動し、Cisco ACE とネットワーク上のルータによってルーティングされます。

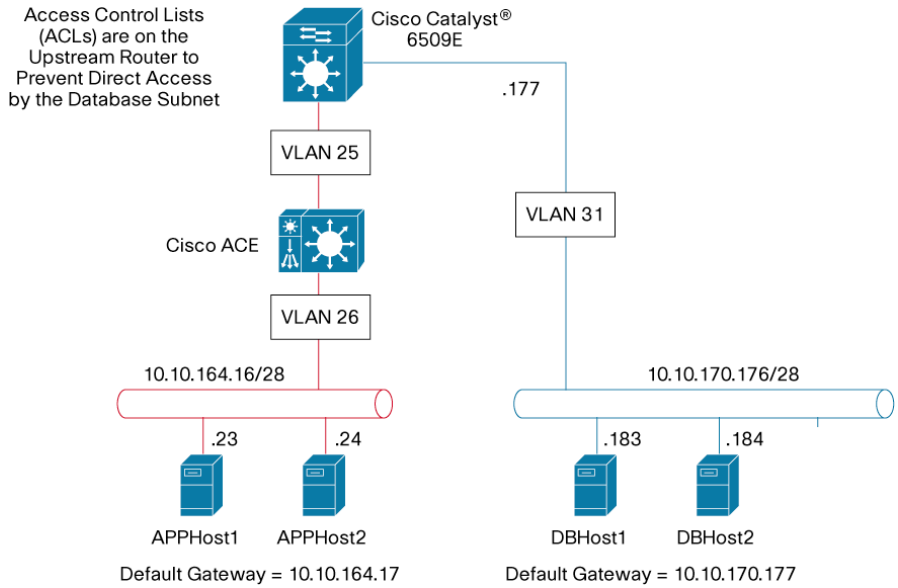
図 2 の赤色の 2 は、このフローを示しています。

ネットワークの設計と設定

ネットワークのトポロジと設計の特徴

図 3 は、論理ネットワーク トポロジを表しており、Cisco ACE がどのように配備されているかを示しています。Cisco ACE はブリッジ モードに設定されており、1 つの VLAN から他の VLAN（VLAN 25から26）へ単純にトラフィックをブリッジングします。VLAN 間のルーティングは、アップストリーム ルータによって管理されます。

図 3　詳細なネットワーク トポロジ



ここでは、ネットワーク設計の主な特徴の一部を説明します。

1. ブリッジ モード

- このネットワーク設計では、Cisco ACE モジュールを、簡単な配備モデルであるブリッジ モードで配備します。
- このモードでは、Cisco ACE は 2 つの VLAN 間のブリッジとして機能し、VIP アドレスへ向かうトラフィックのロード バランシングを行います。
- 各 VLAN ペアはスイッチで設定しますが、アップストリーム ルータの IP アドレスを持つのはクライアント側の VLAN だけです。
- 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 のアップストリーム ルータ（Hot Standby Router Protocol [HSRP]）の IP アドレスを指すように設定します。
- セキュリティ ポリシーで許可されていれば、ダイレクト サーバ アクセスも可能です。

2. 複数のサブネットを使用したサーバのセグメント化

- サーバの各機能グループは、それぞれ固有の IP サブネットに配置します。
- このセグメント化によって、同種の機能を論理グループにまとめ、将来の拡張に備えることができます。

3. アップストリーム ルータ と Cisco ACE によるセキュリティ対策

- アップストリーム ルータの ACL により、目的のトラフィックは Cisco ACE とサーバに直接到達することが許可されます。
- アップストリーム ルータの ACL では、データベース サーバへのダイレクト アクセスを禁止するように設定します。
- Cisco ACE の ACL では、アプリケーション ポートの VIP へのアクセスを許可するように設定します。

4. （オプション）Cisco ACE での SSL 終端

- このドキュメントでは取り上げませんが、Cisco ACE で SSL 終端を設定することは簡単です。
- このシナリオでは、SSL トラフィック（ポート443）は Cisco ACE 上で終端されます。Cisco ACE は、Webcache サービス ポート（ポート8000）上のアプリケーション サーバにプレーンテキスト 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 アドレスが保持されます。
- Cisco ACE はデフォルトで、最大 1000 TPS（トランザクション/秒）の SSL トランザクションをサポートします。より高いパフォーマンスが必要な場合は、Cisco ACE. に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展開されるサーバの概要を示しています。

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
Oracle E-Business Suite 11i APPHost1（app1.ccc.com）	10.10.164.23	255.255.255.240	OHS、JServ、Forms Server 1	8000
Oracle E-Business Suite 11i APPHost2（app2.ccc.com）	10.10.164.24	255.255.255.240	OHS、JServ、Forms Server 1	8000
DBHost1	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	1522
DBHost1	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	1522

注 : 表 1 には、このドキュメントに出てくるフローの外部リスニング ポートだけを示しています。また、各アプリケーション サーバには、管理アクセスに使われる他のポートが存在する場合もあります。ACL の設定では、これらのポートも許可する必要があります。詳細については、Oracleのドキュメントを参照してください。

Oracle E-Business Suite 11i の設定

ここでは、Oracle 11i を Cisco ACE とともに導入する場合に、Oracle 11i で変更する必要のある設定について説明します。

以下のステップを実行します（ここでは手順の概要のみを示します）。

ステップ 1　Oracle E-Business Suite 11i アプリケーションを仮想名（エイリアス）でインストールするか、既存のアプリケーションを仮想名で複製します。この導入例では、appvip.ccc.com という仮想名を使用しています。

ステップ 2　インストールまたは複製が終わったら、仮想名を削除し、インストール時に使用した仮想名と同じ名前で Cisco ACE を設定します。この導入例の場合は、Cisco ACE 上で appvip.ccc.com が VIP1: 10.10.164.24 に解決されます。

次に、アプリケーションが Cisco ACE を使用できるように、各 Oracle E-Business Suite 11i APPHost サーバで変更を行います。この導入例では、2 つの Oracle E-Business Suite 11i APPHost サーバが使われています。Oracle 11i E-Business Suite APPHost1 と Oracle 11i E-Business Suite APPHost2の 2つです。

- Oracle E-Business Suite 11i APPHost1 のDNS（ホスト）名は、app1.ccc.com です。
- Oracle E-Business Suite 11i APPHost2 のDNS（ホスト）名は、app2.ccc.com です。

仮想ホスト名でなく実際のホスト名を使用するために、以下の変更が必要です。

ステップ 3 $TNS_ADMIN/listener.ora を次のように変更します。

```
(ADDRESS= (PROTOCOL= TCP)(Host= app1)(Port= 1621))
```

ステップ 4 $IAS_ORACLE_HOME/Apache/modplsql/plsql.conf を次のように変更します。

```
ProxyPass /pls/http://app1.ccc.com:8000/pls/
```

ステップ 5 $IAS_ORACLE_HOME/Apache/Apache/conf/oprocmgr.conf を次のように変更します。

```
<IfModule mod_oprocmgr.c>
...
ProcNode app1.ccc.com <oprocmgr_port>
```

この oprocmgr_port は、Cisco ACE で設定されるポート（ポート8000）とは関係ありません。

```
...
<Location />
Order Deny,Allow
Deny from all
Allow from localhost
Allow from app1
Allow from app1.ccc.com
</Location>
```

ステップ 6 $IAS_ORACLE_HOME/Apache/Apache/conf/httpd_pls.conf を次のように変更します。

```
...
<VirtualHost _default_:*>
<Location />
...
Allow from app1
Allow from app1.ccc.com
</Location>
</VirtualHost>
...
```

ステップ 7 サーバの仮想名のためのループバック アドレスを設定します。サーバのループバック アドレスが必要な理由は、Oracle 11i 自身が自分宛てに生成したトラフィックを適切にループバックできるようにするためです。ループバック エントリ 127.0.0.1 を /etc/host file for appvip.ccc.com に追加します。

```
127.0.0.1 appvip.ccc.com appvip
```


ステップ 8　ステップ 3 ～ 7 を繰り返して、app2.ccc.com の設定を行います。app1 は app2 に置き換えてください（他も同様）。

ステップ 9　設定が終わったら、アプリケーションを開始し、サービスをテストします。Oracle Parall el Con current Manager（PCP）を実装している場合を除き、Concurrent Manager は 1 つのノードだけを開始します。

ルータの設定

Cisco ACE は、ディストリビューション層の Cisco Catalyst 6509-E スイッチのシャーシ内にインストールします。このシャーシ内の MSFC モジュールは、Cisco ACE のアップストリーム ルータとしての役割も果たします。

この導入例でアップストリーム ルータを設定するには、以下のステップに従います。

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

このトポロジでは、次のように、2 つの Cisco ACE 用 VLAN と 1 つのデータベース サーバ 用 VLAN を MSFC に追加する必要があります。

```
vlan 25
name ACE-APP-CLIENT:10.10.70.164.16/28
!
vlan 26
name ACE-APP-SERVER
!
vlan 31
name ACE-DB-SERVERIDM:10.10.165.176/28
```

注：ここでの name 定義は、説明を目的として使用されています。組織の名前付け規則に従って設定してかまいません。

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

VLAN が ACE モジュールにアクセスできるように Cisco Catalyst 6509E スイッチで特別に設定しない限り、Cisco ACE は VLAN トラフィックを受け入れません。すべての VLAN から ACE へのアクセスを遮断することにより、非 ACE VLAN上 のブロードキャスト ストームが ACE に影響するのを回避できます。この導入例では、Cisco ACE は Cisco Catalyst 6509E シャーシのスロット 4 にインストールしてあります。Cisco ACE 固有の VLAN トラフィックが Cisco ACE に向かうようにするには、以下の設定が必要です。

```
svclc multiple-vlan-interfaces
svclc module 4 vlan-group 11
svclc vlan-group 11 25,26
```

ステップ 3　SVI（Switched Virtual Interface）設定を追加します。

SVI 設定は、ルータ（MSFC）のレイヤ 3 インスタンスを定義します。この導入例では、2 つの SVI を設定する必要があります。Cisco ACE クライアント側の VLAN 用に 1 つ、データベース サーバ側の VLAN 用に 1 つです。

Cisco ACE クライアント側の VLAN SVI を次のように設定します。

```
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 アドレスが APPHost サーバと Cisco ACE のデフォルトのゲートウェイになります。冗長設計では、この IP アドレスを HSRP アドレスとして設定する必要があります。設定例については、次の URL にある Cisco HSRP の設定ガイドを参照してください。

http://www.cisco.com/support/ja/473/62.shtml

データベース サーバ側の VLAN SVI を次のように設定します。

```
interface Vlan31
description ACE-APPSRV-Client-Side
ip address 10.10.170.177 255.255.255.240
no ip redirects
no ip proxy-arp
```

注：この IP アドレスがデータベース サーバのデフォルト ゲートウェイになります。冗長設計では、この IP アドレスを HSRP アドレスとして設定する必要があります。設定例については、次の URL にある Cisco HSRP の設定ガイドを参照してください。

http://www.cisco.com/support/ja/473/62.shtml

Cisco ACE の設定

表 2 は、このアーキテクチャに Cisco ACE を展開する際の設定情報を示しています。

表 2. Cisco ACE の設定情報

ホスト	仮想 IP アドレスとポート	関連サーバ	サーバ ポート	健全性チェック メカニズム	TCP 最適化の適用
appvip.ccc.com:8000	10.10.164.21:8000	10.10.164.23 10.10.164.24	8000 8000	HTTP可	○

Cisco ACE を設定する際には、このガイドで示した図 3 を参照して、トポロジの設定ステップとの関連を確認してください。

ステップ 1：管理アクセスの設定

リモートから Telnet、Secure Shell（SSH）プロトコル、Simple Network Management Protocol（SNMP）、HTTP、または HTTPS を使って Cisco ACE モジュールにアクセスしたり、Cisco ACE モジュールへの Internet Control Message Protocol（ICMP）アクセスを許可するには、ポリシーを定義し、アクセス先となるインターフェイスに適用します。

1. 次のように、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 （XML インターフェイス アクセスの場合に必要）
50 match protocol https any （HTTP[S] の場合に必要）
```

2. 次のように、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
```

ステップ 2：プローブの設定

Cisco ACE は、リアル サーバのアベイラビリティを検証するキープアライブの 1 つの方法として、プローブを使用します。Cisco ACE ではいくつかのタイプのプローブを設定できますが、この導入例では HTTP のプローブを使用します。

この導入に対して、次のプローブを設定します。

```
probe http ACECFG-http
port 8000
interval 30
passdetect interval 10
request method head url /index.html この URI は、サーバ設定に応じて変更する必要があります。
expect status 200 202
```

ステップ 3：リアル サーバの設定

リアル サーバは、対象トラフィックの送信先として、ロード バランサがさまざまな条件に基づいて選択するサーバです。リアル サーバを設定するときは、リアル サーバ名の大文字/小文字が区別されることに注意してください。リアル サーバの設定に最小限必要なパラメータは、IP アドレスと inservice の指定です。

この導入例では、次のリアル サーバを設定します。

```
rserver host app1
ip address 10.10.164.23
inservice
rserver host app2
ip address 10.10.164.24
inservice
```

ステップ 4：サーバ ファームの設定

サーバ ファームはリアル サーバの論理コレクションです。ロード バランサは、さまざまな条件に基づいてこのコレクションの中からリアル サーバを選択します。リアル サーバと同様、サーバ ファームの名前でも大文字/小文字が区別されます。サーバ ファームの設定に最小限必要なパラメータは、リアル サーバとプローブの指定です。

この導入例では、次のサーバ ファームを設定します。

```
serverfarm host aceCFG
probe ACECFG-http
rserver app1
inservice
rserver app2
inservice
```


ステップ 5：セッション持続性（スティッキ）の設定

セッション持続性（スティッキ）を使うと、同じクライアントからの複数の接続を同じリアル サーバに対して確立するように Cisco ACE を設定できます。スティッキは、送信元 IP アドレス、HTTP クッキー、SSL セッション ID（SSL トラフィックの場合のみ）などに基づいて設定できます。この導入例では、送信元 IP アドレスに基づいてスティッキを設定します。

スティッキを設定するには、タイプ（送信元 IP アドレスやクッキーなど）、スティッキ グループ名、タイムアウト値、スティッキ グループに関連付けるサーバ ファームを指定します。

この導入例では、次のスティッキ属性を設定します（この例では、ACECFG-sticky がスティッキ グループ名です）。

```
sticky ip-netmask 255.255.255.0 address both ACECFG-sticky
timeout 720
serverfarm aceCFG
```

ステップ 6：サーバのロード バランシングの設定

Cisco ACE では、クラスマップ、ポリシーマップ、サービスポリシーを使って、着信トラフィックの分類、適用、処理実行を行います。特定のポートの VIP アドレスを目的地とするトラフィックは、レイヤ 4 に分類されます。

次のようにロード バランシングを設定します。

1. match-all タイプのクラスマップを使って、VIP アドレスを設定します。

```
class-map match-all VIP-aceCFG
2 match virtual-address 10.10.164.21 tcp eq 8000
```

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

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

3. multi-match のポリシー マップを設定し、ステップ 1 で設定したクラス マップに関連付けます。

```
policy-map multi-match lb-vip
class VIP-aceCFG
loadbalance vip inservice
loadbalance vip-lb-ACECFG
```

4. 次のように、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
```

ステップ 7：ブリッジ モードの設定

Cisco ACE モジュールは、外部物理インターフェイスを一切含みません。代わりに、内部 VLAN インターフェイスを使用します。Cisco ACE 上のインターフェイスは、ルーテッドまたはブリッジのいずれかのモードに設定できます。ブリッジ モード設定を使うと、Cisco ACE の導入が簡素化されます。この導入例では、VLAN 25 はクライアント側に面し、VLAN 26 はリアル サーバ側に面しています。

Cisco ACE でブリッジ モード設定を実装するには、以下のステップに従って設定を行う必要があります。

1. アクセス リストの設定

接続を許可するためには、アクセス コントロール リスト（ACL）が個々のインターフェイスに設定されている必要があります。ACL が設定されていない場合、Cisco ACE はそのインターフェイスへの全トラフィックを拒否します。この導入例では、各 VLAN インターフェイス で IP と ICMP のトラフィックを許可するために、PERMIT_ALL という名前の 2 つのアクセス リストを設定します。このアクセス リスト PERMIT_ALL をインターフェイス VLAN 25 のセキュリティ ポリシーに割り当てることで、リアル サーバへのダイレクト アクセスを許可します。また、この同じアクセス リストをインターフェイス VLAN 26 のセキュリティ ポリシーにも割り当てることで、リアル サーバ間のトラフィックを許可し、これらのリアル サーバから他のネットワークにもアクセスできるようにします。次の設定を行うと、任意の VLAN インターフェイス上ですべての IP および ICMP トラフィックを許可できます。ただし、必要であれば、送信元アドレス、宛先アドレス、プロトコル、プロトコル固有のパラメータなどの基準に基づいて、VLAN インターフェイス上の着信/発信トラフィックをフィルタするように Cisco ACE を設定することも簡単です。

```
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 モード設定の場合は、クライアント側とサーバ側の両方の VLAN を設定する必要があります。これらのインターフェイス VLAN は、1 つの共通ブリッジ グループを共有します。インターフェイス VLAN には、ACL とロード バランシング サービス ポリシーも関連付けます。

次のようにインターフェイス VLAN を設定します。

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

3. ブリッジ グループ仮想インターフェイス（BVI）の設定

BVI 設定は、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。BVI 設定により、2 つの VLAN 間でトラフィックがブリッジングされるようになります。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。

この導入例では、BVI を次のように設定します。

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


ステップ 8：デフォルト ゲートウェイの設定

リモート マシンにアクセスしたり、他のネットワーク上の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各レイヤ 3 VLAN インターフェイスにデフォルト 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、アップストリーム ルータにあるレイヤ 3 インターフェイスの IP アドレスを指しています。冗長設計では、デフォルト ゲートウェイはインターフェイスのアドレスではなく、HSRP アドレスを指しています。

Cisco ACE におけるインターフェイス VLAN 25 のデフォルト ゲートウェイ設定は、次のとおりです。

```
ip route 0.0.0.0 0.0.0.0 10.10.164.17
```

ロード バランシングを必要とするインターフェイスが他にもある場合は、それらのすべてに対して個別のゲートウェイを設定します。たとえば、VLAN 32 と VLAN 33 のペアであれば、インターフェイス VLAN 32 に対して、適切なゲートウェイを設定することになります。

シスコシステムズ合同会社
〒 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

お問い合せ先

08.06