VMware View アーキテクチャ プランニング ガイド

View 4.0.1

View Manager 4.0.1

View Composer 2.0.0

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-000241-02

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/pubs/）にあります。

VMware の Web サイトでは最新の製品アップデートも提供されています。

このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

本書について

本マニュアル『VMware View アーキテクチャ プランニング ガイド』では、VMware® View の概要について説明します。これには、主な機能および展開オプションの説明と、本番環境で一般的な VMware View コンポーネントのセットアップ方法の概要が含まれます。また、VMware View のインストールの保護を支援するために、セキュリティ機能についても説明します。このガイドは次の疑問に答えます。

- VMware View は解決の必要な問題を解決してくれるのか。
- 会社に VMware View ソリューションを実装することは可能なのか。また、コスト効率は良いのか。

対象読者

本マニュアルの情報は、IT の意思決定者、アーキテクト、管理者、および VMware View のコンポーネントおよび機能に精通する必要があるその他の読者を対象としています。アーキテクトやプランナーはこの情報により、Windows デスクトップおよびアプリケーションを効率的かつ安全にエンド ユーザーに提供するという企業のニーズを VMware View が満たすかどうかを判別できます。アーキテクチャの例が示されているため、プランナーは VMware View を大規模に展開するためのハードウェア要件と必要なセットアップ作業を理解できます。

本書へのフィードバック

VMware では、ドキュメント改善の参考にさせて頂くためにお客様さまからのご意見をお待ちしています。本マニュアルに関するコメントがございましたら、docfeedback@vmware.com までフィードバックをお寄せください。

テクニカル サポートおよびエデュケーション リソース

ここでは、お客様にご利用いただけるテクニカル サポート リソースを紹介します。本書およびその他の本の最新版を入手するには、http://www.vmware.com/jp/support/pubs をご覧ください。

オンラインおよび電話サポート

オンライン サポートを使用して、テクニカル サポート要求の送信、製品および契約情報の閲覧、および製品の登録を行うには、http://www.vmware.com/jp/support をご覧ください。

該当するサポート契約を結んでいるお客様の場合、迅速な対応が必要な Severity 1 の問題に関しては電話でのサポートをご利用ください。http://www.vmware.com/support/phone_support.html をご覧ください。

サポート サービス

当社のサポート サービスがお客様のビジネス ニーズにどのように対応できるかについては、http://www.vmware.com/jp/support/services をご覧ください。

VMware プロフェッショナル サービス

VMware エデュケーション サービスのコースでは、広範なハンズオンラボや事例の紹介をいたします。また、業務の際のリファレンスとしてお使いいただける資料も提供しています。コースはオンサイト、教室、およびオンラインで受講できます。VMware コンサルティング サービスでは、オンサイトのパイロット プログラムおよび導入のベスト

プラクティスのために、仮想環境の評価、計画、構築、および管理を支援するサービスが提供されます。エデュケーション クラス、認定プログラム、およびコンサルティング サービスに関する情報を入手するには、http://www.vmware.com/jp/services をご覧ください。

1 VMware View の概要

VMware View を使用すると、IT 部門はデータセンター内で仮想デスクトップを実行し、デスクトップを管理対象サービスとして従業員に提供することができます。エンド ユーザーは、社内のあらゆる場所にある任意の数のデバイスから、または自宅からアクセスできる、パーソナライズされたなじみのある環境を手にすることができます。管理者は、デスクトップ データをデータセンター内に保持できるため、制御の集中化、効率性、およびセキュリティを確保できます。

この章では次のトピックについて説明します。

VMware View を使用した場合の利点

VMware View によってエンタープライズ デスクトップを管理すると、信頼性、セキュリティ、ハードウェアからの独立性、および利便性の向上などの利点があります。

信頼性とセキュリティ

仮想デスクトップは、VMware vSphere と統合し、サーバ、ストレージ、およびネットワーク リソースを仮想化することによって、中央から管理できるようになります。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データセンター内のサーバに配置することには、次の利点があります。

- データへのアクセスを容易に制限できます。機密データがリモートの従業員の自宅コンピュータにコピーされることを防止できます。
- エンド ユーザーのシステムがいつオフになるかを気にせずに、データのバックアップをスケジュールできます。
- データセンター内でホストされる仮想デスクトップは、ダウンタイムがほとんどないか、まったくありません。仮想マシンは VMware サーバの高可用性クラスタ上に配置できます。

仮想デスクトップをバック エンドの物理システムおよび Windows Terminal Services サーバに接続することもできます。

利便性

VMware View の PC-over-IP プロトコルは、物理 PC を使用した場合の現在の体験に匹敵するエンド ユーザー体験を提供します。

- LAN 上では、従来のリモート表示よりも高速かつ滑らかに表示できます。
- WAN 上では、プロトコルはレイテンシーの増加または帯域幅の減少を補って、ネットワークの状態に関わらずユーザーの生産性を維持できるようにします。

管理性

エンド ユーザー用のデスクトップのプロビジョニングは、短時間で終わるプロセスです。各エンド ユーザーの物理 PC に 1 台ずつアプリケーションをインストールするのではなく、アプリケーションを完備した仮想デスクトップにエンド ユーザーが接続します。エンド ユーザーは、さまざまな場所にあるさまざまなデバイスから同じ仮想デスクトップにアクセスできます。

VMware vSphere を使用して仮想デスクトップをホストすると、次の利点があります。

- 管理の作業が削減されます。管理者はユーザーの物理 PC に手を触れることなく、アプリケーションとオペレーティング システムのパッチ適用およびアップグレードを実行できます。
- ストレージの管理が簡素化されます。VMware vSphere を使用すると、ボリュームおよびファイル システムを仮想化できるため、個別のストレージ デバイスを管理する必要がなくなります。

ハードウェアからの独立性

仮想マシンはハードウェアに依存しません。View デスクトップはデータセンター内のサーバ上で実行され、クライアント デバイスからのみアクセスされるため、クライアント デバイスのハードウェアと互換性がない可能性のあるオペレーティング システムでも View デスクトップで使用できます。

たとえば、Windows Vista は Vista 対応の PC 上のみで実行できますが、仮想マシンに Windows Vista をインストールして、Vista 対応でない PC 上でその仮想マシンを使用することができます。仮想デスクトップは、PC、シン クライアント、およびシン クライアントとして機能する PC 上で実行されます。

VMware View の機能

VMware View に備わる機能は、操作性、セキュリティ、中央からの制御、およびスケーラビリティをサポートします。

次の機能は、エンド ユーザーになじみのある体験を提供します。

- 仮想デスクトップから、クライアント デバイス上で定義されている任意のローカル プリンタまたはネットワーク プリンタで印刷します。仮想プリンタ機能を使用すると、互換性の問題が解決され、仮想マシンに追加のプリンタ ドライバをインストールする必要がなくなります。
- 複数のモニタを使用します。PCoIP では複数モニタがサポートされるため、表示の解像度と回転をモニタごとに調整できます。
- 仮想デスクトップを表示するローカル デバイスに接続されている USB デバイスやその他の周辺機器にアクセスします。

VMware View は、次のようなセキュリティ機能を備えています。

- ログインに RSA SecurID の 2 要素認証またはスマート カードを使用します。
- SSL トンネリングを使用して、すべての接続が完全に暗号化されるようにします。
- VMware High Availability を使用して、デスクトップをホストし、自動フェイルオーバーを実現します。

次の機能は、管理の集中化を実現します。

- Microsoft Active Directory を使用して、仮想デスクトップへのアクセスを管理し、ポリシーを管理します。
- Web ベースの管理コンソールを使用して、任意の場所から仮想デスクトップを管理します。
- テンプレート（マスター イメージ）を使用して、デスクトップのプールをすばやく作成し、プロビジョニングします。
- ユーザーの設定、データ、または環境設定に影響を及ぼすことなく、アップデートおよびパッチを仮想マシンに送信します。

スケーラビリティの機能は、デスクトップとサーバの両方を管理する VMware 仮想化プラットフォームに依存します。

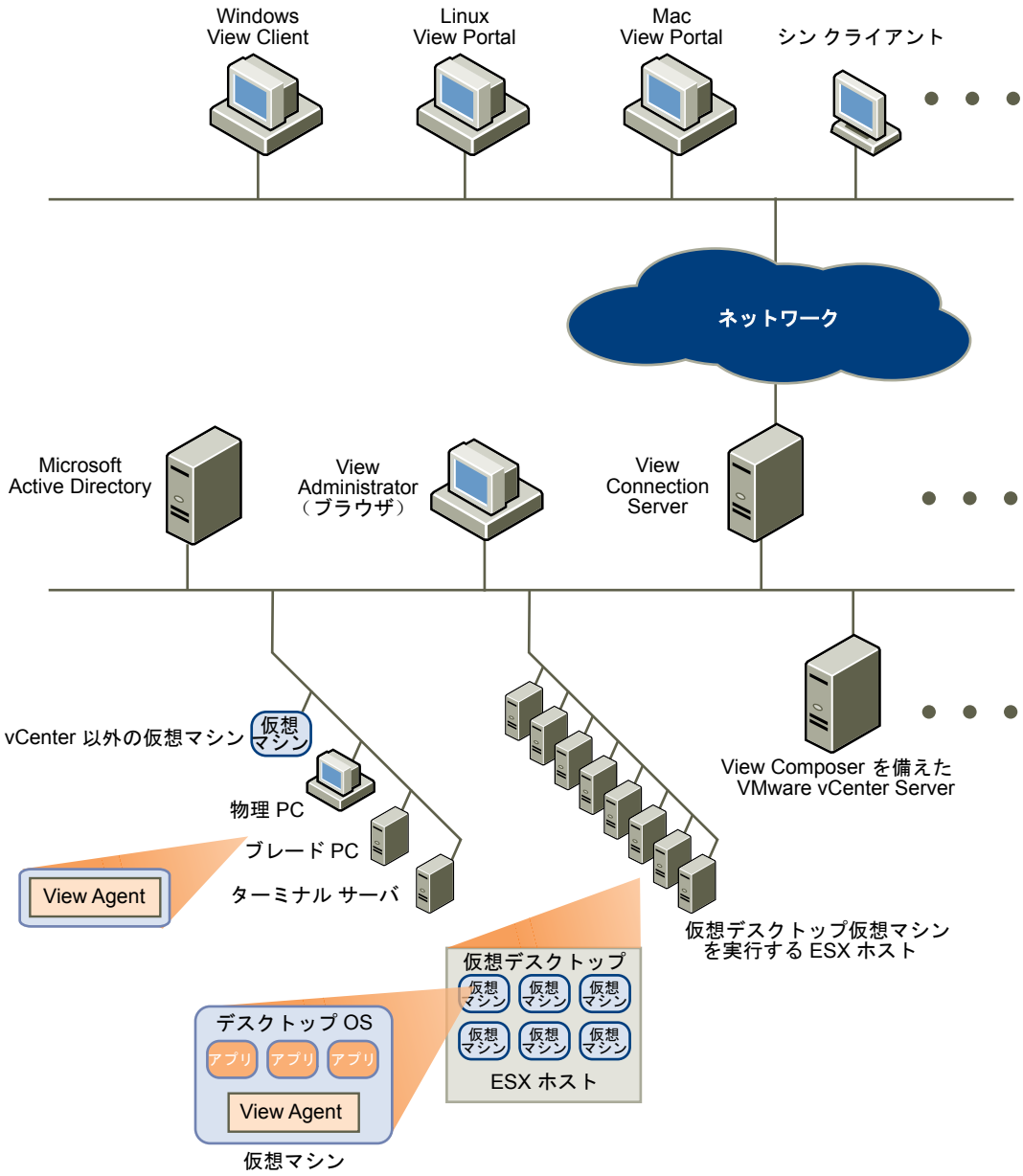
- VMware vSphere との統合により、コスト効率の良い密度、高水準の可用性、および仮想デスクトップのリソース割り当ての高度な制御を実現します。
- エンド ユーザーと、それらのユーザーにアクセスが許可されている仮想デスクトップとの接続を仲介するように View Connection Server を構成します。
- View Composer を使用して、仮想ディスクをマスター イメージと共有するデスクトップ イメージをすばやく作成します。リンク クローンをこの方法で使用すると、ディスク領域を節約でき、オペレーティング システムのパッチおよびアップデートの管理が簡素化されます。

VMware View のコンポーネント間の連携

エンド ユーザーは、View Client を起動するか、View Portal を使用して View Connection Server にログインします。Windows Active Directory と統合されるこのサーバは、VMware ESX サーバ、ブレード PC、物理 PC、または Windows Terminal Services サーバ上でホストされている仮想デスクトップへのアクセスを提供します。

図 1-1 は、VMware View の展開を構成する主要コンポーネントの関係を示しています。

図 1-1. VMware View 環境の高水準での例



クライアント デバイス

VMware View を使用した場合の主な利点は、デバイスや場所に関係なく、デスクトップがエンド ユーザーについて回ることです。ユーザーは、会社のラップトップ、自宅の PC、シン クライアント デバイス、または Mac から、パーソナライズされた自分の仮想デスクトップにアクセスできます。

ラップトップおよび Windows PC からは、エンド ユーザーは View Client を開いて各自の View デスクトップを表示します。Mac または Linux PC からは、エンド ユーザーは Web ブラウザを開き、View Portal を使用して各自の View デスクトップを表示します。Windows デバイスでも View Portal を使用できますが、一部の機能はサポートされていません。

クライアント デバイスは、View シン クライアント ソフトウェアを使用するため、ユーザーがそのデバイス上で直接起動できる唯一のアプリケーションが View Thin Client になるように構成できます。レガシー PC の用途を変更してシン クライアント デスクトップにすると、ハードウェアの寿命を 3 ～ 5 年延長できます。たとえば、シン デスクトップ上で VMware View を使用すると、古いデスクトップ ハードウェア上で Windows Vista などの新しいオペレーティング システムを使用できます。

View Connection Server

このソフトウェア サービスは、クライアント接続のブローカーとして機能します。View Connection Server は Windows Active Directory を介してユーザーを認証し、適切な仮想マシン、物理 PC、ブレード PC、または Windows Terminal Services サーバに要求を送ります。

View Connection Server は、次の管理機能を備えています。

- ユーザーの認証
- ユーザーへの、特定のデスクトップおよびプールに対する資格の付与
- デスクトップ セッションの管理
- ユーザーとデスクトップの安全な接続の確立
- シングル サインオンの有効化
- ポリシーの設定および適用

企業ファイアウォールの内側に、2 つ以上の View Connection Server インスタンスのグループをインストールして構成します。その構成データは組み込み LDAP ディレクトリに格納され、グループのメンバー間で複製されます。

企業ファイアウォールの外側では、DMZ に View Connection Server をセキュリティ サーバとしてインストールできます。DMZ 内のセキュリティ サーバは、企業ファイアウォールの内側の View Connection Server と通信します。セキュリティ サーバは View Connection Server の機能のサブセットを提供するため、Active Directory ドメイン内に配置する必要はありません。

View Connection Server は、Windows Server 2003 サーバ（できれば VMware 仮想マシン上の）にインストールします。

View Client

View デスクトップにアクセスするためのクライアント ソフトウェアは、Windows PC 上でネイティブ Windows アプリケーションとして、または View Client for Linux の場合にシン クライアント上で実行されます。

ユーザーはログインした後、使用を許可されている仮想デスクトップのリストから選択します。認証には、Active Directory の認証情報、UPN、スマート カードの PIN、または RSA SecurID トークンの使用を義務付けることができます。

管理者は、エンド ユーザーが表示プロトコルを選択できるように View Client を構成できます。使用できるプロトコルとしては、PCoIP、Microsoft RDP、および HP Blade 上でホストされている View デスクトップ用の HP RGS があります。PCoIP 表示プロトコルは VMware View 4 で使用可能になりました。PCoIP の速度と表示品質は物理 PC に匹敵します。

View Client with Offline Desktop は、試験的な Offline Desktop 機能をサポートするために拡張された View Client のバージョンです。この機能を使用すると、エンド ユーザーは仮想マシンをダウンロードしてローカル システムで使用できます。

使用する View Client によって機能が異なります。このガイドでは、主に Microsoft Windows 対応の View Client および View Portal について説明します。次のタイプのクライアントについては、このガイドでは詳しく説明しません。

- View Portal for Linux（試験的）および View Portal for Mac OS X（試験的）。
- View Client for Linux（認定されたパートナーからの購入に限定）。
- 様々なサードパーティ クライアント（認定されたパートナーからの購入に 限定）。
- View Open Client（VMware のパートナー認定プログラムをサポート）。View Open Client は正式な View クライアントでないため、サポートされていません。

View Portal

エンド ユーザーは Mac、Windows、または Linux PC から Web ブラウザを開き、View Portal を使用して各自の View デスクトップを表示できます。この View Client の Web ベース バージョンによって、必要な View ソフトウェアがすべてクライアント デバイスにインストールされますが、USB デバイスの接続など一部の拡張機能はインストールされない場合があります。

エンド ユーザーが View Portal を使用するには、Firefox、Internet Explorer、または Safari ブラウザを開き、View Connection Server インスタンスの URL を入力します。View Portal は、必要な View Client コンポーネントのインストールを許可するように要求するメッセージを表示します。Linux クライアントでは、View Portal で仮想デスクトップを表示するために `rdesktop` が必要です。Mac OS/X では、View Portal で仮想デスクトップを表示するために Microsoft Remote Desktop Connection Client for Mac が必要です。

View Agent

View Agent サービスは、View デスクトップのソースとして使用するすべての仮想マシン、物理システム、および Terminal Service サーバにインストールします。このエージェントは View Client と通信して、接続の監視、仮想印刷、ローカルに接続された USB デバイスへのアクセスなどの機能を提供します。

デスクトップ ソースが仮想マシンの場合は、最初に View Agent サービスをその仮想マシンにインストールした後、その仮想マシンをリンク クローンのテンプレートまたは親として使用します。この仮想マシンからプールを作成すると、すべての仮想デスクトップに View Agent が自動的にインストールされます。

このエージェントは、シングル サインオンのオプションを有効にしてインストールできます。シングル サインオンを有効にすると、ユーザーは View Connection Server に接続したときだけログインを要求され、仮想デスクトップに接続したときには 2 回目のログインを要求されません。

View Administrator

この Web ベースのアプリケーションでは、View Connection Server の構成、View デスクトップの展開と管理、ユーザー認証の制御、およびエンド ユーザーの問題のトラブルシューティングを管理者が実行できます。

View Connection Server インスタンスをインストールすると、View Administrator アプリケーションもインストールされます。このアプリケーションを使用すると、管理者は自分のローカル コンピュータにアプリケーションをインストールすることなく、任意の場所から View Connection Server インスタンスを管理できます。

View Composer

このソフトウェア サービスは、仮想マシンを管理する vCenter Server インスタンスにインストールします。View Composer はその後、指定された親仮想マシンからリンク クローンのプールを作成できます。この戦略を採用すると、ストレージ コストが最大 90% 削減されます。

各リンク クローンは一意のホスト名および IP アドレスを持ち、独立したデスクトップのように動作しますが、リンク クローンは基本イメージを親と共有するため、ストレージの必要量がはるかに少なくなります。

リンク クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンを更新するだけで、アップデートおよびパッチをすばやく展開できます。エンド ユーザーの設定、データ、およびアプリケーションは影響を受けません。

vCenter Server

このサービスは、ネットワークに接続されている VMware ESX サーバに対して中央からの管理者の役割を果たします。vCenter Server（旧称 VMware VirtualCenter）は、データセンター内の仮想マシンを構成、プロビジョニング、および管理するための中心点となります。

それらの仮想マシンを View デスクトップ プールのソースとして使用するだけでなく、仮想マシンを使用して、Connection Server インスタンス、Active Directory サーバ、vCenter Server インスタンスなどの VMware View のサーバ コンポーネントをホストすることもできます。

View Composer を vCenter Server と同じサーバにインストールして、リンク クローン デスクトップ プールを作成できます。その場合、物理サーバおよびストレージへの仮想マシンの割り当てと、仮想マシンへの CPU およびメモリ リソースの割り当てが vCenter Server によって管理されます。

vCenter Server は、Windows Server 2003 サーバ（できれば VMware 仮想マシン上の）にインストールします。

豊かなユーザー体験の計画 2

VMware View は、エンド ユーザーが期待する、なじみのあるパーソナライズされたデスクトップ環境を提供します。エンド ユーザーは、各自のローカル コンピュータに接続された USB デバイスやその他のデバイスにアクセスしたり、ローカル コンピュータで検出できる任意のプリンタにドキュメントを送信したり、スマート カードで認証したり、複数のディスプレイ モニタを使用したりできます。

VMware View は、エンド ユーザーに提供されることが望ましい機能を多数備えています。ただし、使用する機能を決定する前に、各機能の制限および制約を理解しておく必要があります。

この章では次のトピックについて説明します。

機能サポート マトリックス

ローカル USB デバイスへのアクセス、仮想印刷、Wyse マルチメディア リダイレクト（MMR）、PCoIP および Microsoft RDP 表示プロトコルなどの機能の多くは、ほとんどのクライアント OS でサポートされています。

エンド ユーザーに提供する表示プロトコルおよび機能を計画するときは、表 2-1 を使用して、その機能をサポートするクライアント OS を判別してください。

表 2-1. 32 ビット Windows クライアントでサポートされる機能

機能	Win 2000	Win XP Pro	Win XP Home	Vista Bus SP1、SP2	Vista Ult SP1、SP2	Vista Ent SP2
USB アクセス		○	○	○	○	○
RDP 表示プロトコル	○	○	○	○	○	○
PCoIP 表示プロトコル		○	○	SP2 のみ	SP2 のみ	○
HP RGS 表示プロトコル		○		○	SP2 のみ	○
Wyse MMR		○	○		SP1 のみ	

表 2-1. 32 ビット Windows クライアントでサポートされる機能 (続き)

機能	Win 2000	Win XP Pro	Win XP Home	Vista Bus SP1、SP2	Vista Ult SP1、SP2	Vista Ent SP2
仮想印刷	○	○	○		SP1 のみ	
Offline Desktop		○				

注意 HP RGS および PCoIP 表示プロトコルは、ネイティブの View Client ではなく Web Portal を使用する場合には使用できません。PCoIP 対応のクライアントのハードウェア要件および View デスクトップの要件の詳細については、「VMware View での PCoIP の使用 (P. 17)」 を参照してください。

表 2-2 に示すように、Web Portal を介して試験的にサポートされている Linux および Mac クライアントについては、オプションが限定されています。

表 2-2. Mac OS X および 32 ビット Linux クライアントについて Web Portal でサポートされる機能

機能	Red Hat Ent Linux 5.1	SUSE Linux Ent Desktop 10	Ubuntu Linux 8.04	Mac OS X（10.5）	Mac OS X（10.4）
USB アクセス					
RDP 表示プロトコル	○	○	○	○	○
PCoIP 表示プロトコル					
HP RGS 表示プロトコル					
Wyse MMR					
仮想印刷					
Offline Desktop					

また、VMware のパートナー数社が、VMware View の展開用のシン クライアント デバイスを提供しています。各シン クライアント デバイスで使用可能な機能は、ベンダおよびモデルと、企業が採用する構成によって決定されます。シン クライアント デバイスのベンダおよびモデルの詳細については、弊社 Web サイトより入手可能な『シン クライアント互換性ガイド』を参照してください。

表示プロトコルの選択

表示プロトコルは、データセンターに存在する View デスクトップへのグラフィカル インターフェイスをエンド ユーザーに提供します。Microsoft RDP（Remote Desktop Protocol）、HP 物理マシン用の HP RGS、または PCoIP（PC-over-IP）を使用できます。

使用するプロトコルを制御するポリシー、またはエンド ユーザーがデスクトップにログインしたときにプロトコルを選択できるようにするポリシーを設定できます。

VMware View での PCoIP の使用

PCoIP は、VMware によって提供される高パフォーマンスな新しいリモート表示プロトコルです。このプロトコルは、仮想マシン、Teradici クライアント、および Teradici 対応のホスト カードを備えた物理マシンをソースとする View デスクトップに使用できます。

PCoIP は、レイテンシーの増加または帯域幅の減少を補って、ネットワークの状態に関わらずユーザーの生産性を維持できるようにします。PCoIP は、LAN または WAN 上の様々なユーザーを対象とするイメージ、オーディオ、およびビデオコンテンツの配信のために最適化されています。PCoIP は次の機能を備えています。

- 最大 4 つのモニタを使用し、各モニタの解像度を個別に調整できます。ディスプレイごとの解像度は最高 1920×1200 です。
- ローカル システムと View デスクトップの間でテキストのコピーと貼り付けを行うことはできますが、フォルダやファイルなどのシステム オブジェクトをシステム間でコピーして貼り付けることはできません。
- Adobe Flash コンテンツによって使用される帯域幅の量を構成して、Web ブラウズ体験全体を向上させ、他のアプリケーションの応答性を高めることができます。
- PCoIP は 32 ビット カラーをサポートします。
- PCoIP は 128 ビットの暗号化をサポートします。
- PCoIP は Advanced Encryption Standard（AES）暗号化をサポートします。これはデフォルトで有効になっています。
- このプロトコルは社内の仮想プライベート ネットワークとともに使用できます。

PCoIP には次の制限があります。

- View デスクトップ上の OS は、Windows XP Professional SP 2 または 3、あるいは Windows Vista SP 1 または 2 である必要があります。
- PCoIP を使用する場合、スマート カードの使用はサポートされません。
- View Portal によって各自の仮想デスクトップにアクセスするユーザーは、PCoIP を使用できません。

クライアントには次のようなハードウェア要件があります。

- 800MHz 以上のプロセッサ速度
- SSE2 拡張命令に対応する x86 ベースのプロセッサ

PCoIP を使用する View クライアントは、View セキュリティ サーバに接続できますが、仮想デスクトップとの PCoIP セッションではセキュリティ サーバが無視されます。PCoIP ではオーディオとビデオのストリーミングに User Datagram Protocol（UDP）を使用します。セキュリティ サーバは TCP のみをサポートします。

Microsoft RDP

Remote Desktop Protocol は、多くのユーザーが自宅のコンピュータから職場のコンピュータにアクセスするためにすでに使用しているものと同じプロトコルです。RDP は、リモート コンピュータ上のすべてのアプリケーション、ファイル、およびネットワーク リソースへのアクセスを提供します。

Microsoft RDP は次の機能を備えています。

- 複数のモニタをスパン モードで使用できます。
- ローカル システムと View デスクトップの間でテキストのコピーと貼り付けを行うことはできますが、フォルダやファイルなどのシステム オブジェクトをシステム間でコピーして貼り付けることはできません。
- Adobe Flash コンテンツによって使用される帯域幅の量を構成して、Web ブラウズ体験全体を向上させ、他のアプリケーションの応答性を高めることができます。
- RDP は 32 ビット カラーをサポートします。

- RDP は 128 ビットの暗号化をサポートします。
- このプロトコルを使用すると、企業 DMZ にある View セキュリティ サーバへの、暗号化された安全な接続を確立できます。

HP RGS プロトコル

RGS は HP の表示プロトコルであり、これを使用すると、ユーザーは標準ネットワーク上にあるリモートの物理コンピュータのデスクトップにアクセスできます。

HP Blade PC、HP Workstation、および HP Blade Workstation に接続するときに、表示プロトコルとして HP RGS を使用できます。VMware ESX サーバ上で実行する仮想マシンへの接続はサポートしていません。

HP RGS は次の機能を備えています。

- 複数のモニタをスパン モードで使用できます。
- Adobe Flash コンテンツによって使用される帯域幅の量を構成して、Web ブラウズ体験全体を向上させ、他のアプリケーションの応答性を高めることができます。

VMware では、HP RGS を VMware View にバンドルしていません。また、ライセンスも付与していません。VMware View で使用するには、HP RGS バージョン 5.2.5 のライセンスを HP より取得してください。HP RGS コンポーネントをインストールして構成する方法の詳細については、http://www.hp.com で入手可能な HP RGS のドキュメントを参照してください。

ローカル コンピュータに接続された USB デバイスへのアクセス

管理者は、サム フラッシュ ドライブ、VoIP（Voice over IP）デバイス、プリンタなどの USB デバイスを View デスクトップから使用できるように構成できます。この機能を USB リダイレクトといいます。

この機能を使用すると、ローカル クライアント システムに接続されているほとんどの USB デバイスを View Client のメニューから使用できるようになります。デバイスの接続と切断にはメニューを使用します。

メニューに表示されなくても View デスクトップで使用可能な USB デバイスとしては、スマート カード リーダと、キーボードやポインティング デバイスなどのヒューマン インターフェイス デバイスがあります。View デスクトップとローカル コンピュータは、これらのデバイスを同時に使用します。

この機能には次の制限があります。

- View Client のメニューから USB デバイスにアクセスして、View デスクトップでそのデバイスを使用しているとき、ローカル コンピュータ上ではそのデバイスにアクセスできません。
- USB リダイレクトは Windows 2000 システムではサポートされません。
- View Portal を使用して View デスクトップにアクセスする場合、この機能は Windows クライアント上のみで、かつ最初に View Client をオプションの USB リダイレクト コンポーネントとともにローカル Windows システムにインストールした場合にのみ使用できます。
- View デスクトップで USB プリンタを使用するには、必要なプリンタ ドライバを View デスクトップにインストールする必要があります。

View デスクトップからの印刷

仮想印刷機能を使用すると、View デスクトップに追加のプリンタ ドライバをインストールする必要なく、エンド ユーザーが View デスクトップからローカル プリンタまたはネットワーク プリンタを使用できます。この機能で使用可能なプリンタごとに、データ圧縮、印刷品質、両面印刷、カラーなどの環境設定ができます。

ローカル コンピュータ上でプリンタを追加すると、View デスクトップで使用可能なプリンタのリストにもそのプリンタが追加されます。何も構成する必要はありません。その場合でも、管理者権限のあるユーザーは、仮想印刷コンポーネントとの競合をもたらすことなく View デスクトップにプリンタ ドライバをインストールできます。

仮想印刷機能には次の制限があります。

- View Portal を使用して View デスクトップにアクセスする場合、この機能は Windows クライアント上のみで、かつ最初に View Client をオプションの USB リダイレクト コンポーネントとともにローカル Windows システムにインストールした場合にのみ使用できます。
- この機能は USB プリンタには使用できません。View デスクトップで USB プリンタを使用するには、必要なプリンタ ドライバを View デスクトップにインストールする必要があります。

View デスクトップへのマルチメディアのストリーミング

Wyse MMR（マルチメディア リダイレクト）を使用すると、View デスクトップにマルチメディア ファイルがストリーミングされたときに、完全に忠実な再生が可能になります。

MMR 機能は次のメディア ファイル形式をサポートしています。

- AC3
- MP3
- MPEG-1、MPEG-2、MPEG-4-part2
- WMA
- WMV 7、8、および 9

この機能には次の制限があります。

- 最高の品質を得るには、Windows Media Player 10 以降を使用し、ローカル コンピュータまたはクライアント アクセス デバイスと View デスクトップの両方にインストールします。
- View デスクトップでのファイアウォールの例外に、Wyse MMR のポート（デフォルトで 9427）を追加する必要があります。

シングル サインオンを使用した View デスクトップへのログイン

シングル サインオン（SSO）機能を使用すると、エンド ユーザーがログインを 1 回だけ要求されるように View Manager を構成できます。

シングル サインオン機能を使用しない場合、エンド ユーザーは 2 回ログインする必要があります。最初に View Connection Server へのログインを要求され、次に View デスクトップへのログインを要求されます。スマート カードも使用する場合、エンド ユーザーはスマート カード リーダに PIN を要求されたときにもログインが必要なため、3 回ログインする必要があります。

SSO は、View Agent をデスクトップ ソースにインストールする際に選択できるオプション コンポーネントとして実装されます。この機能には、Windows XP 用の Graphical Identification and Authentication（GINA）ダイナミック リンク ライブラリと、Windows Vista 用の認証情報プロバイダ ダイナミック リンク ライブラリが含まれます。

View デスクトップでの複数モニタの使用

View デスクトップでは、表示プロトコルに関係なく、複数のモニタを使用できます。

VMware の表示プロトコルである PCoIP を使用する場合は、表示の解像度と回転をモニタごとに調整できます。PCoIP では、スパン モード セッションではなく、実際に複数モニタ セッションが可能です。

スパン モードのリモート セッションは、実際にはシングル モニタ セッションです。モニタのサイズと解像度を同じにする必要があり、モニタのレイアウトが境界ボックスに収まる必要があります。アプリケーション ウィンドウを最大化すると、ウィンドウがすべてのモニタにまたがって表示されます。

実際の複数モニタ セッションでは、モニタの解像度とサイズが異なってもよく、モニタを回転させることもできます。アプリケーション ウィンドウを最大化すると、ウィンドウはそれが表示されているモニタの画面いっぱいに広がるだけです。

この機能には次の制限があります。

- View デスクトップの表示に使用できるモニタの最大数は、RDP 表示プロトコルを使用する場合は 10 台、PCoIP を使用する場合は 4 台です。
- Microsoft RDP 表示プロトコルを使用する場合は、Microsoft Remote Desktop Connection（RDC）6.0 以降を View デスクトップにインストールする必要があります。

3 中央からのデスクトップ プールの管理

デスクトップ プールを作成する場合、含まれる仮想デスクトップは 1 つでも 100 でもかまいません。デスクトップ ソースとしては、仮想マシン、物理マシン、および Windows Terminal Services サーバを使用できます。基本イメージとして 1 つの仮想マシンを作成すれば、VMware View はそのイメージから仮想デスクトップのプールを生成できます。

この章では次のトピックについて説明します。

デスクトップ プールの利点

VMware View は、その集中管理の基礎として、デスクトップのプールを作成し、プロビジョニングする機能を備えています。

仮想デスクトップ プールは、次のいずれかのソースから作成できます。

- 物理デスクトップ PC や Windows Terminal Services サーバなどの物理システム
- ESX サーバ上でホストされ、vCenter Server によって管理される仮想マシン
- VMware Server、または View Agent をサポートする他の何らかの仮想プラットフォームで実行される仮想マシン

vCenter 仮想マシンをデスクトップ ソースとして使用する場合は、同一の仮想デスクトップを必要な数だけ作成するプロセスを自動化できます。プールに作成される仮想デスクトップの最小数と最大数を設定できます。これらのパラメータを設定すると、すぐに使用できる View デスクトップの数を常に十分確保できますが、使用可能なリソースを過剰に使用するほどの数は作成されません。

プールを使用してデスクトップを管理すると、プール内のすべての仮想デスクトップに設定を適用できます。次の例は、使用可能な設定の一部を示しています。

- View デスクトップのデフォルトとして使用する表示プロトコルと、ユーザーにデフォルトのオーバーライドを許可するかどうかの指定。
- Adobe Flash アニメーションの表示品質と帯域幅スロットルの構成。
- 仮想マシンを使用する場合、仮想マシンが使用されていないときに仮想マシンをパワーオフするか、完全に削除するかの指定。

また、デスクトップ プールの使用には多くの利点があります。

通常のプール

各ユーザーが特定の View デスクトップに割り当てられ、ログインするたびに同じ仮想マシンに戻ります。ユーザーは各自のデスクトップをパーソナライズしたり、アプリケーションをインストールしたり、データを格納したりできます。

読み取り専用プール

オプションで、仮想デスクトップが使用後に毎回削除および再作成されるため、高度な制御の可能な環境が提供されます。読み取り専用デスクトップは、各デスクトップに必要なアプリケーションがロードされ、すべてのデスクトップが必要なデータにアクセスできるコンピュータ室またはキオスク環境に似ています。

読み取り専用プールを使用すると、異なるシフトのユーザーが使用できるデスクトップのプールも作成できます。たとえば、ユーザーが一度に 100 人のシフトで勤務している場合、100 のデスクトップのプールを 300 人のユーザーが使用できます。

ストレージ要件の低減と管理

vCenter によって管理される仮想デスクトップを使用すると、以前には仮想化されたサーバのみで利用できたストレージの効率性をすべて実現できます。View Composer を使用すると、プール内のすべてのデスクトップが仮想ディスクを基本イメージと共有するため、ストレージの節減が促進されます。

- vSphere によるストレージの管理 (P. 22)

  VMware vSphere を使用すると、ディスク ボリュームおよびファイル システムを仮想化できるため、データの物理的な格納場所を考慮に入れる必要なく、ストレージを管理および構成できます。

- View Composer によるストレージ要件の低減 (P. 22)

  View Composer を使用すると、仮想ディスクを基本イメージと共有するデスクトップ イメージが作成されるため、必要なストレージ容量を 50 ～ 90% 削減できます。

vSphere によるストレージの管理

VMware vSphere を使用すると、ディスク ボリュームおよびファイル システムを仮想化できるため、データの物理的な格納場所を考慮に入れる必要なく、ストレージを管理および構成できます。

ファイバ チャネル SAN アレイ、iSCSI SAN アレイ、および NAS アレイは広く使用されているストレージ テクノロジであり、データセンターのストレージのさまざまなニーズを満たすために VMware vSphere によってサポートされています。これらのストレージ アレイは、ストレージ エリア ネットワークを介してサーバのグループに接続され、サーバのグループ間で共有されます。このような配置によってストレージ リソースを集約でき、仮想マシンに対してストレージ リソースをより柔軟にプロビジョニングできます。

View Composer によるストレージ要件の低減

View Composer を使用すると、仮想ディスクを基本イメージと共有するデスクトップ イメージが作成されるため、必要なストレージ容量を 50 ～ 90% 削減できます。

View Composer では、基本イメージ、つまり親仮想マシンが使用され、最大 512 のリンク クローン仮想マシンのプールが作成されます。各リンク クローンは一意のホスト名および IP アドレスを持ち、独立したデスクトップのように動作しますが、リンク クローンの方がストレージの必要量がはるかに少なくなります。

リンク クローン デスクトップ プールを作成すると、最初に親仮想マシンから完全なクローンが作成されます。完全クローン、つまりレプリカと、それにリンクされたクローンが、同じデータ ストア、つまり LUN（Logical Unit Number）に配置されます。必要に応じて、再分配機能を使用してレプリカとリンク クローンを 1 つの LUN から別の LUN に移動できます。

通常のデスクトップ プールを作成すると、各仮想デスクトップ用の別個のユーザー データ ディスクも View Composer によって作成されます。エンド ユーザーのプロファイルおよびアプリケーション データは、そのユーザー データ ディスクに保存されます。ユーザー データ ディスクは別のデータストアに保持することをお勧めします。その場合、ユーザー データ ディスクを保持している LUN 全体をバックアップできます。

アプリケーション プロビジョニング

VMware View では、従来のアプリケーション プロビジョンのテクニックを使用したり、VMware ThinApp でアプリケーションを仮想化したり、アプリケーションを View Composer の基本イメージの一部として展開したりできます。

- View Composer によるアプリケーション アップデートおよびシステム アップデートの展開 (P. 23)

  リンク クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンの更新により、アップデートおよびパッチをすばやく展開できます。

- VMware ThinApp によるアプリケーションの仮想化 (P. 23)

  ThinApp™ では、仮想化されたアプリケーション サンドボックスで実行される 1 つのファイルにアプリケーションをパッケージ化できます。この戦略を採用すると、柔軟で競合の発生しないアプリケーション プロビジョニングが可能になります。

- アプリケーション プロビジョニングでの既存のプロセスの使用 (P. 24)

  VMware View では、企業で現在使用しているアプリケーション プロビジョニングのテクニックをそのまま使い続けることができます。ただし、サーバの CPU 使用率およびストレージ I/O の管理と、ユーザーにアプリケーションのインストールを許可するかどうかの決定という 2 つの考慮事項が加わります。

View Composer によるアプリケーション アップデートおよびシステム アップデートの展開

リンク クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンの更新により、アップデートおよびパッチをすばやく展開できます。

再構成機能を使用すると、親仮想マシンを変更し、新しい状態のスナップショットを作成して、イメージの新しいバージョンをすべてのユーザーおよびデスクトップまたはそのサブセットにプッシュすることができます。この機能は次のタスクに使用できます。

- オペレーティング システムとソフトウェアのパッチおよびアップデートの適用
- サービス パックの適用
- アプリケーションの追加
- 仮想デバイスの追加
- 使用可能メモリなど、その他の仮想マシン設定の変更

ソフトウェアの追加・削除、または設定の変更をユーザーに許可しない場合は、更新機能を使用してデスクトップをデフォルト値に戻すことができます。この機能によって、時間の経過とともに大きくなる傾向のあるリンク クローンのサイズも削減できます。

VMware ThinApp によるアプリケーションの仮想化

ThinApp™ では、仮想化されたアプリケーション サンドボックスで実行される 1 つのファイルにアプリケーションをパッケージ化できます。この戦略を採用すると、柔軟で競合の発生しないアプリケーション プロビジョニングが可能になります。

ThinApp で仮想化されたアプリケーションを作成した場合、ユーザーは共有ファイル サーバからアプリケーションをストリーミングするか、アプリケーションを各自の仮想デスクトップにコピーすることができます。仮想化されたアプリケーションをストリーミング用に構成する場合は、アーキテクチャに関する次の考慮事項に対処する必要があります。

- 特定のアプリケーションに対する特定のユーザー グループのアクセス
- 共有リポジトリのストレージ構成
- ストリーミングによって生成されるネットワーク トラフィック（アプリケーションのタイプに大きく左右される）

アプリケーションをストリーミングする場合、ユーザーはアプリケーションを共有ファイル サーバから直接起動するか、デスクトップ ショートカットを使用して間接的に起動することができます。

仮想デスクトップにコピーされ、そこで実行されるように ThinApp パッケージ ファイルを構成する場合も、アーキテクチャに関して、従来の MSI ベースのソフトウェア プロビジョニングを使用する場合と類似の考慮事項があります。

アプリケーション プロビジョニングでの既存のプロセスの使用

VMware View では、企業で現在使用しているアプリケーション プロビジョニングのテクニックをそのまま使い続けることができます。ただし、サーバの CPU 使用率およびストレージ I/O の管理と、ユーザーにアプリケーションのインストールを許可するかどうかの決定という 2 つの考慮事項が加わります。

アプリケーションをほぼ同時刻に多数の仮想デスクトップにプッシュすると、CPU 使用率とストレージ I/O が大きく急上昇することがあります。このピーク ワークロードは、デスクトップのパフォーマンスに顕著な影響を及ぼす場合があります。ベスト プラクティスとしては、アプリケーションの更新がピーク時以外に実行されるようにスケジュールし、可能であれば各デスクトップの更新時刻をずらします。また、ストレージ ソリューションがそのようなワークロードをサポートできるように設計されていることを確認する必要があります。

会社がユーザーにアプリケーションのインストールを許可している場合は、現在のポリシーを継続できますが、View Composer の機能は活用できません。View Composer では、アプリケーションが仮想化されていないか、あるいはユーザーのプロファイルまたはデータ設定に含まれている場合、そのアプリケーションは View Composer の更新、再構成、または再分散操作が実行されるたびに破棄されます。多くの場合、インストールされるアプリケーションをこのように厳格に制御できることは、利点となります。View Composer デスクトップは既知の優れた構成とほぼ同じに保たれるため、サポートが容易です。

ユーザーが独自のアプリケーションをインストールし、仮想デスクトップの有効期限までそれらのアプリケーションを存続させる確固とした必要がユーザー側にある場合は、アプリケーション プロビジョニングに View Composer を使用する代わりに、完全な通常のデスクトップを作成して、ユーザーにアプリケーションのインストールを許可することができます。

Active Directory GPO によるユーザーおよびデスクトップの管理

VMware View には、View Manager と View デスクトップの管理および構成を集中化するためのグループ ポリシー オブジェクト（GPO）が多数含まれています。

これらのテンプレートを Active Directory ディレクトリにインポートしてから、それを使用して次のグループおよびコンポーネントに適用されるポリシーを設定できます。

- ログインするユーザーに関係なく、すべてのシステム
- ユーザーがどのシステムにログインするかに関係なく、すべてのユーザー
- View Connection Server の構成
- View Client の構成
- View Agent の構成

GPO を適用すると、プロパティは指定されたコンポーネントのローカル Windows レジストリに格納されます。

GPO を使用して、View Administrator のユーザー インターフェイス（UI）で選択可能なすべてのポリシーを設定できます。GPO を使用すると、UI で選択できないポリシーを設定することもできます。GPO テンプレートによって使用できる設定の詳細なリストおよび説明については、『View Manager 管理ガイド』を参照してください。

アーキテクチャ設計の要素と計画のガイドライン

4

一般的な VMware View アーキテクチャの設計では、ビルディング ブロック戦略を採用してスケーラビリティを実現します。各ビルディング ブロックは、最大 1,000 の仮想デスクトップをサポートするコンポーネントで構成されます。設計全体では、そのビルディング ブロックが 5 つ統合されます。

このアーキテクチャは、企業環境および特殊な要件に適合できる標準的でスケーラブルな設計を備えています。この章では、VMware View ソリューションの展開に含まれる要素を IT アーキテクトや計画担当者が実務的に理解できるように、メモリ、CPU、ストレージ容量、ネットワーク コンポーネント、およびハードウェアの要件について詳しく説明します。

この章では次のトピックについて説明します。

デスクトップ仮想マシンの構成

エンド ユーザー用の View デスクトップとして使用される仮想マシンには、サーバ仮想マシンと同等のディスク領域および処理能力は必要ありません。

View デスクトップとして使用される仮想マシンを作成する場合、RAM、CPU、およびディスク領域に関して行う選択は、サーバ ハードウェアの選択と費用に大きく影響します。

- 適切なシステム ディスク サイズの選択 (P. 28)

  ディスク領域を割り当てるときは、オペレーティング システム、アプリケーション、およびユーザーがインストールまたは生成する可能性のあるその他のコンテンツを格納できるだけの領域を割り当てます。通常この容量は、物理 PC に搭載されているディスクのサイズを下回ります。

- 仮想マシン デスクトップの構成例 (P. 29)

  仮想マシンに必要な RAM、CPU、およびディスクの容量はゲスト オペレーティング システムによって異なるため、Windows XP と Windows Vista の仮想デスクトップについて、別個の構成例を示します。

就業者のタイプに基づく計画

RAM、CPU、ストレージのサイズ設定など、構成の多くの要素は、仮想デスクトップを使用する就業者のタイプと、インストールする必要があるアプリケーションによって要件が大きく変動します。

アーキテクチャの計画では、就業者をいくつかのタイプに分類できます。

タスク ワーカー タスク ワーカーおよび事務職就業者は、一連の少数のアプリケーションで反復的な作業を行い、通常は据え置き型のコンピュータを使用します。通常それらのアプリケーションは、ナレッジ ワーカーが使用するアプリケーションほど CPU 集約型でも メモリ集約型でもありません。特定のシフトに就業するタスク ワーカーは、各自のデスクトップに同時にログインする可能性があります。タスク ワーカーには、コール センターのアナリスト、小売店の従業員、倉庫作業員などが含まれます。

ナレッジ ワーカー ナレッジ ワーカーの日常業務では、インターネットへのアクセス、電子メールの使用や、複雑なドキュメント、プレゼンテーション、およびスプレッドシートの作成などを行います。ナレッジ ワーカーには、会計士、セールス マネージャー、マーケティング リサーチ アナリストなどが含まれます。

パワー ユーザー パワー ユーザーには、アプリケーション開発者や、グラフィックス集約型アプリケーションのユーザーが含まれます。

ゲスト オペレーティング システムへのメモリの割り当て

サーバには PC よりも多くの RAM コストがかかります。RAM コストはサーバ ハードウェアの総コストの大きな部分を占めるため、デスクトップの展開を計画する際には適切なメモリ割り当てを特定することがきわめて重要です。

RAM の割り当てが少なすぎると、発生するメモリ スワップが多すぎるため、I/O に悪影響を及ぼすことがあります。RAM の割り当てが多すぎると、ゲスト オペレーティング システムのページング ファイルと各仮想デスクトップのスワップ ファイルおよびサスペンド ファイルが大きくなりすぎるため、ストレージ容量に悪影響を及ぼすことがあります。

パフォーマンスに対する RAM サイズ設定の影響

RAM を割り当てるときは、低すぎる設定を選択するのは避けてください。次の点を考慮します。

- RAM の割り当てが不十分な場合、ゲストのスワップが過剰に発生することがあり、そのためにパフォーマンスの大幅な低下とストレージ I/O 負荷の増加を招く I/O が生成されるおそれがあります。
- VMware ESX は、透過的なメモリ共有やメモリのバルーニングなどの高度なメモリ リソース管理アルゴリズムをサポートしています。そのため、ゲストへの特定の RAM 割り当てをサポートするために必要な物理 RAM がこれによって大きく減少する可能性があります。たとえば、仮想デスクトップに 2 GB が割り当てられたとしても、物理 RAM での使用量はそのごく一部となります。
- 仮想デスクトップのパフォーマンスは応答時間に大きく左右されるため、ESX サーバ上では RAM の予約設定を 0 以外の値に設定する必要があります。いくらかの RAM を予約した場合、アイドルでも使用中のデスクトップが完全にディスクにスワップ アウトされることはありません。ただし、予約の設定を高くすると、ESX サーバ上でメモリをオーバーコミットできるかどうかに影響し、VMotion の保守操作にも影響する場合があります。

ストレージに対する RAM サイズ設定の影響

仮想マシンに割り当てる RAM 容量は、仮想マシンで使用される特定のファイルのサイズに直接関連します。

Windows のページ ファイル
デフォルトでは、このファイルのサイズはゲスト RAM の 150% に設定されます。通常 `C:\pagefile.sys` にあるこのファイルは頻繁にアクセスされるため、リンク クローン仮想マシンおよびシン プロビジョニングされたストレージのサイズが大きくなる原因になります。ページ ファイルのサイズを小さくすると、多くの場合リンク クローンの仮想ディスク（`.vmdk` ファイル）のサイズも小さくなります。このサイズは Windows 内から調整できますが、これを調整するとアプリケーションのパフォーマンスに悪影響を及ぼすことがあります。

ラップトップ用の Windows ハイバネーション ファイル
このファイルはゲスト RAM の 100% に相当する場合があります。このファイルは View Client with Offline Desktop を使用する場合でも View の展開には不要なため、削除しても安全です。

ESX スワップ ファイル
`.vswp` 拡張子の付いたこのファイルは、予約した仮想マシンの RAM が 100% 未満の場合に作成されます。スワップ ファイルのサイズは、ゲスト RAM の予約されていない部分に等しくなります。たとえば、ゲスト RAM の 50% を予約していて、ゲスト RAM が 2GB の場合、ESX スワップ ファイルは 1GB です。

ESX サスペンド ファイル
`.vmss` 拡張子の付いたこのファイルは、エンド ユーザーがログオフしたときに仮想デスクトップがサスペンドされるようにデスクトップ プールのログオフ ポリシーを設定した場合に作成されます。このファイルのサイズは、ゲスト RAM のサイズに等しくなります。

PCoIP 使用時における特定のモニタ構成での RAM サイズ設定

VMware の表示プロトコルである PCoIP を使用する場合、必要なメモリ容量は、エンド ユーザー用に構成されたモニタの数とディスプレイ解像度に一部依存します。表 4-1 は、各種の構成に必要なメモリ容量を示しています。各列に示したメモリ容量は、他の PCoIP 機能に必要なメモリ容量に加算されるものです。

RAM は漸増的に割り当てるため、使用する増分を表に示しています。たとえば、VGA を使用するシングル モニタ構成では 37.03MB が必要ですが、RAM の最小増分は 64MB です。

表 4-1. PCoIP クライアント ディスプレイのオーバーヘッド

ディスプレイ解像度の標準	幅（ピクセル単位）	高さ（ピクセル単位）	モニタ 1 台でのオーバーヘッド（RAM の増分）	モニタ 2 台でのオーバーヘッド（RAM の増分）	モニタ 4 台でのオーバーヘッド（RAM の増分）
VGA	640	480	37.03MB（64MB）	44.06MB（64MB）	58.13MB（64MB）
SVGA	800	600	40.06MB（64MB）	51.97MB（64MB）	73.95MB（96MB）
720p	1280	720	51.09MB（64MB）	72.19MB（96MB）	114.38MB（128MB）
UXGA	1600	1200	73.95MB（96MB）	117.89MB（128MB）	205.78MB（256MB）
1080p	1920	1080	77.46MB（96MB）	124.92MB（128MB）	219.84MB（256MB）
WUXGA	1920	1200	82.73MB（96MB）	135.47MB（196MB）	240.94MB（256MB）
QXGA	2048	1536	102.00MB（128MB）	174.00MB（196MB）	318.00MB（384MB）
WQXGA	2560	1600	123.75MB（128MB）	217.50MB（256MB）	405.00MB（512MB）

特定のワークロードおよびオペレーティング システムでの RAM サイズ設定

必要な RAM 容量は就業者のタイプによって大きく異なるため、多くの企業では社内就業者のさまざまなプールに適した設定を特定するためにパイロット段階を設けています。

出発点として適切なのは、Windows XP デスクトップに 1024MB、Windows Vista デスクトップに 1536MB を割り当てることです。パイロット運用中は、各種の就業者に使用されるディスク領域のパフォーマンスを監視し、就業者のプールごとに最適な設定がみつかるまで調整を行います。

仮想デスクトップの CPU 要件の見積もり

CPU の見積もりを行う場合は、社内の各種就業者の平均 CPU 使用率に関する情報を収集する必要があります。また、仮想化のオーバヘッドとピーク使用期間のために、10 ～ 25% の追加処理能力を計算する必要があります。

CPU の要件は、就業者のタイプによって異なります。ソフトウェア開発者や、高パフォーマンスを必要とするその他のパワーユーザーの CPU 要件は、ナレッジ ワーカーよりもはるかに高くなる場合があります。ナレッジ ワーカーの CPU 要件も、データ入力のタスク ワーカーよりも高い可能性があります。パイロット段階で、Perfmon などのパフォーマンス監視ツールを使用して、それらの就業者グループの平均とピークの CPU 使用率レベルを把握してください。

多数の仮想マシンが 1 台のサーバ上で実行されるため、ウィルス対策エージェントなどのすべてのエージェントがまったく同じ時刻にアップデートの有無をチェックすると、CPU 使用率が急上昇するおそれがあります。パフォーマンスの問題を引き起こす可能性のあるエージェントの種類と数を特定し、それらの問題に対処するための戦略を採用します。たとえば、企業では次の戦略が有効な場合があります。

- ソフトウェア管理エージェントを使用して個別のデスクトップごとにソフトウェア アップデートをダウンロードするのではなく、View Composer を使用してイメージを更新する。
- ウィルス対策とソフトウェアの更新が、ログインしているユーザーが少ない可能性が高いオフピークの時間に実行されるようにスケジュールする。
- 更新の実行時刻をずらすか、ランダム化する。

サイズ設定のアプローチとして、1 個の CPU コアで対応できる仮想デスクトップの数を特定することをお勧めします。出発点として適切なのは、コアあたり 8 台の仮想マシンをパイロット運用することです。たとえば、シングル コア、2.2GHz プロセッサの物理 PC を監視して、平均 CPU 使用率が 2.79% であることが判明した場合、CPU の使用量は 130MHz です。2 ソケットのクワッド コア ESX サーバがある場合、パイロット運用中にそのサーバで 64 台の仮想マシンをホストできます。64 台の仮想マシンにそれぞれ 130MHz を割り当てるとすれば、必要な平均 CPU 容量は 8.3GHz ということになります。

ゲスト オペレーティング システムおよびアプリケーションに必要な CPU 容量に加え、デスクトップの仮想化と使用率の急上昇のために必要な追加処理能力も考慮に入れる必要があります。このオーバーヘッドは、平均 CPU 使用量の 10 ～ 25% に相当します。この例では、必要な CPU 容量は、多めに見積もって 8.3GHz の 25% となります。したがって、ESX サーバの合計 CPU 速度を 10.38GHz にする必要があります。

適切なシステム ディスク サイズの選択

ディスク領域を割り当てるときは、オペレーティング システム、アプリケーション、およびユーザーがインストールまたは生成する可能性のあるその他のコンテンツを格納できるだけの領域を割り当てます。通常この容量は、物理 PC に搭載されているディスクのサイズを下回ります。

データセンターのディスク領域は通常、従来の PC 展開でのデスクトップまたはラップトップのディスク領域よりもギガバイトあたりのコストが高いため、オペレーティング システムのイメージ サイズを最適化してください。イメージ サイズを最適化するために、次の提案が有効な場合があります。

- 不要なファイルを削除します。たとえば、一時インターネット ファイルに割り当てられた領域を削減します。
- 将来の増加を十分見越しながらも、非現実的なほど大きくない仮想ディスク サイズを選択します。
- ユーザーが生成するコンテンツおよびユーザーがインストールするアプリケーションには、中央で管理されるファイル共有または VMware View のユーザー データ ディスクを使用します。

必要なストレージ容量については、各仮想デスクトップで使用される次のファイルを考慮に入れる必要があります。

- ESX サスペンド ファイルは、仮想マシンに割り当てられた RAM 容量に等しいサイズになります。
- Windows のページ ファイルは RAM の 150% に相当します。
- ログ ファイルは仮想マシンあたり約 100MB を占有します。
- 仮想ディスク、つまり `.vmdk` ファイルには、オペレーティング システム、アプリケーション、将来のアプリケーション アップデートおよびソフトウェア アップデートを格納する必要があります。ローカル ユーザー データおよびユーザーがインストールするアプリケーションをファイル共有ではなく仮想デスクトップ上に配置する場合は、それらも仮想ディスクに格納する必要があります。

  View Composer を使用すると、時間の経過にともない `.vmdk` ファイルが大きくなりますが、View Composer の更新操作をスケジュールし、View デスクトップ プールに対してストレージのオーバーコミット ポリシーを設定すると、サイズの増加量を抑制できます。

ユーザーのディスク領域不足を確実に防止するため、この見積もりに 15% を加えてもかまいません。

仮想マシン デスクトップの構成例

仮想マシンに必要な RAM、CPU、およびディスクの容量はゲスト オペレーティング システムによって異なるため、Windows XP と Windows Vista の仮想デスクトップについて、別個の構成例を示します。

仮想マシンでのメモリ、仮想プロセッサ数、ディスク容量などの設定例は VMware View に固有のものであり、『VMware View の参照アーキテクチャ（大規模なエンタープライズ向けの VMware View 導入ガイド）』の検証中に収集された情報に基づきます。このアーキテクチャでは、仮想マシンのホストと管理に VMware Infrastructure 3.5 が使用されました。vSphere での仮想マシンの制限事項については、『VMware vSphere 構成の上限』 ドキュメントを参照してください。

表 4-2 に示したガイドラインは、標準の Windows XP 仮想デスクトップについてのものです。

表 4-2. Windows XP のデスクトップ仮想マシンの例

アイテム	例
オペレーティング システム	32 ビット Windows XP（最新のサービス パックを適用）
RAM	1024MB（ロー エンドで 512MB、ハイ エンドで 2048MB）
仮想 CPU	1
システム ディスク容量	16GB（ロー エンドで 8GB、ハイ エンドで 40GB）
ユーザー データの容量（ユーザー データ ディスクまたはリダイレクトされたプロファイルとして）	5GB（出発点）
仮想 SCSI アダプタのタイプ	デフォルトでない LSI Logic を使用
仮想ネットワーク アダプタ	デフォルトを使用（オペレーティング システムに依存）

必要なシステム ディスク容量は、基本イメージに必要なアプリケーションの数に依存します。View リファレンス アーキテクチャによって、8GB のディスク容量を含むセットアップが検証されています。アプリケーションには、Microsoft Word、Excel、PowerPoint、Adobe Reader、Internet Explorer、McAfee Antivirus、および PKZIP が含まれます。

ユーザー データに必要なディスク容量は、エンド ユーザーの役割と、データ ストレージに関する組織のポリシーによって変わります。View Composer を使用する場合、このデータはユーザー データ ディスクに保管されます。他社製のプロファイル管理製品を使用する場合、このデータは Windows ローミング プロファイルで CIFS ファイル システムにリダイレクトされる場合があります。

表 4-3 に示したガイドラインは、標準の Windows Vista 仮想デスクトップについてのものです。

表 4-3. Windows Vista のデスクトップ仮想マシンの例

アイテム	例
オペレーティング システム	32 ビット Windows Vista（最新のサービス パックを適用）
RAM	1536MB（標準）

表 4-3. Windows Vista のデスクトップ仮想マシンの例 (続き)

アイテム	例
仮想 CPU	1
システム ディスク容量	20GB（標準）
ユーザー データの容量（ユーザー データ ディスクまたはリダイレクトされたプロファイルとして）	5GB（出発点）
仮想 SCSI アダプタのタイプ	デフォルトの LSI Logic を使用
仮想ネットワーク アダプタ	デフォルトを使用（オペレーティング システムに依存）

vCenter および View Composer の仮想マシン構成とデスクトップ プールの最大サイズ

vCenter と View Composer を両方とも同じ仮想マシンにインストールします。この仮想マシンはサーバであるため、デスクトップ仮想マシンよりもはるかに多くのメモリと処理能力が必要です。

View Composer は、1 プールにつき最大 512 のデスクトップを作成およびプロビジョニングできます。View Composer は、一度に最大 512 のデスクトップに対して再構成操作を実行することもできます。

vCenter および View Composer は物理マシンにインストールできますが、この例では表 4-4 に示す仕様の仮想マシンを使用します。これらの仮想マシンをホストする ESX サーバは、物理サーバの障害から保護するための VMware HA クラスタに含めることができます。

表 4-4. vCenter 仮想マシンの例とプール サイズの最大値

アイテム	例
オペレーティング システム	32 ビット Windows Server 2003（最新のサービス パックを適用）
RAM	4GB
仮想 CPU	2
システム ディスク容量	20GB
SCSI タイプ	LSI Logic（Windows Server 2003 のデフォルト）
ネットワーク アダプタ	VM Network（デフォルト）
View Composer の最大プール サイズ	512 デスクトップ

重要 vCenter と View Composer が接続するデータベースは、別の仮想マシン上に配置してください。データベースのサイズ設定に関するガイダンスについては、http://www.vmware.com/support/vi3/doc/vc_db_calculator.xls を参照してください。

Connection Server の仮想マシンの構成および最大接続数

View Connection Server をインストールすると、View Administrator ユーザー インターフェイスもインストールされます。このサーバには、vCenter Server インスタンスと同量のメモリおよび処理リソースが必要です。

View Connection Server の構成

View Connection Server は物理マシンにインストールできますが、この例では表 4-5 に示す仕様の仮想マシンを使用します。これらの仮想マシンをホストする ESX サーバは、物理サーバの障害から保護するための VMware HA クラスタに含めることができます。

表 4-5. Connection Server の仮想マシンの例

アイテム	例
オペレーティング システム	32 ビット Windows Server 2003（最新のサービス パックを適用）
RAM	4GB
仮想 CPU	2 または 4
システム ディスク容量	20GB
SCSI タイプ	LSI Logic（Windows Server 2003 のデフォルト）
ネットワーク アダプタ	VM Network（デフォルト）
1 つの NIC	1 ギガビット

View Connection Server の最大接続数

表 4-6 は、VMware View の展開が対応できる同時接続の最大数の詳細を示しています。

表 4-6. View デスクトップの接続

展開あたりの Connection Server 数	接続のタイプ	同時接続の最大数
1 つの Connection Server	直接接続、RDP	2,000
5 つの Connection Server	直接接続、RDP	5,000
3 つの Connection Server	トンネル接続、RDP	2,000
1 つの Connection Server	直接接続、PCoIP	2,000
1 つの Connection Server	物理 PC への Unified Access	100
1 つの Connection Server	ターミナル サーバへの Unified Access	200

社内ネットワークの外部からの RDP 接続に対してセキュリティ サーバを使用する場合は、トンネル接続が必要です。

VMware View ノード

ノードとは、VMware View の展開で仮想マシン デスクトップをホストする 1 台の ESX サーバです。ノードは、コアあたり 8 台の仮想マシン、LUN あたり 64 台の仮想マシンをホストできます。

ESX サーバ上でホストされるデスクトップの数を最大にすると、VMware View のコスト効率が最大限に高まります。サーバの選択には多くの要因が影響しますが、厳密に取得価格に関して最適化する場合は、CPU コアまたは RAM による制限が過剰にならないサーバ構成を見出す必要があります。

一般に、仮想マシン数は CPU コアあたり 8 台にできますが、物理 RAM の要件も考慮に入れる必要があります。各仮想マシンに割り当てる RAM 容量を見積もった後、想定した ESX サーバの構成がコアによって制限されるか、RAM によって制限されるかを判別できます。サーバがコアによって制限される場合、コアあたりの仮想マシン数を最大にしてサーバを稼働させると、RAM に余剰が生じます。サーバが RAM によって制限される場合、コアあたりの仮想マシンの目標数が達成される前に、物理 RAM が枯渇します。

各仮想マシンの CPU 要件の計算については、「仮想デスクトップの CPU 要件の見積もり (P. 28)」を参照してください。仮想マシンごとに必要な RAM 容量の計算については、「ゲスト オペレーティング システムへのメモリの割り当て (P. 26)」を参照してください。また、物理 RAM のコストは線形ではないことと、場合によっては DIMM チップを使用しない小型のサーバを購入した方がコスト効率が良いことも考慮に入れます。別の場合には、ラック密度、ストレージの接続性、管理性、およびその他の考慮事項により、展開のサーバ数を最小限に抑えた方が適切な選択となることもあります。

表 4-7 に示した ESX 3.5 の推奨構成は、VMware View に固有のものです。vSphere での ESX ホストの制限事項については、『VMware vSphere 構成の上限』 ドキュメントを参照してください。

表 4-7. ESX サーバの VMware View ノードの例

アイテム	例
ESX のバージョン	ESX 3.5 U4 または ESX 4.0 U1
筐体のタイプ	ブレードまたはラック
CPU	2 または 4 ソケット クワッド コア
CPU の速度	コアあたり 3.0GHz
RAM	128GB
イーサネット ポート	1 ギガビット
コアあたりの仮想マシン数	8
ノードあたりのコア数	ESX 3.5 では 8、ESX 4.0 U1b では 16
NIC	4（NIC あたり 32 台の仮想マシン）
View デスクトップのストレージ密度（単位は LUN あたりの仮想マシン数）	64
ファイバ チャネル アダプタ ポート	0 以上

注意 VMware View 3.x の vSphere 4 での実行はサポートされません。

vSphere クラスタ

VMware View の展開では、VMware HA クラスタを使用して物理サーバの障害に備えることができます。View クラスタ内の各 ESX サーバがホストする仮想サーバは 40 を超え、View Composer にも制限事項があるため、クラスタに含めるサーバ（ノード）が 8 台を超えないようにする必要があります。

VMware vSphere および vCenter は、View デスクトップをホストするサーバのクラスタを管理するための豊富な機能セットを備えています。View デスクトップ プールはそれぞれ vCenter リソース プールに関連付ける必要があるため、クラスタの構成も重要です。したがって、プールあたりのデスクトップの最大数は、実行を予定するサーバおよび仮想マシンのクラスタあたりの数に関連します。

非常に大規模な VMware View の展開では、クラスタ オブジェクトを 1 つのデータセンター オブジェクトにつき 1 つだけにすると、vCenter のパフォーマンスと応答性を向上させることができます。これはデフォルトの動作ではありません。デフォルトでは、VMware vCenter によって、同じデータセンター オブジェクト内に新規クラスタが作成されます。

高可用性の要件の特定

VMware vSphere ではその効率性およびリソース管理により、サーバあたりの仮想マシン数を、業界をリードするレベルまで高めることができます。しかし、サーバあたりの仮想マシンの密度を高くするということは、サーバに障害が発生した場合に影響を受けるユーザーが多くなるということです。

高可用性の要件は、デスクトップ プールの目的に応じて大きく異なる場合があります。たとえば、読み取り専用プールの目標復旧ポイント（RPO）の要件は、通常プールとは異なる場合があります。読み取り専用プールの場合、受容可能な解決策として、ユーザーが使用しているデスクトップが使用できなくなったとき、それらのユーザーを別のデスクトップにログインさせるという方法が考えられます。

可用性の必要性が高い場合は、VMware HA の適切な構成が不可欠です。VMware HA を使用していて、サーバあたりのデスクトップ数を固定する予定の場合は、各サーバを低減容量で稼働させます。サーバに障害が発生した場合、デスクトップが別のホスト上で再起動しても、サーバあたりのデスクトップ数の容量を超えません。

たとえば、各ホストが 128 のデスクトップを実行でき、1 台のサーバの障害に耐えることを目標とする 8 ホストのクラスタでは、そのクラスタ上で実行されるデスクトップの数を必ず 128 × (8 - 1) = 896 以内にします。VMware DRS（Distributed Resource Scheduler）を使用して、8 台のホストすべてにデスクトップを均等に分散させることもできます。どのホット スペア リソースもアイドルにしておくことなく、余ったサーバ容量を最大限に利用できます。また、DRS は障害の発生したサーバがサービスに復帰した後のクラスタの再分散にも役立ちます。

サーバの障害に応答して多数の仮想マシンが一斉に再起動するために発生する I/O 負荷をサポートするため、ストレージが適切に構成されていることも確認する必要があります。ストレージの IOPS は、デスクトップがサーバの障害から復旧する速さに最も大きく影響します。

例 4-1. クラスタ構成の例

表 4-8 に示した設定は、VMware View に固有のものです。vSphere での HA クラスタの制限事項については、『VMware vSphere 構成の上限』ドキュメントを参照してください。

表 4-8. HA クラスタの例

アイテム	例
ノード（ESX サーバ）	8 (1 台のホット スペアを含む)
クラスタ タイプ	DRS（Distributed Resource Scheduler）/HA
ネットワーク コンポーネント	標準の ESX 3.5 または 4 クラスタ ネットワーク
スイッチ ポート	ESX 3.5 の場合は 48、ESX 4 の場合は 80 のマネージド GigE

ネットワークの要件は、サーバのタイプ、ネットワーク アダプタの数、および vMotion の構成方法に依存します。

VMware View ビルディング ブロック

1,000 ユーザーのビルディング ブロックは、物理サーバ、VMware vSphere インフラストラクチャ、VMware View サーバ、共有ストレージ、および 1,000 台の仮想マシン デスクトップで構成されます。View ポッドには最大 5 つのビルディング ブロックを含めることができます。

表 4-9. LAN ベースの View ビルディング ブロックの例

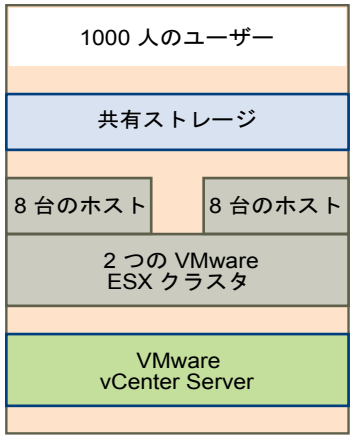
アイテム	例
vSphere クラスタ	2（各クラスタ内に 8 台の ESX ホスト）
48 ポートのネットワーク スイッチ	1
共有ネットワーク ストレージ コンポーネント	1
View Composer を備えた vCenter Server	1（ブロック自体で実行可能）
データベース	MS 2005 SQL Server または Oracle データベース サーバ（ブロック自体で実行可能）
共有ストレージ コンポーネント	1（LUN あたり 64 台の仮想マシン）
ネットワーク	3（管理ネットワーク、ストレージ ネットワーク、および VMotion ネットワークにそれぞれ 1 ギガビットのイーサネット ネットワーク）

ポッドにビルディング ブロックが 1 つしかない場合は、冗長性を確保するために 2 つの View Connection Server インスタンスを使用します。

この情報は、『VMware View の参照アーキテクチャ（大規模なエンタープライズ向けの VMware View 導入ガイド）』から取得したものです。

図 4-1 は、View ビルディング ブロックのコンポーネントを示しています。

図 4-1. VMware View ビルディング ブロック



View ビルディング ブロックの共有ストレージ

ストレージに関する考慮事項は、企業が仮想化テクノロジを採用する主な理由の 1 つです。アーキテクチャに最大の影響を及ぼす決定は、リンク クローン テクノロジを使用する View Composer デスクトップを採用するかどうかです。

VMware vSphere で使用できる外部ストレージは、ファイバ チャネルまたは iSCSI の SAN（ストレージ エリア ネットワーク）、あるいは NFS（ネットワーク ファイル システム）または CIFS（Common Internet File System）の NAS（ネットワーク接続ストレージ）です。ESX バイナリ、仮想マシンのスワップ ファイル、および親仮想マシンの View Composer レプリカはこのシステムに格納されます。

アーキテクチャの観点から見た場合、View Composer を使用するかどうかの決定は、ストレージの計画に最大の影響を及ぼします。View Composer では、基本イメージを共有するデスクトップ イメージが作成されるため、ストレージの必要量を 50% 以上削減できます。デスクトップを定期的に元の状態に戻し、最終更新操作以降の変更の追跡に使用される領域を回収する更新ポリシーを設定すると、さらにストレージの必要量を削減できます。

また、View Composer のユーザー データ ディスクまたは共有ファイル サーバをユーザー プロファイルおよびユーザー ドキュメントのプライマリ リポジトリとして使用すると、オペレーティング システムのディスク領域も削減できます。View Composer ではユーザー データをオペレーティング システムから分離できるため、データ ディスクのみをバックアップまたは複製するだけでよい場合があり、そのためにストレージの必要量がさらに削減されます。詳細については、「View Composer によるストレージ要件の低減 (P. 22)」を参照してください。

例 4-2. ストレージの例

ストレージの例として、『VMware View の参照アーキテクチャ（大規模なエンタープライズ向けの VMware View 導入ガイド）』に掲載されているストレージ コンポーネントを表 4-10 に示します。この表は、1,000 ユーザーに対応できる View ビルディング ブロックに必要なストレージ構成について、一定の考え方を示しています。

表 4-10. EMC NS20FC ストレージ構成の例

アイテム	数
CLARiiON CX3-10F バック エンド アレイを備えた Celerra NS20FC	1
CLARiiON 書き込みキャッシュ	259MB
X-Blade 20 構成	2
2.8GBz Pentium IV CPU	2
ダブル データ レート RAM（266MHz）	4
バック エンド ストレージ接続用のファイバ チャネル ポート	2
10/100/1000 BaseT イーサネット ポート	4
300GB/15K 2/4GB ファイバ チャネル ディスク	30

View ビルディング ブロックおよびポッドのハードウェアの例

VMware View ビルディング ブロックのポッドの仮想インフラストラクチャは、物理サーバ上に存在します。VMware はそのビルディング ブロックのアーキテクチャの検証にブレード サーバ筐体を使用しましたが、同じハードウェア仕様であれば任意のタイプのサーバを使用できます。

例 4-3. VMware View インフラストラクチャのハードウェア

表 4-11 に示したものと同様のハードウェアは、View ビルディング ブロックのインフラストラクチャ コンポーネントをホストできる能力を備えています。インフラストラクチャ コンポーネントには、Active Directory、DNS、DHCP、View Connection Server インスタンス、View Composer を備えた vCenter、および vCenter 用のデータベースをホストする仮想マシン サーバが含まれます。

表 4-11. インフラストラクチャ コンポーネントを含むビルディング ブロックのハードウェアの例

アイテム	数
16 スロット ブレード筐体	1
ブレード サーバ	4
クワッド コア 2.66GHz プロセッサ	4
RAM	32GB
72GB SAS ドライブ	1
Broadcom Gb イーサネット アダプタ	4

4 台のブレード サーバのうち、2 台はクライアントのロード用、1 台は View Connection Server インスタンス用、1 台は Active Directory、DNS、および DHCP 用です。

例 4-4. VMware View デスクトップをホストするハードウェア

表 4-12 に示したものと同様のハードウェアは、1000 ユーザーに対応する View ビルディング ブロックの仮想デスクトップをホストできる能力を備えています。

表 4-12. View ビルディング ブロックのハードウェアの例

アイテム	数
16 スロット ブレード筐体	ビルディング ブロック 2 つにつき 1
ブレード サーバ	16（各クラスタに 8）
クワッド コア 2.66GHz プロセッサ	4
RAM	64GB（各クラスタに 32GB）
72GB SAS ドライブ	2
Broadcom Gb イーサネット アダプタ	12（各クラスタに 6）
4 ポート ギガビット アップリンク モジュール	12（各クラスタに 6）
Cisco 6500 コア ネットワーク スイッチ	1

インフラストラクチャ コンポーネントと View デスクトップは、どちらも物理サーバの障害から保護するための VMware HA クラスタに含まれます。

この情報は、『VMware View の参照アーキテクチャ（大規模なエンタープライズ向けの VMware View 導入ガイド）』から取得したものです。

View ビルディング ブロックの帯域幅に関する考慮事項

VMware View 環境をサポートするストレージ システムの設計には重要な要素が多数ありますが、サーバ構成の観点から見た場合、適切な帯域幅の計画が不可欠です。また、ポート統合ハードウェアの影響も考慮する必要があります。

ピーク ワークロード

VMware View 環境では、すべての仮想マシンが同時にアクティビティを実行しているときに、I/O ストームの負荷が発生することがあります。I/O ストームは、ウィルス対策ソフトウェアやソフトウェア更新エージェントなどのゲスト ベースのエージェントによってトリガされることがあります。また、従業員全員が朝のほぼ同じ時刻にログインした場合のように、人間の動作によって I/O ストームがトリガされることもあります。

仮想マシンごとに更新の時刻をずらすなどの運用上のベスト プラクティスによって、このストーム ワークロードを最小限に抑えることができます。また、パイロット段階でさまざまなログアウト ポリシーをテストして、ユーザーがログアウトした場合のサスペンドまたは電源オフによって I/O ストームが発生するかどうかを判別することもできます。

ベスト プラクティスの特定に加え、帯域幅の平均使用量が 1Gbps の 10 分の 1 未満であっても、仮想マシン 100 台あたり 1Gbps の帯域幅を提供することをお勧めします。このように余裕をもって計画すると、ピーク時の負荷にも十分なストレージの接続性を確保できます。

ディスプレイ トラフィック

ディスプレイ トラフィックについては、使用されるプロトコル、モニタの解像度と構成、ワークロードに含まれるマルチメディア コンテンツの量など、多くの要素がネットワーク帯域幅に影響を及ぼします。ストリーミングされた複数のアプリケーションを同時に起動した場合も、使用量が急増することがあります。

これらの問題による影響は大きく変動する場合があるため、多くの企業ではパイロット プロジェクトの一環として帯域幅の使用量を監視しています。パイロットの出発点として、一般的なナレッジ ワーカー用に 150 ～ 200Kbps の容量を計画してください。

WAN のサポート

WAN（ワイド エリア ネットワーク）については、帯域幅の制約とレイテンシーの問題を考慮する必要があります。

RDP 表示プロトコルを使用する場合は、支社または小規模オフィスのユーザー向けにアプリケーションを高速化する WAN 最適化製品が必要です。

表 4-13. WAN の最適化による中小規模のオフィスのサポート

アイテム	小規模オフィス	中規模の支社
ユーザー数	最大 15	最大 100
リンク タイプ	T1	10Mbps
帯域幅	1.544Mbps	10Mbps
レイテンシー	最大 100ms	最大 100ms

RDP 表示プロトコルを使用する View デスクトップに DSL またはケーブル モデム経由で自宅からアクセスするユーザーには、WAN 最適化製品を使用できない場合があります。その場合、ネットワークは 3 ～ 5 人のユーザーに対応できます。

この情報は、『VMware View WAN Reference Architecture』から取得したものです。

VMware View ポッド

VMware View ポッドは、1,000 ユーザーのビルディング ブロック 5 つを統合して、1 つのエンティティとして管理できる View Manager インストールにします。

ポッドとは、VMware View のスケーラビリティの制限によって決定される編成の単位です。表 4-14 に、View ポッドのコンポーネントを示します。

表 4-14. VMware View ポッドの例

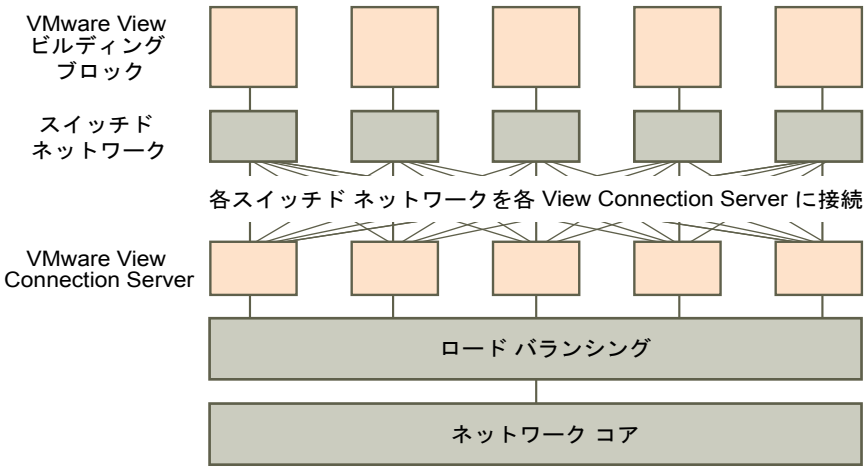
アイテム	数
View ビルディング ブロック	5
View Connection Server	5（各ビルディング ブロックに 1 台）
View Security Server	2 ～ 5（DMZ でロード バランシング）
10Gb イーサネット モジュール	1
モジュラ型コア ネットワーク スイッチ	1
ロード バランシング モジュール	1
WAN 用 VPN	1（オプション）
RDP を使用する場合、WAN アクセラレータ	1（オプション）

ネットワーク コアによって、受信したリクエストの View Connection Server インスタンス間でのロード バランシングが実行されます。通常はネットワーク レベルで冗長性およびフェイルオーバーがサポートされるため、ロード バランサが単一点障害になることが防止されます。たとえば、Virtual Router Redundancy Protocol（VRRP）はロード バランサと通信して、冗長性およびフェイルオーバーの機能を追加します。

View Connection Server インスタンスに障害が発生するか、アクティブなセッション中に応答がなくなった場合でも、ユーザーのデータは失われません。デスクトップの状態は仮想マシン デスクトップに保存されているため、ユーザーは別の View Connection Server インスタンスに接続でき、障害が発生した時点の状態からデスクトップ セッションが再開されます。

図 4-2 は、すべてのコンポーネントを管理の容易な 1 つのエンティティにどのように統合できるかを示しています。

図 4-2. 5,000 の View デスクトップのポッド図



5 セキュリティ機能の計画

View Manager は、企業の機密データを保護するための強力なネットワーク セキュリティ機能を備えています。セキュリティを強化するため、View Manager を他社製のユーザー認証ソリューションと統合したり、セキュリティ サーバを使用したり、制限付き資格の機能を実装したりできます。

この章では次のトピックについて説明します。

クライアント接続について

View Client および View Administrator は、安全な HTTPS 接続を介して View Connection Server ホストと通信します。

ユーザー認証と View デスクトップの選択に使用される最初の View Client 接続は、ユーザーが View Client に IP アドレスを入力したときに作成されます。View Administrator 接続は、管理者が Web ブラウザに View Administrator の URL を入力したときに作成されます。

View Manager にはデフォルトで、クライアントが View Connection Server ホストに接続するときに使用できる自己署名 SSL 証明書が含まれています。デフォルトでは、クライアントが View Administrator などの安全なページにアクセスすると、この自己署名証明書が提示されます。

デフォルトの SSL 証明書はテストに使用できます。デフォルトの SSL 証明書はクライアントから信頼されていないもので、サービスの正しい名前も含まれていないため、置き換える必要があります。独自の自己署名証明書を作成するか、証明機関 (CA) から署名付き証明書を取得するか、すでに持っている SSL 証明書を使用してください。

- Microsoft RDP を使用するトンネル クライアント接続 (P. 40)

  ユーザーが Microsoft RDP 表示プロトコルを使用する View デスクトップに接続すると、View Client は View Connection Server ホストへの第 2 の HTTPS 接続を確立します。この接続は、RDP データを送信するためのトンネルになるため、トンネル接続と呼ばれます。

- PCoIP および HP RGS を使用する直接クライアント接続 (P. 40)

  管理者は、View デスクトップ セッションが View Connection Server ホストをバイパスしてクライアント システムと View デスクトップ仮想マシンとの間で直接確立されるように View Connection Server の設定を構成できます。このタイプの接続を直接クライアント接続といいます。

- View Client with Offline Desktop のクライアント接続 (P. 41)

  View Client with Offline Desktop は、モバイル ユーザーが特定のタイプの View デスクトップのクローン インスタンスをローカル コンピュータ上にチェックアウトできるようにする試験的な機能です。

Microsoft RDP を使用するトンネル クライアント接続

ユーザーが Microsoft RDP 表示プロトコルを使用する View デスクトップに接続すると、View Client は View Connection Server ホストへの第 2 の HTTPS 接続を確立します。この接続は、RDP データを送信するためのトンネルになるため、トンネル接続と呼ばれます。

トンネル接続には次の利点があります。

- RDP データが HTTPS によってトンネリングされ、SSL を使用して暗号化されます。この強力なセキュリティ プロトコルは、オンライン バンキングやクレジット カードの支払いに使用されるような他の安全な Web サイトで提供されているセキュリティに一致しています。
- クライアントは単一の HTTPS 接続を介して複数のデスクトップにアクセスできるため、プロトコル全体のオーバーヘッドが削減されます。
- それらの HTTPS 接続は View Manager によって管理されるため、基盤となるプロトコルの信頼性が大幅に向上します。ユーザーが一時的にネットワーク接続を失った場合に、ネットワーク接続が復元された後、ユーザーが再接続して再度ログインしなくても HTTP 接続が再確立され、RDP 接続が自動的に再開されます。

View Connection Server インスタンスの標準展開では、HTTPS の安全な接続の終点は View Connection Server になります。DMZ 展開では、HTTPS の安全な接続の終点はセキュリティ サーバになります。DMZ 展開およびセキュリティ サーバの詳細については、「セキュリティ サーバを使用するための準備 (P. 43)」を参照してください。

PCoIP または HP RGS 表示プロトコルを使用するクライアントでは、トンネル接続は使用されません。詳細については、「PCoIP および HP RGS を使用する直接クライアント接続 (P. 40)」を参照してください。

PCoIP および HP RGS を使用する直接クライアント接続

管理者は、View デスクトップ セッションが View Connection Server ホストをバイパスしてクライアント システムと View デスクトップ仮想マシンとの間で直接確立されるように View Connection Server の設定を構成できます。このタイプの接続を直接クライアント接続といいます。

直接クライアント接続でも、ユーザーが認証して View デスクトップを選択するための HTTPS 接続がクライアントと View Connection Server ホストとの間に確立されますが、その第 2 の HTTPS 接続（トンネル接続）は使用されません。

クライアントが PCoIP または HP RGS 表示プロトコルを使用する場合は、直接クライアント接続を有効にする必要があります。

PCoIP 接続では、次の組み込みのセキュリティ機能が使用されます。

- PCoIP は Advanced Encryption Standard（AES）暗号化をサポートします。これはデフォルトで有効になっています。
- PCoIP のハードウェア実装では、AES および IP Security（IPsec）が使用されます。
- PCoIP は他社製の VPN クライアントとも連動します。

Microsoft RDP 表示プロトコルを使用するクライアントでは、展開が企業ネットワーク内に限定される場合にのみ直接クライアント接続が適切です。直接クライアント接続を使用すると、RDP トラフィックがその接続を介してクライアントと View デスクトップ仮想マシンの間で暗号化されないまま送信されます。詳細については、「Microsoft RDP を使用するトンネル クライアント接続 (P. 40)」を参照してください。

View Client with Offline Desktop のクライアント接続

View Client with Offline Desktop は、モバイル ユーザーが特定のタイプの View デスクトップのクローン インスタンスをローカル コンピュータ上にチェックアウトできるようにする試験的な機能です。

View Client with Offline Desktop では、LAN ベースのデータ転送用に、トンネリングされた通信とトンネリングされていない通信の両方がサポートされています。トンネリングされた通信では、すべてのトラフィックが View Connection Server ホストを介してルーティングされ、通信およびデータ転送を暗号化するかどうかの指定が可能です。トンネリングされていない通信では、暗号化されていないデータが Offline Desktop クライアント システムと View デスクトップ仮想マシンとの間で直接転送されます。

オフライン データは、トンネリングされた通信またはトンネリングされていない通信のどちらを構成したかに関係なく、ユーザーのコンピュータ上で常に暗号化されます。

ユーザー認証方法の選択

View Manager はデフォルトで、ユーザーを認証および管理するために既存の Active Directory インフラストラクチャを利用します。セキュリティを強化するため、View Manager を RSA SecurID およびスマート カード認証ソリューションと統合することができます。

- Active Directory 認証 (P. 41)

  各 View Connection Server インスタンスは Active Directory ドメインに参加しており、ユーザーは参加しているドメインを利用するために Active Directory に対して認証されます。

- RSA SecurID 認証 (P. 42)

  RSA SecurID は、2 要素認証によってセキュリティの向上をもたらします。これには、ユーザーの PIN およびトークン コードに関する知識が必要です。トークン コードは、物理 SecurID トークンでのみ入手できます。

- スマート カード認証 (P. 42)

  スマート カードは、コンピュータ チップが埋め込まれた小さなプラスチック カードです。多くの官公庁や大企業が、そのコンピュータ ネットワークにアクセスするユーザーの認証にスマート カードを使用しています。スマート カードは Common Access Card（CAC）とも呼ばれます。

- 「現在のユーザーとしてログイン」機能 (P. 43)

  View Client ユーザーが [現在のユーザーとしてログイン] チェック ボックスを選択すると、ユーザーがクライアント システムへのログイン時に入力した認証情報が、View Connection Server インスタンスおよび View デスクトップへの認証に使用されます。それ以上のユーザー認証は必要ありません。

Active Directory 認証

各 View Connection Server インスタンスは Active Directory ドメインに参加しており、ユーザーは参加しているドメインを利用するために Active Directory に対して認証されます。

信頼契約の存在する追加ユーザー ドメインがある場合、ユーザーはそのドメインに対しても認証されます。

たとえば、View Connection Server インスタンスがドメイン A のメンバーであり、ドメイン A とドメイン B の間に信頼契約が存在する場合、ドメイン A とドメイン B の両方のユーザーが View Client を使用して View Connection Server インスタンスに接続できます。

同様に、ドメイン混在環境でドメイン A と MIT Kerberos 領域の間に信頼契約が存在する場合、Kerberos 領域のユーザーは View Client で View Connection Server に接続するときに Kerberos 領域名を選択できます。

View Connection Server は、ホストが存在するドメインから始めて、信頼関係をたどって、アクセスできるドメインを決定します。小さく、十分に接続されているドメインのセットであれば、View Connection Server は短時間でドメインの完全なリストを決定できますが、ドメインの数が増えたり、ドメイン間の接続が不十分であったりすると、要する時間は長くなります。リストには、デスクトップにログインしたユーザーに提供しない方がよいドメインも含まれる場合があります。

管理者は、**vdmadmin** コマンドを使用して、ドメインのフィルタ処理を構成できます。フィルタを使用すると、View Connection Server インスタンスまたはセキュリティ サーバが検索してエンド ユーザーに表示するドメインを制限できます。詳細については、『Command-Line Tool for View Manager』テクニカル ノートを参照してください。

ログインを許可する時間を制限したり、パスワードの失効日を設定するなどのポリシーも、Active Directory の既存の運用手順に従って処理されます。

RSA SecurID 認証

RSA SecurID は、2 要素認証によってセキュリティの向上をもたらします。これには、ユーザーの PIN およびトークン コードに関する知識が必要です。トークン コードは、物理 SecurID トークンでのみ入手できます。

管理者は、View Connection Server ホストに RSA SecurID ソフトウェアをインストールし、View Connection Server の設定を変更することで、個別の View Connection Server インスタンスで RSA SecurID 認証を有効にできます。

ユーザーは、RSA SecurID 認証が有効になっている View Connection Server インスタンスを介してログインすると、最初に RSA ユーザー名とパスコードを入力して認証するように求められます。ユーザーがこのレベルで認証されないと、アクセスが拒否されます。ユーザーが RSA SecurID によって正しく認証された場合は、通常どおり続行することになり、次に Active Directory の認証情報の入力を求められます。

View Connection Server インスタンスが複数ある場合は、一部のインスタンスで RSA SecurID 認証を構成し、他のインスタンスでは別のユーザー認証方法を構成することができます。たとえば、インターネットを介してリモートで View デスクトップにアクセスするユーザーのみに RSA SecurID 認証を構成できます。

View Manager は RSA SecurID Ready プログラムによって認定されており、新規 PIN モード、次のトークン コード モード、RSA Authentication Manager、ロード バランシングなど、SecurID のあらゆる機能をサポートしています。

スマート カード認証

スマート カードは、コンピュータ チップが埋め込まれた小さなプラスチック カードです。多くの官公庁や大企業が、そのコンピュータ ネットワークにアクセスするユーザーの認証にスマート カードを使用しています。スマート カードは Common Access Card（CAC）とも呼ばれます。

管理者は、個別の View Connection Server インスタンスでスマート カード認証を有効にできます。View Connection Server インスタンスでのスマート カードの使用を有効にすると、通常は信用ストアにルート証明書が追加された後、View Connection Server の設定が変更されるという処理が伴います。

スマート カード認証を使用するクライアント接続は、SSL に対応している必要があります。管理者は、View Administrator でグローバル パラメータを設定して、クライアント接続の SSL を有効にできます。

スマート カード認証を使用するクライアント システムごとに、Windows 互換のスマート カード リーダと、製品固有のアプリケーション ドライバが必要です。

スマート カード認証は View Client のみでサポートされます。View Client with Offline Desktop、View Portal、または View Administrator ではサポートされません。

スマート カード認証は、PCoIP 表示プロトコルを使用するクライアントではサポートされません。

「現在のユーザーとしてログイン」機能

View Client ユーザーが［現在のユーザーとしてログイン］チェック ボックスを選択すると、ユーザーがクライアント システムへのログイン時に入力した認証情報が、View Connection Server インスタンスおよび View デスクトップへの認証に使用されます。それ以上のユーザー認証は必要ありません。

この機能をサポートするため、ユーザー認証情報は View Connection Server インスタンスとクライアント システムの両方に格納されます。

- View Connection Server インスタンスでは、ユーザー認証情報は暗号化され、ユーザー名、ドメイン、およびオプションの UPN とともにユーザー セッションに格納されます。この認証情報は、認証が行われると追加され、セッション オブジェクトが破壊されるとパージされます。セッション オブジェクトは、ユーザーがログアウトしたとき、セッションがタイムアウトになったとき、または認証が失敗したときに破壊されます。セッション オブジェクトは揮発性メモリ内に存在し、LDAP やディスク ファイルには格納されません。
- クライアント システムでは、ユーザー認証情報は暗号化され、View Client のコンポーネントである認証パッケージのテーブルに追加されます。認証情報は、ユーザーがログインしたときにテーブルに追加され、ログアウトしたときにテーブルから削除されます。このテーブルは揮発性メモリ内に存在します。

管理者は、View Client のグループ ポリシー設定を使用して、［現在のユーザーとしてログイン］チェック ボックスを使用可能にするかどうかを制御し、そのデフォルト値を設定することができます。

注意 スマート カード認証が必要な場合は、［現在のユーザーとしてログイン］チェック ボックスを選択したユーザーの認証は失敗します。このようなユーザーは、View デスクトップにログインするときにスマート カードと PIN で再認証する必要があります。

セキュリティ サーバを使用するための準備

セキュリティ サーバは、View Connection Server 機能のサブセットを実行する、View Connection Server の特殊なインスタンスです。セキュリティ サーバを使用すると、インターネットと内部ネットワークとの間にセキュリティのレイヤを追加できます。

セキュリティ サーバは非武装地帯（DMZ）内に存在し、信頼されるネットワーク内の接続に対してプロキシ ホストの役割を果たします。各セキュリティ サーバは View Connection Server のインスタンスと対になっていて、すべてのトラフィックをそのインスタンスに転送します。この設計では、公衆網に接するインターネットから View Connection Server インスタンスを遮断し、保護されていないすべてのセッション要求が強制的にセキュリティ サーバを通過するようにして、セキュリティのレイヤを追加します。

DMZ 展開では、クライアントが DMZ 内のセキュリティ サーバに接続できるようにファイアウォール上で数個のポートを開く必要があります。また、セキュリティ サーバと内部ネットワーク内の View Connection Server インスタンスが通信できるように、数個のポートを構成する必要があります。個別のポートの詳細については、「DMZ ベースのセキュリティ サーバのファイアウォール ルール (P. 50)」を参照してください。

内部ネットワーク内からはユーザーが任意の View Connection Server インスタンスに直接接続できるため、LAN ベースの展開にはセキュリティ サーバを実装する必要はありません。

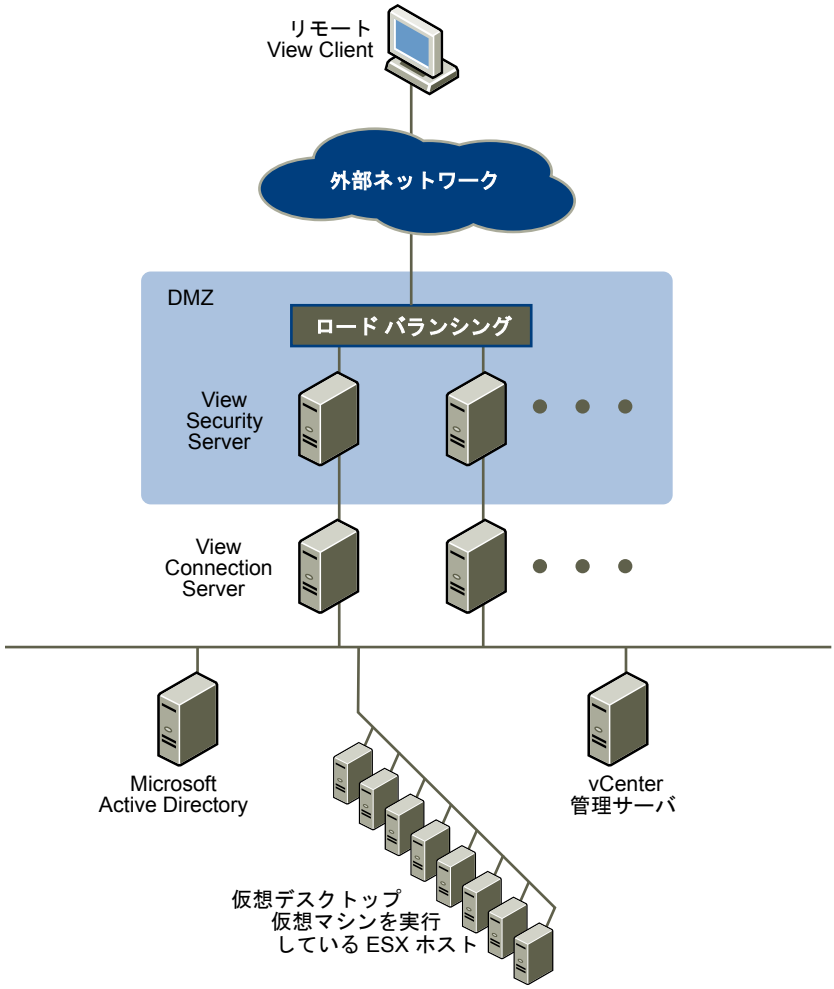
PCoIP を使用する View クライアントは、View セキュリティ サーバに接続できますが、仮想デスクトップとの PCoIP セッションではセキュリティ サーバが無視されます。PCoIP ではオーディオとビデオのストリーミングに User Datagram Protocol（UDP）を使用します。セキュリティ サーバは TCP のみをサポートします。

セキュリティ サーバのトポロジ

複数の異なるセキュリティ サーバ トポロジを実装できます。

図 5-1 のトポロジは、ロード バランスされた 2 台のセキュリティ サーバを DMZ に配置した高可用性環境を示しています。これらのセキュリティ サーバは、内部ネットワーク内の 2 つの View Connection Server インスタンスと通信します。

図 5-1. DMZ 内のロード バランスされたセキュリティ サーバ

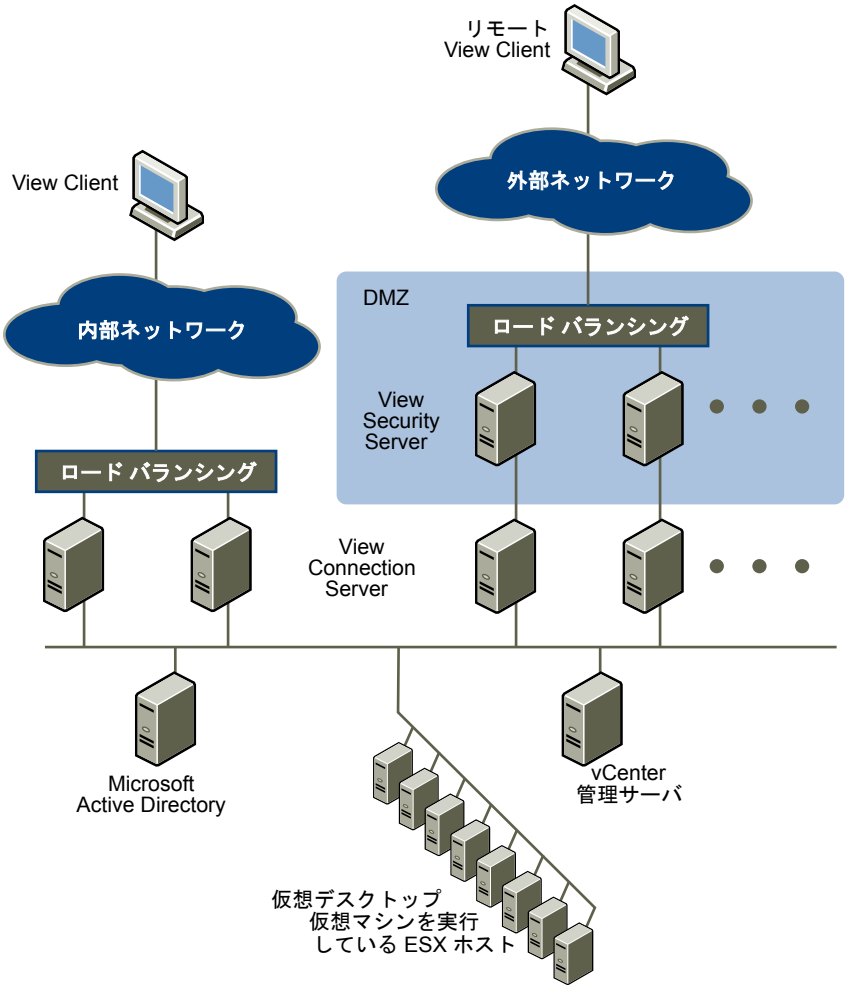


リモート ユーザーがセキュリティ サーバに接続する場合、View デスクトップにアクセスするには、認証に成功する必要があります。DMZ の両側に適切なファイアウォール ルールが適用されるため、このトポロジは、インターネット上のクライアント デバイスから View デスクトップにアクセスする場合に適しています。

View Connection Server の各インスタンスに複数のセキュリティ サーバを接続できます。DMZ 展開を標準展開と組み合わせて、内部ユーザーと外部ユーザーにアクセスを提供できます。

図 5-2 のトポロジは、View Connection Server の 4 つのインスタンスが 1 つのグループとして機能する環境を示しています。内部ネットワーク内のインスタンスは内部ネットワークのユーザー専用であり、外部ネットワーク内のインスタンスは外部ネットワークのユーザー専用です。セキュリティ サーバと対になっている View Connection Server インスタンスで RSA SecurID 認証を有効にすると、すべての外部ネットワーク ユーザーに RSA SecurID トークンを使用した認証が義務付けられます。

図 5-2. 複数のセキュリティ サーバ



セキュリティ サーバを複数インストールする場合は、ハードウェアまたはソフトウェアのいずれかのロード バランシング ソリューションを実装する必要があります。View Connection Server は他社製の標準的なロード バランシング ソリューションと連動します。View Connection Server 自体はロード バランシング機能を提供しません。

DMZ ベースのセキュリティ サーバのファイアウォール

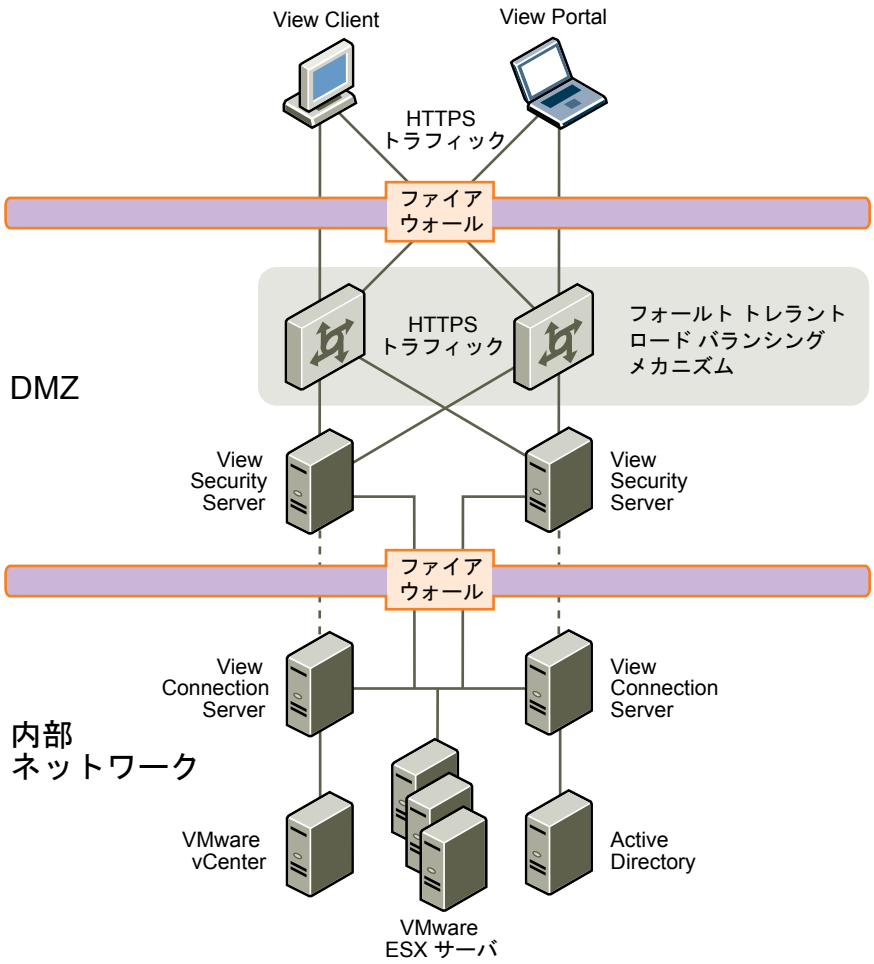
DMZ ベースのセキュリティ サーバの展開には、2 つのファイアウォールを含める必要があります。

- DMZ と内部ネットワークの両方を保護するために、外部ネットワークに接しているフロント エンド ファイアウォールが必要です。外部からのネットワーク トラフィックが DMZ に到達できるように、このファイアウォールを構成します。
- 2 つ目のセキュリティの層を提供するために、DMZ と 内部ネットワークの間のバック エンド ファイアウォールが必要です。DMZ 内のサービスから送信されたトラフィックだけを受け入れるように、このファイアウォールを構成します。

ファイアウォール ポリシーによって DMZ サービスからの受信通信が厳格に制御されるため、内部ネットワークが侵害されるリスクが大幅に軽減されます。

図 5-3 は、フロント エンド ファイアウォールとバック エンド ファイアウォールを含む構成の例を示しています。

図 5-3. デュアル ファイアウォール トポロジ

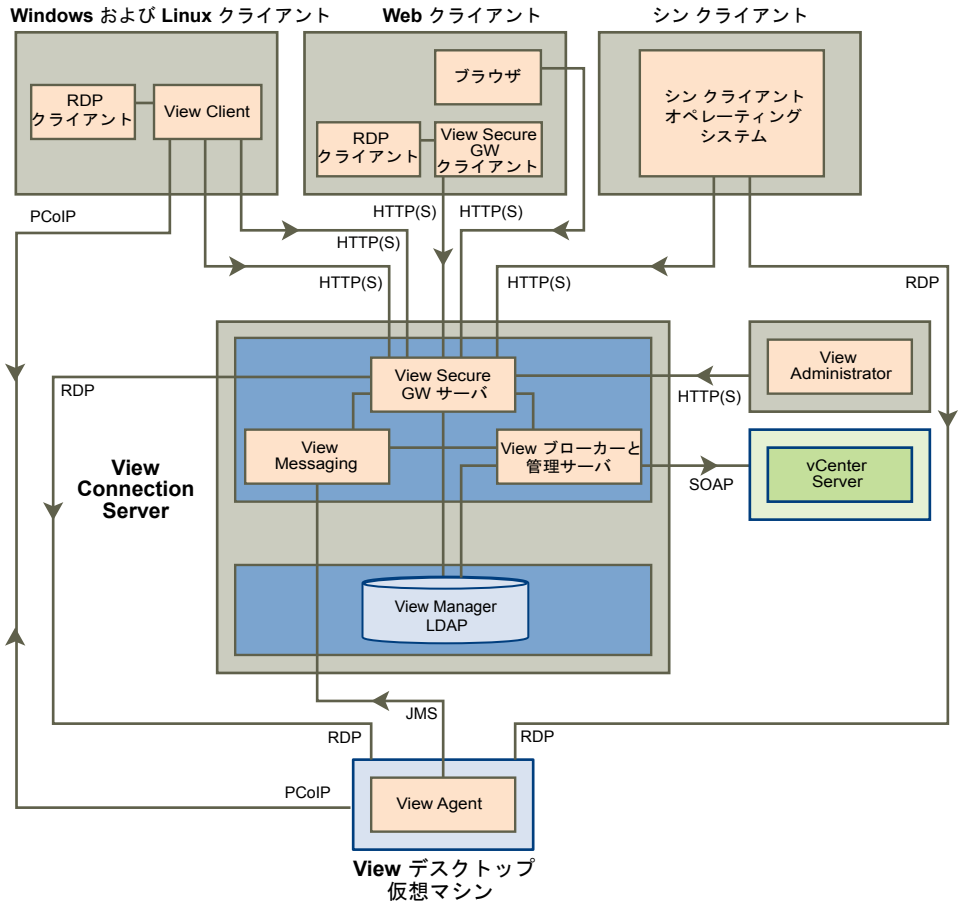


View Manager のコンポーネントとプロトコル

View Manager のコンポーネントは、複数の異なるプロトコルを使用してメッセージをやりとりします。

図 5-4 は、セキュリティ サーバが構成されていない場合に各コンポーネントが通信に使用するプロトコルを含め、View Manager コンポーネント間の関係を表しています。

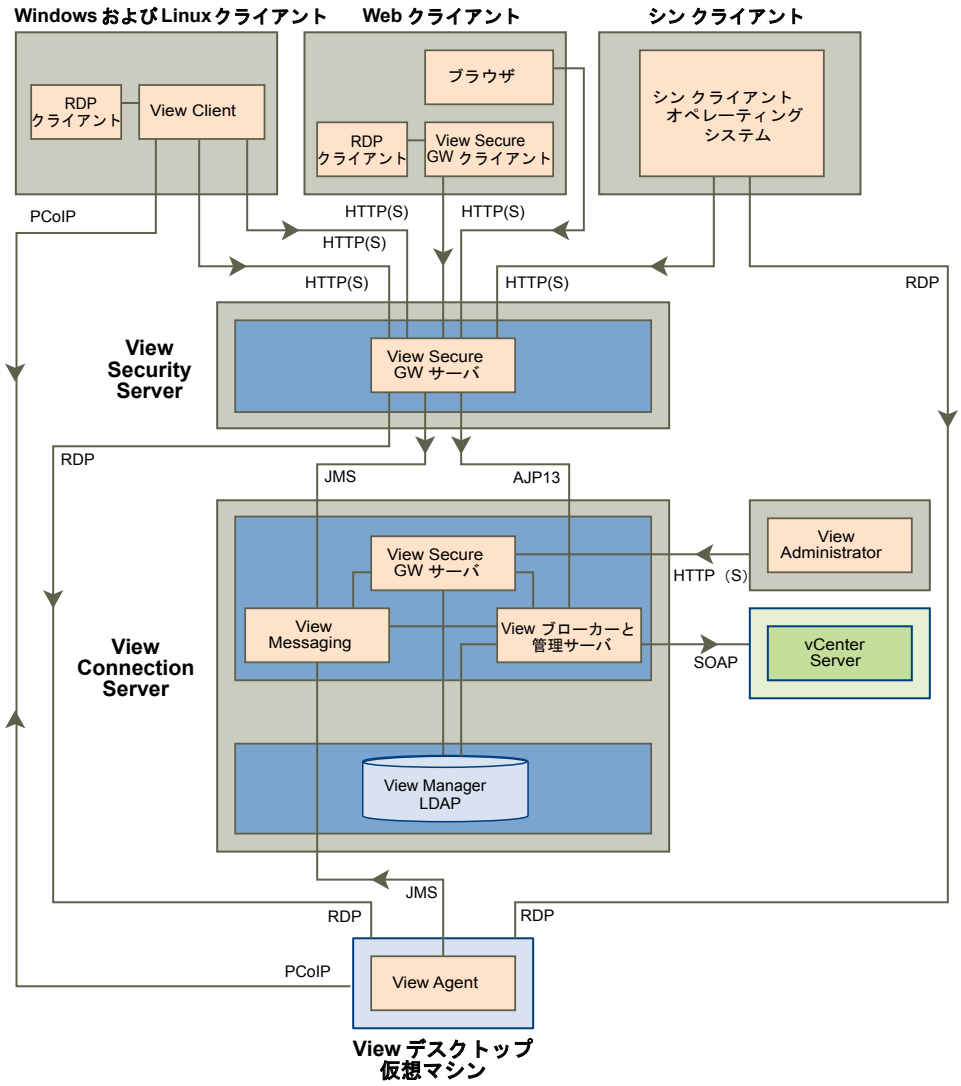
図 5-4. セキュリティ サーバが構成されていない View Manager のコンポーネントとプロトコル



各プロトコルで使用されるデフォルト ポートについては、表 5-1 を参照してください。

図 5-5 は、セキュリティ サーバが構成されている場合に各コンポーネントが通信に使用するプロトコルを含め、セキュリティ サーバとその他のすべての View Manager コンポーネント間の関係を表しています。

図 5-5. セキュリティ サーバが構成されている View Manager のコンポーネントとプロトコル



各プロトコルで使用されるデフォルト ポートを、表 5-1 に示します。

表 5-1. デフォルト ポート

プロトコル	ポート
JMS	TCP ポート 4001
AJP13	TCP ポート 8009 **注意** AJP13 はセキュリティ サーバの構成のみで使用されます。
HTTP	TCP ポート 80
HTTPS	TCP ポート 443
RDP	TCP ポート 3389 USB リダイレクトには、RDP とともに TCP ポート 32111 が使用されます。MMR には、RDP とともに TCP ポート 9427 が使用されます。 **注意** View Connection Server インスタンスが直接クライアント接続用に構成されている場合、それらのプロトコルはクライアントから View デスクトップに直接接続され、View Secure Gateway Server コンポーネントを介してトンネリングされません。

表 5-1. デフォルト ポート (続き)

プロトコル	ポート
SOAP	TCP ポート 80 または 443
PCoIP	View Client から View デスクトップへの TCP ポート 50002。 PCoIP では双方向で UDP ポート 50002 も使用されます。 USB リダイレクトには、クライアントから View デスクトップへ PCoIP とともに TCP ポート 32111 が使用されます。

View ブローカーと管理サーバ

View Connection Server のコアである View Broker コンポーネントは、View クライアントと View Connection Server 間のすべてのユーザー操作を管理します。View Broker には、View Administrator Web クライアントに使用される Administration Server も含まれます。

View Broker は vCenter Server と緊密に連動して、仮想マシン作成や電源操作を含む View デスクトップの高度な管理を実現します。

View Secure Gateway Server

View Secure Gateway Server は、View クライアントとセキュリティ サーバまたは View Connection Server インスタンスとの安全な HTTPS 接続を実現するサーバ側コンポーネントです。

View Connection Server のトンネル接続を構成すると、RDP、USB、およびマルチメディア リダイレクト（MMR）トラフィックが View Secure Gateway コンポーネントを介してトンネリングされます。直接クライアント接続を構成すると、それらのプロトコルはクライアントから View デスクトップに直接接続され、View Secure Gateway Server コンポーネントを介してトンネリングされません。

注意 PCoIP および HP RGS ではトンネリングが使用されません。

View Secure Gateway Server は、View クライアントから View Broker コンポーネントへの、ユーザー認証やデスクトップ選択トラフィックを含むその他の Web トラフィックの転送も管理します。また、View Secure Gateway Server は View Administrator クライアントの Web トラフィックを Administration Server コンポーネントに渡します。

View LDAP

View LDAP は View Connection Server の組み込み LDAP ディレクトリであり、すべての View Manager 構成データの構成リポジトリです。

View LDAP には、各 View デスクトップ、アクセス可能な各 View デスクトップ、まとめて管理される複数の View デスクトップ、および View コンポーネントの構成設定を表すエントリが含まれています。

View LDAP には、他の View コンポーネントに自動化および通知サービスを提供する、一連の View プラグイン DLL も含まれています。

View Messaging

View Messaging コンポーネントは、View Connection Server コンポーネント間、および View Agent と View Connection Server との間のメッセージング ルータとして機能します。

View Messaging は、View でのメッセージングに使用される Java Message Service（JMS）API をサポートしています。

DMZ ベースのセキュリティ サーバのファイアウォール ルール

DMZ ベースのセキュリティ サーバには、フロント エンド ファイアウォールとバック エンド ファイアウォールに関する特定のファイアウォール ルールが必要です。

フロント エンド ファイアウォールのルール

外部のクライアント デバイスが DMZ 内のセキュリティ サーバに接続できるようにするには、フロント エンド ファイアウォールで、受信トラフィックを特定の TCP ポートで許可する必要があります。表 5-2 にフロント エンド ファイアウォールのルールの概要を示します。

表 5-2. フロント エンド ファイアウォールのルール

送信元	プロトコル	ポート	送信先	備考
任意	HTTP	80	セキュリティ サーバ	SSL が無効になっている場合、外部クライアント デバイスは DMZ 内のセキュリティ サーバへの接続にポート 80 を使用します。
任意	HTTPS	443	セキュリティ サーバ	SSL が有効になっている場合（デフォルト）、外部クライアント デバイスは DMZ 内のセキュリティ サーバへの接続にポート 443 を使用します。

バック エンド ファイアウォールのルール

セキュリティ サーバが、内部ネットワーク内に存在する各 View Connection Server インスタンスと通信できるようにするには、バック エンド ファイアウォールで、受信トラフィックを特定の TCP ポートで許可する必要があります。View デスクトップと View Connection Server インスタンスが互いに通信できるようにするために、バック エンド ファイアウォールの背後で、内部のファイアウォールが同様に構成されている必要があります。表 5-3 にバック エンド ファイアウォールのルールの概要を示します。

表 5-3. バック エンド ファイアウォールのルール

送信元	プロトコル	ポート	送信先	備考
セキュリティ サーバ	AJP13	8009	View Connection Server	セキュリティ サーバは、AJP13 によって転送された Web トラフィックを View Connection Server インスタンスに送信するために、ポート 8009 を使用します。
セキュリティ サーバ	JMS	4001	View Connection Server	セキュリティ サーバは、Java Message Service（JMS）トラフィックを View Connection Server インスタンスに送信するために、ポート 4001 を使用します。
セキュリティ サーバ	RDP	3389	View デスクトップ	セキュリティ サーバは、RDP トラフィックを View デスクトップに送信するために、ポート 3389 を使用します。 **注意** USB リダイレクトには、RDP とともに TCP ポート 32111 が使用されます。MMR には、RDP とともに TCP ポート 9427 が使用されます。

View Connection Server の通信に使用される TCP ポート

View Connection Server インスタンスのグループは、互いに通信するために追加の TCP ポートを使用します。たとえば View Connection Server インスタンスは、JMS のルータ間トラフィックを互いに送信するために、ポート 4100 を使用します。

通常、ファイアウォールはグループ内の View Connection Server インスタンス間では使用されないため、それらの TCP ポートについてはここでは説明しません。

View Manager コンポーネントの一般的なファイアウォール ルール

どのようなファイアウォール構成でも、特定の View Manager コンポーネント間のトラフィックを許可するために TCP ポートを開く必要があります。

セキュリティ サーバの実装に固有のファイアウォール ルールについては、「DMZ ベースのセキュリティ サーバのファイアウォール ルール (P. 50)」を参照してください。

View Agent のファイアウォール ルール

表 5-4 に、View Agent のインストール プログラムによってファイアウォール上で開かれる TCP ポートを示します。これらのポートは、特に記述のない限り受信 TCP ポートです。プロトコルのダイレクションの詳細については、「View Manager のコンポーネントとプロトコル (P. 46)」を参照してください。

表 5-4. View Agent のインストール時に開かれる TCP ポート

プロトコル	ポート
RDP	3389
USB リダイレクト	32111
MMR	9427
PCoIP	50002（TCP および UDP）
HP RGS	42966

View Agent インストーラによって、ホスト OS の現在の RDP ポート（通常は 3389）に合わせて受信 RDP 接続のローカル ファイアウォール ルールが構成されます。この RDP ポート番号を変更する場合は、関連するファイアウォール ルールも変更する必要があります。

HP RGS Sender アプリケーションは、HP RGS リモート表示プロトコルのサーバ側コンポーネントであり、デフォルトでポート 42966 を使用します。

仮想マシン テンプレートをデスクトップ ソースとして使用する場合は、そのテンプレートがデスクトップ ドメインのメンバーである場合にのみ、展開されたデスクトップにファイアウォールの例外が継承されます。Microsoft のグループ ポリシー設定を使用して、ローカルでのファイアウォールの例外を管理できます。詳細については、Microsoft のサポート技術情報（KB）の記事 875357 を参照してください。

Active Directory のファイアウォール ルール

View 環境と Active Directory サーバの間にファイアウォールがある場合は、必要なポートがすべて開いていることを確認する必要があります。たとえば View Connection Server は、Active Directory グローバル カタログおよび Lightweight Directory Access Protocol（LDAP）サーバにアクセスできる必要があります。使用しているファイアウォール ソフトウェアによってグローバル カタログと LDAP のポートがブロックされると、管理者がユーザーの資格を構成する際に問題が発生します。

ファイアウォールを介して Active Directory を正常に機能させるために開く必要があるポートの詳細については、使用する Active Directory サーバのバージョンに関する Microsoft のマニュアルを参照してください。

View Client with Offline Desktop のファイアウォール ルール

View Client with Offline Desktop のデータはポート 902 を介してダウンロードおよびアップロードされます。View Client with Offline Desktop の機能を使用する予定の場合は、ESX ホストがこのポートにアクセスできるようにする必要があります。

View デスクトップ アクセスの制限

制限付き資格の機能を使用し、ユーザーが接続する View Connection Server インスタンスに基づいて View デスクトップ アクセスを制限できます。

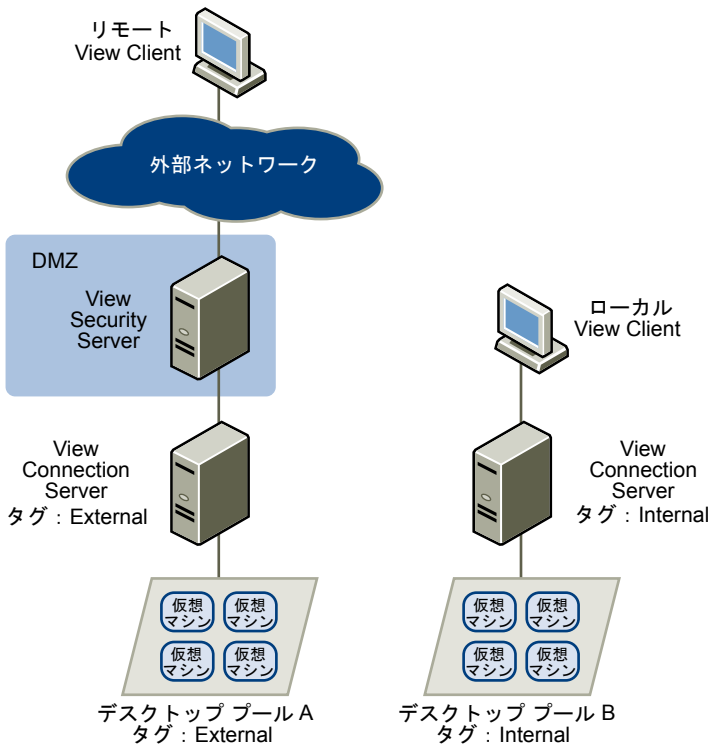
制限付き資格では、1 つ以上のタグを View Connection Server インスタンスに割り当てます。その後、デスクトップまたはデスクトップ プールを構成するときに、デスクトップまたはデスクトップ プールにアクセスできるようにする View Connection Server インスタンスのタグを選択します。ユーザーがタグ付きの View Connection Server インスタンスを通してログインするとき、ユーザーは少なくとも 1 つのタグが一致するか、タグがないデスクトップおよびデスクトップ プールにのみアクセスできます。

たとえば、展開に 2 つの View Connection Server インスタンスが含まれるものとします。第 1 のインスタンスは内部ユーザーをサポートします。第 2 のインスタンスはセキュリティ サーバと対になって、外部ユーザーをサポートします。外部ユーザーが特定のデスクトップにアクセスできないようにするには、次のように制限付き資格を設定します。

- タグ「Internal」を、内部ユーザーをサポートする View Connection Server インスタンスに割り当てます。
- タグ「External」を、セキュリティ サーバと対になって外部ユーザーをサポートする View Connection Server インスタンスに割り当てます。
- 内部ユーザーのみがアクセスできるようにするデスクトップおよびデスクトップ プールに、「Internal」タグを割り当てます。
- 外部ユーザーのみがアクセスできるようにするデスクトップおよびデスクトップ プールに、「External」タグを割り当てます。

外部ユーザーは「External」というタグの付いた View Connection Server を使用してログインするので、「Internal」というタグの付いたデスクトップおよびデスクトップ プールにはアクセスできません。同様に、内部ユーザーは「Internal」というタグの付いた View Connection Server を使用してログインするので、「External」というタグの付いたデスクトップおよびデスクトップ プールにはアクセスできません。この構成を図 5-6 に示します。

図 5-6. 制限付き資格の例



制限付き資格を使用して、特定の View Connection Server インスタンスに対して構成されているユーザー認証方法に基づいて、デスクトップ アクセスを制御することもできます。たとえば、スマート カードで認証されているユーザーのみが特定のデスクトップを使用できるようにすることができます。

制限付き資格の機能は、タグの一致を適用するだけです。特定のクライアントが特定の View Connection Server インスタンスを通して接続するように、ネットワーク トポロジを設計する必要があります。

VMware View 環境のセットアップ手順の概要

6

View のインストールとセットアップのチェック リストは、View の展開を作成するための高水準のタスクとその実行順序、および手順が記載されているドキュメントを示しています。

表 6-1. View のインストールおよびセットアップのチェックリスト

ステップ	タスク
1	必要な管理者ユーザーおよびグループを Active Directory で設定します。 手順：『VMware View Manager 管理ガイド』および vSphere のマニュアル
2	（オプション）VMware ESX サーバおよび vCenter Server をインストールして設定します。 手順：vSphere のマニュアル、ドキュメント ロードマップ
3	（オプション）View Composer を vCenter Server にインストールします。 手順：『VMware View Manager 管理ガイド』
4	View Connection Server をインストールします。 手順：『VMware View Manager 管理ガイド』
5	Active Directory GPO テンプレートを View Connection Server マシンから Active Directory サーバにコピーしてインポートします。 手順：『VMware View Manager 管理ガイド』
6	View Connection Server の初期構成を行います。 手順：『VMware View Manager 管理ガイド』
7	完全クローン デスクトップ プールのテンプレートとして、またはリンク クローン デスクトップ プールの親として使用できる仮想マシンを 1 台以上作成します。必要なアプリケーションまたは VMware ThinApp アプリケーションをインストールします。 手順：vSphere のマニュアル、ドキュメント ロードマップ、および VMware View の『Windows XP Deployment Guide』
8	デスクトップ ソースとして使用する仮想マシンおよび物理マシンに View Agent をインストールします。 手順：『VMware View Manager 管理ガイド』
9	個別の View デスクトップまたは View デスクトップ プール、あるいはその両方を作成します。 手順：『VMware View Manager 管理ガイド』
19	ユーザーまたはユーザー グループ、あるいはその両方に、デスクトップに対する資格を付与します。 手順：『VMware View Manager 管理ガイド』
11	デスクトップ ポリシーを設定します。 手順：『VMware View Manager 管理ガイド』
12	エンド ユーザーのマシンに View Client をインストールするか、View Portal を使用して必要なコンポーネントをインストールするようにエンド ユーザーに指示します。 手順：『VMware View Manager 管理ガイド』

表 6-1. View のインストールおよびセットアップのチェックリスト (続き)

ステップ	タスク
13	エンド ユーザーに各自のデスクトップにアクセスしてもらいます。 手順：『VMware View Manager 管理ガイド』
14	ユーザーとデスクトップを管理し、監視します。 手順：『VMware View Manager 管理ガイド』

インデックス