VMware Virtual Desktop Infrastructure 用 Cisco Application Networking Services

目次

はじめに

本書の目的

VMware® View 3.0 などのデスクトップ バーチャライゼーション ソリューションによって、従来の PC はバーチャル マシンで置き換えられ、データセンターから管理されるようになります。その結果、運用コストが削減され、デスクトップ管理が容易になり、ビジネス継続性と障害回復のための機能を企業のデスクトップでも利用できるようになります。

しかし、デスクトップ バーチャライゼーション ソリューションが WAN を介して展開された場合は、遅延と帯域幅の制約によって、その効果をフルに発揮することができません。企業のためのバーチャル デスクトップ ソリューションの展開において直面する課題には、次のようなものがあります。

- WAN を経由するディスプレイプロトコルのパフォーマンスが低く、従業員の生産性に影響が及ぶ。
- 大量の帯域幅が使用されるため、コストが増加する。
- スケーラビリティに限界があるため、サポート可能なユーザ数が少なくなる。
- 中央集中管理型の印刷のパフォーマンスが低く、ブランチでの印刷コストが増加する。
- 障害回復のためにデータセンターのバーチャル デスクトップ インフラストラクチャをバックアップするのに、かなりの時間と帯域幅が必要となる。

今日の複雑なユーザ デスクトップに関連する課題に対処するため、シスコと VMware は共同で、VMware VIEW 向けの共同ソリューションを提供しています。このソリューションは、Cisco® Application Networking Services（ANS; アプリケーション ネットワーキング サービス）を使用して VMware VIEW を展開するための、設計ベスト プラクティスと実装ガイダンスを備えたエンタープライズ ネットワーク アーキテクチャで、企業のあらゆるタイプのユーザに対するデスクトップ配信を最適化します。

シスコと VMware は、この共同ソリューションの提供に向けて、協力しながらラボのセットアップ、ソリューションのテスト、およびテスト結果の検証などを行いました。この共同で検証したラボのセットアップとソリューションのテストに、シスコと VMware がお客様の実際の展開の再現とその展開の正確な文書化のために行った最善の努力の結果が表れています。

VMware VIEW 配信を最適化するシスコと VMware の共同ソリューションは、次の利点を実現します。

- WAN を経由するバーチャル デスクトップのパフォーマンスが 70 % 向上し、LAN に近づきます。
- VMware VIEW クライアント数のスケーラビリティが 2 ～ 4 倍に増加し、VMware VIEW データセンター インフラストラクチャのスケーラビリティもきわめて高くなります。
- コストのかかる WAN 帯域幅所要量を 60 ～ 70 % 削減します。
- WAN 経由の印刷を最適化し、所要時間を 70 % 短縮します。Cisco Wide Area Application Services（WAAS）アプライアンス上でローカル プリンタ サーバをホスティングすることも可能です。
- バーチャル イメージのバックアップを 10 倍以上高速化すると共に、帯域幅の使用量を 90 % 以上削減することで、ビジネスの継続性を向上させます。

本書の目的は、シスコと VMware の共同ソリューションのための設計ベスト プラクティスと展開ガイドを提供して、企業のあらゆるタイプのユーザに対するデスクトップ配信を最適化することです。

前提条件

シスコと VMware の共同ソリューションを展開するには、次の前提条件を満たす必要があります。

- VMware VIEW の実用的な知識
- 基本的なネットワーキングとトラブルシューティングの経験
- このネットワーク設計の対象となるシスコ製品（Cisco WAAS および Cisco Application Control Engine（ACE; アプリケーション コントロール エンジン）製品ファミリーなど）の設置経験
- Cisco IOS® ソフトウェアの実用的な知識

本書の構成

表 1 で各項を簡単に説明します。

表 1. 本書の構成

項	説明
ソリューションの概要	ソリューションのハイレベルな概要を示します。ソリューション、背景、潜在的な利点、適用範囲、制限を紹介します。
ソリューションのアーキテクチャ	共同ソリューションのアーキテクチャを説明します。
Cisco WAAS ソリューションの実装と設定	共同ソリューション内での Cisco WAAS の設定と実装について説明します。
Cisco ACE ソリューションの実装と設定	共同ソリューション内での Cisco ACE の設定と実装について説明します。
NetQoS を使用したネットワーク モニタリング	ソリューションのテストに使用するソフトウェアのネットワーク モニタリングについて説明します。
ソリューションのテストと結果	使用されたテスト手順を説明し、その結果を示します。

ソリューションの概要

Cisco WAAS および ACE を VMware VIEW と組み合わせることにより、コストのかかる帯域幅のアップグレードを行わずに WAN 経由のバーチャル デスクトップ配信を最適化して、デスクトップ管理のコストと複雑さを低減できます。

- この共同で検証されたソリューションでは、VMware VIEW がデスクトップをバーチャル化して中央集中管理するとともに、Cisco WAAS が VMware VIEW のトラフィックを圧縮して高速化したり、ブランチ オフィスでの印刷を最適化することにより、従業員の生産性が向上します。
- Cisco WAAS によってスケーラビリティが向上し、WAN 経由でサポートされる VMware VIEW ユーザの数が増大するとともに、Cisco ACE によってデータセンターの VMware VIEW インフラストラクチャのアベイラビリティとスケーラビリティが向上します。
- データセンターの VMware VIEW インフラストラクチャのバックアップおよびレプリケーションに要する時間が短縮され、企業のビジネスの継続性が向上します。

ソリューションの説明

シスコと VMware の共同ソリューションによって、最適化されたスケーラブルなエンタープライズ ネットワーク アーキテクチャが提供され、これによって Cisco ANS 製品を使用した VMware VIEW の展開が実現します。Cisco ANS によって、データセンターおよびブランチ オ

フィスにおける VMware VIEW 展開のための最適化サービスとアプリケーションのスケーラビリティが得られます。このソリューションの主要コンポーネントを次に示します。

- VMware VIEW 3.0：デスクトップのバーチャル化と中央集中管理

ステップ 1. バーチャル デスクトップはデータセンターの VMware Infrastructure 3 ESX Server でホスティングされます。

ステップ 2. VMware View Manager によって、VMware ESX Server を実行しているデータセンター内のバーチャル デスクトップにリモートのブランチ ユーザが接続できます。

ステップ 3. Cisco WAAS によって、バーチャル デスクトップのパフォーマンスを向上し、帯域幅需要の低減とバックアップの最適化を実現します。

ステップ 4. WAN の両側に展開された Cisco WAAS によって、エンド ユーザとデータセンター間のディスプレイ プロトコルのトラフィックが最適化されます。TCP 最適化の高度な組み合わせを使用して、WAN の影響を低減し、セッションベースの持続的な圧縮とデータの冗長性の削減を実現します。Cisco WAAS によってディスプレイ プロトコルの配信が最適化されます。これには、現在のバージョンの VMware VIEW MANGER に使用され、現在さまざまなバーチャル デスクトップ実装に主要プロトコルとして使用されている Microsoft Remote Desktop Protocol（RDP）の配信も含まれます。

ステップ 5. ブランチ オフィスの Cisco WAAS アプライアンスは、Microsoft Windows の印刷サービスの実行によりブランチ オフィス ユーザにローカルで印刷サービスを提供します。

ステップ 6. Cisco WAAS をデータセンター間に展開して、障害回復に備えて VMware VIEW インフラストラクチャのバックアップを最適化することもできます。

- Cisco ACE：データセンターの VMware VIEW インフラストラクチャのスケーラビリティとアベイラビリティの向上

ステップ 7. Cisco ACE アプライアンスによって複数の VMware VDM Connection Server 間のロード バランシングが行われ、VMware VIEW ソリューションにスケーラビリティと復元力が与えられます。

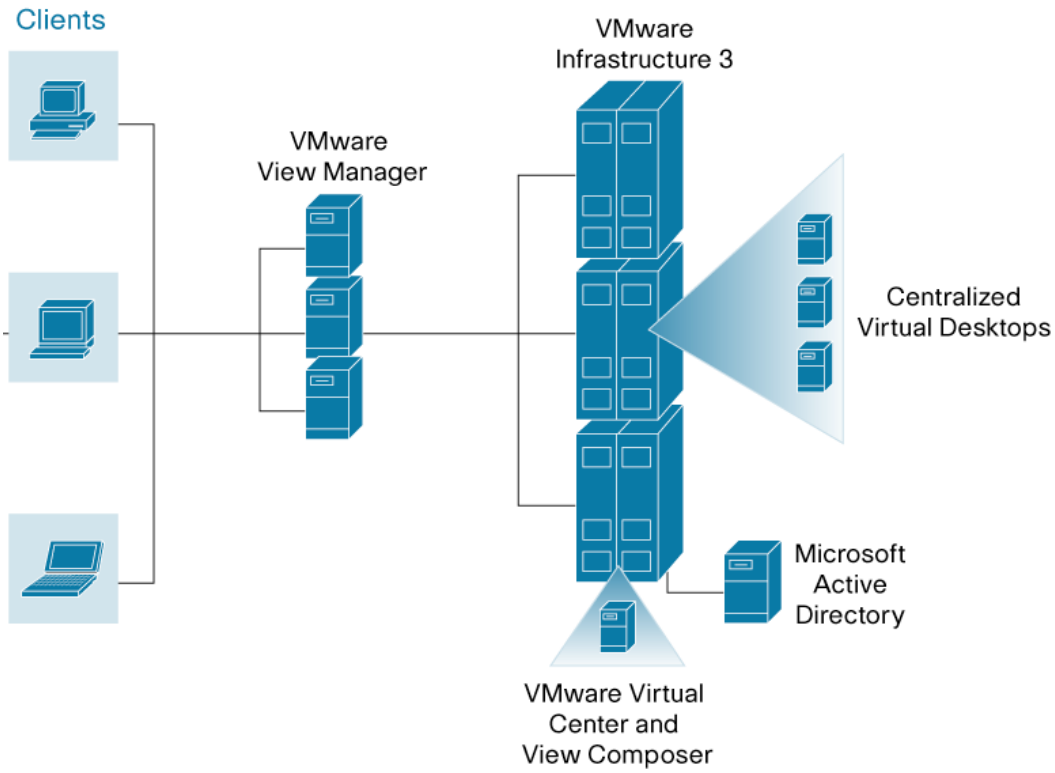
VMware View 3.0

VMware VIEW は、エンタープライズ クラスの制御と管理を行う統合デスクトップ バーチャライゼーション ソリューションです。業界をリードする VMware のバーチャライゼーション プラットフォーム上に構築された VMware VIEW は、効率的で信頼性の高いバーチャル デスクトップ環境を実現します。

VMware VIEW ソリューションには次のコンポーネントが含まれます（図 1）。

- VMware Infrastructure 3 ソフトウェア。VMware ESX および VMware ESXi ソフトウェアなどのバーチャル デスクトップをホスティングするプラットフォームです。
- VMware VDM。ユーザからデータセンターのバーチャル デスクトップへのセキュリティの高い接続を実現するデスクトップ管理サーバで、使いやすい Web ベースのインターフェイスによって中央集中型環境を管理できます。
- VMware VIEW Client。Windows PC 上で実行され、ユーザが VMware VIEW MANAGER を通じてバーチャル デスクトップに接続できます。クライアントでは Microsoft RDP または VMware VIEW Client ソフトウェアを使用できます。

図 1. VMware VIEW ソリューションのコンポーネント



VMware VIEW を使用することによってユーザは、データセンターのサーバにあるバーチャル マシン上で、デスクトップのオペレーティング システムおよびアプリケーションを実行できます。バーチャル マシン上で実行されるこれらのデスクトップ システムは、バーチャル デスクトップと呼ばれます。ユーザはリモート ディスプレイ プロトコルを使用して、デスクトップ PC クライアントまたはシン クライアント（VMware VIEW クライアントと呼ばれる）からバーチャル デスクトップおよびアプリケーションにアクセスします。

VMware VIEW クライアントは、まず VMware View Manager に接続されます。次に VMware View Manager によって、この接続が端末のバーチャル デスクトップに送信されます。VMware ESX Server 上で実行されるバーチャル デスクトップのセントラル インベントリは VMware View Manager によって保持されます。管理者は VMware ESX Server のバーチャル デスクトップのプロビジョニングを行い、それらを VMware View Manager に登録します。大規模な環境では、複数の VMware View Manager サーバを使用してクライアント要求を共有できます。このような場合、1 台の VMware View Manager サーバをプライマリとして、VMware View Manager サーバのレプリケーションが作成されます。

VMware VIEW の主要な利点は次のとおりです。

- デスクトップ環境が切り離される。
- データセンターでデータのセキュリティが確保される。
- すべてのアプリケーションがバーチャル マシン上で動作する。
- 標準の管理ツールがバーチャル マシンで動作する。
- イメージが中央集中管理される。
- ハードウェアを統合できる。

- デスクトップが常時稼動し、接続された状態になる。
- ユーザは任意の場所から自分のデスクトップにアクセスできる。

Cisco Application Networking Service

Cisco ANS はアプリケーション ネットワーキングのソリューションおよびテクノロジーの包括的なポートフォリオです。データセンターとブランチ オフィスの両方におけるアプリケーション配信ネットワークをサポートします。Cisco ANS 製品のポートフォリオには次のコンポーネントが含まれます。

- **Cisco WAAS**：中央集中管理されるアプリケーションのリモート ユーザへの配信を高速化し、リソースの統合、WAN の最適化、クリティカルなアプリケーションのローカルでのホスティングに役立ちます。
- **Cisco ACE**：アプリケーションのスイッチングとロード バランシングにより、アプリケーション全体のアベイラビリティ、セキュリティ、パフォーマンスを最適化します。

Cisco Wide Area Application Service

Cisco WAAS は包括的な WAN 最適化ソリューションで、WAN 経由のアプリケーションの高速化、ブランチ オフィスへのビデオ配信、ブランチ オフィスの IT サービスのローカル ホスティングを行います。Cisco WAAS によって IT 部門は、LAN 同様のアプリケーション パフォーマンスを維持しながら、アプリケーションを中央集中管理してデータセンターに保管できます。また、次のアプリケーション高速化および WAN 最適化機能を通じて、ブランチ オフィスのデバイスの設置面積を最小に抑えながら、ローカルのブランチ オフィスの IT サービスを迅速に得られます。

- **Transport Flow Optimization（TFO）**：TFO は、遅延が長く、ロスが大きく、帯域幅の広いネットワークにおける TCP パフォーマンスの制限に対処します。TFO では次の主要な最適化を採用しています。
  - **Selective acknowledgement（SACK）およびその拡張機能**：ロスが検出された場合に再送信が必要なデータ量を低減します。
  - **広い初期ウィンドウ**：使用可能な帯域幅をよりタイムリーに使用できるようにし、スロースタート モードで費やされる各接続時間の合計量を減らします。
  - **TCP ウィンドウのバーチャル ウィンドウ スケーリング**：一定時間に未処理、未承認のままネットワーク内に存在可能なデータ量を増やすことによって、より大容量のデータをエンド ノードで送受信できます。
  - **高度な輻輳回避**：各 TCP 接続の輻輳ウィンドウをインテリジェントに管理することにより、ロスが検出された場合のスループットに関するパフォーマンスへの影響を低減します。この輻輳回避モードでは、アプリケーションを効率的に使用するための最適化も有効になり、使用可能な帯域幅をより有効に活用した TCP スループットが得られます。
- **Data Redundancy Elimination（DRE）**：DRE は、TCP バイト ストリーム内に見られるデータのブロックの双方向データベースです。DRE は 着信側の TCP トラフィックを点検し、データ パターンを識別します。パターンは識別されて DRE データベースに追加され、圧縮履歴として将来使用できます。また繰り返されるパターンは容量の非常に小さいシグネチャで置き換えられ、オリジナル メッセージを再構築する方法を遠隔地の装置に伝えます。DRE では、交換の必要があるパケットが最小限に抑えられるため、帯域幅の使用量だけでなくデータ転送に関連する遅延も低減されます。遠隔地の Cisco Wide Area Application Engine（WAE）デバイスによって再構築されたオリジナル メッセージは常に複数レベルで精度が検証され、アプリケーションに依存しないため、DRE ではアプリケーションおよびプロトコルの統一性と正確性が最大限に維持されます。1 つのアプリケーション フロー

から学習されたパターンは、別のフローを識別する場合に使用可能です。アプリケーションが異なる場合も使用できます。DRE では、アプリケーション、データ、ワークロードに応じて 2:1 から 100:1 の圧縮率が得られます。

- **持続的な Lempel-Ziv（LZ）圧縮**：Cisco WAAS によってコネクション型圧縮履歴を伴う LZ 圧縮が実装され、TCP 接続によって消費される帯域幅をさらに低減します。持続的な LZ 圧縮は、単独で、または DRE と組み合わせて使用できます。使用されるアプリケーションと送信されるデータに応じて、DRE による圧縮に加えて 2:1 から 5:1 までの圧縮を行います。

Cisco Application Control Engine（ACE）

Cisco ACE のアプリケーション スイッチは、コア サーバのロードバランシング サービス、高度なアプリケーション高速化、セキュリティ サービスを提供し、アプリケーションのアベイラビリティ、パフォーマンス、セキュリティを向上させます。Cisco ACE アプリケーション スイッチによって、バーチャル化されたハードウェア プラットフォーム、アプリケーション固有のインテリジェンス、強力なパフォーマンス、きめ細かなロールベースの管理が実現します。Cisco ACE アプリケーション スイッチは、一般的にデータセンターの非対称ソリューションに展開されます。

Cisco ACE アプリケーション スイッチは Cisco ファミリーのデータセンター 3.0 ソリューションの一部で、次の点で役立ちます。

- アプリケーションのアベイラビリティの向上
- アプリケーションのパフォーマンスのスケーリング
- アプリケーション配信のセキュリティ確保
- データセンター統合の促進

Cisco ACE では、インテリジェントなレイヤ 4 のロードバランシング と、先進の高速化およびセキュリティ機能が組み込まれたレイヤ 7 のコンテンツスイッチング テクノロジーの広範な組み合わせにより、これらの目標を達成します。アプリケーションのアベイラビリティを向上するため、Cisco ACE はクラス最高のアプリケーション スイッチング アルゴリズムと、アベイラビリティの高いシステム ソフトウェアおよびハードウェアを使用しています。Cisco ACE によって、業界をリードするアプリケーション トラフィックのスケーラビリティおよびスループットが実現します。Cisco ACE はフレキシビリティの高いアプリケーション トラフィック管理と CPU 中心のタスク（SSL 暗号化および復号化処理や TCP セッション管理など）のオフローディングによってサーバの効率を大幅に向上します。

ソリューションの利点

共同ソリューションは、ユーザにバーチャル デスクトップを提供することによって、バーチャル デスクトップのアベイラビリティ、パフォーマンス、セキュリティ、コストの最適化を実現します。

バーチャル デスクトップのパフォーマンス

Cisco WAAS 製品ファミリーは、バーチャル デスクトップ配信のためのアプリケーション最適化サービスを提供し、VMware VIEW クライアントの高いパフォーマンスをサポートします。

- **WAN の最適化**：インテリジェントなキャッシング、圧縮、プロトコル最適化を実現（3 ～ 25 倍の印刷高速化、90 %の トラフィック低減など）
- **トラフィックの圧縮**：スケーラブルな LZ 圧縮を実現

- **オブジェクト キャッシング**：サーバへの要求を低減
- **印刷の最適化**：WAN を通過する印刷データの低減および印刷待ち時間の短縮

バーチャル デスクトップのアベイラビリティ

Cisco ACE 製品ファミリーは、VMware VIEW MANAGER コネクション ブローカに対してロードバランシング サービスを提供します。

- **サーバおよびアプリケーションのヘルス モニタリング**：VMware VIEW MANAGER Connection Server のアベイラビリティを連続してインテリジェントにモニタリング
- **サーバのロードバランシング**：エンドユーザのデスクトップ接続要求をアベイラビリティの最も高い VMware VIEW MANAGER Connection Server に効率的にルーティング

ソリューションのアーキテクチャ

このソリューションでは、バーチャル デスクトップが VMware ESX Server 上で実行されており、このアーキテクチャでは 2 台の VMware ESX Server を使用します。これらのサーバを共有ストレージに接続して、VMware VMotion、VMware Distributed Resource Scheduler（DRS）、およびハイ アベイラビリティ機能を利用します。VMware ESX Server および VMware ESX Server で実行されるバーチャル マシンは、個別のサーバ上で実行される VMware VirtualCenter で管理します。

すべてのバーチャル デスクトップのインベントリは、VMware VIEW MANAGER コネクション ブローカ サーバによって保持されます。このアーキテクチャでは、2 台の VMware VIEW MANAGER コネクション ブローカ サーバを使用します。ユーザが要求すると、これらのサーバが Cisco ACE ロード バランサによって負荷分散されます。

ブランチ オフィスとデータセンター間の接続は、Cisco WAAS によって最適化されます。ブランチ オフィス側とデータセンター側の両ルータが、Web Cache Communication Protocol（WCCP）のトラフィックをインターセプトするため、2 台の Cisco WAAS アプライアンス（ブランチ オフィス側とデータセンター側に各 1 台）を使用してトラフィックを最適化します。データセンター側では 1 台の Cisco WAAS Central Manager を使用して、トラフィックのモニタリングと Cisco WAAS の設定を行います。

ユーザは、さまざまな印刷オプションを使用できます。データセンターとブランチ オフィスの両方のプリント サーバが、バーチャル デスクトップからの要求を受け入れます。さらに、ブランチ オフィスの VMware VIEW クライアントがローカル プリンタに接続されます。

バーチャル デスクトップ マシンのインストールと設定

バーチャル デスクトップ マシンは VMware ESX Server 上で実行されます。バーチャル マシンの作成とプロビジョニングについては、最新の VMware ドキュメントを参照してください。バーチャル デスクトップを作成するために、このソリューションでは次の手順を使用しました。

ステップ 1.　VMware VirtualCenter から、バーチャル マシンを作成します。図 2 は、このソリューションで使用した設定例を示しています。

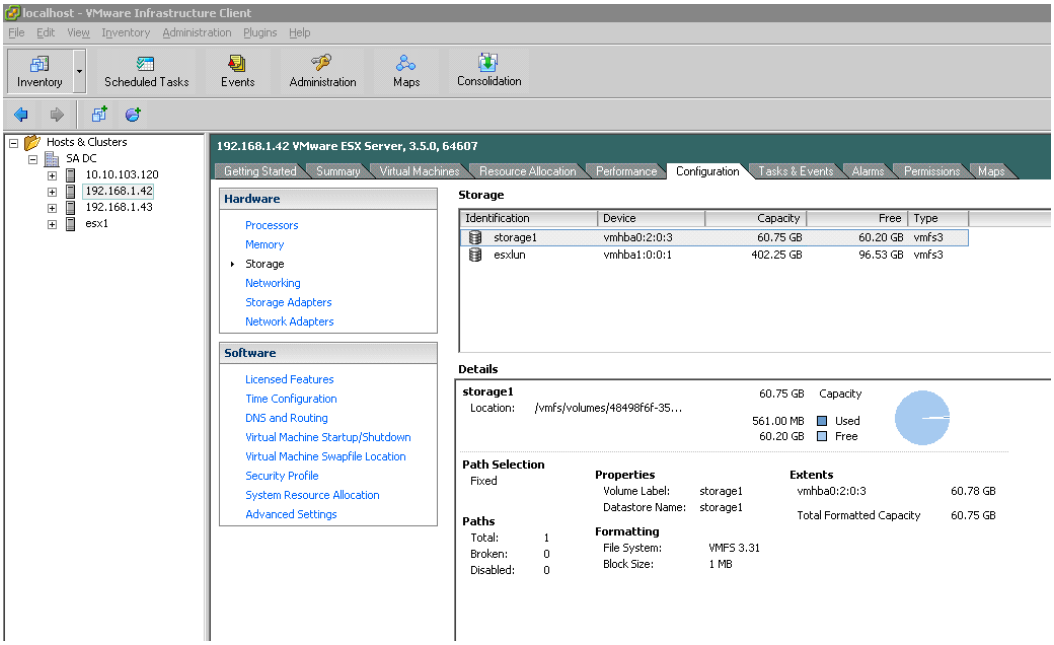
ステップ 2.　バーチャル マシンに Microsoft Windows XP をインストールします。

ステップ 3.　バーチャル マシンに VMware ツールをインストールします。

ステップ 4.　最新の VMware VIEW エージェントを Microsoft Windows XP バーチャル マシンにダウンロードしてインストールします。

ステップ 5.　バーチャル マシンのテンプレートを作成して、VMware VIEW MANAGER のデスクトップにプロビジョニングします。

図 2.　ソリューション設定例



注: このソリューションのパフォーマンスに対するバーチャル マシンの最適化については、「最適化のためのバーチャル デスクトップの設定」を参照してください。

VMware VIEW MANAGER Connection Server のインストールと設定

VMware VIEW MANAGER Connection Server のインストールと設定については、最新の VMware ドキュメントを参照してください。VMware VIEW MANAGER Connection Server をインストールするために、このソリューションでは次の手順を使用しました。

ステップ 1.　Microsoft Windows Server 2003 をインストールします。

ステップ 2.　VMware VIEW MANAGER Connection Server の実行可能ファイル（VMware-viewconnectionserver-3.0.0-<xxx>.exe）をダウンロードしてインストールします。1 台目のサーバを標準サーバとしてインストールします(図 3)。

ステップ 3.　2 台目のサーバでもここまでの手順を繰り返しますが、今回は [Replica] を選択します。

ステップ 4.　次に、VMware VIEW MANAGER Connection Server を設定するために 1 回限りの設定が要求されます。

ステップ 5.　ブラウザを起動して http://hostname_or_ip.of.View Manager.server/admin にアクセスし、適切なクレデンシャルでログインします。通常は、任意のローカル管理者グループのユーザを使用できます。

ステップ 6.　[Configuration] セクションで、ライセンス キーを追加します。

ステップ 7. [VirtualCenter Servers] セクションで [Add] をクリックし、VMware VIEW MANAGER で使用する VMware VirtualCenter の詳細を入力します。

ステップ 8. VMware VIEW MANAGER サーバのリストから選択して [Enable] をクリックすることで、VMware VIEW MANAGER Connection Server をイネーブルにします。

VMware View Composer

VMware View ドキュメントに記載された手順を実行して、VMware View Composer をインストールします。

バーチャル デスクトップのプロビジョニング

デスクトップを VMware VIEW MANAGER にプロビジョニングする必要があります。このソリューションでは次の手順が実行されました。

ステップ 1. Vmware VIEW MANAGER Connection Server にログインして（前項を参照）、[Inventory] をクリックします。

ステップ 2. [All Desktops] セクションで、[Desktops] タブをクリックして [Add] をクリックします。

ステップ 3. [Desktop Pool (persistent)] を選択し、手順に従って必要な数のデスクトップをプロビジョニングします。VMware VirtualCenter インベントリからバーチャル デスクトップのテンプレートを選択します（要求された場合）。

ステップ 4. すべてのデスクトップを作成してプールに追加したら（しばらく時間がかかります）、デスクトップをユーザに指定します。必要に応じてユーザまたはグループを選択します。

VMware VIEW Client のインストールと接続

VMware VIEW Client をインストールして接続します。このソリューションでは次の手順が実行されました。

ステップ 1. VMware VIEW Client ソフトウェア（VMware-viewclient-3.0.0-<xxx>.exe）をダウンロードして実行します。

ステップ 2. 標準インストールの手順を実行して、VMware VIEW Client ソフトウェアをインストールします。

ステップ 3. VMware VIEW Client ソフトウェアを実行して、接続する VMware VIEW MANAGER サーバの IP またはホスト名を入力します。接続するバーチャル マシンをリストから選択します。ハードウェア ロード バランサを使用する場合（このソリューションの場合など）、[VMware VIEW Client] ウィンドウでロード バランサの IP またはホスト名を入力します。

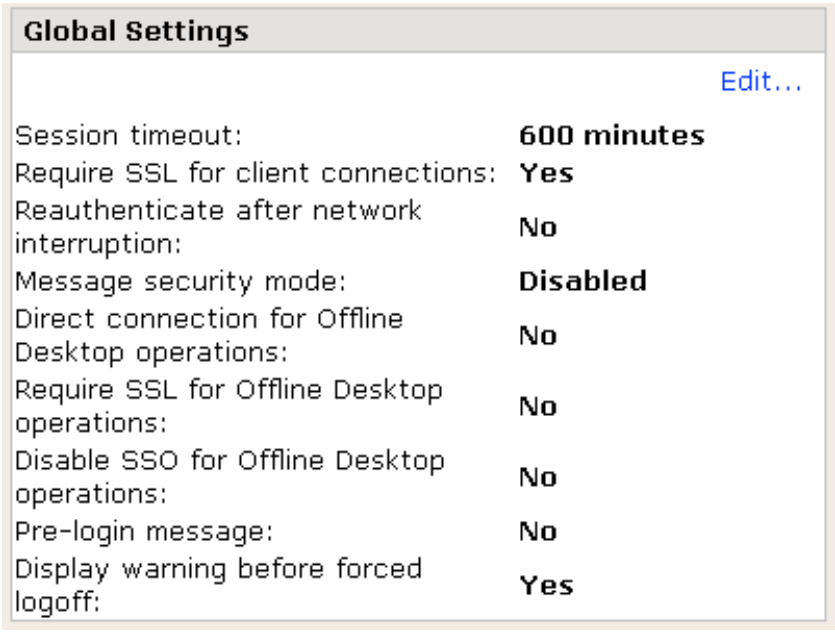
SSL 接続のための VMware View の準備

View Client と View Manager 間の通信に SSL を使用するための VMware View Manager の設定については、VMware のドキュメントに記載された詳細な手順に従ってください。なお、便宜を計って、簡単な手順を次に示します。

1. 前項に記載されているように、VMware View Manager にログインします。
2. 『VMware View Administrator guide』の「Creating SSL Server Certificates」の項を参照します。

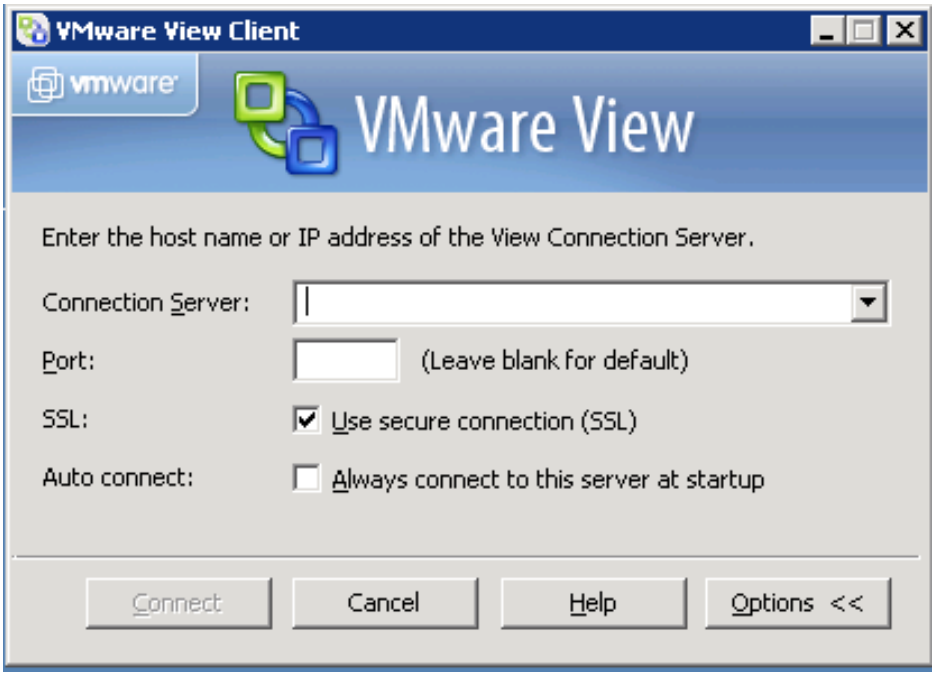
3. [Configuration] の [Global Settings] で（図 3 を参照）、[Require SSL for client connections] を選択します。

図 3. [Global Settings]



4. View Client からの接続時に [Use secure connection (SSL)] チェックボックスはオンになっていることを確認します（図 4 を参照）。

図 4. VMware View



サーバのハードウェアとソフトウェア

VMware ESX
VMware ESX Server では、すべてのデスクトップ バーチャル マシンが実行されます。テストでは、次のハードウェアを使用します。

- ホスト デスクトップ バーチャル マシンのイメージが実行される VMware ESX 3 Server × 2
- VMware VIEW MANAGER Connection Server × 2
- VMware VirtualCenter Server および View Composer × 1

VMware ESX Server 環境は、次の設定の VMware ESX 3i が実行される 2 台の物理サーバで構成されます。

- デュアルコア Intel Xeon CPU（3.06 GHz） × 2
- 4 GB RAM
- VMware ESX 3.5

VMware VIEW MANAGER Connection Server、Virtual Center、および View Composer
VMware VIEW MANAGER Connection Server は、ユーザが接続や認証を行うミドル クライアントです。その後、ユーザは自分のデスクトップを選択して、エンド バーチャル デスクトップに接続します。テストでは、次のハードウェアとソフトウェアが VMware VIEW MANAGER Connection Server に使用されます。

- Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1
- デュアルコア Intel Xeon プロセッサ（3.06 GHz） × 2
- 1 GB RAM
- ローカル ストレージ

VMware VMotion のストレージ
物理 VMware ESX Server をファイバ チャネルを介して EMC Clariion ストレージに接続します。2 台のサーバが同時に物理ストレージ上の Virtual Machine File System（VMFS; バーチャル マシン ファイル システム）に書き込むことが可能です（VMware VMotion の前提条件）。

バーチャル デスクトップ
各 VMware ESX Server によって、次の設定で実行される 10 台のバーチャル マシンがホスティングされます。

- CPU × 1
- 1 GB RAM
- 8 GB ハード ディスク
- Microsoft Windows XP Service Pack 2

その他のコンポーネント
データセンター ネットワーク全体を取り扱う VMware バーチャル マシンとして実行される Microsoft Windows 2003 Server には、次のものが含まれます。

- Microsoft Active Directory
- Domain Name System（DNS; ドメイン ネーム システム）
- Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）

印刷

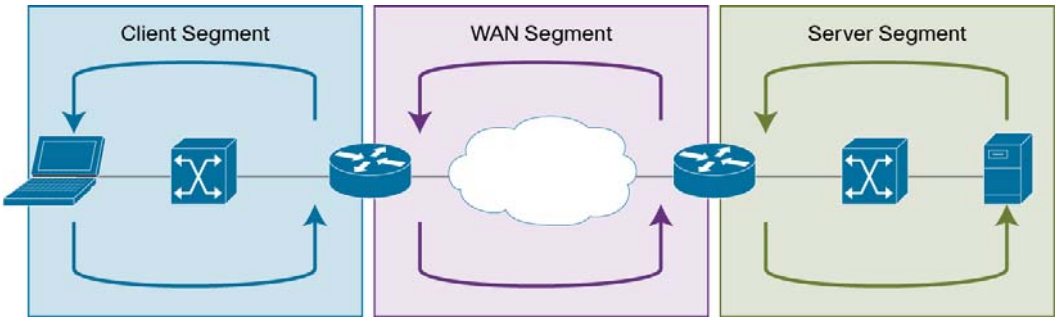
プリント サーバがブランチ オフィス側とデータセンター側のどちらで実行されるかは、印刷する状況によって異なります。詳細については、実装の項を参照してください。印刷テストでは、次のプリンタを使用しました。

- HP LaserJet 4000（Jetdirect ネットワークポートを装備）

Cisco WAAS および Cisco ACE を使用しないソリューションのワークフロー

リモート サイトからのパケット フローは、3 つのセグメント（クライアント、WAN、サーバ）に分類できます（図 5）。

図 5. パケット フロー



クライアント セグメント

クライアント セグメントはユーザが接続する場所であり、ユーザはデータセンターのバーチャル マシンに接続することができます。PC またはシン クライアントをローカルの外部スイッチ、または統合スイッチや統合ルータに接続します。PC またはシン クライアント上で [VMware VIEW Client] を開き、データセンターで実行されているバーチャル デスクトップに接続すると、PC からスイッチへデータが送信されます。スイッチから WAN に接続されているルータへそのデータが転送されます。

WAN セグメント

WAN では、クライアント ロケーションからサーバ ファームがあるデータセンターへ接続できます。サービス プロバイダーによって、WAN に特定の Service-Level Agreement（SLA; サービスレベル契約）が提供されます。WAN は本質的にデータ トラフィック（データ パケット）に遅延やパケット損失を発生させます。

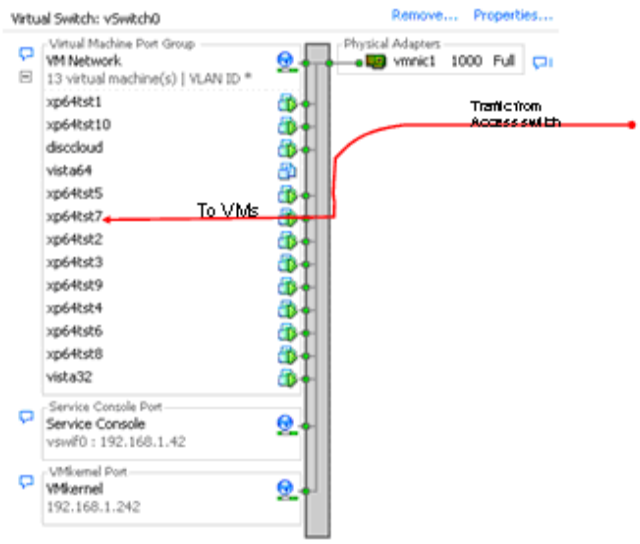
VMware ESX Server セグメント

このサーバ セグメントは、ハイ アベイラビリティと復元力を備えたコア、アグリゲーション レイヤ、およびアクセス レイヤのイーサネット スイッチングで構成されます。コアでは、WAN とアグリゲーション レイヤ間でデータ トラフィックが転送されます。アグリゲーション レイヤでは、複数のアクセス レイヤを統合でき、アクセス レイヤのトラフィックがコアに転送されます。また、アグリゲーション レイヤでは、コア レイヤからデータ トラフィックが受信され、適切なアクセス レイヤに送信されます。アクセス レイヤでは、バーチャル デスクトップが常駐する VMware VIEW MANAGER Connection Server および VMware ESX Server へ接続できます。クライアント セグメントからのデータ トラフィックは、適切なサーバで受信されるまでデータセンターを横断します。

VMware ESX Server 内部

外部のアクセス スイッチからのトラフィックは、その後 VMware ESX Server 内部のバーチャル スイッチにリダイレクトされます。バーチャル スイッチがバーチャル マシンに接続されて、トラフィックが渡されます（図 6）。詳細については、シスコと VMware 共同の White Paper を参照してください。

図 6. VMware ESX Server 内部のトラフィック フロー



VMware VIEW 向けの Cisco ANS アーキテクチャ

Cisco ACE と WAAS は、データセンター内に常駐し、複数の VMware VIEW MANAGER サーバ グループ、およびその他のエンタープライズ アプリケーション向けのバーチャル化アプリケーション最適化サービスを提供するよう設定されています。

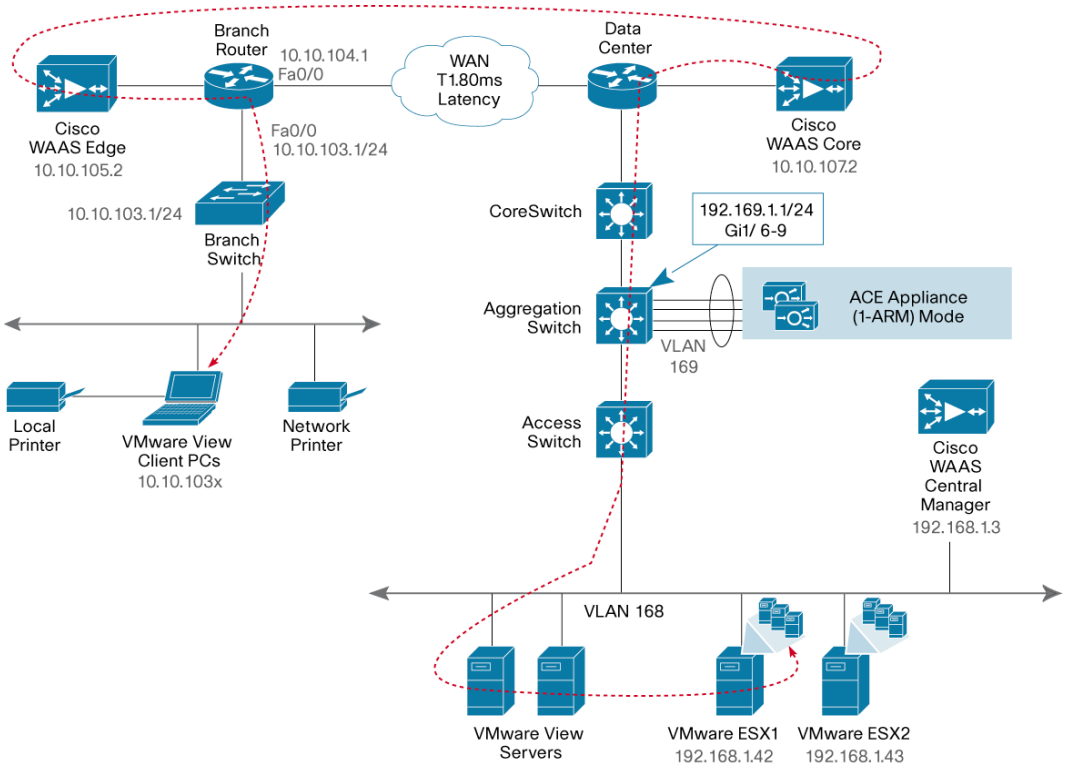
これらのソリューションは固有の場所に配置されるため、エンドユーザ トラフィックがエンド バーチャル デスクトップへ転送される前に、そのトラフィックに対してインテリジェントな処理を実行できます（サーバ ロード バランシング、サーバ ヘルス モニタリング、エンドユーザ アクセス コントロールなど）。

また、Cisco WAAS もブランチ オフィス内に常駐し、そのオフィスのすべてのアプリケーション ユーザに対してバーチャル化アプリケーション最適化サービスを提供するよう設定されています。Cisco WAAS をブランチ オフィスとデータセンターに展開することで、インテリジェントなキャッシング、圧縮、およびプロトコル最適化を使用して、WAN 最適化サービスが提供されます。

エンド ユーザが VMware VIEW MANAGER Server を介してバーチャル デスクトップにアクセスするとき、Cisco WAAS によって応答が圧縮された後、最小の帯域幅使用量と高速化により、WAN 上で効率的に転送されます。一般的に使用される情報は、ブランチ オフィス内の Cisco WAAS ソリューションとデータセンター内の Cisco WAAS ソリューションの両方でキャッシュされ、これによってサーバと WAN の負荷が大幅に軽減されます。

図 7 は、Cisco ANS アーキテクチャを示しています。

図 7. VMware VIEW と Cisco WAAS のネットワーク構成



VMware VIEW と Cisco ANS ソリューションは、主に次の 2 つの部分で構成されています。

- データセンター
- 企業のブランチ オフィス

データセンター

データセンターは、『Data Center Infrastructure Design Guide 2.1』内の設計ガイドライン「Cisco Validated Design」（http://www.cisco.com/go/srnd）に従っています。この設計は、データセンターの WAN ルータ、コア、アグリゲーション レイヤ、およびアクセス レイヤのイーサネット スイッチングと、アプリケーションが常駐するサーバ ファームで構成されています。本書では、データセンターの WAN ルータ、アグリゲーション レイヤ、およびサーバ ファームについて説明します。

コア イーサネット スイッチングでは、データセンターの WAN ルータおよびアグリゲーション レイヤとのルーティングが提供されます。アクセス レイヤ イーサネット スイッチングでは、サーバ ファーム用にアグリゲーション レイヤとのレイヤ 2 接続が提供されます。

データセンターの WAN ルータでは、データセンターの Cisco WAE にトラフィックがリダイレクトされることで、ブランチ オフィスの WAN ルータと同じ機能が実行されます。データセンターの Cisco WAE では、次の機能が実行されます。

- **ローカルにキャッシュされたデータ**：要求されているデータがローカルにキャッシュされている場合、Cisco WAE は要求側に対してキャッシュされたデータで応答し、ブランチ オフィスの必要なデータだけを要求します。このプロセスでは必要なデータだけが要求されるため、WAN が効率化されます。

- **新しいデータ**：ブランチ オフィスへ転送している、またはブランチ オフィスから着信するデータが新しい場合、Cisco WAE がそのデータに対して圧縮アルゴリズムを実行することで、WAN が効率化されます。

データセンターには Cisco WAAS Central Manager があり、Cisco WAE アプライアンス上で実行されます。Cisco WAAS Central Manager では、Cisco WAAS 機能を設定したり、Cisco WAAS のトラフィックを監視するための中央集中型のメカニズムが提供されます。また、Cisco WAE の何千もの ノードを含むトポロジを管理し、SSL を使用して任意の Web ブラウザからアクセスすることが可能です。Cisco WAAS Central Manager は、2 つの Cisco WAE アプライアンスをセントラル マネージャとして展開することで、ハイ アベイラビリティを実現できます。

Cisco WAAS トポロジ内では、各 Cisco WAE によって Configuration Management System（CMS; 構成管理システム）と呼ばれるプロセスが実行されます。CMS プロセスでは、Cisco WAAS Central Manager と Cisco WAE アプライアンス間の SSL 暗号化済み双方向の設定同期化が行われます。また、CMS プロセスは、設定可能な時間間隔でレポート情報と統計を交換するためにも使用されます。管理者が Cisco WAE アプライアンスの 1 つまたはグループに設定やポリシーの変更を適用すると、その変更が Cisco WAAS Central Manager によって管理下にある各 Cisco WAE アプライアンスに自動的に伝送されます。その変更を受信できない Cisco WAE アプライアンスは、次回利用可能になった際に変更を受信できます。

アグリゲーション レイヤには Cisco ACE が含まれており、次の機能が提供されます。

- **バーチャライゼーション**：バーチャライゼーションでは、デバイスが複数のコンテキストに分割されます。分割された各コンテキストは別々のアプリケーション用に設定することが可能で、互いに独立しています。共同ソリューションでは、Cisco ACE アプライアンスが Admin コンテキストと VMware VIEW コンテキストで設定されています。
- **サーバ ロード バランシング**：Cisco ACE VMware VIEW コンテキストは、VMware VIEW MANAGER Connection Server のインテリジェントなロード バランシングを提供するよう設定されています。
- **セッション持続性**:セッション持続性は、クライアント要求をセッション期間中に同じサーバに転送する機能です。Cisco ACE は、ソース IP ベースのセッション持続性用に設定されています。

企業のブランチ オフィス

企業のブランチ オフィスのセットアップでは、Cisco WAE アプライアンスをローカルのブランチ オフィス ルータ（通常は Cisco Integrated Services Router）に接続します。

PC またはシン クライアントをローカルの外部スイッチ、または統合スイッチや統合ルータに接続します。PC またはシン クライアント上で [VMware VIEW Client] を開き、データセンターで実行されているバーチャル デスクトップに接続すると、PC からスイッチへデータが送信されます。スイッチから WAN に接続されているルータへそのデータが転送されます。

トラフィックは、WCCP によってブランチ オフィス ルータから Cisco WAE へリダイレクトされます。

Cisco WAE では次の機能が実行されます。

- **ローカルにキャッシュされたデータ**：要求されているデータがローカルにキャッシュされている場合、Cisco WAE は要求側に対してキャッシュされたデータで応答し、サーバ ファームの必要なデータだけを要求します。この方法では必要なデータだけが要求されるため、WAN が効率化されます。
- **新しいデータ**：サーバ ファームへ転送している、またはサーバ ファームから着信するデータが新しい場合、Cisco WAE がそのデータに対して圧縮アルゴリズムを実行することで、WAN が効率化されます。

ブランチ オフィスとデータセンター間の WAN シミュレーション

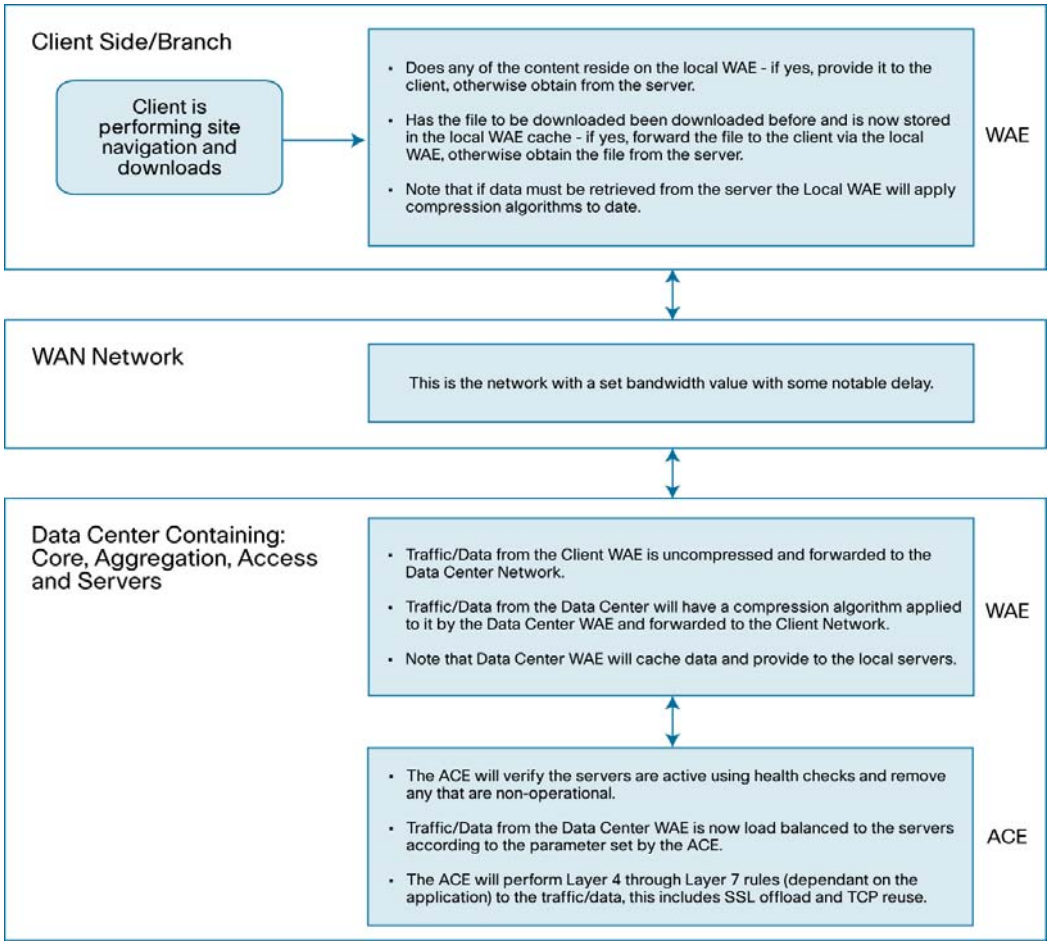
実際の WAN のような状況でソリューション テストを行うために、WAN ブリッジを使用しました。WAN シミュレータでは、次の WAN リンクをシミュレートできます。

- WAN タイプ 1 T1
  - 帯域幅：1.544 Mbps
  - 遅延：100 ミリ秒（ms）
- WAN タイプ 2
  - 帯域幅：10 Mbps
  - 遅延：50 ms

Cisco WAAS と Cisco ACE を使用したプロセス フロー

図 8 は、ネットワーク内で Cisco ACE と Cisco WAAS が接続されている場合のプロセスのデータ フローを示しています。

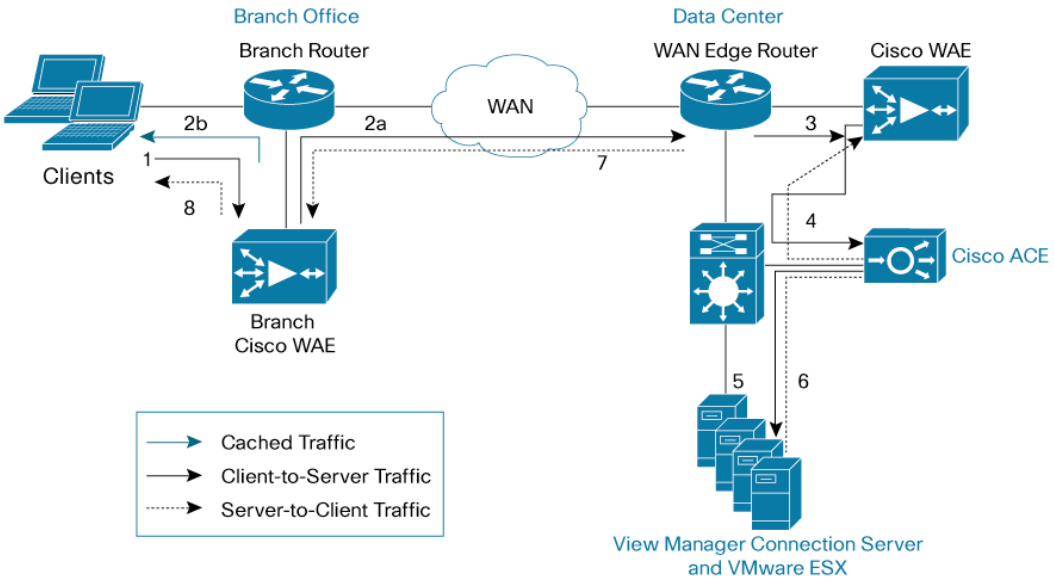
図 8. Cisco WAAS と Cisco ACE のプロセス フロー



Cisco WAAS と Cisco ACE を使用したパケット フロー

図 9 は、クライアントと VMware ESX Server 間のハンドシェイクのシーケンスと、データ転送フェーズを示しています。

図 9. Cisco WAAS と Cisco ACE のパケット フロー



次のシーケンスでは、クライアントと VMware ESX Server 間のハンドシェイクと、データ転送フェーズを説明しています。

1. クライアントが、TCP 同期（SYN）パケットを VMware VIEW MANAGER Connection Server のロード バランシング用に Cisco ACE で設定したバーチャル IP アドレスに送信します。そのパケットはブランチ ルータに転送されます。ブランチ ルータは WCCP を使用してパケットをインターセプトし、ブランチ オフィスの Cisco WAE アプライアンスに転送します。
2. アプリケーション分類子によってアプリケーションの最適化が分類されると、ブランチ オフィスの Cisco WAE は、新しい TCP オプション（0x21）をパケットに適用します。ブランチ オフィスの Cisco WAE は、対象のデバイス ID とアプリケーション ポリシーのサポートを新しい TCP オプション フィールドに追加します。このオプションはパス内の他の Cisco WAE によって検証され、最初の Cisco WAE デバイスの ID およびポリシー フィールドとして認識されます。最初の ID および ポリシー フィールドは、別の Cisco WAE によって変更されません。パケットはブランチ オフィス ルータに転送されてから、WAN に転送されます。
3. データ転送フェーズにおいて、要求されたデータがキャッシュに入れられた場合は、ブランチ オフィスの Cisco WAE がキャッシュされたデータをクライアントに返します。トラフィックが WAN を通過してサーバ ファームまで伝送されることはありません。したがって、応答時間と WAN リンク使用率の両方が改善されます。
4. パケットが WAN エッジ ルータに到達します。WAN エッジ ルータは WCCP を使用してパケットをインターセプトし、そのパケットをデータセンターの Cisco WAE に転送します。
5. データセンターの Cisco WAE がパケットをインターセプトします。最初のデバイス ID とポリシーが投入されたことを確認すると、データセンターの Cisco WAE は最後のデバイス ID フィールドを更新します（最初のデバイス ID とポリシーのパラメータは変更さ

れません）。データセンターの Cisco WAE は、パケットを WAN エッジ ルータに転送します。エッジ ルータはそのパケットをアグリゲーション スイッチに転送し、アグリゲーション スイッチがそのパケットを Cisco ACE に転送します。Cisco ACE は、サーバ ファームのいずれかの VMware VIEW MANAGER Connection Server の接続のロード バランシングを実行します。

以降の手順では、反転トラフィック フローについて説明します。

6. VMware VIEW MANAGER Connection Server は、TCP オプションを使用せずに SYN/ACK パケットをクライアントへ返します。サーバからのパケットは、アグリゲーション スイッチで Policy-Based Routing（PBR; ポリシーベース ルーティング）ルールによって照合されて Cisco ACE に転送されてから、WAN エッジ ルータに転送されます。WAN エッジ ルータは、パケットをデータセンターの Cisco WAE に転送します。データセンターの Cisco WAE は、TCP オプション（0x21）を使用してパケットをマークします。データ転送フェーズにおいて、データがキャッシュに存在しない場合は、データセンターの Cisco WAE が対象のデータをキャッシュします。
7. データセンターの Cisco WAE が、パケットを WAN エッジ ルータに送信します。
8. パケットは WAN を通過してブランチ オフィス ルータに到達します。ブランチ オフィス ルータはパケットをインターセプトし、それをブランチ オフィスの Cisco WAE に転送します。SYN/ACK TCP オプション（0x21）には ID とアプリケーション ポリシーが含まれているため、ブランチ オフィスの Cisco WAE は、Cisco WAE がデータセンターに属していることを認識します。ブランチ オフィスの Cisco WAE が、アプリケーション固有のポリシーを TCP オプションで定義されるリモート ピアと比較すると、ポリシーの自動ネゴシエーションが発生します。この時点で、データセンターの Cisco WAE とブランチ オフィスの Cisco WAE は、この特定の TCP フローにアプリケーションの最適化を適用することを決定します。データ転送フェーズにおいて、データがキャッシュに存在しない場合は、ブランチ オフィスの Cisco WAE が対象のデータをキャッシュします。
9. パケットはブランチ オフィス ルータに転送されてから、VMware VIEW クライアントに転送されます。

Cisco WAAS ソリューションの実装と設定

実装の概要

Cisco WAAS ソリューションでは、自動検出を行ってアプリケーションの最適化を適切に実行するために、少なくとも 3 台の Cisco WAE アプライアンスが必要です。Cisco WAE の 1 台は企業のデータセンターに、もう 1 台はブランチ オフィス サイトに配置します。企業のデータセンターの Cisco WAE は、WAN ルータに接続された WAN エッジ上に配置します。3 台目の Cisco WAE はセントラル マネージャとして使用します。このアーキテクチャでは、ローカルのブランチ オフィス ルータから Cisco WAE デバイスがオフロードされ、ローカル スイッチで使用可能なポートが活用されます。この設計は、ソリューションにスケーラビリティとアベイラビリティをもたらします。

ネットワークの統合

Cisco WAAS テクノロジーでは、成果を生み出すためにアプリケーション トラフィックの効率的かつ予測可能なインターセプトが必要になります。これは Cisco WAE デバイスが TCP 通信全体を参照する場合に重要です。WAN エッジにおいて、Cisco ルータは次の 4 つのトラフィック インターセプト方式をサポートしています。

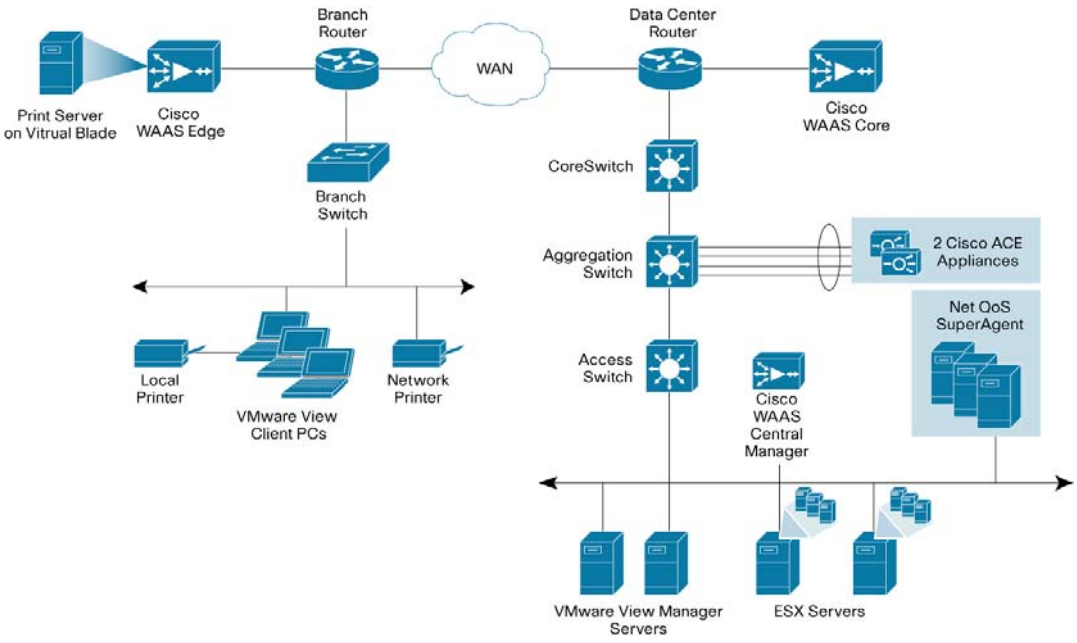
- インライン ハードウェア
- WCCP バージョン 2
- Cisco ACE におけるサービス ポリシー
- PBR

WCCPv2 は、リモート ブランチ オフィス環境で最も一般的に使用されている方式です。そのため、このソリューションには WCCPv2 を使用しています。

ネットワーク トポロジ

図 10 は、このソリューションで使用したネットワーク トポロジを示しています。

図 10. Cisco WAAS ソリューションのネットワーク トポロジ



ハードウェア

- Cisco WAE-674-K9
- Cisco WAE-7341-K9
- Cisco WAE-612-K9

ソフトウェア

- Cisco WAAS ソフトウェア バージョン 4.1.3

機能、サービス、およびアプリケーション設計に関する考慮事項

VMware VIEW ソリューションでは、ポート 80 を使用して VMware VIEW クライアント マシンからバーチャル マシンへの RDP 接続が送信されます。Cisco WAAS のコンテキストにおいて、ポート 80 はデフォルトで高速化されるため、アプリケーションにデフォルトのアプリケーション プロファイルに含まれないポートが必要な場合を除き、Cisco WAE でこれ以上の設定は不要です。デフォルトのアプリケーション プロファイルで定義されていない TCP ポートを使用するアプリケーションの場合は、既存のアプリケーション プロファイルでポートを定義するか、関連付けられているポートを使用した新しいアプリケーション プロファイルを作成します。

WAN エッジで Cisco WAAS の推奨設計を使用することで、クライアント データが入力または出力時に Cisco WAE を一度だけ経由してデータセンターに伝送されます。VMware VIEW MANAGER コネクション ブローカとバーチャル マシンはデータセンターに存在するため、これらの間の通信はデータセンターのネットワーク内にとどまります。

Cisco WAAS の主要な技術には TFO、DRE、LZ 圧縮の 3 つがあり、デフォルトでイネーブルに設定されています。これらの各機能については、本書の「Cisco Wide Area Application Service」の概要の項（前出）で説明しています。最終的に、WAN 上でのトラフィックが軽減されて遅延が減少します。Cisco WAAS の展開はネットワークやアプリケーションに対して透過的であるため、追加した機能をアプリケーションに認識させる必要がなく、作業はそのままで継続されますが、応答時間が短縮されてトラフィックのスループットとトランザクションが増加します。

スケーラビリティと容量計画

Cisco WAE ファームでは、WCCP の使用で最大 32 台、Cisco ACE ロード バランシングの使用で最大 16,000 台までデバイスの拡張が可能です。Cisco WAAS サービスは、N+1 型構成では線形に拡張します。TCP 接続を最大限に最適化することに加え、データセンターの Cisco WAE とブランチ オフィスのファンアウト比を考慮する必要があります。ファンアウト比は、ブランチ オフィス内の Cisco WAE の台数、ネットワーク トラフィック量、TCP 接続数など、複数の要因によって決定されます。シスコ内部で使用可能なサイジング ツールによって、サイズの決定を自動化できます。NetFlow、NetQoS、およびその他のネットワーク解析ツールでは、スケーラビリティやキャパシティ プラニングの精度を上げるために詳細なトラフィック フロー情報が表示されます。

ハイ アベイラビリティ

デバイスのハイ アベイラビリティ

Cisco WAAS の導入環境は、アプリケーションに透過的です。Cisco WAAS がトラフィック フローを最適化していることは、アプリケーションのクライアントとサーバから認識されません。ハイ アベイラビリティは、WCCP によるインターセプトに含まれた機能です。WCCP がアクティブでない場合、または Cisco WAAS デバイスが動作していない場合、WCCP は Cisco WAE にトラフィックを転送しないため、トラフィック フローは最適化されません。こうしたワーストケース シナリオでは、トラフィック フローが最適化されない状態で継続します。

N+1 アベイラビリティ

Cisco WAE やシスコのネットワークには、別のハイ アベイラビリティ機能があります。ルータの冗長構成により、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）サービスや Gateway Load Balancing Protocol（GLBP）サービスを提供できます。Cisco WAE は、スケーラビリティとアベイラビリティを備えた N+1 型構成で設定できます。この設計では、特定の作業負荷に対して N 台の Cisco WAE と 1 台のスタンバイ Cisco WAE

が必要になります。作業負荷は、Cisco WAE 間で常に均等に分散されるので、スタンバイ Cisco WAE を使用して全体の作業負荷を軽減します。1 台の Cisco WAE に障害が発生しても、残りの Cisco WAE は通常の作業負荷で引き続き稼動します。

設定作業

各 Cisco WAE アプライアンスは、アプリケーション アクセラレータまたはセントラル マネージャとして設定できます。ベスト プラクティスとして、セントラル マネージャには、プライマリとスタンバイの導入を推奨します。この 2 台のデバイスで、ネットワーク上にあるその他すべての WAE デバイスを設定します。アプリケーション アクセラレータは、コア サイトとエッジ サイトに配置します。これらのデバイスが、実際に WAN アクセラレーションを実行します。

デバイスは、一定の順序に従ってネットワーク上でアクティブにする必要があります。

1. プライマリ セントラル マネージャをネットワークに設定します。
2. スタンバイ セントラル マネージャをネットワークに設定します。
3. アプリケーション アクセラレータを設定します。

アプリケーション アクセラレータは、ネットワーク上で設定すると、セントラル マネージャに登録されます。セントラル マネージャを先に設定しておくと、登録が正常に行われます。

詳細な設定

Cisco WAAS を実行するデバイスに対して、次の 2 種類の設定を適用します。

- 基本設定
- セントラル マネージャ設定

基本設定は、コンソール ポートからコマンドライン インターフェイス（CLI）を使用して、各 Cisco WAE に最初に適用する設定です。基本設定には、Cisco WAE をネットワーク上で始動し、セントラル マネージャに登録するための最小構成の設定が含まれています。基本設定の中で、次の情報が各 Cisco WAE に設定されます。

- ホスト名
- インターフェイス設定（速度、デュプレックス モード、IP アドレス、サブネット マスク）
- デフォルト ゲートウェイ
- ドメイン名
- Domain Name Server（DNS; ドメイン ネーム サーバ）
- プライマリ インターフェイス
- セントラル マネージャのアドレス

基本設定が完了したら、Cisco WAE をセントラル マネージャに登録できます。セントラル マネージャへの登録には、基本設定手順をすべて完了していること、および Cisco WAE をセントラル マネージャに接続できることが必要になります。Cisco WAE がセントラル マネージャに登録されてアクティブになったら、セントラル マネージャのデバイス グループからその他すべての設定オプションを設定できます。

セントラル マネージャ設定では、Cisco WAAS 全体に対して残りの設定を行います。セントラル マネージャ設定オプションは、デバイス レベルまたはデバイス グループ レベルで適用

できます。Cisco WAAS ソリューションでは、導入と管理を簡素化するために、プライマリ セントラル マネージャ設定方式でデバイス グループを使用します。

セントラル マネージャの設定

セントラル マネージャは、Cisco WAAS の管理コンポーネントです。セントラル マネージャでは、ブランチ オフィスやデータセンターにある複数の Cisco WAE の設定、モニタリング、管理に共通の GUI を使用します。大規模な導入では、数千台の Cisco WAE デバイスをサポートするために、セントラル マネージャを拡張できます。Web インターフェイスで設定を変更する場合は、セントラル マネージャが必要です。セントラル マネージャに障害が発生した場合、Cisco WAE は動作を継続しますが、セントラル マネージャがオンラインに復帰するまで、セントラル マネージャで Web ページを使用して変更を加えることはできません。

Cisco WAE は、初期設定時にセントラル マネージャに接続する必要があります。登録プロセスにより、Cisco WAE がセントラル マネージャに追加され、ローカルの Cisco WAE データベースが初期化されます。Cisco WAE のディスク暗号化をイネーブルにした場合、Cisco WAE のリブート時に暗号鍵を配布するためには、セントラル マネージャが稼動している必要があります。

集中レポートは、セントラル マネージャから取得できます。基本統計情報は、Cisco WAE から CLI やローカル デバイスの GUI を通して個々に出力されます。システム全体のアプリケーション統計情報は、セントラル マネージャの GUI で表示されます。トラフィック削減合計、アプリケーション ミックス情報、パススルー トラフィックなどの詳細なレポートは、セントラル マネージャの GUI から取得できます。

次の例で、Cisco WAAS 用にセントラル マネージャを設定するために必要となる設定手順を示します。

注: 少なくとも 1 台の Cisco WAE をセントラル マネージャにする必要があります。バックアップ セントラル マネージャを追加すると、アベイラビリティが向上します。セントラル マネージャは、他の重要なサーバとともにデータセンター内にインストールする必要があります。ブランチ オフィスや WAN に直結するセグメント付近にはインストールしないでください。

ステップ 1. デバイスをセントラル マネージャとして設定します。このデバイスは、デフォルトでアプリケーション アクセラレータ モードに設定されます。

```
device mode central-manager
```

ステップ 2. セントラル マネージャの IP アドレスを設定します。

```
interface GigabitEthernet 1/0
ip address 192.168.1.3 255.255.255.0
```

ステップ 3. デフォルト ゲートウェイを設定します。

```
ip default-gateway 192.168.1.1
```

ステップ 4. プライマリ インターフェイスを設定します。Cisco WAAS は、複数のネットワーク インターフェイス タイプ、PortChannel、スタンバイ インターフェイスをサポートします。Cisco WAAS は、トラフィックのインターセプトと転送にプライマリ インターフェイスを使用します。プライマリ インターフェイスの定義は必須です。

```
primary-interface GigabitEthernet 1/0
```

ステップ 5. Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバを定義します。キャプチャされたトラフィック統計情報は、セントラル マネージャと NetQoS に転送されます。各パケットのタイム スタンプは、正確さが求められます。すべての Cisco WAE とシスコ ルータは、同じ NTP サーバに同期する必要があります。

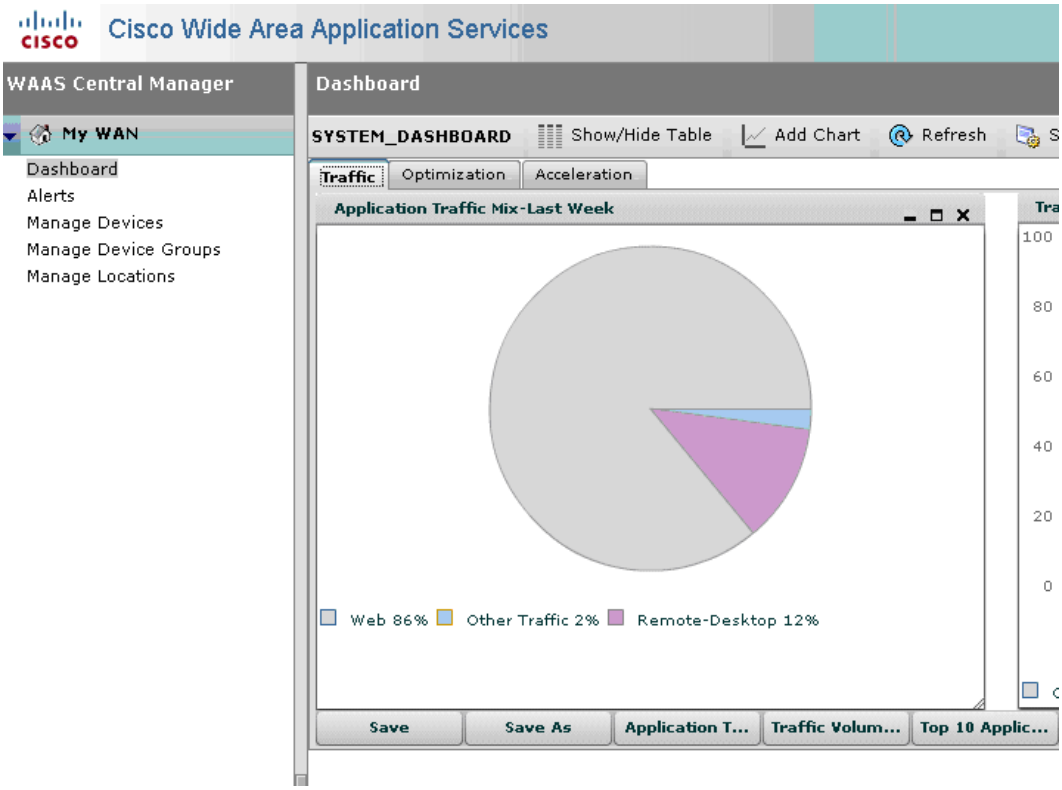
```
ntp server 192.168.1.20
```

ステップ 6. CMS データベースを初期化します。CMS データベースは、設定に関する規則と情報を格納しています。セントラル マネージャは、CMS データのリポジトリです。

```
cms enable
```

ステップ 7. セントラル マネージャのアップと稼動が完了したら、ポート 8443 でセントラル マネージャの Web GUI にログインします。セントラル マネージャの初期画面には、システムの状態の概要が表示されます。デバイスの数、ステータス、アプリケーション トラフィック、最適化率などの情報が含まれています（図 11）。

図 11. Cisco WAAS セントラル マネージャ管理コンソール



ブランチ オフィスおよびデータセンターのルータの設定

ブランチおよびデータセンターのルータは、Cisco WAAS の WCCP インターセプト ポイントになります。WCCP リダイレクションにより、ルータは、最適化のためにトラフィックを Cisco WAAS にリダイレクトします。さまざまな方式のインターセプトとリダイレクションが、ルータやスイッチでサポートされています。リダイレクション方式は、速度要件とルータまたはスイッチのプラットフォームに応じて異なります。ここでは、Generic Router Encapsulation（GRE; 総称ルーティング カプセル化）リダイレクションを使用します。

次の例で、ブランチ オフィスとデータセンターのルータを設定する手順を示します。

WCCP サービス 61 および 62 は、ループバック インターフェイスから WCCP グループにトラフィックを再ルーティングする指示をルータに与えます。サービス 61 は、入トラフィックをリダイレクトし、サービス 62 は、出トラフィックをリダイレクトします。双方向トラフィック フローをリダイレクトするには、サービス 61 と 62 の両方が必要です。WCCP はオープン スタンダードのプロトコルです。WCCP プロトコルを実装する機器であれば、WCCP グループに追加できます。

ステップ 1.　WCCP サービス 61 および 62 を設定します。

```
ip wccp 61
ip wccp 62
```

ステップ 2. この例では、Cisco WAE は WCCP インターセプトのために独自のサブネットに配置されます。WCCP が GRE を使用して返信する出力方式に設定されている場合は、Cisco WAE をクライアントまたはサーバと同じサブネットに配置することもできます。

```
interface FastEthernet1/3
Description WAE Interface
No switchport
Ip address 10.10.105.1 255.255.255.0
```

ステップ 3. この設定では、1 つのインターフェイスで着信パケットと発信パケットをインターセプトするため、WAE のサブネットをインターセプトから除外します。インターセプトからの除外が必要になるのは、Cisco WAE のトラフィックがクライアント用か、サーバ用かをルータが区別しないからです。Cisco WAE からのトラフィックは、ルータでもリダイレクトしないでください。リダイレクトすると、ループが発生します。

```
ip wccp redirect exclude in
```

ステップ 4. Cisco WAE の発信トラフィックに対する NetFlow 収集をイネーブルにします。

```
ip flow egress
```

ステップ 5. Cisco WAE VLAN を物理ポートに割り当てます。

```
interface FastEthernet1/0
description WAE port
switchport access vlan 301
```

ステップ 6. クライアント VLAN を設定します。これは WCCP インターセプト用の VLAN またはインターフェイスです。

```
interface Vlan300
description client vlan - 300
ip address 10.1.11.1 255.255.255.0
```

ステップ 7. WCCP インターセプト サービス 61 および 62 をクライアント VLAN に設定します。この VLAN またはインターフェイスのすべての入力パケットと出力パケットは、最適化のために Cisco WAE に転送されます。

```
ip wccp 61 redirect in
ip wccp 62 redirect out
```

ステップ 8. すべての発信トラフィックに NetFlow 統計情報を設定します。

```
ip flow egress
```

ステップ 9. マスター クロックと同期するように NTP を設定します。キャプチャされたトラフィック統計情報は、セントラル マネージャと NetQoS に転送されます。各パケットのタイム スタンプは、正確さが求められます。すべての Cisco WAE とシスコ ルータは、同じ NTP サーバと同期する必要があります。

```
ntp server 192.168.1.20
```

ステップ 10. 収集装置に情報を送信するように、NetFlow を設定します。また、NetFlow は、ループバック インターフェイスをソース アドレスとして使用します。NetFlow は、Cisco WAE とシスコ ルータの統計情報を NetFlow アグリゲータに送信します。NetFlow 統計情報は、接続数が少ない場合でも破壊的な量になる可能性があるため、Cisco WAAS は NetFlow 転送を最適化する必要があります。

```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 192.168.1.163 9995
```

注: VIEW MANAGER Connection Server がバーチャル デスクトップと直接接続するように設定されている場合は（Direct Connect to virtual desktop =「YES」）、WAE でポート 3389 の最適化（DRE および LZ）をオンにします。

ブランチ オフィスおよびデータセンターの Cisco WAE の設定

ブランチ オフィスとデータセンターに Cisco WAE-674-K9 を設定するには、次の手順を実行します。

ステップ 1. デバイス モードを application-accelerator に設定します。Cisco WAE は、アプリケーション アクセラレータまたはセントラル マネージャとして設定できます。デフォルトでは、application-accelerator はイネーブルになっています。

```
device mode application-accelerator
```

ステップ 2. Cisco WAE の IP アドレスを設定します。

```
interface GigabitEthernet 1/0
ip address 10.10.105.3 255.255.255.0
```

ステップ 3. デフォルト ゲートウェイを設定します。

```
ip default-gateway 10.10.105.1
```

ステップ 4. プライマリ インターフェイスを設定します。Cisco WAAS は、ローカル ネットワークのフェールオーバーなど、各種インターフェイスをサポートしています。プライマリ インターフェイスの指定は必須です。Cisco WAAS は、このインターフェイスを使用してインターセプトとリダイレクションを行います。

```
primary-interface GigabitEthernet 1/0
```

ステップ 5. WCCPv2 をオンにします。

```
wccp version 2
```

ステップ 6. ルータをルータ リストに追加します。

```
wccp router-list 1 10.10.105.1
```

ステップ 7. インターフェイスからのすべてのトラフィックを受け付けるために、TCP 無差別モードを設定します。

```
wccp tcp-promiscuous router-list-num 1
```

ステップ 8. NTP サーバを設定します。キャプチャされたトラフィック統計情報は、セントラル マネージャと NetQoS に転送されます。各パケットのタイム スタンプは、正確さが求められます。すべての Cisco WAE とシスコ ルータは、同じ NTP サーバと同期する必要があります。

```
ntp server 192.168.1.20
```

ステップ 9. セントラル マネージャのアドレスを設定します。統計情報レポートや管理のために、Cisco WAE をセントラル マネージャに登録する必要があります。デバイスごとの設定は、CLI とデバイスの GUI で実行できます。サイト全体または Cisco WAAS グループの設定は、セントラル マネージャで実行する必要があります。セントラル マネージャは多数の Cisco WAE で一度に操作を実行できるので、Cisco WAAS インフラストラクチャを管理するうえで大幅な時間の節約になります。

```
central-manager address 192.168.1.3
```

ステップ 10. CMS をイネーブルにします。このコマンドは、ローカル データベースを初期化して、セントラル マネージャに接続します。

```
cms enable
```

ステップ 11. Cisco WAAS 統計情報を NetFlow アグリゲータに送信するように、NetFlow を設定します。ホストの IP アドレスは NetFlow アグリゲータではなく、管理ステーションを指定します。管理ステーションで Cisco WAE の接続画面を新しく開き、アグリゲータの IP アドレスを入力します。

```
flow monitor tcpstat-v1 host 192.168.1.164
flow monitor tcpstat-v1 enable
```

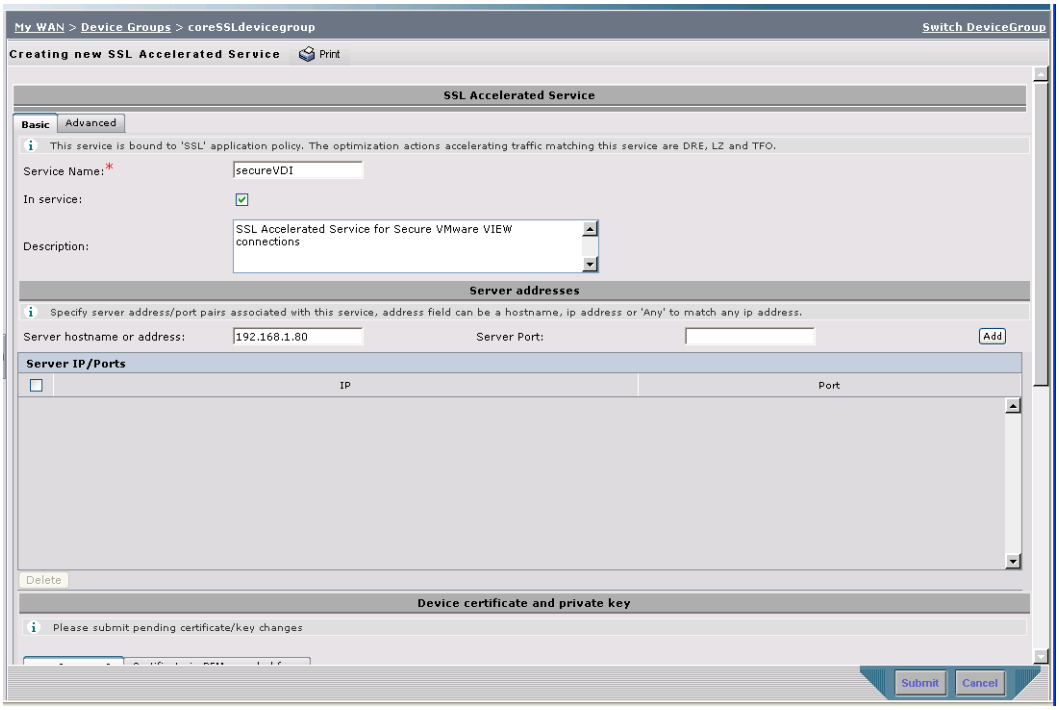
コア WAE での VDI セキュア接続用に SSL アクセラレーション サービスを設定します。SSL アクセラレーションを設定するための 3 つの簡単な手順については、表 2 を参照してください。

表 2. SSL アクセラレーションの設定

ステップ	設定	適用先
ステップ 1	Central Manager セキュア ストアの初期化およびオープンを行います。	WAAS Central Manager
ステップ 2	エッジとコアの両方の WAE デバイスで SSL AO がイネーブルになっていることを確認します。	すべての WAE デバイス
ステップ 3	コア WAE で SSL アクセラレーション サービスを設定します。 • 名前付きのサービスを作成します。 • セキュア VDI コネクション サーバの IP アドレスおよびポート情報を追加します。 • セキュア VDI サーバの証明書および秘密鍵データを追加します。 • サービスをイネーブルにします。	コア WAE デバイス

ステップ 12. 図 12 は、VMware VIEW のセキュア接続を最適化するために SSL アクセラレーション サービスを設定する方法を示しています。

図 12. VMware VIEW セキュア接続を最適化するための SSL アクセラレーション サービスの設定



設定およびメニュー

Cisco WAE の設定については、「付録 A」を参照してください。

設定のトラブルシューティング

設定に伴う問題のトラブルシューティングには、show コマンドを使用できます。

Cisco WAE コマンド

- **sh wccp status**：WCCP V2 がイネーブルであることを確認します。
- **sh wccp services**：WCCP サービス 61 および 62 がアクティブであることを確認します。サービス 61 および 62 はアクティブにする必要があります。
- **sh wccp routers**：Cisco WAE がルータに認識されていることを確認します。ルータ ID は、ルータのループバック アドレスです。Sent To は、Cisco WAE VLAN でのルータ インターフェイスを示します。すべてのルータは、Cisco WAE で定義して表示します。
- **sh stat connection optimized**：Cisco WAAS クライアントが接続に Cisco WAAS を使用していることを確認します。Show TFO Connections は、Cisco WAE で最適化されたパスをすべて表示します。Policy フィールドは、指定したリンクに対してアクティブな最適化方式を示しています。F は、リンクが十分に最適化されていることを示しています。最適化には、DRE、TFO（TCP Optimization として表示）、および LZ 圧縮などがあります。パススルー接続は、最適化されていない接続です。

- **sh statistics dre または sh connection conn-id <1-1048576>**：DRE の使用をチェックします。統計情報は 2 つのセクションで構成されています。Encode セクションは、クライアントまたはサーバから Cisco WAE に着信するトラフィックを示します。Cisco WAE は、着信トラフィックを LZ 圧縮で圧縮した後、DRE を適用します。Decode セクションは、ピアリング Cisco WAE からのトラフィックを表示します。DRE ルックアップが実行され、トラフィックが圧縮解除されます。この統計情報は、データの圧縮性を判定する場合に役立ちます。

ルータ コマンド

- **sh ip wccp 61**：WCCP サービス 61 および 62 がアクティブであることを確認します。このコマンドは、WCCP のグローバル情報およびパケットのリダイレクト方法を表示します。このコマンドの出力を使用すると、リダイレクトやグループ アクセス リストに伴う問題のトラブルシューティングが簡単になります。また、sh ip wccp 62 でサービス 62 もチェックします。
- **sh ip wccp 61 detail**：WCCP クライアントのハッシュまたはレイヤ 2 の割り当てをチェックします。また、このコマンドは、WCCP クライアント（Cisco WAE）のステータスをチェックします。sh ip wccp 61 コマンドは WCCP のグローバル情報を表示しますが、detail の付いたコマンドは詳細な WCCP クライアント情報を表示します。ハッシュの割り当て（Cisco WAE のバケットへの割り当て）、クライアント ID、クライアント ステータスなどが出力されます。
- **sh ip wccp interface detail**：WCCP を設定したインターフェイスを確認します。このコマンドは、WCCP を設定した、ルータ内またはスイッチ内のすべてのインターフェイスを、リダイレクションを除外する入力や出力とともに表示します。この情報を取得する別の方法として、sh run を使用する方法があります。各インターフェイスで実行する必要があります。
- **sh ip wccp 61 view**：WCCP グループ メンバシップを確認します。また、このコマンドは、サービス 62 をチェックします。

Cisco ACE ソリューションの実装と設定

実装の概要

Cisco ACE は、データセンターのアグリゲーション レイヤにワンアームで導入されます。Cisco ACE 4710 アプライアンスは 2 台以上必要です。Cisco ACE 4710 アプライアンスは、PortChannel を使用してアグリゲーション レイヤの Cisco Catalyst® 6500 シリーズ スイッチに接続し、ハイ アベイラビリティを実現します。トラフィック フローに組み込まれない Cisco ACE 4710 アプライアンスは、アグリゲーション スイッチに VLAN 169 で接続します。また、VMware VIEW MANAGER Connection Server に対する接続のロード バランス、およびセッション パーシステンスを提供します。

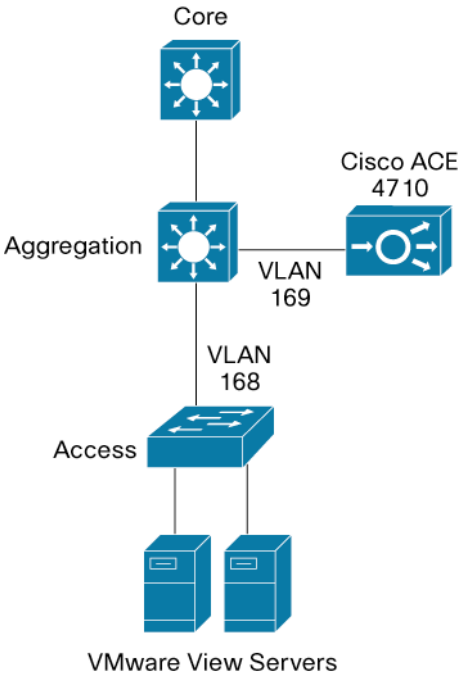
このソリューションで Cisco ACE アプライアンスに実装されている主な機能は、次のとおりです。

- VMware VIEW MANAGER Connection Server のロード バランシング
- VMware VIEW MANAGER Connection Server のヘルス モニタリング
- クライアントの IP アドレスに基づくセッション パーシステンス
- ハイ アベイラビリティ

ネットワーク トポロジ

図 13 は、このソリューションで使用したネットワーク トポロジを示しています。

図 13. Cisco ACE ソリューションのネットワーク トポロジ



ハードウェア

- Cisco ACE 4710

ソフトウェア

- Cisco ACE ソフトウェア バージョン 3.0(0)A3(1.0)

機能、サービス、およびアプリケーション設計に関する考慮事項

データセンターのバーチャル デスクトップにアクセスする必要があるユーザは、Cisco ACE に設定されたバーチャル IP アドレスに接続します。Cisco ACE は、アプリケーションの URL を照会し、取得した結果に対して正規表現を適用することによって、VMware VIEW アプリケーションの状態を定期的にチェックします。このプローブ情報を使用して、Cisco ACE は、最高のパフォーマンスとアベイラビリティでユーザの要求に対応できる VMware VIEW MANAGER Connection Server を決定し、ユーザの要求を VMware VIEW MANAGER Connection Server に転送します。

Cisco ACE は、特定のクライアント セッションが常に同じサーバに送られるように、クライアントと VMware VIEW MANAGER Connection Server の間で複数のセッション パーシステンス メカニズムをサポートしています。このトポロジでは、クライアントの IP アドレスに基づいてセッション パーシステンスを維持するように、Cisco ACE アプライアンスを設定しています。

ハイ アベイラビリティを実現するために、Cisco ACE の導入は、ステートフル リダンダント アクティブ - スタンバイ設計にします。Cisco ACE は、接続情報とパーシステンス情報の

両方をスタンバイ デバイスに複製し、アプリケーション サービスのフェールオーバーを即座に実行します。

Cisco ACE の設定

管理コンテキストの設定

- 管理コンテキストは、次の項目の設定に使用します。
- 物理インターフェイス
- 管理アクセス
- VMware VIEW MANAGER Connection Server のロード バランシングに使用するバーチャル コンテキスト
- ハイ アベイラビリティ

物理インターフェイスの設定

Cisco ACE アプライアンスは、Cisco Catalyst スイッチに設定された VLAN 経由でクライアントおよびサーバと通信します。この VLAN は、Cisco ACE の物理インターフェイスに設定する必要があります。このように設定しなければ、デフォルトで Cisco ACE はスイッチから受信したトラフィックを処理しません。

次のように、Cisco ACE アプライアンスの物理インターフェイスを PortChannel で設定し、必要な VLAN を構築します。

```
interface gigabitEthernet 1/1
  channel-group 200
  no shutdown
interface gigabitEthernet 1/2
  channel-group 200
  no shutdown
interface gigabitEthernet 1/3
  channel-group 200
  no shutdown
interface gigabitEthernet 1/4
  channel-group 200
  no shutdown
interface port-channel 200
  ft-port vlan 170
  switchport trunk allowed vlan 168-169
  port-channel load-balance src-dst-port
  no shutdown
```

リモート管理アクセスの設定

Telnet、Secure Shell（SSH; セキュア シェル）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、HTTP、HTTPS を使用して、Cisco ACE にリモートからアクセスする場合、または Cisco ACE に対して Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）アクセスを許可する場合、ポリシーを定義し、アクセス先のインターフェイスに適用する必要があります。

この項に示す設定手順は、管理コンテキストおよび VMware VIEW コンテキストに必要です。次の例は、管理コンテキスト用の手順です。

ステップ 1.　type management のクラス マップを設定します。

```
class-map type management match-any REMOTE-MGMT
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
50 match protocol https any
```

ステップ 2.　type management のポリシー マップを設定し、管理クラス マップを呼び出します。

```
policy-map type management first-match REMOTE-ACCESS
  class REMOTE-MGMT
    permit
```

ステップ 3.　VLAN インターフェイスとデフォルト ゲートウェイの IP アドレスを設定します。

```
interface vlan 168
  ip address 192.168.1.40 255.255.255.0
  alias 192.168.1.41 255.255.255.0
  peer ip address 192.168.1.42 255.255.255.0
  no normalization
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ステップ 4.　ポリシー マップを VLAN インターフェイスに適用します。

```
interface vlan 168
  service-policy input REMOTE-MGMT
```

VMware VIEW 用のバーチャル コンテキストの設定

一般に Cisco ACE を導入する場合、管理コンテキストを使用して、他のバーチャル コンテキストの管理とプロビジョニングを行います。この設計では、VMware VIEW というバーチャル コンテキストを、VMware VIEW MANAGER Connection Server のロード バランシング用に作成します。

次のように、バーチャル コンテキストを設定し、リソース クラスと関連付けます。

```
resource-class STICKY
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
context VIEW
  allocate-interface vlan 169
  member STICKY
```

冗長性とハイ アベイラビリティの設定

ハイ アベイラビリティと冗長性のために、冗長性モードで Cisco ACE の設定と構成を行うことができます。Cisco ACE は、一般的なアクティブ - バックアップ冗長性モードまたは（コンテキストごとの）アクティブ - アクティブ冗長性モードで設定できます。

次のように、ハイ アベイラビリティを設定します。

```
ft interface vlan 170
  ip address 192.170.1.1 255.255.255.0
  peer ip address 192.170.1.2 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 170
ft group 1
  peer 1
  no preempt
  priority 200
  associate-context Admin
  inservice
ft group 2
  peer 1
  no preempt
  priority 200
  associate-context VIEW
  inservice
```

VMware VIEW コンテキストの設定

VLAN インターフェイス、ルーティング、およびアクセス リストの設定

ステップ 1. VLAN 169 の IP アドレスを使用して、VLAN インターフェイスとデフォルト スタティック ルートを、ネクスト ホップのアグリゲーション スイッチに設定します。

```
interface vlan 169
  ip address 192.169.1.4 255.255.255.0
  alias 192.169.1.1 255.255.255.0
  peer ip address 192.169.1.5 255.255.255.0
  no normalization
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.169.1.2
```

ステップ 2. IP トラフィックを許可するようにアクセス リストを設定し、VLAN インターフェイスに適用します。

```
access-list 102 line 8 extended permit tcp any any eq www
access-list 102 line 24 extended permit icmp any any
interface vlan 169
access-group input 102
```

実サーバおよびサーバ ファームの設定

ステップ 1. 次の例で示すように、実サーバを Cisco ACE に設定します。

```
rserver host CB1
  ip address 192.168.1.80
  inservice
rserver host CB2
  ip address 192.168.1.81
inservice
```

ステップ 2. サーバ ファームを設定し、実サーバをサーバ ファームの配下に追加します。

```
serverfarm host VIEW_CB
  rserver CB1
    inservice
  rserver CB2
    inservice
```

VIEW MANAGER Connection Server のヘルス モニタリングの設定

Cisco ACE は、サーバのアベイラビリティを測定するために、複数のヘルスモニタリング プローブをサポートしています。

ステップ 1. VMware VIEW MANAGER Connection Server で動作するアプリケーションを監視するには、次の HTTP プローブを使用します。

```
probe http VIEW_PROBE
  interval 5
  faildetect 2
  passdetect interval 5
  passdetect count 2
  request method get url /admin/
  expect status 200 200
  open 1
expect regex "VIEW Administrator"
```

ステップ 2. ヘルス プローブをサーバ ファームに適用し、VMware VIEW MANAGER Connection Server の監視を開始します。

```
serverfarm host VIEW_CB
probe VIEW_PROBE
```

ロード バランシング アルゴリズムの設定

Cisco ACE は、VMware VIEW MANAGER Connection Server 間で負荷をインテリジェントに分散するロード バランシング アルゴリズムを複数備えています。この設計では、最小負荷経路選択アルゴリズムをサーバ ファームに設定します。VMware VIEW MANAGER Connection Server への新規コネクションは、Cisco ACE によって、接続数が最も少ないサーバにロード バランスされます。

```
serverfarm host VIEW_CB
   predictor leastconns
```

ロード バランシング ポリシーの設定

Cisco ACE は、着信トラフィックに対する分類、ポリシーの適用、アクションの実行のために、クラス マップ、ポリシー マップ、およびサービス ポリシーを使用します。ロード バランシング ポリシーを設定するには、次の手順が必要です。

ステップ 1. ポート 80 をリッスンし、バーチャル IP アドレスを使用するレイヤ 3 またはレイヤ 4 のクラスを設定します。

```
class-map match-all VIEW_VIP_80
2 match virtual-address 192.169.1.254 tcp eq www
```

ステップ 2.　ソース IP アドレスに基づいてパーシステンスを維持するスティッキ グループを設定し、VMware VIEW MANAGER Connection Server のサーバ ファームを割り当てます。

```
sticky ip-netmask 255.255.255.255 address source
VIEW_IP_STICKY
  timeout 10
  replicate sticky
  serverfarm VIEW_CB
```

ステップ 3.　ロード バランシング ポリシーを設定し、前のステップで作成したスティッキ サーバ ファームへのロード バランシングをイネーブルにします。

```
policy-map type loadbalance first-match VIEW_LB
  class class-default
    sticky-serverfarm VIEW_IP_STICKY
```

ステップ 4.　multi-match タイプのポリシー マップを設定し、ロード バランシングをバーチャル IP アドレスに結合します。

```
policy-map multi-match VM_LB
  class VIEW_VIP_80
    loadbalance vip inservice
    loadbalance policy VIEW_LB
    loadbalance vip icmp-reply
```

ステップ 5.　ポリシー マップをインターフェイス VLAN 169 に適用します。

```
interface vlan 169
service-policy input VM_LB
```

Cisco Catalyst 6500 マルチレイヤ スイッチ フィーチャ カード（MSFC）の PBR 設定

Cisco ACE アプライアンスは、ワンアーム設計に導入されるため、アグリゲーション レイヤで Cisco Catalyst 6500 Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）に PBR を設定し、VMware VIEW MANAGER Connection Server からのリターン トラフィックを Cisco ACE アプライアンスに確実に戻す必要があります。

ステップ 1.　リターン トラフィックに一致するようにアクセス リストを設定します。

```
ip access-list extended ACE_RETURN
permit tcp any eq www any
```

ステップ 2. ルート マップを設定し、Cisco Catalyst 6500 MSFC VLAN インターフェイスに適用します。この VLAN インターフェイスで VMware VIEW MANAGER Connection Server からのリターン トラフィックが認識されます。

```
route-map VM permit 10
 match ip address ACE_RETURN
 set ip next-hop 192.169.1.1
!
interface Vlan168
 ip policy route-map VM
```

設定のトラブルシューティング

次の show コマンドは、設定に伴う問題のトラブルシューティングに役立ちます。

- **show stats**：Cisco ACE の動作に関連する統計情報を表示します。
- **show service-policy policy_name**：特定のインターフェイス内またはコンテキスト内でグローバルにイネーブルにしたサービス ポリシーの統計情報を表示します。
- **show serverfarm name detail**：サーバ ファームに関する統計情報の要約または詳細を表示します。
- **show rserver rserver_name detail**：指定した実サーバまたはすべての実サーバに関する統計情報の要約または詳細を表示します。
- **show probe**：スクリプト プローブの情報など、プローブ情報を表示します。
- **show arp**:ARP テーブルで現在アクティブな IP アドレスと MAC アドレスのマッピング、統計情報、またはインスペクションやタイムアウトの設定を表示します。
- **show arp statistics**：すべての VLAN インターフェイスに関する ARP 統計情報を表示します。
- **show context**：すべてのコンテキストの autosync 設定を確認します。
- **show ft group status**:Cisco ACE に設定されているすべてのコンテキストの Fault Tolerant（FT; 耐障害性）ステータスを確認します。
- **show ft peer detail**：FT ピアの状態を確認します。
- **show resource usage**：各コンテキストのリソースの使用率を表示します。
- **show np NP_number**：ネットワーク プロセッサに保存されたハードウェア情報を表示します。

NetQoS を使用したパフォーマンスの計測

この項では、監視や結果の表示に使用するネットワーク モニタリング システムについて、Cisco WAAS による最適化の利点を実際に示しながら説明します。ネットワーク パフォーマンスの計測に使用したツールは、NetQoS Collector と NetQoS Reporter を組み込んだ NetQoS SuperAgent です。NetQoS Collector は、最適化前のトラフィックを収集し、NetQoS SuperAgent にデータを報告します。NetQoS SuperAgent は、ネットワークを通過するプロトコルやアプリケーションの詳細を表示します。その内容は次のとおりです。

- 応答時間
- データ転送時間
- 再送信遅延

- ネットワーク Round Trip Time（RTT; ラウンドトリップ時間）
- 有効ネットワーク RTT
- サーバごとのパフォーマンス
- ネットワークごとのパフォーマンス

この情報は、有効な総トランザクション時間とともに、テスト時のアプリケーションのベースラインを表します（エンドユーザ エクスペリエンス）。

NetQoS Reporter は、最適化後のトラフィックを収集し、NetQoS SuperAgent にデータを報告します。NetQoS SuperAgent は、NetQoS Collector のデータ（最適化前）を使用して、最適化後のトラフィックと比較します。図 14、15、および 16 の一般的な例に示すように、ここから Cisco WAAS を使用した場合の最適化の利点がわかります。

図 14. Cisco WAAS を使用した最適化の利点：アプリケーション応答時間

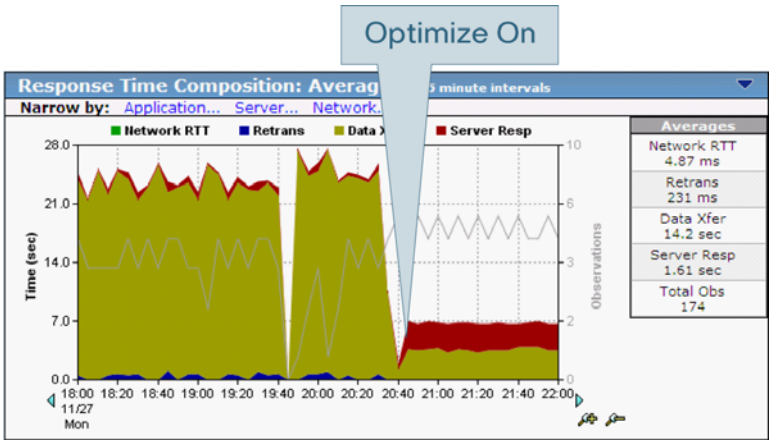


図 15. Cisco WAAS を使用した最適化の利点：アプリケーション データ レート

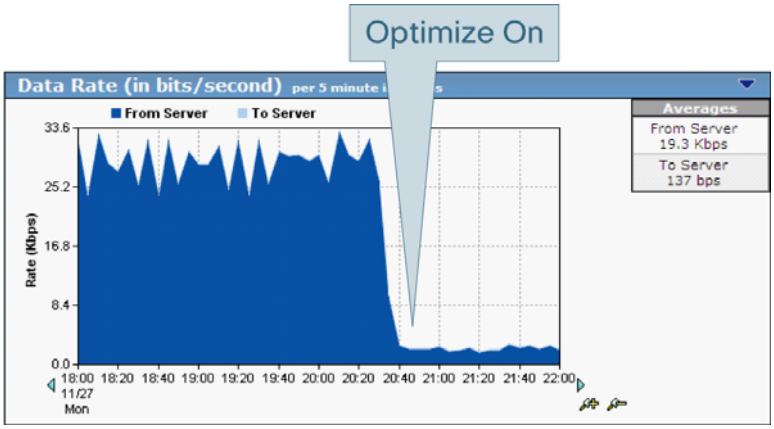
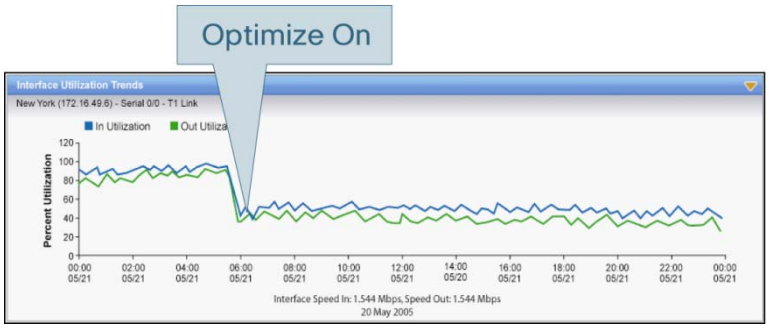


図 16. Cisco WAAS を使用した最適化の利点：リンク使用率



NetQoS デバイスは、シスコのルータおよびスイッチの Remote Switched Port Analyzer（RSPAN; リモート スイッチド ポート アナライザ）機能を使用して、受動的にデータを収集します。サーバにポーリングしないため、サーバの負荷になりません。

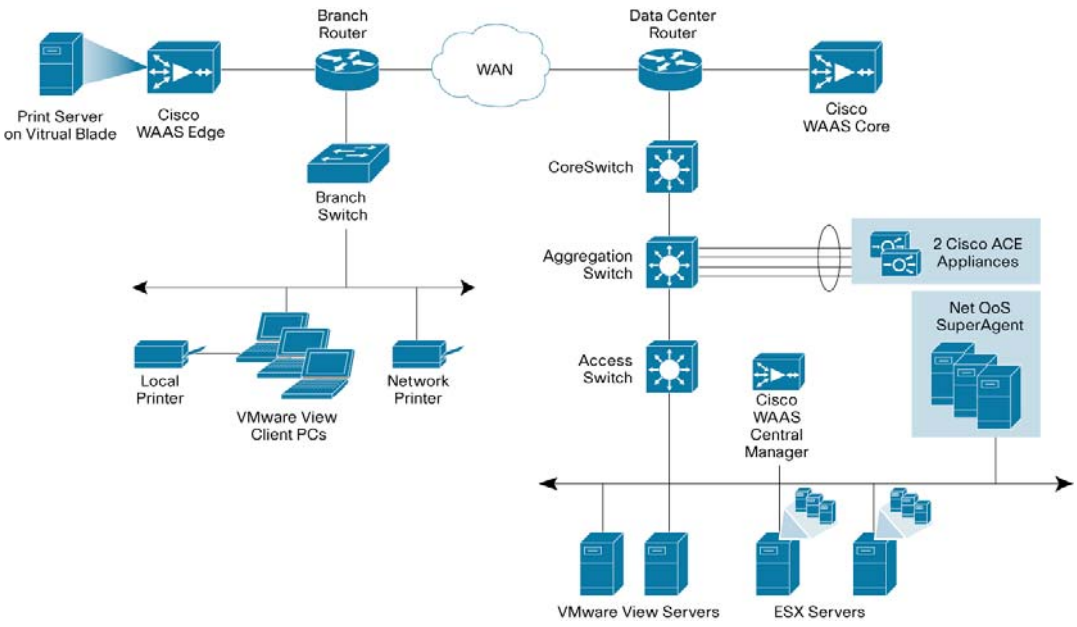
ソリューションのテストと結果

次の項では、シスコと VMware による共同ソリューションのテストに使用したテスト環境を説明し、得られた結果を示します。

テスト環境

シスコと VMware は、共同ソリューションから得られるお客様の利点をテストして正当性を確認しました。図 17 に、テスト環境の主要コンポーネントを示します。

図 17. テスト環境のトポロジ



テスト設計

最適化された環境の動作とパフォーマンスを、ベースラインの Vmware VIEW セッションと比較するために、複数のテスト シナリオやネットワーキング環境でテストしました。

WAN シミュレーション

次の 2 つの WAN 設定を使用し、標準的なエンタープライズ環境を再現しました。

- 小規模ブランチ オフィス：T1 リンク（1.5 Mbps）、100 ms RTT
- 地域オフィス：大規模な接続（10 Mbps）、50 ms RTT

テスト計画と手順

各種アプリケーションのパフォーマンスを明確に把握するために、次のテストを実施しました。

- **インターネット ブラウジング**：このテストでは、複数の Web サイトにアクセスして、ブラウザで表示しました。グラフィカル コンテンツやアニメーションを多彩に利用するさまざまなサイトでテストを行いました。
- **電子メールおよびコラボレーション**：このテストでは、Microsoft Outlook を使用して、社内のメール アカウントにアクセスし、新着メールのメッセージ（一部は添付ファイルあり）を開く、カレンダや連絡先を表示する、新しいコンテンツを作成するなど、複数の一般的な操作をテストしました。
- **Microsoft Office**：このテストでは、Word、PowerPoint、Excel のさまざまな文書を開く、プレゼンテーション のスライドショーを表示する、新規文書を作成する、Excel スプレッドシートでグラフを表示するなど、Microsoft Office アプリケーションをテストしました。
- **ファイル転送**：VMware VIEW 環境では、デスクトップ上のファイルは、ユーザと異なる場所に存在するので、バーチャル デスクトップからエンドユーザの USB ドライブまでファイルを転送するテストを実施しました。
- **印刷**：VMware VIEW 環境では、プリント サーバの場所に関係なく、印刷は WAN 経由で行われます。バーチャル デスクトップとプリンタが WAN で切り離されているため、印刷をテストしました。

テスト ツールと手順

実際の状況では、WAN を独占することはほとんどありません。また、一般に、VMware VIEW を導入すると、ブランチ オフィスのユーザ全員が VMware VIEW に移行します。こうした理由により、VMware VIEW ユーザが増えることを想定して、テスト用のトラフィックを生成しました。

このトラフィックを再現するために、AutoIT スクリプトを実行して複数のクライアント接続を生成しています。前述のテストのうち、ファイル転送と印刷を除くすべてのテストは、架空のユーザが操作します。

架空の VMware VIEW ユーザを実在のユーザに近づけるために、次のランダム化を加えました。

- テスト順序のランダムな選択
- 表示するファイル、サイト、電子メールのランダムな選択
- 操作にコンテンツの追加を含めるか、コンテンツの確認だけを行うかについてのランダムな選択
- 操作と操作の間隔、サブ操作とサブ操作の間隔のランダム化

最適化のためのバーチャル デスクトップの設定

VMware VIEW トラフィックを最適化するためには、基本プロトコルの暗号化と圧縮をディセーブルにする必要があります。Microsoft RDP は、現在のバージョンの VMware VIEW で使用されている基本プロトコルであり、VMware VIEW の多様な実装で広く使用されている一般的なプロトコルです。

RDP の暗号化をディセーブルにするには、バーチャル デスクトップの設定を変更する必要があります。変更を行うには、グループ ポリシー設定を利用するか、レジストリを変更します。いずれの方法でも、Microsoft Active Directory により、大規模なバーチャル デスクトップ グループに変更内容を配布できます。

圧縮をディセーブルにするには、VMware VIEW クライアントの設定を変更する必要があります。グループ ポリシーで設定できるので、Microsoft Active Directory により、大規模なクライアント グループに対して変更内容を簡単に反映できます。

RDP ファイルでの圧縮のディセーブル

RDP コンフィギュレーション ファイルで圧縮をディセーブルにするには、次の手順を実行します。

ステップ 1.　RDP 接続（.rdp）ファイルをメモ帳で開きます。

ステップ 2.　compression:i:1 の行を compression:i:0 に変更します。

ステップ 3.　ファイルを保存します。

変更後、変更したファイルで開始した接続には、RDP 圧縮が使用されません。

圧縮解除された RDP セッションを使用するための VMware VIEW の設定

圧縮解除された RDP セッションを使用するように VMware VIEW を設定するには、次の手順を実行します。

ステップ 1.　c:¥ Program Files¥VMware¥VMware View¥Server¥Extras¥GroupPolicyFiles¥vdm_client.adm ファイルを、コネクション ブローカ サーバから VMware VIEW クライアント PC にコピーします。

ステップ 2.　このファイルを Group Policy Object（GPO; グループ ポリシー オブジェクト）にインポートします。インポートするには、View クライアント マシンで [Start] > [Run] を選択して gpedit.msc と入力します。

ステップ 3.　[Administrative templates] を右クリックし、[Add/Remove templates] をクリックします。View Manager サーバからコピーした vdm_client.adm ファイル（ステップ 1）を選択します。

ステップ 4.　GPO で、[User Configuration] > [VMware VIEW Client] を選択し、[Enable Compression] ポリシーをディセーブルにします。

暗号化のディセーブル

Windows バーチャル デスクトップのレジストリ キーで暗号化をディセーブルにするために、次の手順を使用しました。

- HKLM¥System¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp¥MinEncryptionLevel を 1 に設定します。
- HKLM¥System¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp¥SecurityLayer を DWORD 値で作成し、0 を設定します。

大規模な導入では、Microsoft Active Directory を使用して、これらの変更内容をバーチャル デスクトップに反映する必要があります。

注: Windows XP 32 ビット版のバーチャル デスクトップ マシンでは、Microsoft から提供されるホットフィックスを使用して、RDP プロトコルの暗号化をディセーブルにする機能が追加されました。なお、Windows XP 64 ビット版および Windows Vista のデスクトップで RDP プロトコルの暗号化をディセーブルにする場合、このホットフィックスは必要ありません。ホットフィックスは http://support.microsoft.com/default.aspx?scid=kb;EN-US;956072 から入手できます。

テスト結果と成果

テスト対象の各メトリック（アプリケーション パフォーマンス、帯域幅使用量、スケーラビリティ、印刷最適化）は、まずネイティブのプロトコルによる圧縮を使用してベースラインを計測した後、Cisco WAAS を有効にした（ネイティブのプロトコルによる圧縮は無効）パフォーマンスと比較しました。Cisco WAAS は、テスト対象のすべてのメトリックにおいて、ディスプレイ プロトコルを十分に最適化しています。

VMware VIEW リモート デスクトップのパフォーマンス結果

トラフィックの削減

トラフィック削減テストでは、WAN 経由で送信されるトラフィック総量に注目し、ベースライン テスト（ネイティブの暗号化と圧縮をイネーブルにする）の結果と比較しました。

テスト対象の各メトリック（アプリケーション パフォーマンス、帯域幅使用量、スケーラビリティ、印刷最適化）は、まずネイティブのプロトコルによる圧縮を使用してベースラインを計測した後、Cisco WAAS を有効にした（ネイティブのプロトコルによる圧縮は無効）パフォーマンスと比較しました。Cisco WAAS は、テスト対象のすべてのメトリックにおいて、ディスプレイ プロトコルを十分に最適化しています。

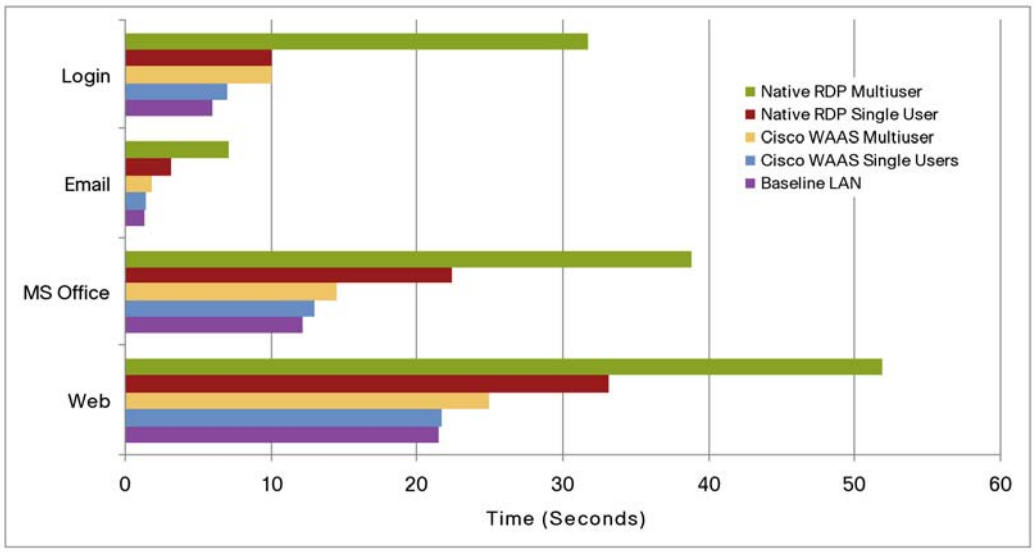
パフォーマンス アクセラレーション

Cisco WAAS により、ディスプレイ プロトコルのパフォーマンスは 70 % 向上し、ユーザ エクスペリエンスは LAN とほとんど変わりません。

VMware VIEW 使用時の各種アプリケーションのパフォーマンスをテストし、バーチャル デスクトップへのログイン、Microsoft Outlook 画面の表示、Microsoft PowerPoint スライドショーの表示など、作業を完了するまでの所要時間を計測しました（図 18）。

- Cisco WAAS を使用すると、VMware VIEW ユーザ が 1 ユーザおよび複数ユーザのいずれの場合も、各種アプリケーション作業を完了するまでの時間が最大 70 % 減少しました。
- Cisco WAAS で最適化された VMware VIEW セッションのパフォーマンスは、WAN 上に他のユーザが存在しても、LAN のパフォーマンスとほとんど差がありません。

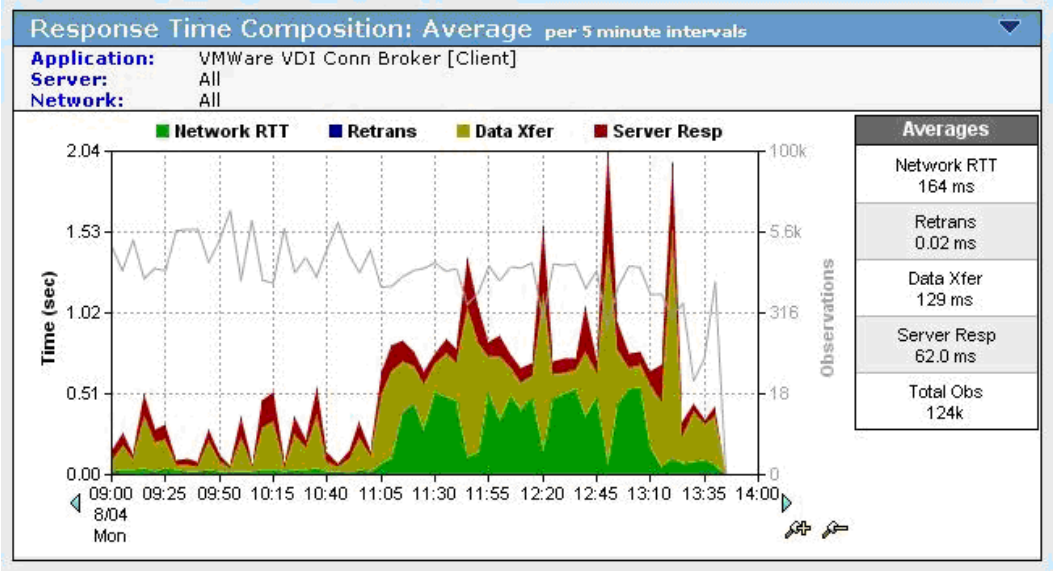
図 18. 作業完了時間（1.5 Mbps アップストリーム/ダウンストリーム、100 ms RTT）



また、NetQoS デバイスや Cisco WAAS に統合されている SuperAgent から報告される NetQoS のアプリケーション パフォーマンス統計情報を計測しました。

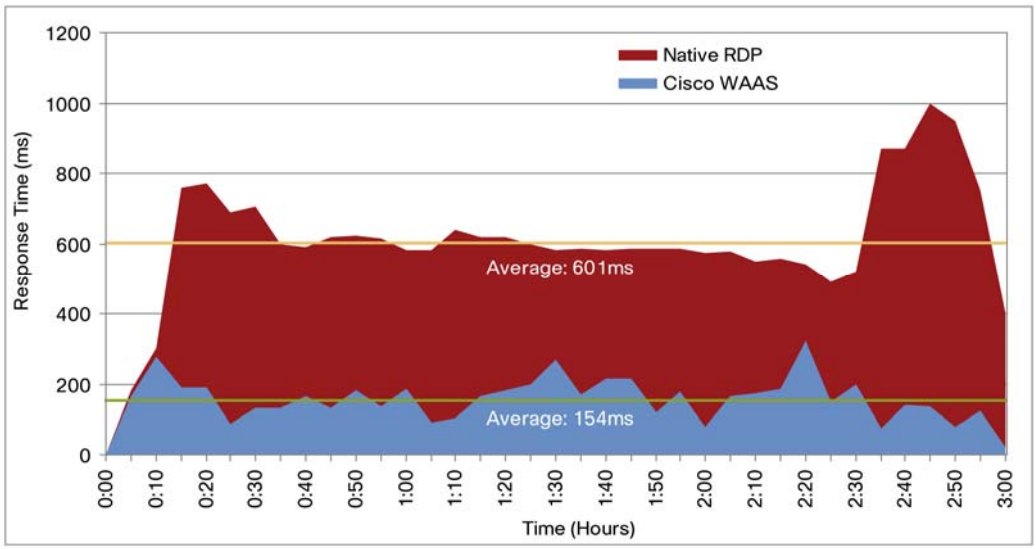
VMware VIEW MANAGER Connection Server で計測した単一ユーザの応答時間は、Cisco WAAS の最適化を利用すると（午前 9 時～午前 11 時）、ネイティブの VMware VIEW（午前 11 時～午後 1 時 40 分）に比べ、4 分の 1 から 6 分の 1 に短縮されました（図 19）。

図 19. NetQoS 応答時間分析：単一ユーザ



VMware VIEW で 15 の同時セッションをテストしたときにリモート側のブランチ オフィスで計測した応答時間は、4 倍に向上しています。Cisco WAAS のアクセラレーションの結果、平均応答時間は 154 ms を示しています。一方、ネイティブの VMware VIEW の平均応答時間は 601 ms です（図 20）。

図 20. 応答時間分析：マルチユーザ



帯域幅最適化

Cisco WAAS により、帯域幅の所要量が 60 ～ 70 % 減少するため、WAN 帯域幅のコストが低下します。

トラフィック削減テストでは、WAN 経由の VMware VIEW トラフィックによる帯域幅使用量を、ネイティブのプロトコルによる圧縮を実行しながらベースラインとして計測した後、Cisco WAAS を使用したテストと比較しました（図 21）。

図 21. アプリケーション テストにおけるトラフィックの減少

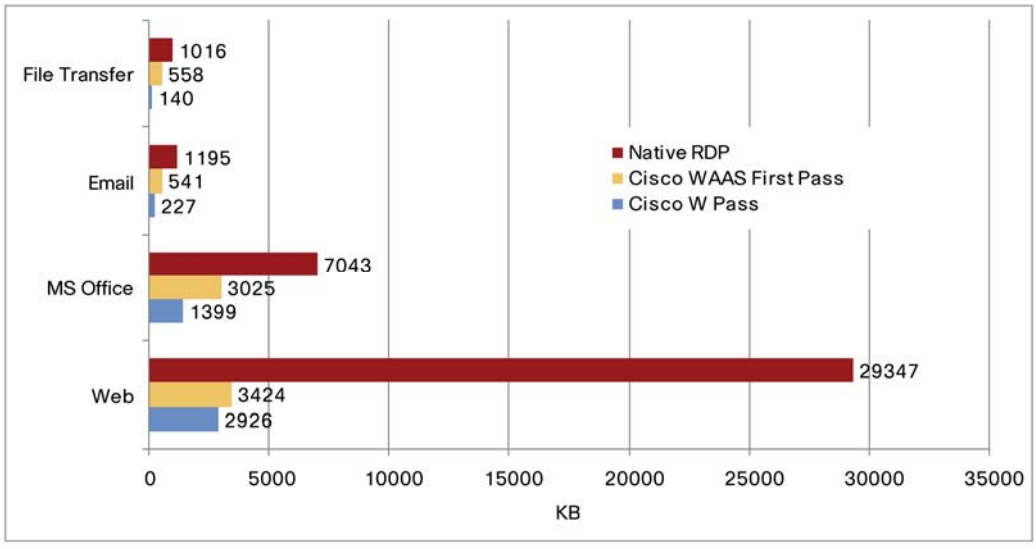
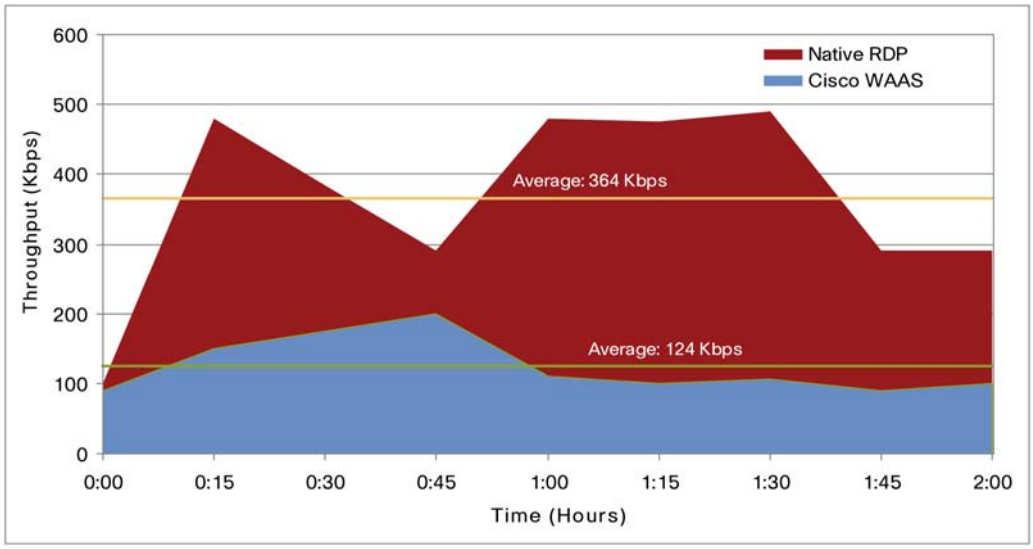


図 21 から、アプリケーション テスト ケースを実行している場合でも、トラフィックが減少していることがわかります。これらの結果によると、トラフィックの減少は、54 ～ 90 % 以上の範囲であり、1 回目のテストでは平均 67 %、2 回目のテストでは平均 84 % を示しています。ファイル転送の結果は、バーチャル デスクトップからクライアント マシンに接続された取り外し可能なドライブにファイルをコピーしたものです。

現実的にシミュレートした VMware VIEW の単一セッションから 2 時間で生成されたトラフィックを、Cisco WAAS による最適化の前後で比較しました。シミュレートしたセッションあたりの平均帯域幅は、Cisco WAAS を使用することによって、66 % 減少しました（図 22）。

図 22. 2 時間のシミュレーションでのユーザ スループット



この図に示された結果は、Cisco WAAS DRE の優れた圧縮能力を表しています。テスト期間全体でネイティブのプロトコルによる圧縮を上回っており、反復データを削減することによって、最大で 90 % を超える圧縮率を記録しています。

ユーザ数のスケーラビリティ

Cisco WAAS では、1 つのネットワークでサポート可能なユーザ数が 2 ～ 4 倍に増えています。

Cisco WAAS のアクセラレーションとデータ削減テクノロジーを連携することで、VMware VIEW ソリューションのスケーラビリティが向上します。RDP は、帯域幅と遅延の制約に合わせてセッションの品質を下げようとします。このため、マルチユーザ テストの結果が示すように、セッションの品質が大幅に低下し、最大で LAN の 10 分の 1 になります（図 23 と図 24）。

図 23. ユーザの増加に伴うセッション応答時間への影響

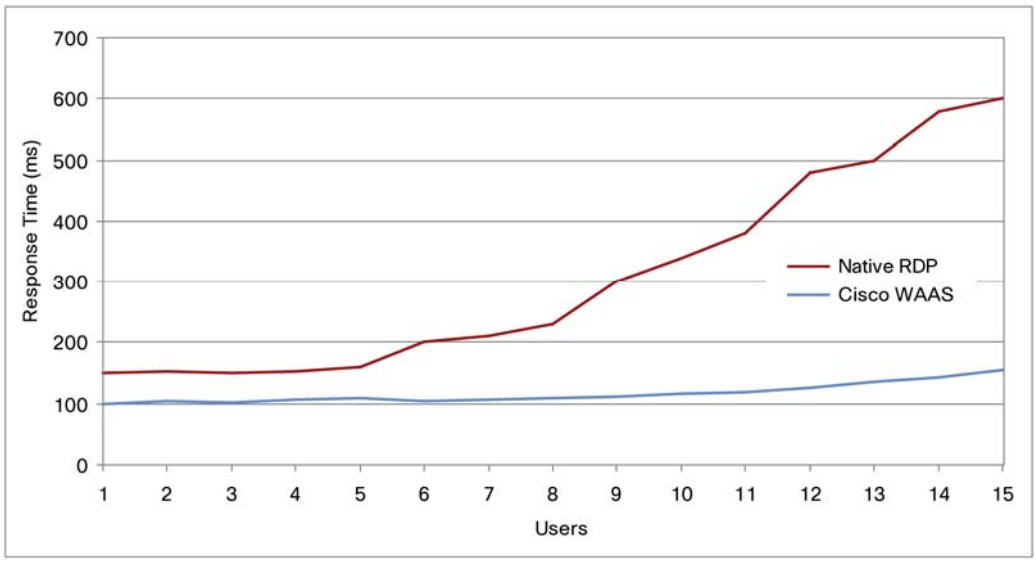


図 24. ユーザの増加に伴うスループットへの影響

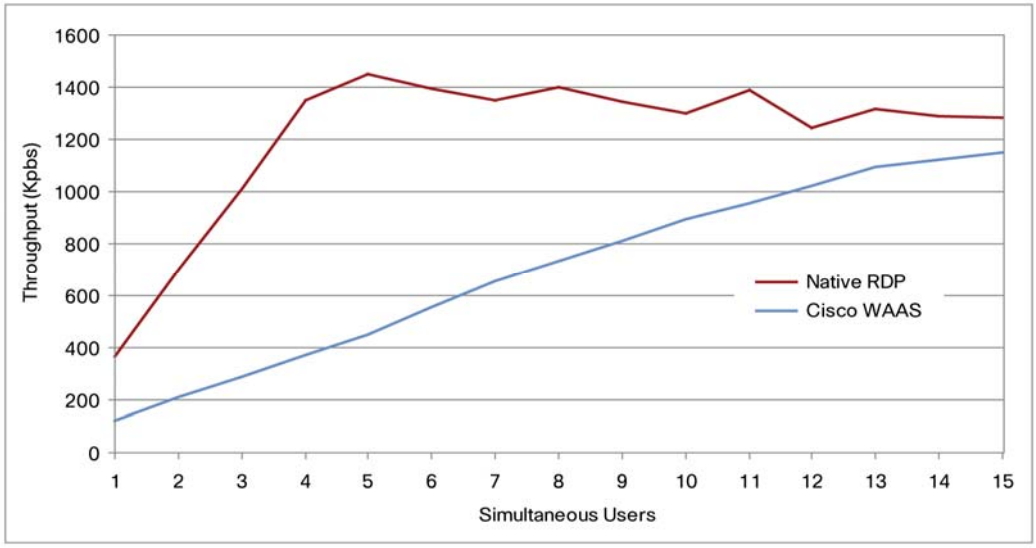


図 23 と図 24 は、RTT が 100 ms の 1.5 Mbps リンクでユーザが増加する場合に、ブランチ オフィスのネットワークで計測した応答時間とスループットの結果を示しています。

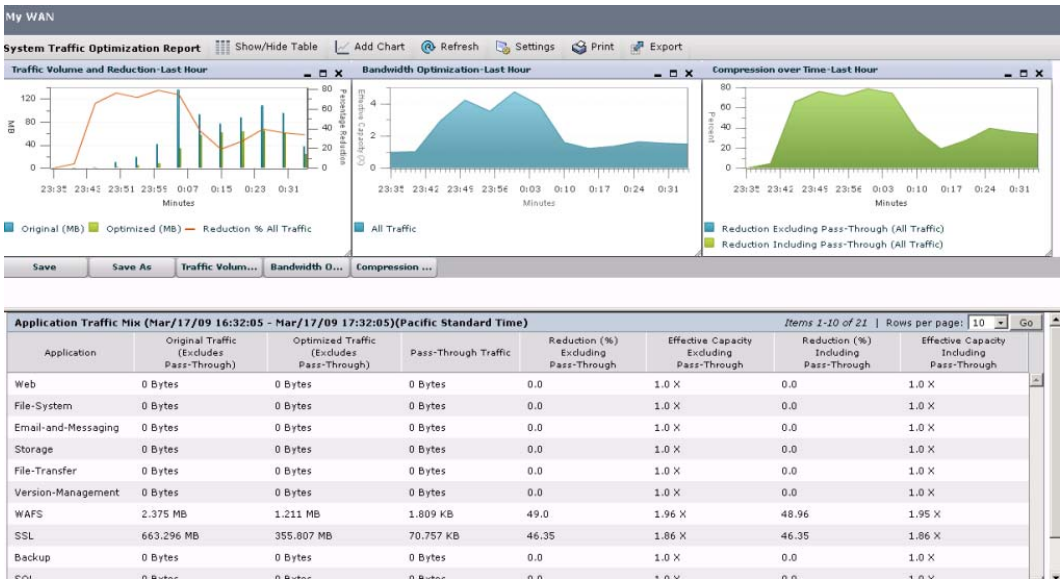
- ネイティブのプロトコルを使用した場合は、ネットワークのユーザがわずか 6 人に増えた時点でセッション品質の低下が始まり、9 人に増えると、測定された応答時間は約 300 ms、つまり単一ユーザが WAN を使用する場合の 3 倍に上昇し、システムはほとんど使用不能の状態になります。
- Cisco WAAS の最適化を使用した場合は、ネットワークのユーザが増えてもほとんど悪影響を受けません。同一のネットワークで最大 4 倍のセッションを使用できるほか、優れた応答性を保ち、ユーザ エクスペリエンスは単一ユーザのときと変わりません。
- スループットの結果は、意外なように見えますが、実際にはユーザ数が増えると、ネイティブのプロトコルの品質が低下することを表しています。スループットの低下は、セッション

の品質を下げる RDP の組み込みアルゴリズムによるものです。使用されるメカニズムとして、画面のリフレッシュ回数の減少があります。その結果、スムーズな作業が行えず、使いにくい状態に陥ります。

セキュア VIEW 接続の場合の VMware VIEW リモート デスクトップのパフォーマンス結果

Cisco WAAS は、VMware VIEW セキュア接続についても、SSL を使用しない前述のケースで達成されたものと同様の圧縮と最適化の利点を提供します。図 25 から、アプリケーション テスト ケースを実行している場合でも、トラフィックが減少していることがわかります。これらの結果によると、Cisco WAAS を介して同時に 100 個の VMware VIEW セキュア接続を実行しているときに、トラフィックが減少しています。

図 25. WAAS Central Manager に表示された 100 個の VMware VIEW 接続に対する最適化



Application	Original Traffic (Excludes Pass-Through)	Optimized Traffic (Excludes Pass-Through)	Pass-Through Traffic	Reduction (%) Excluding Pass-Through	Effective Capacity Excluding Pass-Through	Reduction (%) Including Pass-Through	Effective Capacity Including Pass-Through
Web	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X
File-System	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X
Email-and-Messaging	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X
Storage	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X
File-Transfer	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X
Version-Management	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X
WAFS	2.375 MB	1.211 MB	1.809 KB	49.0	1.96 X	48.96	1.95 X
SSL	663.296 MB	355.807 MB	70.757 KB	46.35	1.86 X	46.35	1.86 X
Backup	0 Bytes	0 Bytes	0 Bytes	0.0	1.0 X	0.0	1.0 X

VMware VIEW を使用した印刷

Cisco WAAS は、印刷を 70 % 最適化し、ブランチ オフィスにサーバを増設しなくても、プリント サーバを提供できるようにします。

デスクトップ マシンをデータセンターに移行したとしても、印刷は、リモートのブランチ オフィスにあるプリンタを使用する必要があります。未加工のデータの 10 倍にも増える印刷スプールの性質上、VMware VIEW 環境では、印刷の設計に十分な注意が必要です。VMware VIEW 環境で印刷する場合の導入に関する考慮事項を次に示します。

- **プリント サーバの場所**：プリント サーバ（印刷スプーラ）は、WAN のいずれかのサイト側（ブランチ オフィスまたはデータセンター）に配置できます。
- **印刷方式**：2 つの方式を使用できます。
  - **直接印刷**：バーチャル デスクトップにプリンタを定義し、印刷ジョブを直接スプーラに送信します。プリント サーバの場所に応じて、Common Internet File System（CIFS）または RAW/PostScript の印刷トラフィックが WAN 経由で送信されます。
  - **RDP 印刷**：プリンタは、クライアント マシン上で定義され、バーチャル デスクトップ上では RDP を使用してバーチャル化されます。この場合、印刷ジョブは、まず RDP で

クライアント マシンに送信された後、クライアント コンピュータでスプーラに送信されます。プリント サーバがデータセンターに配置されている場合は、CIFS および RAW/PS の印刷トラフィックが WAN 経由で送信されます。

- Cisco WAAS はすべての VMware VIEW 印刷環境（中央集中型およびローカル）を最適化します。
- **中央集中型プリンタ**：Cisco WAAS には、印刷に応じた最適化、データの削減、圧縮、TCP 最適化などの機能があり、印刷の大幅な改善を図ることができます。
- **ブランチ オフィスのプリント サーバ**：Cisco WAAS は、Microsoft Windows プリント サーバを Cisco WAAS アプライアンス上にバーチャル化し、ブランチ オフィスにサーバを増設しなくてもプリント サーバを装備できます。

表 3 に、10 ページの Microsoft Word 文書を、遅延が 100 ms の T1 回線経由で印刷した結果を示します。

表 3. 10 ページの Microsoft Word 文書の印刷結果

アクション	ベースライン	Cisco WAAS 使用時
クライアント上のローカル プリンタ、RDP を使用	**50.1 秒/3.67 MB**	**16.1 秒/1.6 MB**
データセンターのプリント サーバ		
RDP による印刷	287.1 秒/10.8 MB	62.6 秒/1.1 MB
直接印刷	140.1 秒/3.62 MB	94.3 秒/556 MB
ブランチ オフィスのプリント サーバ（Microsoft Windows プリント サーバを Cisco WAAS 上でバーチャル化）		
RDP による印刷	42.5 秒/2.22 MB	22.1 秒/1.53 MB
直接印刷	520.7 秒/20.17 MB	21 秒/546 MB

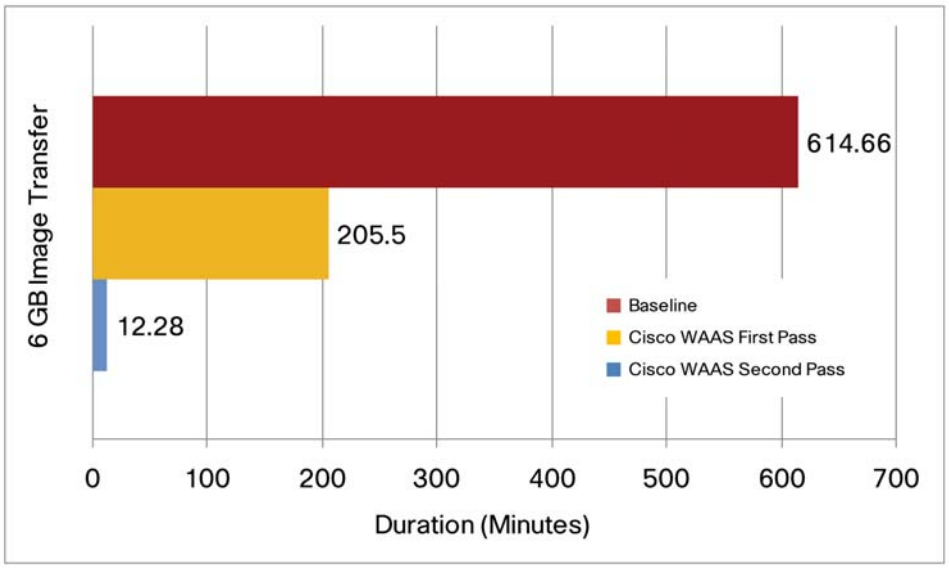
表 3 に示すように、Cisco WAAS により、すべての構成で印刷環境が大きく向上しています。印刷ジョブの実行に必要な帯域幅が減少し、トラフィックの削減は平均 70 %、最大で 97 % に達しています。そのうえ、印刷ジョブを完了するスピードが 3 ～ 25 倍に高速化しています。

WAN 経由でのバーチャル マシン イメージのコピー

導入を改善し、VMware VIEW の導入環境の管理を促進するには、バーチャル マシン イメージを WAN 経由で定期的に転送してバックアップする必要があります。

図 26 に、Microsoft Windows XP デスクトップの 6 GB のバーチャル マシン イメージを、VMware Network File Copy（NFC）プロトコルを使用して転送した結果を示します。転送スピードは、1 回目の転送では 3 倍、2 回目の転送では 50 倍に高速化されています。

図 26. VMware NFC プロトコルを使用したイメージ コピー



バーチャル デスクトップ間でのユーザ ファイルのコピー

VIEW ユーザは、USB や CD ドライブに保存したファイルなどのローカル ファイルを、リモートのバーチャル デスクトップに転送できます。VMware VIEW を使用してローカル ドライブをマッピングすると、ファイルのコピー データが RDP で転送されます。

表 4 に、ユーザ ファイルのコピー結果を示します。

表 4. ファイル転送

	時間		データ		2 回目のコピー	
	ベースライン	Cisco WAAS	ベースライン	Cisco WAAS	経過時間	WAN 経由データ
クライアントからバーチャル デスクトップ	10.5 秒	10 秒	1,054,596 バイト	1,630,398 バイト		
バーチャル デスクトップからクライアント	9 秒	4.2 秒	520,544 バイト	281,216 バイト	3 秒	71,815 バイト

クライアントからリモート デスクトップへの接続は、暗号化されているため、この構成では最適化されません。したがって、大量のデータを、Microsoft Windows PC からバーチャル デスクトップに転送する場合は、CIFS ファイル共有を使用する必要があります。Cisco WAAS は、CIFS の最適化を適用して、遅延と帯域幅使用量を削減することにより、CIFS ファイル転送を最適化できます。

表 4 に示すように、VMware VIEW によるバーチャル デスクトップからクライアントへのファイル転送は、1 回目で 50 % 以上、2 回目で 66 % 短縮されています。

付録 A：Cisco WAE の設定

ブランチ オフィスの Cisco WAE の設定

```
! WAAS version 4.1.3 (build b19 Mar 6 2009)
!
device mode application-accelerator
!
!
hostname edge-2
!
!
clock timezone PST8PDT -7 0
!
!
interface GigabitEthernet 1/0
 ip address 10.10.105.3 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
!
ip default-gateway 10.10.105.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
wccp router-list 1 10.10.105.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
```

```
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE
7D891AB402CAF2E89CCDD33ED54333AC
!
!
!
!
windows-domain workgroup "SA"
windows-domain netbios-name "CORE"
!
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
central-manager address 192.168.1.3
cms enable
!
!
!
flow monitor tcpstat-v1 host 192.168.1.161
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
!
! The VMware VIEW uses TCP port 80. The default Web Policy is applied
to this traffic
!
policy-engine application
   set-dscp copy
   service-class default weight 10
   name Web
   classifier HTTP
      match dst port eq 80
      match dst port eq 8080
      match dst port eq 8000
```

```
      match dst port eq 8001
      match dst port eq 3128
   exit
   classifier HTTPS
      match dst port eq 443
   exit
   classifier VMware-VMConsole
      match dst port eq 902
   exit
   classifier netqos
      match dst port eq 7878
   exit
! Full Optimization policy is applied to the VMware VIEW traffic
traversing the WAN
   map basic
      name Web classifier HTTP action optimize full accelerate http
      name FlowAgent classifier netqos action optimize full
      name Remote-Desktop classifier VMware-VMConsole action optimize
full
   exit
   map other optimize full
exit
!
! kernel kdb is enabled in WAAS by default
!
!
! End of WAAS configuration
```

コア Cisco WAE の設定

```
! WAAS version 4.1.3 (build b19 Mar 6 2009)
!
device mode application-accelerator
!
!
hostname Core
!
!
clock timezone PST8PDT -7 0
```

```
!
!
interface GigabitEthernet 1/0
 ip address 10.10.107.3 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
!
ip default-gateway 10.10.107.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
wccp router-list 1 10.10.107.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE
7D891AB402CAF2E89CCDD33ED54333AC
!
!
!
!
windows-domain workgroup "SA"
windows-domain netbios-name "CORE"
!
authentication login local enable primary
authentication configuration local enable primary
!
```

```
!
!
!
central-manager address 192.168.1.3
cms enable
!
!
!
flow monitor tcpstat-v1 host 192.168.1.161
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
!
! The VMware VIEW uses TCP port 443 while operating in secure (SSL) mode.
The SSL accelerated-service configuration below will be applicable to
VIEW traffic going over SSL.
!
crypto ssl services global-settings
   version all
   exit
!
!
crypto ssl services accelerated-service secureVDI
   server-cert-key secureVDI.p12
   server-ip 192.168.1.80 port 443
   inservice
   exit
!
!
! The VMware VIEW uses TCP port 80 while operating in non secure (HTTP)
mode. The default Web Policy is applied to this traffic.
!
!
policy-engine application
   set-dscp copy
   service-class default weight 10
```

```
   name Web
   classifier HTTP
      match dst port eq 80
      match dst port eq 8080
      match dst port eq 8000
      match dst port eq 8001
      match dst port eq 3128
   exit
   classifier HTTPS
      match dst port eq 443
   exit
   classifier VMware-VMConsole
      match dst port eq 902
   exit
   classifier netqos
      match dst port eq 7878
   exit
! Full Optimization policy is applied to the VMware VIEW traffic
traversing the WAN
   map basic
      name Web classifier HTTP action optimize full accelerate http
      name FlowAgent classifier netqos action optimize full
      name Remote-Desktop classifier VMware-VMConsole action optimize
full
   exit
   map other optimize full
exit
!
! kernel kdb is enabled in WAAS by default
!
!
! End of WAAS configuration
```

付録 B：Cisco ACE の設定

Cisco ACE 管理コンテキスト

```
resource-class STICKY
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
boot system image:c4710ace-mzg.A1_8_0a.bin
peer hostname 4710_VIEW_2
hostname 4710_VIEW_1
interface gigabitEthernet 1/1
  channel-group 200
  no shutdown
interface gigabitEthernet 1/2
  channel-group 200
  no shutdown
interface gigabitEthernet 1/3
  channel-group 200
  no shutdown
interface gigabitEthernet 1/4
  channel-group 200
  no shutdown
interface port-channel 200
  ft-port vlan 170
  switchport trunk allowed vlan 168-169
  port-channel load-balance src-dst-port
  no shutdown
class-map type management match-any MGMT-TRAFFIC
  description "allowed mgmt traffic to ACE"
  2 match protocol http any
  3 match protocol https any
  4 match protocol icmp any
  5 match protocol ssh any
  6 match protocol telnet any
  7 match protocol xml-https any
policy-map type management first-match REMOTE-MGMT
  class MGMT-TRAFFIC
    permit
interface vlan 168
```

```
  ip address 192.168.1.220 255.255.255.0
  peer ip address 192.168.1.221 255.255.255.0
  alias 192.168.1.222 255.255.255.0
  service-policy input REMOTE-MGMT
  no shutdown
ft interface vlan 170
  ip address 192.170.1.1 255.255.255.0
  peer ip address 192.170.1.2 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 170
ft group 1
  peer 1
  no preempt
  priority 200
  associate-context Admin
  inservice
ip route 0.0.0.0 0.0.0.0 192.168.1.1
context VIEW
  allocate-interface vlan 168-169
  member STICKY
ft group 2
  peer 1
  no preempt
  priority 200
  associate-context VIEW
  inservice
```

Cisco ACE VMware VIEW コンテキスト

```
access-list 102 line 8 extended permit tcp any any eq www
access-list 102 line 24 extended permit icmp any any
probe http VIEW_PROBE
  interval 5
  faildetect 2
  passdetect interval 5
  passdetect count 2
  request method get url /admin/
  expect status 200 200
  open 1
rserver host CB1
  ip address 192.168.1.80
  inservice
rserver host CB2
  ip address 192.168.1.81
  inservice
serverfarm host VIEW_CB
   probe VIEW_PROBE
   predictor leastconns
  rserver CB1 80
    inservice
  rserver CB2 80
    inservice
sticky ip-netmask 255.255.255.255 address source VIEW_IP_STICKY
  timeout 10
  replicate sticky
  serverfarm VIEW_CB
class-map match-all VIEW_VIP_80
  2 match virtual-address 192.169.1.254 tcp eq www
policy-map type loadbalance first-match VIEW_LB
  class class-default
    sticky-serverfarm VIEW_IP_STICKY
policy-map multi-match VM_LB
  class VIEW_VIP_80
    loadbalance vip inservice
    loadbalance policy VIEW_LB
```

```
    loadbalance vip icmp-reply
interface vlan 169
  ip address 192.169.1.4 255.255.255.0
  alias 192.169.1.1 255.255.255.0
  peer ip address 192.169.1.5 255.255.255.0
  no normalization
  access-group input 102
  service-policy input VM_LB
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.169.1.2
```

付録 C：参考資料

- Cisco ANS for VMware：http://www.cisco.com/go/optimizevmware
- Cisco ANS：http://www.cisco.com/go/applicationservices
- Cisco Application Networking パートナー ポータル：http://www.cisco.com/go/optimizemyapp
- Cisco WAAS ソフトウェア製品情報：http://www.cisco.com/go/waas
- Cisco ACE 製品情報：http://www.cisco.com/go/ace
- VMware バーチャル デスクトップ製品情報：http://vmware.com/products/desktop_virtualization.html
- VMware VIEW 製品情報：http://vmware.com/products/vdi/
- http://www.vmware.com/pdf/viewmanager3_admin_guide.pdf
- http://www.vmware.com/support/pubs/view_pubs.html

Cisco WAAS のデータセンター設計およびブランチ オフィス設計の詳細については、次のドキュメントでも提供しています。

- 『Enterprise Data Center Wide Area Application Services (WAAS) Design Guide』：http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/WAASDC11.pdf
- 『Enterprise Branch Wide Area Application Services Design Guide (Version 1.1)』：http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c649/ccmigration_09186a008081c7d5.pdf

VMware Virtual Desktop Manager および VMware ESX 環境のネットワーキングの詳細については、次のサイトにアクセスしてください。

- http://www.vmware.com/pdf/vdm21_manual.pdf
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns304/c649/ccmigration_09186a00807a15d0.pdf

詳細については、次のサイトにアクセスしてください。

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
http://www.cisco.com/web/JP/contact/index.html
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
USA
www.vmware.com
Tel: 1-877-486-9273 or 650-427-5000
Fax: 650-427-5001

c11-550350-01-J 08/09