





# 目次

本書について	7
VDM クイック スタート ガイド	11
ハードウェアの要件	12
前提条件	12
インストール前のチェックリスト	13
デスクトップ仮想マシンの準備	13
VDM Connection Server のインストール	15
シングルサーバのインストール	15
ワンタイム構成	16
デスクトップの作成	17
個別デスクトップの作成	17
デスクトップへの資格の付与	19
デスクトップへの接続	20
VDM の概要とシステム要件	23
VDM の概要	23
システム要件	25
VDM Connection Server	25
VDM Client	26
VDM Web Access	27
VDM Agent 仮想デスクトップ	27
前提条件	28
VDM のアップグレード	29
VDM のインストールおよび設定	31
デスクトップ仮想マシンの準備	32
複数の NIC を使用する仮想マシン上での VDM Agent の使用	34
VDM Connection Server のインストール	34
シングルサーバのインストール	34
マルチサーバのインストール	36
ワンタイム構成	37
VDM Connection Server の有効化と無効化	38

End-to-End 構成	39
ブール デスクトップの構成	41
デスクトップへの資格の付与	49
デスクトップへの接続	50
エンド ユーザーのパスワードの変更	52
デフォルト デスクトップのシン クライアント ユーザー用の設定	52
VDM Administrator のユーザー インターフェイス	54
[ インベントリ ] ページ	55
[ 構成 ] ページ	57
[ イベント ] ページ	57
デスクトップおよび資格のあるユーザーとグループの検索	57
アクティブなセッションの操作	59
グローバル構成設定	60
イベントの表示	62
RSA SecurID	62
VDM オブジェクトの削除	63
SSL 証明書のインストール	65
CSR の作成	65
ロード バランシング	68
非 DMZ 展開でのロード バランシング	69
セッションのセットアップとロード バランシング	69
ロードバランスされたソリューションの DNS 要件	70
ロードバランシングソリューション	71
DMZ の展開	72
DMZ のインストール	72
DMZ 展開でのロード バランシング	74
DMZ 展開のためのファイアウォール ポートの構成	74
VDM 構成データのエクスポートおよびインポート	76
クライアントのコマンドライン パラメータ	76
VDM 診断情報の収集	77
VDM Support ツールを使用した診断情報の収集	78
VDM Support スクリプトを使用した診断情報の収集	78
サポート要求の更新	79
VDM のトラブルシューティング	80
VDM Client での詳細な Active Directory RDP の設定	81
詳細設定での Active Directory グループ ポリシーの使用	84
VDM グループ ポリシー オブジェクト	85
コンピュータの構成	85

VDM Agent の構成	85
VDM Client の構成	86
VDM Server の構成	87
VDM Client の VDM ユーザー構成	88

用語集	91
-----	----

インデックス	95
--------	----



# 本書について

---

本マニュアル『インストールおよび管理ガイド』では、VMware® Virtual Desktop Manager のセットアップ、インストール、および構成に関する情報を提供します。これには各種ソフトウェア コンポーネントをインストールする方法、サーバを展開する方法、および仮想デスクトップの構成方法と仮想デスクトップへの接続方法が含まれます。また、ロードバランシングとセキュリティ、サポート対象の OS、およびシンクライアント デバイスをセットアップする方法に関する情報も提供します。

この章では次のトピックについて説明します。

- › [改訂履歴](#) (P.7)
- › [対象読者](#) (P.8)
- › [本書へのフィードバック](#) (P.8)
- › [スタイル](#) (P.8)
- › [テクニカル サポートおよびエデュケーション リソース](#) (P.8)

## 改訂履歴

本マニュアルは、製品のリリースごとに、あるいは必要に応じて改訂されます。改訂版には大小の変更が加えられます。表 1 は、本マニュアルの各バージョンにおける主な変更点を示したものです。

表 1 改訂履歴

リビジョン	説明
20080527	VDM マニュアルの初版。

## 対象読者

本書は、VDM をインストール、管理、または構成するすべての方を対象としています。本書に記載されている情報は、仮想マシンのテクノロジーとデータセンターの操作に精通した、経験豊富な Windows または Linux システム管理者向けに書かれています。

## 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、下記の電子メールアドレスまでフィードバックをお寄せください。

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

## スタイル

本書では、表 2 のスタイル規則を使用しています。

表 2 本マニュアルのスタイル規則

スタイル	対象エレメント
青字 (オンラインのみ)	相互参照、Web アドレス、リンク、メールアドレスに使用
LucidaMonoEFO (等倍フォント)	コマンド、ファイル名、ディレクトリ、パスに使用
LucidaMonoEFO (等倍フォント太字)	ユーザー入力を示す場合に使用
[角カッコ]	インターフェイス オブジェクト、ボタンに使用
< 山カッコ >	キー、変数およびパラメータに使用
太字	用語集の用語、見出し語に使用
下線	強調したい箇所に使用
『二重かぎカッコ』	文献名に使用

## 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。本マニュアルおよび他のマニュアルの最新バージョンを以下のアドレスからご利用いただけます。

<http://www.vmware.com/support/pubs>

## セルフ サービス サポート

お客様が問題を自身で解決するツールとして、あるいはテクニカル情報として、以下の VMware Technology Network (VMTN) をご利用いただけます。

- › 製品情報 <http://www.vmware.com/products/>
- › 技術情報 <http://www.vmware.com/vcommunity/technology>
- › ドキュメント <http://www.vmware.com/support/pubs>
- › VMTN ナレッジベース <http://kb.vmware.com>
- › ディスカッション フォーラム <http://www.vmware.com/community>
- › ユーザー グループ <http://www.vmware.com/vcommunity/usergroups.html>

VMware Technology Network の詳細については、<http://www.vmtn.net> をご覧ください。

## オンラインおよび電話によるサポート

テクニカル サポート リクエストの提出や、製品および契約情報の確認、製品の登録は、オンラインで行うことができます。詳しくは、<http://www.vmware.com/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。詳しくは、[http://www.vmware.com/support/phone\\_support.html](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を、<http://www.vmware.com/support/services> にてご確認ください。

## VMware エデュケーション サービス

当社が提供する有償トレーニングでは、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。詳しくは、VMware Web サイトにある VMware Education Services のページ (<http://mylearn1.vmware.com/mgreg/index.cfm>) をご覧ください。



# VDM クイックスタート ガイド

---

# 1

この章では、VDM 管理者ユーザー インターフェイスおよび基本的なインストール方法について説明します。また、基本的な構成を行って仮想デスクトップを作成するための一般的なガイドラインを説明し、基本的な管理タスクを紹介します。

VDM は VMware Virtual Desktop Infrastructure の一部であり、これによって企業では VMware ソフトウェアを使用して自社のデータセンターでデスクトップ仮想マシンをホストできます。また、ユーザーはリモート表示用のプロトコルを使用して、PC またはシンクライアントからアクセスできるようになります。VDM には、仮想デスクトップ環境をセットアップし、構成するためのソフトウェア ツールが用意されています。

この章では次のトピックについて説明します。

- › [ハードウェアの要件](#) (P.12)
- › [前提条件](#) (P.12)
- › [インストール前のチェックリスト](#) (P.13)
- › [デスクトップ仮想マシンの準備](#) (P.13)
- › [VDM Connection Server のインストール](#) (P.15)
- › [ワンタイム構成](#) (P.16)
- › [デスクトップの作成](#) (P.17)
- › [デスクトップへの接続](#) (P.20)

## ハードウェアの要件

VDM を実行するには、以下の仕様を満たす専用の物理サーバまたは仮想サーバが必要です。

- › Pentium IV 2.0GHz 以上のプロセッサ。デュアル プロセッサの使用をお勧めします。
- › 2GB 以上の RAM。50 台以上のデスクトップに展開する場合は、3GB の RAM をお勧めします。
- › 10/100Mbps 以上の NIC 一枚。1Gbps の NIC をお勧めします。

VDM Connection Server は 32 ビットと 64 ビットのいずれかのハードウェアにインストールできます。

DMZ での展開については、VDM は同様の仕様を満たす追加の専用ハードウェアまたはソフトウェアサーバを必要とします。

高可用性を備えた展開では、各 VDM Connection Server に同様の仕様を満たす専用物理サーバまたは仮想サーバが必要です。

## 前提条件

VDM Connection Server には以下の前提条件があります。

- › VMware Infrastructure  
ESX ホストと VirtualCenter インスタンスをそれぞれ 1 つ以上持つ VMware Infrastructure 3.5 (ESX Server と Virtual Center の現行バージョン) をお勧めします。VMware Infrastructure 3.02 がサポートされています。
- › Active Directory ドメインに参加している VDM Connection Server の標準インスタンスまたはレプリカ インスタンスを実行するサーバ

---

注意 VDM Connection Server では、Active Directory に対するスキーマまたは構成のアップデートが作成されることも、要求されることもありません。

---

- › VC Server にインストールされている Microsoft Sysprep ツール
- › クローンの仮想マシンの AD ドメインへの参加を許可するカスタマイズ仕様 (オプション)
- › VDM に有効なライセンス キー

VDM Agent、VDM Client、および VDM Web Access には、次の前提条件があります。

- › Windows ゲスト デスクトップと Windows クライアントについては、VDM Client と VDM Agent をインストールする管理権限が必要です。

- > VDM Web Access を使用してデスクトップにアクセスする Windows クライアントのユーザーには、ActiveX コントロールおよび Internet Explorer 6 以上が必要です。
- > Linux または Mac OS X を使用する Web Access では、Java JRE version 1.5.0 または 1.6.0 が必要です。
- > Microsoft Remote Desktop Connection 6.0 をお勧めします ( 必須ではありません ) 。  
 Microsoft Remote Desktop Connection ( RDC ) 6.0 を使用するには VDM Client マシンをアップグレードすることをお勧めします。この推奨は、Windows XP と Windows XPe を実行しているマシンが対象です。Windows 2000 は RDC 6.0 をサポートしていません。Windows Vista には RDC 6.0 があらかじめインストールされています。  
 RDC 6.0 は、Microsoft 社の Web サイトからダウンロードできます。
- > Linux クライアントを使用して Windows Vista デスクトップに接続する場合は、rdesktop リモート デスクトップ プロトコル クライアント バージョン 1.5.0 をインストールする必要があります。これは rdesktop の Web サイトからダウンロードできます。  
 rdesktop をダウンロードした後、readme ファイルの指示に従って操作してください。

## インストール前のチェックリスト

VDM をインストールする前に、次のチェックリストを確認してください。

- > コネクション サーバとして動作するマシンが Windows ドメインにあること。
- > コネクション サーバの FQDN に ping コマンドが通ること。
- > VDM の以前のバージョンがアンインストールされていること。

## デスクトップ仮想マシンの準備

VDM ソフトウェアをインストールする前に、使用するデスクトップ仮想マシンを準備してください。VirtualCenter の変更が必要な場合は、その各手順については最新の VirtualCenter のドキュメントを参照してください。

以下の前提条件を満たしていることを確認してください。

- > ユーザーに展開する基本デスクトップ仮想マシンを確定済みで、最新の OS とアプリケーションのサービスパックおよびパッチがインストールされている。  
 Windows XP デスクトップ仮想マシンについては、Microsoft KB の記事 323497 で指定されているパッチ ( VDM で必要 ) が適用されていることを確認してください。Microsoft KB の記事の詳細は、Microsoft 社の Web サイトでご覧になれます。

- › 最新の VMware Tools がインストールされている (VI 3.5 とともに提供)。
- › ネットワーク設定 (プロキシなど) がデスクトップ仮想マシンで適切に構成されている。
- › VDM Agent がインストールされている。

---

注意 大規模な環境で VDM Agent を自動的に更新する場合は、標準的な Windows 更新メカニズム (Altiris、SMS、LanDesk、BMC などのシステム管理システム) を使用することをお勧めします。

---

- › デスクトップ仮想マシンに対する管理者権限がある。

VDM Agent をインストールするには、次の手順に従ってください。

- 1 VDM インストーラ ファイルを VMware の安全な Web サイトからローカルドライブにダウンロードします。

安全な Web サイトの場所の詳細は、VMware の担当者にお問い合わせください。

- 2 VMware-vdmagent-2.1.0-<xxx>.exe を実行します。

<xxx> には、デスクトップ仮想マシンにインストールするソフトウェア コンポーネントのビルド番号を指定します。

インストールウィザードが開きます。

- 3 [次へ] をクリックします。
- 4 ライセンス条件に同意して、[次へ] をクリックします。
- 5 以下のようにカスタム セットアップのオプションを選択します。

- › 直接的な RDP 接続を制限するには、VDM Authentication GINA コンポーネントをインストールします。デフォルトでは、あらゆるソースからの仮想マシンへの RDP 接続が許可されています。VDM Authentication GINA がインストールされていると、接続が VDM Connection Server を経由して行われる場合のみ RDP 接続が許可されます。

GINA コンポーネントをインストールしてシングルサインオン (SSO) を有効にする必要があります。SSO が有効な場合、エンドユーザーはユーザー認証情報を一度入力するだけですみます。ユーザーがユーザー認証情報をコネクションサーバに入力すると、資格が付与されたデスクトップに自動的にログインすることになります。

- › 仮想デスクトップユーザーがローカルに接続されている USB デバイスに、自身の仮想デスクトップを使ってアクセスできるようにするには、USB リダイレクション コンポーネントをインストールします。

- 6 インストール先フォルダを受け入れるか、変更して、[次へ]をクリックします。
- 7 [インストール]をクリックしてインストールプロセスを開始します。
- 8 [完了]をクリックします。

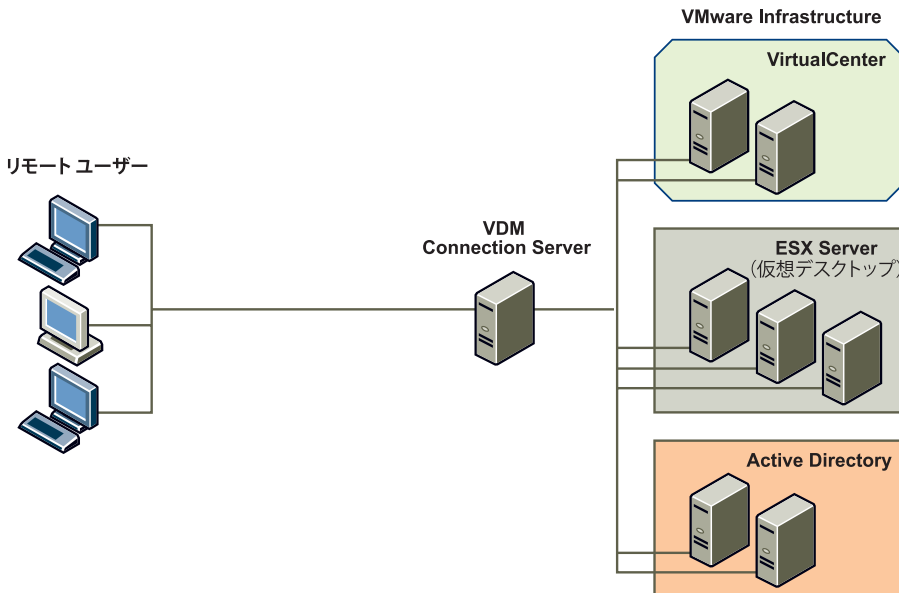
## VDM Connection Server のインストール

VDM Connection Server は Windows 2003 Server を実行している必要があります。コネクションブローカー専用の物理サーバまたはスタンドアロン仮想マシンのどちらかである必要があります。オプションで、そのサーバを使用するための SSL 証明書を手に入れることもできます。

### シングルサーバのインストール

最も基本的な展開方法は、シングルサーバでの展開です。図 1-1 は、クライアントデバイス、コネクションサーバ、Web ベースの管理、Active Directory、および VMware Virtual Infrastructure によるシングルサーバの展開を示したものです。

図 1-1 VDM シングルサーバの展開



シングル サーバのインストールを行うには、次の手順に従ってください。

- 1 コネクション サーバとして動作するマシン上で  
VMware-vdmconnectionserver-2.1.0-<xxx>.exe を実行します。  
  
<xxx> には、インストールするソフトウェア コンポーネントのビルド番号を指定します。  
  
インストール ウィザードが開きます。
- 2 [次へ] をクリックします。
- 3 VMware のライセンス条件に同意して、[次へ] をクリックします。
- 4 インストール先フォルダを受け入れるか、変更して、[次へ] をクリックします。
- 5 [標準] 展開オプションを選択します。
- 6 [次へ]-[インストール]-[完了] をクリックします。

「[VDM Connection Server のインストール](#) (P.34)」を参照してください。

## ワンタイム構成

ワンタイム構成を VDM Connection Server 上で実行して、これによって展開タスクを実行するようにセットアップしてください。

ワンタイム構成を行うには、次の手順に従ってください。

- 1 [https://<hostname\\_or\\_ipaddress>/admin](https://<hostname_or_ipaddress>/admin) にアクセスして VDM Administrator を起動します。  
  
<hostname\_or\_ipaddress> には、VDM Connection Server またはロード バランサのホスト名または IP アドレスを指定します。
- 2 該当する認証情報を使用してログインします。  
  
最初は、VDM Connection Server 上のローカル管理者グループのメンバーであるドメイン ユーザー全員が VDM 管理者ユーザー インターフェイスにログインできるようになっています。VDM 管理者のリストを後から変更するには、このインターフェイスを使用してください。  
  
最初にログインすると、[構成] ページが表示されます。ライセンス情報を入力すると、ログイン時には [インベントリ] ページが表示されるようになります。
- 3 ログイン時に [構成] ページが表示されていない場合は、[構成] ボタンをクリックすると、[構成] ページに切り替わります。

- 4 [構成] ページで、次の操作を実行します。
  - a [アクセスとセキュリティの設定] で、VMware VDM のライセンス キーを入力します。
  - b [VirtualCenter Servers] で、[追加] をクリックして VDM で使用する VirtualCenter の詳細をすべて入力します。

DNS 名または URL を使用してサーバを入力すると、そのサーバがその IP アドレスを使用して以前に入力されたことがあるかどうかを確認する DNS 検索は実行されません。VirtualCenter サーバがその DNS 名と IP アドレスの両方を使用して追加されると、競合が生じます。
  - c [管理者] の下の [追加] をクリックして、VDM Administrator へのログインアクセスを必要とする各 AD ユーザーの詳細をすべて入力します。
- 5 VDM Server のリストから VDM Connection Server を選択して [有効にする] を選択することで、VDM Connection Server を有効にします。

## デスクトップの作成

VDM コネクション サーバをインストールしたら、仮想デスクトップを作成し、これらの仮想デスクトップにアクセスする資格をユーザーに付与してください。

### 個別デスクトップの作成

エンドユーザーが VDM サービスにアクセスできるようにデスクトップを作成します。

個別デスクトップを作成するには、次の手順に従ってください。

- 1 [インベントリ] タブをクリックします。
- 2 [すべてのデスクトップ] で、[デスクトップ] タブをクリックして [追加] をクリックします。
- 3 [デスクトップの種類を選択] で、[個別デスクトップ] をクリックして、[次へ] をクリックします。
- 4 [デスクトップ ID] と [デスクトップ表示名] に入力します。

デスクトップ ID は、VDM がデスクトップを識別するために使用する名前です。デスクトップ表示名は、エンドユーザーがデスクトップにログインしたときに表示される名前です。デスクトップ ID は、デスクトップごとに一意である必要がありますが、表示名は一意にする必要はありません。デスクトップ ID と表示名は、お使いの環境と関連のあるものにしてください (部署名や場所など)。表示名を指定しないと、ユーザーにはデスクトップ ID が表示されます。

5 (オプション) デスクトップの説明を入力します。

説明にはスペースを含めて 1024 文字までの英数字を使用できます。この説明は、管理者のユーザー インターフェイスのみに表示され、エンド ユーザーには表示されません。

6 [次へ] をクリックします。

7 デスクトップのパラメータを次のように設定します。

▷ デスクトップの状態 [有効にする] を選択すると、デスクトップが作成された後、自動的に有効になります。[無効にする] に設定した場合、デスクトップを作成した後、これをアクティブにするには、手動で設定を [有効にする] に変更する必要があります。

▷ 仮想マシンの電源ポリシー エンド ユーザーまたは管理者によってシャットダウンされるまで、デスクトップをパワーオンのままにするには、[オンのまま] を選択します。この設定を選択している場合、デスクトップは手動で再びパワーオンにされるまではパワーオフのままとなります。エンド ユーザーまたは管理者がパワーオフにしようとした場合でも、デスクトップをパワーオンのままにしておく場合は、[常にパワーオン] を選択します。この設定を選択している場合、電源障害後にデスクトップは自動的にパワーオンとなります。ユーザーがログインしていない場合に、デスクトップをサスペンドするには、[使用していない場合にサスペンド] を選択します。使用していない場合にデスクトップをパワーオフするには、[使用していない場合にパワーオフ] を選択します。

電源ポリシーは、ユーザーがログオフまたは切断後に再接続すると、個別デスクトップに適用されます。

▷ 切断後に自動的にログオフ デスクトップユーザーが切断直後にログオフするには [直後] を選択し、ユーザーがログオフしないようにするには [ログオフしない] を選択します。または、[時間が経過した後] を選択して、ユーザーが切断後にログオフするまでの分数を入力します。

▷ ユーザーによるデスクトップのリセットを許可する デスクトップユーザーが管理者を通さずに自身のデスクトップをリセットできるようにするには、このチェックボックスをオンにします。リセットとは、デスクトップ仮想マシンがパワーオフし、再びパワーオンすることを意味します。この機能は、通常のデスクトップ上およびユーザーがアクティブなセッションを持つ読み取り専用のデスクトップ上で利用できます。

8 [次へ] をクリックします。

9 VirtualCenter サーバのリストから、デスクトップで使用する VirtualCenter サーバを選択して、[次へ] をクリックします。

- 10 [仮想マシンの選択] ページのテーブルで、デスクトップで使用する仮想マシンを選択します。

サポートされているゲスト OS を実行する仮想マシン、および別の仮想デスクトップが使用していない仮想マシンがすべて一覧表示されます。これには、中断されているものやパワーオン状態ではないものも含まれます。

- 11 [次へ] をクリックします。
- 12 [完了の確認] の情報を見直して、[完了] をクリックして受け入れるか、[戻る] をクリックして修正します。

- 13 [完了] をクリックします。

デスクトッププールの作成の詳細については、「[プールデスクトップの構成](#) (P.41)」を参照してください。

## デスクトップへの資格の付与

デスクトップのユーザーに、それぞれに割り当てられているデスクトップへの資格を付与することで、個別デスクトップまたはプールデスクトップへのアクセス権を付与してください。

AD ユーザーまたはグループにデスクトップへの資格を付与するには、次の手順に従ってください。

- 1 [インベントリ] タブの [すべてのデスクトップ] で、資格を与えるデスクトップを選択します。
- 2 [資格付与] をクリックします。
- 3 [追加] をクリックします。
- 4 [オブジェクトタイプの選択] で、[ユーザー]、[グループ]、またはその両方を選択します。
- 5 資格を付与するオブジェクトが常駐するドメインを選択するか、[ディレクトリ全体] を選択して、Active Directory ドメイン フォレスト全体を検索します。  
名前または説明で検索できます。
- 6 資格割り当てに追加するオブジェクトを選択します。
- 7 [OK] をクリックします。
- 8 [資格付与] で、[OK] をクリックします。

## デスクトップへの接続

VDM には、デスクトップ仮想マシンへの接続用として VDM Client または VDM Web Access が用意されています。クライアントマシンに対する管理者権限があることを確認してください。

VDM Client を使用してデスクトップに接続するには、次の手順に従ってください。

- 1 VMware-vdmclient-2.1.0-<xxx>.exe をダウンロードして実行します。  
  
<xxx> には、インストールするソフトウェアコンポーネントのビルド番号を指定します。  
  
インストールウィザードが開きます。
- 2 [次へ] をクリックします。
- 3 VMware のライセンス条件に同意して、[次へ] をクリックします。
- 4 カスタム セットアップで次のいずれかのオプションを選択します。
  - ▶ [次へ] をクリックしてデフォルトの設定を受け入れます。デフォルト設定では、クライアントおよび USB のリダイレクション機能がインストールされます。
  - ▶ [USB リダイレクト] を選択して、[この機能を使用できないようにします] を選択し、この機能をインストールしないようにします。この機能をインストールするには、ハードドライブ上の領域が必要です。そのため、インストールしないと、インストールに必要な領域が解放されます。
- 5 [次へ] をクリックして、デフォルトのインストール先のフォルダを受け入れます。別のインストール先を使用する場合は、[変更] をクリックして [次へ] をクリックします。
- 6 (オプション) クライアントの接続先のデフォルト サーバを入力して、[次へ] をクリックします。  
  
このエントリは、サーバの IP アドレスまたは FQDN です。
- 7 VDM クライアントのショートカットを設定します。ショートカットを使用しない場合は、すべての選択を選択解除します。
- 8 [次へ]-[インストール]-[完了] をクリックします。
- 9 VMware VDM Client を起動します。
- 10 [VDM Server] ドロップダウンメニューで、VDM Server のホスト名または IP アドレスを入力します。
- 11 [接続] をクリックします。

12 資格を付与されたユーザーの認証情報を入力し、ドメインを選択して [ ログイン ] をクリックします。

13 資格が付与されたデスクトップを選択して、[OK] をクリックします。

デスクトップ仮想マシンが接続されます。

VDM Web Access を使用してデスクトップに接続するには、次の手順に従ってください。

1 ブラウザを起動して、VDM Connection Server の URL に移動します。

たとえば、[https://<hostname\\_or\\_ipaddress>](https://<hostname_or_ipaddress>) に移動します。ここで <hostname\_or\_ipaddress> には、VDM Connection Server のホスト名または IP アドレスを指定します。

2 資格が付与されたユーザーの名前とパスワードを入力して、ドロップダウンメニューから正しいドメインを選択します。

3 [ ログイン ] をクリックします。

4 [ アクセスの状態 ] が [ 作動可能 ] のときは、リストからデスクトップを選択して [ 接続 ] をクリックします。

デスクトップが接続されます。



# 2

## VDM の概要とシステム要件

---

この章では、VDM とは何かについて説明し、VDM をインストールおよび実行するためのシステム要件について説明します。VDM は VMware Virtual Desktop Infrastructure 用のコネクション ブローカーです。VDM は VMware Virtual Infrastructure 上で実行している仮想デスクトップにユーザーを接続し、セキュリティ、アクセス制御、デスクトップ管理全体で重要な役割を果たします。

この章では次のトピックについて説明します。

- › [VDM の概要](#) (P.23)
- › [システム要件](#) (P.25)
- › [前提条件](#) (P.28)

### VDM の概要

VDM は Active Directory と VMware VirtualCenter を統合し、デスクトップを管理してエンドユーザーに展開します。また、Windows PC、シンクライアント、Linux デスクトップ、Macintosh コンピュータのいずれかを使用して仮想デスクトップに接続できるクライアントを提供します。VDM は仮想デスクトップを展開してアクセスするための安全な環境を提供し、VDM では既存の Active Directory の機能を使用して認証とユーザー グループの管理が実行されます。

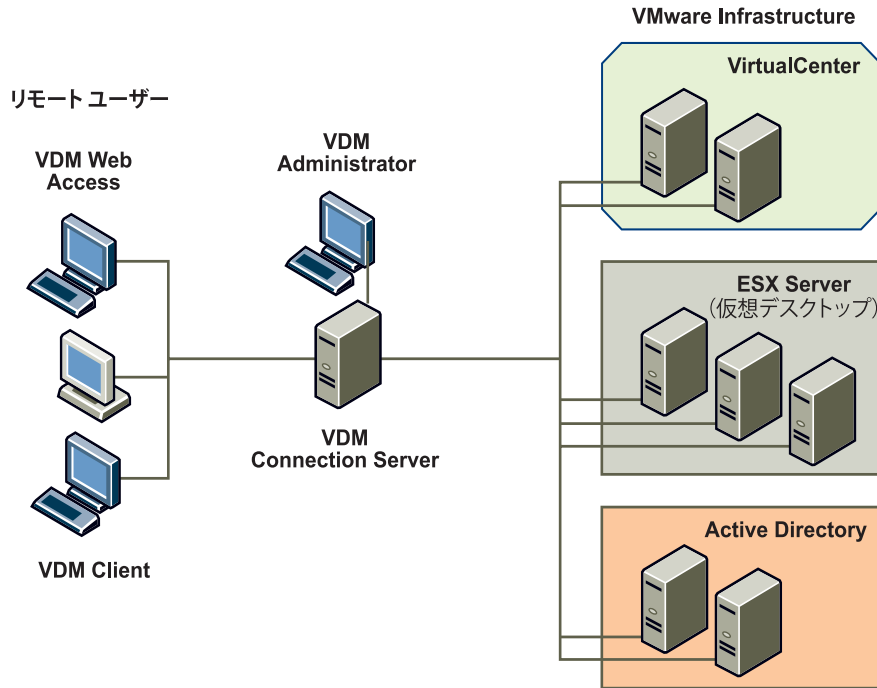
VDM のメイン コンポーネントは次のとおりです。

- › VDM Client 仮想デスクトップに接続するために VDM Connection Server に接続するユーザー側のコンポーネント。さまざまな機能を備えたネイティブ Windows アプリケーションです。
- › VDM Web Access 仮想デスクトップに接続するために VDM Connection Server に接続するユーザー側コンポーネント。VDM Web Access は、ユーザーの最初の接続時にクライアントを (Windows クライアント上に) インストールして、Web ブラウザを使用して仮想デスクトップに接続します。
- › VDM Administrator VDM の構成およびユーザーとデスクトップの管理を実行するプライマリ メカニズムである Web アプリケーション。
- › VDM Connection Server コネクション ブローカーとして機能するソフトウェアで、仮想マシンに対する管理とユーザー認証を提供します。VDM Connection Server は、受信したリモート デスクトップ ユーザーの要求を適切な仮想デスクトップにダイレクトして、ユーザー エクスペリエンスを向上させます。
- › VDM Agent デスクトップ仮想マシンにインストールするソフトウェアで、RDP 接続の監視、リモート USB のサポート、シングル サイン オンなどの機能を可能にします。VDM を実行するには、すべてのゲスト (デスクトップ仮想マシン) がこのエージェントをインストールしている必要があります。

VDM は、既存の AD インフラストラクチャを使用して認証とユーザー管理を実行します。また、VMware VirtualCenter と統合して VMware ESX サーバ上で実行している仮想デスクトップを管理します。

図 2-1 は、VDM 環境とそのメイン コンポーネントの高水準での概観を示したものです。これらのコンポーネントについては、本書で詳しく後述します。

図 2-1 VDM 環境の高水準での概観



## システム要件

以下のセクションでは、VDM コネクション サーバのハードウェア要件、VDM クライアントのサポート対象のシンクライアントデバイス、および VDM Connection Server、VDM Client、VDM Agent のサポート対象の OS について説明します。

### VDM Connection Server

VDM Connection Server には以下のハードウェアおよびソフトウェアの要件があります。

#### コネクション サーバのハードウェア要件

VDM Connection Server には以下のハードウェア要件があります。

- › VDM を実行するための以下の仕様を満たす専用の物理サーバまたは仮想サーバ。





## 前提条件

VDM Connection Server には以下の前提条件があります。

- › VMware Infrastructure  
ESX ホストと VirtualCenter インスタンスをそれぞれ 1 つ以上持つ VMware Infrastructure 3.5 ( ESX Server と Virtual Center の現行バージョン ) をお勧めします。VMware Infrastructure 3.02 がサポートされています。
- › Active Directory ドメインに参加している VDM Connection Server の標準インスタンスまたはレプリカ インスタンスを実行するサーバ

---

注意 VDM Connection Server では、Active Directory に対するスキーマまたは構成のアップデートが作成されることも、要求されることもありません。

---

- › VC Server にインストールされている Microsoft Sysprep ツール
- › クローンの仮想マシンの AD ドメインへの参加を許可するカスタマイズ仕様 ( オプション )
- › VDM に有効なライセンス キー

VDM Agent、VDM Client、および VDM Web Access には、次の前提条件があります。

- › Windows ゲスト デスクトップと Windows クライアントについては、VDM Client と VDM Agent をインストールする管理権限が必要です。
- › VDM Web Access を使用してデスクトップにアクセスする Windows クライアントのユーザーには、ActiveX コントロールおよび Internet Explorer 6 以上が必要です。
- › Linux または Mac OS X を使用する Web Access では、Java JRE version 1.5.0 または 1.6.0 が必要です。
- › Microsoft Remote Desktop Connection 6.0 をお勧めします ( 必須ではありません )

Microsoft Remote Desktop Connection ( RDC ) 6.0 を使用するために VDM Client マシンをアップグレードすることをお勧めします。この推奨は、Windows XP と Windows XPe を実行しているマシンが対象です。Windows 2000 は RDC 6.0 をサポートしていません。Windows Vista には RDC 6.0 があらかじめインストールされています。

RDC 6.0 は、以下の Web サイトからダウンロードできます。

<http://www.microsoft.com/downloads/details.aspx?FamilyId=26F11F0C-0D18-4306-ABCF-D4F18C8F5DF9&displaylang=en>

- › Linux クライアントを使用している Windows Vista デスクトップに接続する場合は、rdesktop リモート デスクトップ プロトコル クライアント バージョン 1.5.0 をインストールする必要があります。これは以下の URL からダウンロードできます。  
<http://www.rdesktop.org/>  
rdesktop をダウンロードした後、readme ファイルの指示に従って操作してください。
- › VDM Web Access では、USB リダイレクション機能を使用するために VDM Client をフルインストールする必要があります。
- › USB リダイレクションを使用する場合は、VDM Client をインストールする際に USB リダイレクション機能を必ずインストールするようにしてください。

## VDM のアップグレード

VDM ソフトウェアのアップグレードは、他のタイプのインストールと違いはありません。すべての VDM コンポーネントに同じバージョンがインストールされるように、VDM Connection Server をアップグレードするときには VDM Client と VDM Agent もアップグレードする必要があります。新しいバージョンのソフトウェアにアップグレードしても、既存の構成データは保持されます。



# VDM のインストールおよび 設定

# 3

VDM のインストールは、VDM ソフトウェア コンポーネントのインストールおよび VirtualCenter での準備をすることによって行います。本書では、VDM コンポーネントのインストール方法について詳しく説明しますが、管理者が VMware Virtual Infrastructure の管理に精通していることを前提としています。VMware では、VDM をエンドユーザーに展開する前に、管理者が End-to-End テストを行うことをお勧めします。

VDM をインストールする前に、「[第 2 章 VDM の概要とシステム要件](#) (P.23)」を参照してシステム要件とハードウェアおよびデバイスのサポートを確認してください。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準備](#) (P.32)
- › [VDM Connection Server のインストール](#) (P.34)
- › [ワンタイム構成](#) (P.37)
- › [End-to-End 構成](#) (P.39)
- › [VDM Administrator のユーザー インターフェイス](#) (P.54)
- › [デスクトップおよび資格のあるユーザーとグループの検索](#) (P.57)
- › [グローバル構成設定](#) (P.60)
- › [イベントの表示](#) (P.62)
- › [RSA SecurID](#) (P.62)
- › [VDM オブジェクトの削除](#) (P.63)
- › [SSL 証明書のインストール](#) (P.65)
- › [ロード バランシング](#) (P.68)

- › [DMZの展開](#) ( P.72 )
- › [DMZ 展開でのロード バランシング](#) ( P.74 )
- › [VDM 構成データのエクスポートおよびインポート](#) ( P.76 )

## デスクトップ仮想マシンの準備

VDM ソフトウェアをインストールする前に、使用するデスクトップ仮想マシンを準備してください。VirtualCenter の変更が必要な場合は、その各手順については最新の VirtualCenter のドキュメントを参照してください。

以下の前提条件を満たしていることを確認してください。

- › ユーザーに展開する基本デスクトップ仮想マシンを確定済みで、最新のオペレーティングシステムおよびアプリケーションのサービスパックとパッチがインストールされている。Windows XP デスクトップ仮想マシンについては、VDM で必要とされる以下の Microsoft パッチが適用されていることを確認してください。

<http://support.microsoft.com/kb/323497>

- › 最新の VMware Tools がインストールされている ( VI 3.5 とともに提供 )。
- › ネットワーク設定 ( プロキシなど ) がデスクトップ仮想マシンで適切に設定されている。
- › VMware VDM Agent がインストールされている。

---

注意 大規模な環境で VDM Agent を自動的に更新する場合は、標準的な Windows 更新メカニズム ( Altiris、SMS、LanDesk、BMC などのシステム管理システム ) を使用することをお勧めします。

---

- › デスクトップ仮想マシンに対する管理者権限がある。

VMware VDM Agent をインストールするには、次の手順に従ってください。

- 1 VDM インストーラ ファイルを VMware の安全な Web サイトからローカルドライブにダウンロードします。

安全な Web サイトの場所の詳細は、VMware の担当者にお問い合わせください。

- 2 VMware-vdmagent-2.1.0-<xxx>.exe を実行します。

<xxx> には、デスクトップ仮想マシンにインストールするソフトウェア コンポーネントのビルド番号を指定します。

VMware インストール ウィザードが開きます。

- 3 [次へ] をクリックします。
- 4 VMware のライセンス条件に同意して、[次へ] をクリックします。
- 5 カスタム セットアップのオプションを選択します。

直接的な RDP 接続を制限するには、VDM Authentication GINA コンポーネントをインストールします。デフォルトでは、あらゆるソースからの仮想マシンへの RDP 接続が許可されています。VDM Authentication GINA がインストールされていると、接続が VDM Connection Server を経由して行われる場合のみ RDP 接続が許可されます。また、VDM Authentication GINA をインストールすると、シングルサインオン (SSO) も有効になります。

仮想デスクトップユーザーがローカルに接続されている USB デバイスに、自身の仮想デスクトップを使ってアクセスする必要がある場合は、USB リダイレクション コンポーネントをインストールします。
- 6 インストール先フォルダを受け入れるか、変更して、[次へ] をクリックします。
- 7 [インストール] をクリックしてインストールプロセスを開始します。
- 8 [完了] をクリックします。

デスクトップ仮想マシンのテンプレートを作成するには、次の手順に従ってください。

- 1 VirtualCenter で、デスクトップ仮想マシンをテンプレートに変換します。

VDM でデスクトップ プールを使用するには、デスクトップ仮想マシン テンプレートを作成する必要があります。
- 2 (オプション) VirtualCenter で、ゲストのカスタマイズ仕様を作成します。

仕様に DHCP を使用してコンピュータ名を仮想マシン名に設定します。また、VDM シングルサインオン機能が必要な場合には、クローンの仮想マシンも AD ドメインに参加できる必要があります。
- 3 テストとして、テンプレートから仮想マシンを展開し、そのカスタマイズが正常に機能することを検証します。

AD ドメインの参加と認証が機能していることを確認してください。
- 4 フォルダが自動的に作成されていない場合は、[仮想マシンとテンプレート] インベントリ ビューでフォルダを作成します。

## 複数の NIC を使用する仮想マシン上での VDM Agent の使用

複数の仮想 NIC を使用するゲスト仮想マシンに関しては、VDM Agent が使用するサブネットを設定する必要があります。これによって、クライアント RDP 接続のために VDM Agent が VDM Server に提供するネットワーク アドレスが決まります。このサブネットを設定するには、VDM Agent がインストールされている仮想マシンに、以下の REG\_SZ レジストリ値を作成します。

```
HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m  
(REG_SZ)
```

レジストリ値では、n.n.n.n に TCP/IP サブネットを指定し、m にサブネットマスク内のビット数を指定します。

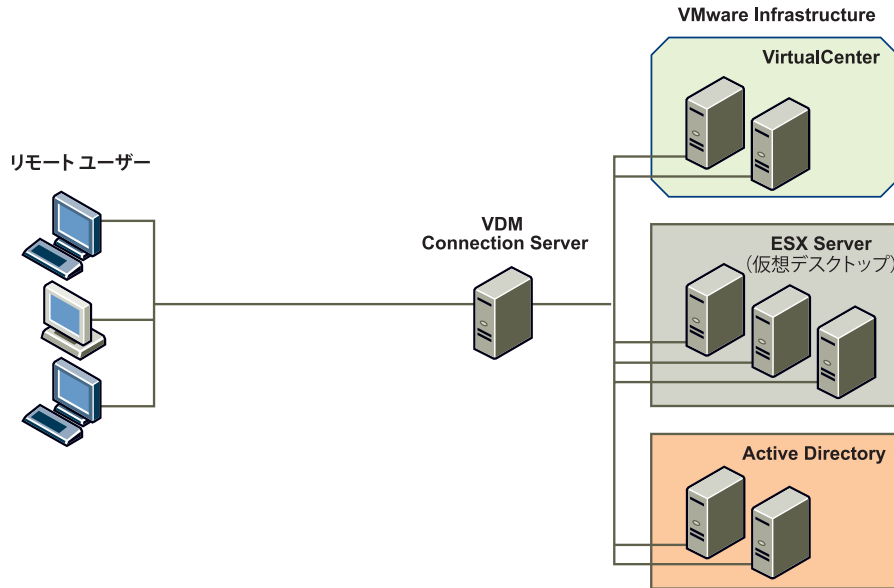
## VDM Connection Server のインストール

VDM Connection Server は、Windows 2003 Server 上で動作する必要があり、コネクション ブローカー専用の物理サーバまたは仮想サーバのいずれかに配置されている必要があります。コネクション サーバーには、その他の機能やロールを実行させないでください（たとえば、VirtualCenter サーバと同じサーバを指定しないでください）。コネクション サーバはドメインに参加する必要があります（ただし、サーバ自身はドメイン コントローラにはできません）。また、各コネクション サーバには固定 IP アドレスを割り当てることをお勧めします。コネクション サーバのインストールに使用されるドメイン ユーザー アカウントは、そのサーバ上での管理権限を持っている必要があります。また、コネクション サーバの管理者は、VirtualCenter の認証情報も知っておく必要があります。その VDM Connection Server に使用する SSL 証明書を手入することをお勧めします。SSL 証明書のインストールの詳細については、「[SSL 証明書のインストール](#) (P.65)」を参照してください。

## シングルサーバのインストール

最も基本的な展開のタイプは、シングルサーバの展開です。以下の図は、クライアント デバイス、コネクション サーバ、Web ベースの管理、Active Directory、および VMware Virtual Infrastructure を備えたシングルサーバの展開を示したものです。

図 3-1 VDM シングル サーバの展開



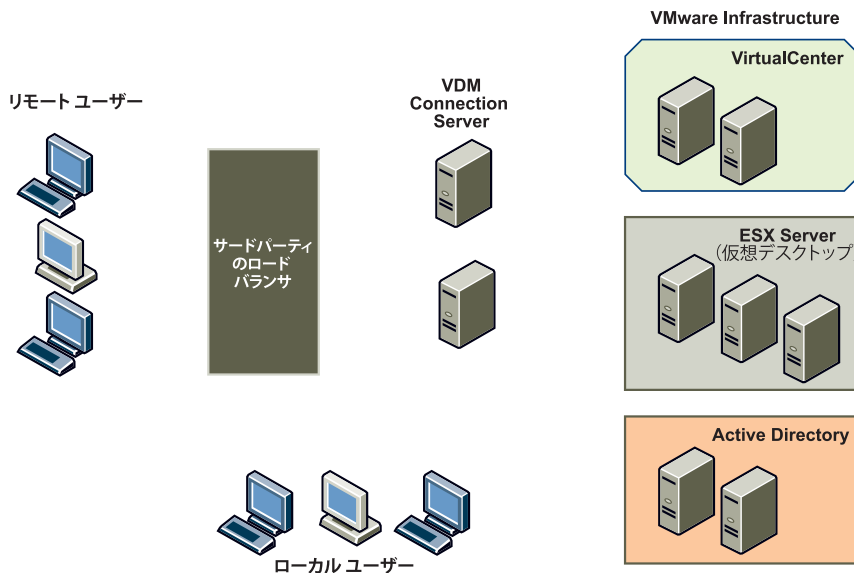
シングル サーバのインストールを行うには、次の手順に従ってください。

- 1 コネクション サーバとして機能するマシン上で  
VMware-vdmconnectionserver-2.1.0-<xxx>.exe を実行します。  
 <xxx> には、インストールするソフトウェア コンポーネントのビルド番号を指定します。  
 VMware インストール ウィザードが開きます。
- 2 [次へ] をクリックします。
- 3 VMware のライセンス条件に同意して、[次へ] をクリックします。
- 4 インストール先フォルダを受け入れるか、変更して、[次へ] をクリックします。
- 5 [標準] 展開オプションを選択します。
- 6 [次へ]-[インストール]-[完了] をクリックします。

## マルチサーバのインストール

VDM Connection Server は、高可用性とロード バランシングを実現するマルチサーバ構成で展開することもできます。以下の高水準構成図は、マルチサーバの展開、コネクションサーバ、ロード バランサ、Web ベースの管理、Active Directory、および VMware Virtual Infrastructure (仮想デスクトップをホスティングする ESX サーバを含む) を示しています。

図 3-2 VDM マルチサーバの展開



注意 マルチサーバのインストールでは、VDM Connection Server の 1 つのインスタンスが標準展開オプションを使用してインストールされていることを想定しています。マルチサーバのインストールは、2 番目以降のサーバで実行されます。詳細については、「[シングルサーバのインストール](#) (P.34)」を参照してください。

マルチサーバのインストールを行うには、次の手順に従ってください。

- 1 コネクションサーバとして機能するマシン上で  
`VMware-vdmconnectionserver-2.1.0-<xxx>.exe` を実行します。  
 <xxx> には、インストールするソフトウェア コンポーネントのビルド番号を指定します。  
 VMware インストール ウィザードが開きます。

- 2 [次へ] をクリックします。
- 3 VMware のライセンス条件に同意して、[次へ] をクリックします。
- 4 インストール先フォルダを受け入れるか、変更して、[次へ] をクリックします。
- 5 [レプリカ] 展開オプションを選択します。
- 6 複製する既存のコネクション サーバのホスト名または IP アドレスを入力します。
- 7 [次へ] をクリックします。
- 8 [インストール] をクリックします。
- 9 [完了] をクリックします。

## ワンタイム構成

ワンタイム構成を VDM Connection Server 上で実行して、これによって展開タスクを実行するようにセットアップしてください。

ワンタイム構成を行うには、次の手順に従ってください。

- 1 `https://<hostname_or_ipaddress>/admin` にアクセスして VDM Administrator を起動します。  
  
<hostname\_or\_ipaddress> には、VDM Connection Server またはロード バランサのホスト名または IP アドレスを指定します。
- 2 該当する認証情報を使用してログインします。  
  
最初に、VDM Connection Server 上のローカル管理者グループのメンバーであるドメイン ユーザーの全員が VDM 管理者ユーザー インターフェイスへのログインを許可されます。このインターフェイスを使用して、VDM 管理者のリストを後から変更することができます。  
  
最初にログインすると、[構成] ページが表示されます。ライセンス情報を入力すると、ログイン時に [インベントリ] ページが表示されます。
- 3 ログイン時に [構成] ページが表示されていない場合は、[構成] ボタンをクリックすると、[構成] ページに切り替わります。

- 4 [構成] ページで、次の操作を実行します。
  - a [アクセスとセキュリティの設定] で、VMware VDM のライセンス キーを入力します。
  - b [VirtualCenter Servers] で、[追加] をクリックして VDM で使用する VirtualCenter の詳細をすべて入力します。

DNS 名または URL を使用してサーバを入力すると、そのサーバがその IP アドレスを使用して以前に入力されたことがあるかどうかを確認する DNS 検索は実行されません。VirtualCenter サーバがその DNS 名と IP アドレスの両方を使用して追加されると、競合が生じます。
  - c VDM Administrator へのログイン アクセス権を持つ AD ユーザーに管理者権限を付与します。

## VDM Connection Server の有効化と無効化

ユーザーがログインできるように VDM Connection Server を有効にしてください。ユーザーのログインを防ぐには、VDM Connection Server を無効にします。VDM Connection Server を無効にした場合、その時点でログインしているユーザーへの影響はありません。VDM Connection Server の無効化は、なんらかの理由でサービス停止にする必要がある場合に便利です。VDM Connection Server を無効にすると、ログインしようとするエンドユーザーに対して、VDM Server Connection に障害があり、VDM Server は現在無効化されていることを示すメッセージが表示されます。

VDM Connection Server を有効にするには、次の手順に従ってください。

- 1 [構成] タブをクリックします。
- 2 VDM Server のリストから VDM Connection Server を選択して [有効にする] をクリックします。

VDM Connection Server を無効にするには、次の手順に従ってください。

- 1 [構成] タブをクリックします。
- 2 VDM Server のリストから VDM Connection Server を選択して [無効にする] を選択します。

VDM Connection Server を無効にしても、現在アクティブなデスクトップセッションには影響しません。また、新しいデスクトップセッションの確立が妨げられることもありません。

## End-to-End 構成

End-to-End 構成を新しいインストールで実行すると、インストールおよび構成の問題を簡単に解決できます。ここでは、個別デスクトップとプール デスクトップの両方について説明します。

個別デスクトップに対して構成を実行するには、次の手順に従ってください。

- 1 [インベントリ] タブをクリックします。
- 2 [すべてのデスクトップ] で、[デスクトップ] タブをクリックして [追加] をクリックします。
- 3 [デスクトップの種類を選択] で、[個別デスクトップ] をクリックして、[次へ] をクリックします。
- 4 [デスクトップ ID] と [デスクトップ表示名] に入力します。

デスクトップ ID は、VDM がデスクトップを識別するために使用する名前です。デスクトップ表示名は、エンド ユーザーがデスクトップにログインしたときに表示される名前です。デスクトップ ID は、デスクトップごとに一意である必要がありますが、表示名は一意にする必要はありません。デスクトップ ID と表示名は、お使いの環境と関連のあるものにしてください (部署名や場所など)。表示名を指定しないと、ユーザーにはデスクトップ ID が表示されます。

- 5 (オプション) デスクトップの説明を入力します。

説明には英数字を使用でき、スペースを含め 1024 文字まで入力できます。この説明は、管理者のユーザー インターフェイスのみに表示され、エンド ユーザーには表示されません。

- 6 [次へ] をクリックします。
- 7 デスクトップのパラメータを次のように設定します。
  - ▷ デスクトップの状態 [有効にする] を選択すると、デスクトップが作成された後、自動的に有効になります。[無効にする] に設定した場合、デスクトップを作成した後、これをアクティブにするには、手動で設定を [有効にする] に変更する必要があります。

- 仮想マシンの電源ポリシー エンドユーザーまたは管理者によってシャットダウンされるまで、デスクトップをパワーオンのままにするには、[オンのまま]を選択します。この設定を選択している場合、デスクトップは手動で再びパワーオンにされるまではパワーオフのままとなります。エンドユーザーまたは管理者がパワーオフにしようとした場合でも、デスクトップをパワーオンのままにしておく場合は、[常にパワーオン]を選択します。この設定を選択している場合、電源障害後にデスクトップは自動的にパワーオンとなります。ユーザーがログインしていない場合に、デスクトップをサスペンドするには、[使用していない場合にサスペンド]を選択します。使用していない場合にデスクトップをパワーオフするには、[使用していない場合にパワーオフ]を選択します。

電源ポリシーは、ユーザーがログオフまたは切断後に再接続すると、個別デスクトップに適用されます。

- 切断後に自動的にログオフ デスクトップユーザーが切断直後にログオフするには[直後]を選択し、ユーザーがログオフしないようにするには[ログオフしない]を選択します。または、[時間が経過した後]を選択して、ユーザーが切断後にログオフするまでの分数を入力します。
- ユーザーによるデスクトップのリセットを許可する デスクトップユーザーが管理者を通さずに自身のデスクトップをリセットできるようにするには、このチェックボックスをオンにします。リセットとは、デスクトップ仮想マシンがパワーオフし、再びパワーオンすることを意味します。この機能は、通常のデスクトップ上およびユーザーがアクティブなセッションを持つ読み取り専用のデスクトップ上で利用できます。

8 [次へ]をクリックします。

9 VirtualCenter サーバのリストから、デスクトップで使用する VirtualCenter サーバを選択して、[次へ]をクリックします。

10 [仮想マシンの選択] ページのテーブルで、デスクトップで使用する仮想マシンを選択します。

サポートされているゲスト OS を実行する仮想マシン、および別の仮想デスクトップが使用していない仮想マシンがすべて一覧表示されます。これには、中断されているものやパワーオン状態ではないものも含まれます。

11 [次へ]をクリックします。

12 [完了の確認] の情報を見直して、[完了] をクリックして受け入れるか、[戻る] をクリックして修正します。

13 [完了]をクリックします。

デスクトップが追加されたら、AD ユーザーまたはグループに対する資格を付与します。「[デスクトップへの資格の付与](#) (P.49)」を参照してください。

デスクトップ起動のテストの詳細は、「[デスクトップへの接続](#) (P.50)」を参照してください。

## プール デスクトップの構成

構成を新しいインストールで実行すると、インストールおよび構成の問題を簡単に解決できます。1つの仮想マシンをテンプレートから展開して、仮想マシンがこのテンプレートから展開できることを確認してください。

プール デスクトップを展開する前に、テンプレートとカスタマイズ仕様 (カスタマイズを使用している場合) を VirtualCenter に作成してください。手で仮想マシンを作成できること、およびそのカスタマイズ仕様を使用して仮想マシンをカスタマイズできることを確認してください。シングル サインオン (SSO) 機能を確保するために、カスタマイズ仕様では動的なアドレスの指定 (特に DHCP) を使用する必要があります。コンピュータ名は仮想マシン名に設定する必要があります。また、仮想マシンが自動的にドメインに加わるようにする必要があります。テンプレートとカスタマイズ仕様の作成の詳細は、最新の VirtualCenter のドキュメントを参照してください。

これらのテンプレートとカスタマイズ仕様のアイテムを完了したら、仮想マシンが正常にドメインに参加していることを確認してください。最後に、すべてのゲスト仮想マシン名が、プール デスクトップのテンプレートから展開されたものも含め、DNS に登録されます。動的に割り当てられた IP アドレスを使用しているため、AD 統合 DNS を使用して DHCP クライアントが仮想マシンを動的 DNS で登録できるようにしてください。

---

注意 プールをテストする前に、個別デスクトップをテストしてください。

---

### VDM に対する VirtualCenter の権限

VirtualCenter を VDM で使用するには、VirtualCenter 内で特定の操作を行う権限を VDM 管理者が持っている必要があります。これらの権限は、VirtualCenter ロールを作成して VDM 管理者に割り当てることで付与されます。プールが作成されるデータセンターまたはクラスタに対する管理者のロールを VDM 管理者に割り当てて、VDM 管理者が必要な変更をできるようにしてください。VDM 管理者がグローバルなカスタマイズ仕様を読み取ることができるロールを割り当ててください。これらの権限は、VDM が VirtualCenter と連動するために必要です。

VirtualCenter の VDM 管理者ロールを作成するには、次の手順に従ってください。

- 1 VirtualCenter で、[管理] ボタンをクリックします。
- 2 未選択の場合は、[ロール] タブをクリックして [ロールの追加] をクリックします。
- 3 ロールの名前を入力します (VDM 管理者など)。
- 4 [特権] リストで、[フォルダ] を展開して、[フォルダの作成] と [フォルダの削除] を選択します。
- 5 [仮想マシン] を展開して、次の手順を実行します。
  - a [インベントリ] を展開して [作成] を選択し、[削除] を選択します。
  - b [相互作用] を展開して [パワーオン]、[パワーオフ]、[サスペンド]、[リセット] の順にクリックします。
  - c [構成] を展開して [新しいディスクの追加]、[デバイスの追加または削除]、[デバイス設定の変更]、[詳細] の順に選択します。
  - d [プロビジョニング] を展開して、[カスタマイズ]、[テンプレートのデプロイ]、[カスタマイズ仕様の読み取り] の順に選択します。
- 6 [リソース] を展開して [仮想マシンのリソース プールへの割り当て] を選択します。
- 7 [OK] をクリックします。

新しいロールがロールのリストに表示されます。

管理者または VDM 管理者に VirtualCenter ロールを割り当てるには、次の手順に従ってください。

- 1 VirtualCenter で、データセンターまたはクラスタを選択します。
- 2 [権限] タブをクリックします。
- 3 [ユーザー / グループ] リストの下のページを任意場所で右クリックします。
- 4 [権限の追加] をクリックします。
- 5 [ユーザーおよびグループ] で、[追加] をクリックします。
- 6 [ドメイン] ドロップダウン メニューから管理者のドメインを選択します。
- 7 [ユーザーおよびグループ] で、リストから管理者を選択します。
- 8 [追加] と [OK] をクリックします。

- 9 [割り当てられたロール]で、ロールを選択します。

データセンターまたはクラスタに対するフル コントロールを与えるには、[システム管理者]を選択してください。管理者ロールは、VirtualCenter にあらかじめ設定されています。

作成した VDM Administrator ロールの、より制限されたアクセスと権限を与えるには [VDM Administrator] を選択してください。

- 10 [OK] をクリックします。

カスタマイズ仕様を読み取るための VirtualCenter ロールを作成するには、次の手順に従ってください。

- 1 VirtualCenter で、[管理] をクリックします。
- 2 [ロール] タブをクリックし、[ロールの追加] をクリックします。
- 3 ロールの名前を入力します (Read Only Customization Specifications など)。
- 4 権限のリストで、[仮想マシン] を選択します。
- 5 [プロビジョニング] を展開して、[カスタマイズ仕様の読み取り] を選択します。
- 6 [OK] をクリックします。

VDM に対する VirtualCenter ロールを割り当てるには、次の手順に従ってください。

- 1 VirtualCenter で、[インベントリ] ビューの [ホストおよびクラスタ] をクリックします。
- 2 [権限] タブをクリックします。
- 3 [ユーザー / グループ] リストの下のページを任意場所で右クリックします。
- 4 [権限の追加] をクリックします。
- 5 [ユーザーおよびグループ] で、[追加] をクリックします。
- 6 [ドメイン] ドロップダウン メニューから管理者のドメインを選択します。
- 7 [ユーザーおよびグループ] で、リストから管理者を選択します。
- 8 [追加] と [OK] をクリックします。
- 9 [割り当てられたロール] で、[グローバル読み取り専用カスタム仕様] を選択して、[OK] をクリックします。

---

注意 プールをテストする前に、個別デスクトップをテストしてください。

---

プールデスクトップに対する構成を実行するには、次の手順に従ってください。

- 1 [インベントリ] タブをクリックします。
- 2 [デスクトップ] で、[デスクトップ] タブをクリックして [追加] をクリックします。
- 3 [デスクトップの種類を選択] で、[デスクトップ プール- 通常] または [デスクトップ プール- 読み取り専用] を選択します。

通常のデスクトップ プールでは、ユーザーは毎回同じデスクトップにログインできます。同じデスクトップに戻るため、ユーザーは通常のデスクトップにドキュメントとファイルを保存できます。

読み取り専用のプールは、ユーザーのログイン時には使用できますが、ログオフ時には元のプールに戻ります。ユーザーは毎回別のデスクトップにログインするため、デスクトップにドキュメントやファイルを保存できません。

- 4 [次へ] をクリックします。
- 5 [デスクトップ ID] と [デスクトップ表示名] に入力します。

デスクトップ ID は、VDM がデスクトップ (この場合は、デスクトップ プール) を識別するために使用する名前です。ユーザーがデスクトップにログインすると、デスクトップ表示名が表示されます。デスクトップ ID は、デスクトップごとに一意である必要がありますが、表示名は一意にする必要はありません。デスクトップ ID と表示名は、お使いの環境に関連する固有のものにする必要はありません。表示名を指定しないと、ユーザーにはデスクトップ ID が表示されます。

- 6 (オプション) プールデスクトップの説明を入力します。

説明には英数字を使用でき、スペースを含め 1024 文字まで入力できます。この説明は、管理者のユーザー インターフェイスのみに表示され、エンドユーザーには表示されません。

- 7 [次へ] をクリックします。
- 8 デスクトップのパラメータを次のように設定します。

▷ デスクトップの状態 [有効にする] を選択すると、プールは作成後に自動的に有効になり、エンドユーザーはすぐに使用できます。[無効にする] に設定した場合、プールを作成した後、手動で設定を [有効にする] に変更してプールをアクティブにする必要があります。[無効にする] は、仮想マシンのアップグレードや、メンテナンス目的でデスクトップをオフラインにする場合に使用します。

- > プロビジョン [有効にする]に設定した場合、プールデスクトップの追加手順の完了後すぐに、プール用の仮想マシンが作成されます。[無効にする]に設定した場合、プールを作成した後、プール用の仮想マシンを作成するには、手動で設定を[有効にする]に変更する必要があります。
- > プールサイズ 任意の仮想デスクトップの数を設定します。
- > エラー時にプロビジョニングを停止する エラー検出時に仮想マシンのプロビジョニングを停止します。
- > 仮想マシンの電源ポリシー [オンのまま]を選択すると、仮想マシンは常にオンのままとなります。[常にパワーオン]を選択すると、割り当てられている仮想マシンはパワーオンのままとなります。[使用していない場合に中断]を選択すると、ユーザーがログインしていないときに、仮想マシンは中断されます。[使用していない場合にパワーオフ]を選択すると、仮想マシンは使用していないときにパワーオフに設定されます。

ユーザーがログオフまたは切断後に再接続すると、割り当てられている通常のプールデスクトップに電源ポリシーが適用されます。アイドル状態の通常および読み取り専用プールデスクトップの電源ポリシーは、ユーザーが次に再接続したときに適用されます。

- > 仮想マシン名のプリフィックス 仮想マシンをそのプールの一部として識別する各プールの値を設定します。このプール用に作成された仮想マシンは、このプリフィックスから始まる名前を持ちます。
- > 初めて使用した後、仮想マシンをパワーオフして削除する（読み取り専用プールのみ） ユーザーが最初の使用後にログアウトしたとき、仮想マシンを削除します。必要に応じて、新しい仮想マシンのクローンが作成され、仮想マシンが削除された後も特定のプールサイズが保持されます。
- > 切断後に自動的にログオフ デスクトップユーザーが切断直後にログオフされるようにするには[直後]を選択し、ユーザーがログオフしないようにするには[ログオフしない]を選択します。または、[時間が経過した後]を選択して、ユーザーが切断後にログオフするまでの分数を入力します。
- > ユーザーによるデスクトップのリセットを許可する デスクトップユーザーが管理者を通さずに自身のデスクトップをリセットできるようにするには、このチェックボックスをオンにします。
- > ユーザーごとに複数のセッションを許可する（読み取り専用プールのみ） デスクトップユーザーが各種クライアントデバイスからプール内の複数のデスクトップを同時に使用できるようにする場合は、このチェックボックスをオンにします。

9 [次へ]をクリックします。

- 10 VirtualCenter サーバのリストから、デスクトップで使用する VirtualCenter サーバを選択して、[次へ]をクリックします。

複数の VirtualCenter サーバが動作している環境では、別の VirtualCenter サーバが VirtualCenter 固有の ID を使用していないことを確認してください。デフォルトでは、ID 値はランダムに生成されますが、編集できます。VirtualCenter の固有 ID 値の編集の詳細については、最新の VirtualCenter のドキュメントを参照してください。

- 11 [テンプレートの選択]で、デスクトップ プール用の仮想マシンの展開元となるテンプレートを選択します。
- 12 仮想マシン フォルダの場所を選択します。

VDM では、デスクトップ ID と同じ名前のフォルダが作成され、新しく作成された仮想マシンはそのフォルダに置かれます。
- 13 このデスクトップが使用する仮想マシンを実行するホストまたはクラスタを選択し、[次へ]をクリックします。
- 14 このデスクトップが使用する仮想マシンを実行するリソース プールを選択し、[次へ]をクリックします。
- 15 仮想マシン ファイルを保存するデータストアを 1 つまたは複数選択し、[次へ]をクリックします。

選択するデータストアに、新しい仮想マシンを保存するのに十分な空き領域があることを確認してください。空き領域の量は、使用可能なデータストアのリストの下に表示されます。空き領域の量は、選択するデータストアごとに増加します。利用できる十分な空き領域がない場合は、別のデータストアを選択して空き領域を追加する必要があります。

- 16 このデスクトップで使用される仮想マシン用にゲスト OS をカスタマイズするカスタマイズ仕様を選択し、[次へ]をクリックします。
- 17 [完了の確認]の情報を見直して、[次へ]をクリックして受け入れるか、[戻る]をクリックして修正します。
- 18 [完了]をクリックします。

プールデスクトップが追加されたら、これに AD ユーザーまたはグループへの資格を付与します。「[デスクトップへの資格の付与](#) (P.49)」を参照してください。

デスクトップ起動のテストの詳細は、「[デスクトップへの接続](#) (P.50)」を参照してください。

## 高度なプール設定

高度なプール設定では、デフォルトのプール設定を上書きして、プールデスクトップを展開および管理する方法を決定できます。高度なプール設定は、デスクトップの追加ウィザードの[デスクトップの設定]で、通常のプールまたは読み取り専用のプールを作成する場合に選択できます。

デスクトップ設定を構成する際に、[詳細設定]を展開して、[高度なプール設定を有効にする]を選択すると、高度な設定にアクセスして有効にすることができます。高度なプール設定の主なオプションは次のとおりです。

- > **最小仮想マシン数** プールに使用できるデフォルトの最小仮想マシン数を上書きします。この数には、最初の展開時に、予測される仮想マシンの最小数を設定してください。
- > **最大仮想マシン数** プールに使用できるデフォルトの最大仮想マシン数を上書きします。この数は、任意の時点でプールに展開される仮想マシンの最大数に設定してください。この設定は、ハードウェアリソースへの過度の負担を避けるために必要です。
- > **使用可能な仮想マシンの数** プールに使用できるデフォルトの仮想マシン数を上書きします。この設定によって、すぐに使用できる仮想マシンの数が決まります。電源ポリシーによって指定されている場合、この制限を超える使用可能な仮想マシンは、必要に応じて中断またはパワーオフされます。読み取り専用のプールについては、この設定によって、仮想デスクトップへの新しいユーザーログインとしてプロビジョニング(追加)される仮想マシンの数が決まります。通常のプールについては、ユーザーが環境に追加される比率とこの設定が一致する必要があります(つまり、1日に2人のユーザーを追加する場合は、通常のプールに対してはこの数を2に設定してください)。

さらに、[構成]ページの高度なVirtualCenter設定を使用して、特定のVirtualCenter Serverを使用するデスクトップ用に、仮想マシンの動作を指定することができます。[構成]ページでは、現在のコンカレントプロビジョニング(デスクトップ仮想マシンの作成)の最大数、およびコンカレント電源操作の最大数を制御できます。

## 高度なプーリングシナリオ例

VDMのプーリングはフレキシブルで、さまざまな設定の組み合わせが可能です。次のシナリオ例では、いくつかの可能な設定の組み合わせを示し、VDMの動作方法を説明します。

### プーリング例1

プーリング例1の設定は次のとおりです。

- > **プールの種類** 読み取り専用

- › 最小仮想マシン数 100
- › 最大仮想マシン数 200
- › 使用可能な仮想マシン数 20
- › 仮想マシンの電源ポリシー 使用していない場合に中断

この例では、プールで最初に 100 台の仮想マシンのクローンが作成され、カスタマイズされます。仮想マシンが 20 台を超えると、使用可能な数（つまり電源が入り、使用可能な状態のもの）が 20 台を超えないように新しいクローン作成された仮想マシンはサスペンド状態になります。最小値と最大値がクローン作成のみに影響し、使用可能な仮想マシン数は影響しません。

ユーザーがログインすると、使用可能な仮想マシン数の設定によって、正しいレベルを保つためにより多くの仮想マシンに電源が投入されます。80 人目のユーザーがログインすると、設定によってクローンの作成が開始されます。ユーザーがログアウトすると、仮想マシンが（電源ポリシーに基づいて）中断され、使用可能な仮想マシンの数が制限されます。

#### プーリング例 2

プーリング例 2 の設定は次のとおりです。

- › プールの種類 通常
- › 最小仮想マシン数 100
- › 最大仮想マシン数 200
- › 使用可能な仮想マシン数 20
- › 仮想マシンの電源ポリシー 使用していない場合に中断

ユーザーがログオフした場合に仮想マシンが中断される点を除いては、例 1 と同じ動作です。使用された仮想マシンは、現在割り当てられているためプールに戻されません。

#### プーリング例 3

プーリング例 3 の設定は次のとおりです。

- › プールの種類 読み取り専用
- › 最小仮想マシン数 100
- › 最大仮想マシン数 200
- › 使用可能な仮想マシン数 20
- › 仮想マシンの電源ポリシー オンのまま

プールで最初に 100 台の仮想マシンのクローンが作成され、カスタマイズされます。これらの仮想マシンは動作し続けます。80 人目以降のユーザーがログインすると、使用可能な数に応じてクローン作成が再開され、容量が保持されます。

#### プーリング例 4

プーリング例 4 の設定は次のとおりです。

- › プールの種類 読み取り専用
- › 最小仮想マシン数 200
- › 最大仮想マシン数 200
- › 使用可能な仮想マシン数 20
- › 仮想マシンの電源ポリシー オンのまま

プールでは 200 台の仮想マシンのクローンが作成されます。それを超える仮想マシンのクローン作成は行われません。電源ポリシーは、仮想マシンがパワーオフされないことを意味します。

#### プーリング例 5

プーリング例 5 の設定は次のとおりです。

- › プールの種類 読み取り専用
- › 最小仮想マシン数 200
- › 最大仮想マシン数 200
- › 使用可能な仮想マシン数 20
- › 仮想マシンの電源ポリシー 使用していない場合に中断

プールでは 200 台の仮想マシンのクローンが作成されます。20 番目のクローンの作成後、プール管理者は仮想マシンの中断を開始して、使用可能な数である 20 を維持します。ユーザーがログインすると、仮想マシンが再開され、予備の数が維持されます。

## デスクトップへの資格の付与

個別デスクトップまたはプールデスクトップが追加された後、AD ユーザーまたはグループにそのデスクトップへの資格を付与します。

AD ユーザーまたはグループにデスクトップへの資格を付与するには、次の手順に従ってください。

- 1 [インベントリ] タブの [すべてのデスクトップ] で、資格を与えるデスクトップを選択します。
- 2 [資格付与] と [追加] をクリックします。
- 3 [オブジェクトタイプの選択] で、[ユーザー] または [グループ] をクリックします。
- 4 資格を付与するオブジェクトが常駐するドメインを選択するか、[ディレクトリ全体] を選択して、Active Directory ドメイン フォレスト全体を検索します。  
名前または説明で検索できます。
- 5 資格割り当てに追加するオブジェクトを選択します。  
複数のユーザーとグループに、デスクトップに対する資格を割り当てることができます。その場合、デスクトップは読み取り専用のプールと同じように動作します。読み取り専用のプールの詳細については、「[プール デスクトップの構成 \(P.41\)](#)」を参照してください。
- 6 [OK] をクリックします。
- 7 [資格付与] で、[OK] をクリックします。

## デスクトップへの接続

VDM には、デスクトップ仮想マシンへの接続用として VDM Client または VDM Web Access が用意されています。

---

**注意** クライアント マシンに対する管理者権限があることを確認してください。

---

VDM Client を使用してデスクトップに接続するには、次の手順に従ってください。

- 1 VMware-vdmclient-2.1.0-<xxx>.exe をダウンロードして実行します。  
<xxx> には、インストールするソフトウェア コンポーネントのビルド番号を指定します。  
インストールウィザードが開きます。
- 2 [次へ] をクリックします。
- 3 VMware のライセンス条件に同意して、[次へ] をクリックします。

- 4 カスタム セットアップで次のいずれかのオプションを選択します。
  - ▶ [次へ] をクリックしてデフォルトの設定を受け入れます。デフォルト設定では、クライアントおよび USB のリダイレクション機能がインストールされます。
  - ▶ [USB リダイレクト] を選択して、[この機能を使用できないようにします] を選択し、この機能をインストールしないようにします。この機能をインストールするには、ハードドライブ上の領域が必要です。そのため、インストールしないと、インストールに必要な領域が解放されます。
- 5 [次へ] をクリックして、デフォルトのインストール先のフォルダを受け入れます。別のインストール先を使用する場合は、[変更] をクリックして [次へ] をクリックします。
- 6 (オプション) クライアントの接続先のデフォルト サーバを入力して、[次へ] をクリックします。

このエントリは、サーバの IP アドレスまたは FQDN です。
- 7 VDM クライアントのショートカットを設定します。ショートカットを使用しない場合は、すべての選択を選択解除します。
- 8 [次へ]-[インストール]-[完了] をクリックします。
- 9 VMware VDM Client を起動します。
- 10 [VDM Server] ドロップダウン メニューで、VDM Server のホスト名または IP アドレスを入力します。
- 11 [接続] をクリックします。
- 12 資格を付与されたユーザーの認証情報を入力し、ドメインを選択して [ログイン] をクリックします。
- 13 資格が付与されたデスクトップを選択して、[OK] をクリックします。

デスクトップ仮想マシンが接続されます。

VDM Web Access を使用してデスクトップに接続するには、次の手順に従ってください。

- 1 ブラウザを起動して、VDM Connection Server の URL に移動します。

たとえば、[https://<hostname\\_or\\_ipaddress>](https://<hostname_or_ipaddress>) に移動します。ここで <hostname\_or\_ipaddress> には、VDM Connection Server のホスト名または IP アドレスを指定します。
- 2 資格が付与されたユーザーの名前とパスワードを入力して、ドロップダウン メニューから正しいドメインを選択します。
- 3 [ログイン] をクリックします。

- 4 [アクセスの状態]が[作動可能]のときは、リストからデスクトップを選択して[接続]をクリックします。

デスクトップが接続されます。

VDM Web Access を使用してデスクトップに接続するには、次の手順に従ってください。

- 1 ブラウザを起動して、VDM Connection Server の URL に移動します。  
例：https://<hostname or ipaddress> に移動します。ここで <hostname or ipaddress> には VDM Connection Server のホスト名または IP アドレスを指定します。
- 2 Windows クライアントを使用してログインしている場合、VDM Client は自動的にインストールされます。
- 3 資格が付与されたユーザーの名前とパスワードを入力して、ドロップダウンメニューから正しいドメインを選択します。
- 4 [ログイン]をクリックします。
- 5 [アクセスの状態]が[作動可能]のときは、リストからデスクトップを選択して[接続]をクリックします。  
デスクトップが接続されます。

## エンドユーザーのパスワードの変更

VDM は AD ドメインからのパスワードポリシーをサポートしています。パスワードが期限切れになるように AD グループポリシーが設定されている、または AD 管理者がユーザーにパスワードを変更するよう要求している場合、ユーザーが Client または Web Access を使用して VDM にログインすると、パスワードを変更するよう要求するメッセージが表示されます。ユーザーが入力するパスワードは、設定されている AD グループポリシーに準拠している必要があり、準拠しているかどうかチェックされます。

## デフォルト デスクトップのシンクライアントユーザー用の設定

VDM 管理者は、シンクライアントユーザーが VDM Connection Server の VDMAdmin.EXE コマンドラインコマンドを使用してログインするデフォルトのデスクトップを設定できます。このユーティリティは英語（米国）のシステムのみで使用できます。

シンクライアントユーザー用のデフォルト デスクトップを設定するには、次の手順に従ってください。

- 1 VDM Connection Server でコマンドプロンプトを開きます。

- 2 コマンドラインから、次のコマンドを実行します。

```
C:¥Program Files¥VMware¥VMware VDM¥Server¥bin¥vdmadmin -D -d
mydesktop -u <Domain>¥<Username>
```

コマンドを実行すると、LDAP にエントリが作成され、複数のデスクトップに対して資格を付与されているシンクライアントユーザーは、このコマンドを実行した後、デフォルトのデスクトップへのアクセス権だけを持つことになります。ユーザーはシンクライアントにログインした後でだけ、自身のデフォルトデスクトップを設定できます。

### Connection Server に外部的に解決可能な名前を設定

VDM クライアントが `https://<hostname>` (ここで `<hostname>` には VDM Connection Server のホスト名を指定) を使用して VDM Connection Server に直接アクセスできない場合、VDM Connection Server に対して外部的に解決可能な名前を指定する必要があります。VDM Connection Server にインターネットからアクセスする場合は、インターネット上で解決するものに名前を設定してください。たとえば、`https://vdmservername.mycompany.com` などをこの名前に設定できます。この状況が発生した場合は常に、解決できない VDM Connection Server ごとに名前を設定する必要があります。

名前を設定するプロセスは、すべてのインストールタイプで同じというわけではありません。標準インストールやレプリカインストールでは、Administrator のユーザー インターフェイスを使用して名前を設定できます。セキュリティ サーバのインストールでは、設定を含むファイルを編集または作成して、これをセキュリティサーバに保存する必要があります。

標準インストールまたはレプリカインストールで名前を設定するには、次の手順に従ってください。

- 1 [構成] ページの [VDM Servers] で、VDM Connection Server を選択します。
- 2 [編集] をクリックします。
- 3 [外部 URL] フィールドに名前を入力して [OK] をクリックします。
- 4 変更が反映されるように、VDM Connection Server のサービスを再起動します。
- 5 [スタート]-[管理ツール]-[サービス] をクリックして、サービスのリストから VMware VDM Connection Server を選択します。

サービスを実行している場合は、[サービスの再起動] をクリックします。サービスを実行していない場合は、[サービスの起動] をクリックします。

セキュリティ サーバインストールで名前を設定するには、次の手順に従ってください。

- 1 プロパティ ファイル ( `locked.properties` ) を、セキュリティ サーバ、ポート番号、クライアント プロトコルの外部的に解決可能な名前へのエントリを含むように作成、または編集します。

プロパティ ファイルはテキスト ファイルです。すでに存在する場合は、`C:\Program Files\VMware\VMware VDM\Server\sslgateway\conf\locked.properties` にあります。ファイルがすでに存在していてもなくても、常に同じ場所に保存してください。

たとえば、セキュリティ サーバの外部的に解決可能な名前が `vdmservname.mycompany.com` であり、ポート番号は 443、クライアント プロトコルが HTTPS である場合は、テキスト エディタを使用してプロパティ ファイルを次のエントリで編集または作成してください。

```
> clientHost=vdmservname.mycompany.com  
> clientPort=443  
> clientProtocol=https
```

これらのキーワードを持つエントリを含むプロパティ ファイルがすでに存在する場合は、そのエントリをこのリストの新しいエントリと置き換えてください。

- 2 ファイルを保存します。
- 3 変更が反映されるように、VDM Security Server のサービスを再起動します。
- 4 [ スタート ] - [ 管理ツール ] - [ サービス ] をクリックして、サービスのリストから VMware VDM Security Server を選択します。

サービスを実行している場合は、[ サービスの再起動 ] をクリックします。サービスを実行していない場合は、[ サービスの起動 ] をクリックします。

## VDM Administrator のユーザー インターフェイス

VDM Administrator のユーザー インターフェイスでは、VDM の構成、展開、および管理タスクのすべてを行います。[ インベントリ ]、[ 構成 ]、および [ イベント ] ボタンは常に管理者ユーザー インターフェイスの上部に表示されます。これらのボタンを使用すると、インターフェイスのその他の領域に移動して、管理タスクと構成タスクを行うことができます。ここでは、各ボタンによって表示されるページについて、およびこれらのページに関連付けられたオプションについて説明します。

管理者ユーザー インターフェイスのボタンをクリックして、開いたページ上のタブを選択すると、背景が白くなります。選択されていないタブの背景は紫になります。

## [ インベントリ ] ページ

[ インベントリ ] ページは、VDM Administrator のユーザー インターフェイスにログインすると開きます (ただし、初めてログインしたときには [ 構成 ] ページが開きます)。[ インベントリ ] ページでは、すべての仮想マシンにアクセスして、仮想デスクトップを展開し、これらのデスクトップを変更できます。[ 表示 ] ドロップダウンメニューを使用すると、[ デスクトップ ] ビューと [ 資格のあるユーザーとグループ ] ビューとを切り替えることができます。

[ インベントリ ] ページでは、デスクトップ、仮想マシン、およびアクティブなセッションに関する情報を検索してフィルタできます。また、複数のページが存在する場合はページ間をスクロールできます (各ページは 200 個のオブジェクトを含みます)。

- > [ デスクトップ ] ビュー [ デスクトップ ]、[ 仮想マシン ]、または [ アクティブなセッション ] タブから選択します。[ デスクトップ ] タブでは、デスクトップまたはデスクトッププールを追加、編集、資格付与、有効化、無効化、または削除できます。[ 仮想マシン ] タブでは、仮想マシンを表示して削除できます。[ アクティブなセッション ] タブでは、アクティブなセッションを表示、切断、または再起動できます。

各タブに関連付けられているテーブル内の情報はフィルタできます。また、[ デスクトップ ] ビューが選択されている場合は、フィルタして検索する列を選択することもできます。

- > [ デスクトップ ] タブ [ デスクトップ ID ] または [ タイプ ] 列をフィルタおよび検索します。
- > [ 仮想マシン ] タブ [ 仮想マシン名 ]、[ IP アドレス ]、[ ユーザー ]、または [ ステータス ] 列をフィルタおよび検索します。
- > [ アクティブなセッション ] タブ [ ユーザー ] または [ デスクトップ ] 列をフィルタおよび検索します。

[ デスクトップ ] ビューを表示している場合は、ページの左側にある [ インベントリ ] タブと [ 検索 ] タブから選択できます。

- > [ インベントリ ] すべてのデスクトップがこのタブ上のリストに表示されます。リストからデスクトップを選択すると、デスクトップに関する情報がページの右側に表示されます。ページの右側には [ 全般 ]、[ ユーザーとグループ ]、[ 仮想マシン ]、および [ アクティブなセッション ] タブも表示されます。

- ▶ [ 検索 ] [ デスクトップの検索 ] フィールドが表示されます。このフィールドに検索テキストを入力してデスクトップを検索します。検索条件を選択するには、[ これらのカテゴリ内で検索 ] チェック ボックスをオンにします。リストからデスクトップを選択すると、デスクトップに関する情報がページの右側に表示されます。さらに、ページの右側には [ 全般 ]、[ ユーザーとグループ ]、[ 仮想マシン ]、および [ アクティブなセッション ] タブも表示されます。

[ インベントリ ] ページでは、デスクトップの種類ごとに別々のアイコンが使用されています。個別デスクトップのアイコンは、青い正方形を1つ含む実線の枠線、通常のプールデスクトップのアイコンは、2つの青い正方形を含む実線の枠線、そして読み取り専用のプールデスクトップのアイコンは2つの青い正方形を含む破線の枠線でそれぞれ表示されます。

- ▶ [ 資格のあるユーザーとグループ ] ビュー

[ 資格のあるユーザーとグループ ] ビューでは、[ 資格のあるユーザーとグループ ] タブと [ アクティブなセッション ] タブから選択できます。ここでは、仮想デスクトップ、またはデスクトップのプールへの資格が付与されたユーザーとグループを表示でき、アクティブなセッションを切断できます。

各タブに関連付けられているテーブル内の情報はフィルタできます。また、[ 資格のあるユーザーとグループ ] ビューのタブが選択されている場合は、フィルタして検索する列を選択することもできます。

- ▶ [ 資格のあるユーザーとグループ ] タブでは、[ 表示名 ] 列または [ ドメイン ] 列をフィルタおよび検索するように選択できます。
- ▶ [ アクティブなセッション ] タブでは、[ ユーザー ] 列または [ デスクトップ ] 列をフィルタおよび検索するように選択できます。

[ 資格のあるユーザーとグループ ] ビューを表示している場合は、[ インベントリ ] ページの左側にある [ インベントリ ] タブと [ 検索 ] タブから選択できます。

- ▶ [ インベントリ ] タブを選択すると、資格が付与されたユーザーとグループがすべて [ インベントリ ] タブ上のリストに表示されます。リストからユーザーまたはグループを選択すると、ユーザーまたはグループに関する情報がページの右側に表示されます。さらに、ページの右側には [ 全般 ]、[ デスクトップ ]、および [ アクティブなセッション ] という3つのタブが表示されます。

[ 検索 ] タブを選択すると、[ デスクトップの検索 ] フィールドが表示されます。このフィールドに検索テキストを入力してユーザーまたはグループを検索します。[ これらのカテゴリ内で検索 ] チェック ボックスを使用して検索条件を選択してください。

## [構成] ページ

初めて (ライセンス情報を追加する前) VDM Administrator のユーザー インターフェイスにログインすると、[構成] ページが開きます。これは [構成] をクリックすると開くページと同じものです。[構成] ページは次のフィールドを含みます。

- › [アクセスとセキュリティの設定] ライセンスシリアル番号の情報を編集します。
- › [VirtualCenter Servers] 使用するコネクション サーバに対して VirtualCenter サーバを追加、編集、または削除します。
- › [VDM Servers] VDM サーバ (VDM Connection Servers) を有効または無効にし、VDM サーバ設定を編集し、RSA SecurID を有効にします。
- › [グローバル設定] デスクトップへの接続がクライアントから仮想マシンに直接確立されるように仮想デスクトップへの直接的な接続を有効にします。また、USB リダイレクションを有効にします。これによって仮想デスクトップ上のローカルに接続されている USB デバイスを使用できます。さらに、セキュリティサーバに SSL を設定し、クライアントと VDM Connection Server との間の通信に HTTP と HTTPS のいずれを使用するかを決定し、セッション タイムアウトを設定してタイムアウトとなるまでのセッションの全期間を決定します。
- › [管理者] コネクション サーバに対して管理者を追加または削除し、Active Directory でユーザーまたはグループを検索し、これらを管理者として追加します。

## [イベント] ページ

個々のコネクション サーバが生成するイベントを表示するには、[イベント] ページを使用します。[含む] フィールドにテキストを入力し、メッセージの種類、メッセージの時間、またはメッセージ テキストそのもので検索できます。また、メッセージを表示する日数も決定できます。

## デスクトップおよび資格のあるユーザーとグループの検索

デスクトップおよび資格のあるユーザーとグループに関する情報を検索するには、[インベントリ] ページを使用します。ページの右側に表示されているテーブル内の列と、ページの左側に表示されているカテゴリのいずれかを使用して検索できます。

[デスクトップ] インベントリ ビューで列を検索するには、次の手順に従ってください。

- 1 [インベントリ] ページの [表示] メニューから [デスクトップ] を選択します。
- 2 [デスクトップ] フィールド ( ページの右側 ) で、[デスクトップ]、[仮想マシン]、または [アクティブなセッション] タブをクリックします。
- 3 [含む] の後の矢印をクリックして、該当する列のチェックボックスをオンにします。
- 4 [完了] をクリックします。
- 5 検索テキストを入力して [実行] をクリックします。

[デスクトップ] 検索ビューでカテゴリを検索するには、次の手順に従ってください。

- 1 [インベントリ] ページの [表示] メニューから [デスクトップ] を選択します。
- 2 [デスクトップの検索] フィールド ( ページの左側 ) に、検索テキストを入力します。
- 3 [これらのカテゴリ内で検索] フィールドで、検索するカテゴリを [表示名]、[デスクトップ ID]、[タイプ]、[ユーザー]、[Virtual Center 名] から選択します。
- 4 [検索] をクリックします。

[資格のあるユーザーとグループ] インベントリ ビューで列を検索するには、次の手順に従ってください。

- 1 [インベントリ] ページの [表示] メニューから [資格のあるユーザーとグループ] を選択します。
- 2 [資格のあるユーザーとグループ] フィールド ( ページの右側 ) で、[資格のあるユーザーとグループ] または [アクティブなセッション] タブをクリックします。
- 3 [含む] の後の矢印をクリックして、該当する列のチェックボックスをオンにします。
- 4 [完了] をクリックします。
- 5 検索テキストを入力して [実行] をクリックします。

[資格のあるユーザーとグループ] 検索ビューでカテゴリを検索するには、次の手順に従ってください。

- 1 [インベントリ] ページの [表示] メニューから [資格のあるユーザーとグループ] を選択します。
- 2 [ユーザーの検索] フィールド ( ページの左側 ) に、検索テキストを入力します。
- 3 [これらのカテゴリ内で検索] フィールドで、検索するカテゴリを [ 共通名 ]、[ 名前 ]、[ 説明 ]、[ ユーザー ]、[ 電子メール ]、[ 表示名 ]、[ ドメイン名 ] から選択します。
- 4 [ 検索 ] をクリックします。

## アクティブなセッションの操作

仮想デスクトップまたはデスクトップ プールに接続すると、アクティブなセッションはインベントリに存在します。アクティブなセッションには、[インベントリ] ページでアクセスできます。

アクティブなセッションを表示、切断、または再起動するには、次の手順に従ってください。

- 1 [インベントリ] タブをクリックします。
- 2 [デスクトップ] で、[アクティブなセッション] をクリックします。  
アクティブなセッションごとにユーザー、デスクトップ ID、VM の DNS 名、開始時間、期間、およびサーバの状態 ( 接続または切断 ) を表示できます。
- 3 アクティブなセッションの任意の場所をクリックします。  
[セッションの切断] オプションと [仮想マシンの再起動] オプションが有効になります。
- 4 [セッションの切断] をクリックして選択したアクティブ セッションを切断するか、[仮想マシンの再起動] をクリックしてアクティブなセッションを再起動します。

## グローバル構成設定

特定の要件に応じて VDM の動作を設定するには、グローバル構成設定を使用します。  
表 3-1 はグローバル構成設定の一覧です。

表 3-1. グローバル構成設定

オプション	説明
セッション タイムアウト (分)	ユーザーがコネクション サーバにログインしたときから数えたセッション全体の時間制限。セッションが終了するまでにユーザーがログインしていることができる合計時間です。
仮想デスクトップに直接接続	<p>このオプションを選択すると、リモートデスクトップセッションは VDM Connection Server をバイパスして (つまり、トンネリングされた接続を使用せず) VDM Client とデスクトップ仮想マシンとの間に直接確立されます。</p> <p>ただし、初回の接続に関しては VDM Connection Server に対して実行されます。これはユーザーがそれぞれ資格を持つ適切なデスクトップを認証および選択するために必要です。</p> <p>クライアントとデスクトップ仮想マシンとの間の接続では RDP トラフィックが暗号化されずに送信されるため、このオプションは企業ネットワーク内の展開のみに適しています。</p> <p>この設定はデフォルトで無効になっています。</p> <p>この設定への変更は、各ユーザーが次にログインするときに反映されます。</p>
USB リダイレクション	<p>このオプションを選択すると、ネイティブクライアントは、アクティブ時にすべての USB 機能を無効にします。</p> <p>この設定への変更は、各ユーザーが次にデスクトップを起動するときに反映されます。</p>
クライアント接続に SSL を要求する	<p>[クライアント接続に SSL を要求する] を選択すると、クライアントと VDM Connection Server との間の通信プロトコルとして HTTPS が使用されます。HTTP を使用して接続しようとするクライアントは、自動的に HTTPS にリダイレクトされます。</p> <p>この設定を変更した場合、VDM Connection Server を再起動して設定を有効にする必要があります。</p>

表 3-1. グローバル構成設定 ( 続き )

オプション	説明
ネットワークへの割り込み後の再認証	<p>このオプションを選択すると、ネットワークへの割り込み後に、ユーザーの認証情報を再認証する必要があるかどうかが決まります。選択した場合、ユーザーは認証情報を再入力する必要があり、Active Directory に対して再認証されます。この設定は、仮想デスクトップ設定への直接接続が選択されている場合は使用できません。</p> <p>この設定を有効にした場合、クライアントは終了し、ユーザーは VDM Connection Server にもう一度ログインする必要があります ( セッションは切断された状態のままとなります )。</p> <p>入力を有効にするには、VMware VDM Connection Server を再起動する必要があります。</p>
ログイン前メッセージ	<p>このオプションを選択すると、Client と Web Access のユーザーには、管理者が入力した情報または指示を含む、免責事項またはログイン メッセージが表示されます。</p>

グローバル設定を構成するには、次の手順に従ってください。

1 [ 構成 ] タブの [ グローバル設定 ] で、[ 編集 ] をクリックします。

2 セッションのタイムアウトを設定します。

ユーザーがコネクション サーバにログインした後、セッションを開いておくことができる時間を決定し、この値を分単位で入力してください。[ セッション タイムアウト ] フィールドに値を指定する必要があります。

3 オプションのグローバル設定を設定します。

- › クライアントから仮想マシンへの直接的な接続を有効にするには、[ 仮想デスクトップに直接接続 ] を選択します。
- › ネイティブクライアントがすべての USB 機能を無効にするように指定する場合は、[ USB リダイレクト ] を選択します。
- › クライアントとコネクション サーバとの間の通信プロトコルとして HTTPS を有効にする場合は、[ クライアント接続に SSL を要求する ] を選択します。

HTTP を有効にするには、このチェック ボックスをオフにしてください。

- ネットワークの割り込み後に、仮想デスクトップのユーザーにそれぞれの Active Directory 認証情報を再入力させるには、[インターネットへの割り込み後の再認証]を選択します。
- Web Access または Client のユーザーがログインしたときに表示されるメッセージを管理者が設定する必要がある場合は、[ログイン時にユーザーにログイン前メッセージを表示する]を選択します。

このチェック ボックスをオンにした後、テキスト フィールドにメッセージを入力してください。

- 4 [OK] をクリックします。

## イベントの表示

VDM には、個々のコネクション サーバのイベントを表示するページが用意されています。[イベント] ページの情報を利用して、サーバ上の問題を診断したり、アクティビティを表示したりできます。

イベントを表示するには、次の手順に従ってください。

[イベント] タブをクリックします。

[イベント] ページが開き、表示されるイベントのサーバ名が一覧表示されます。

イベントを検索するには、次の手順に従ってください。

- 1 [含む] の後の矢印をクリックし、検索する列を選択します ([メッセージ]、[時間]、[タイプ])。
- 2 リストから、[イベント] テーブルにメッセージを表示する日数を選択します。
- 3 [完了] をクリックします。
- 4 テキスト ボックスに検索テキストを入力します。
- 5 [実行] をクリックします。

検索結果が [イベント] テーブルに表示されます。イベントの詳細を表示するには、各メッセージの最後の [ < 詳細 ] をクリックします。

## RSA SecurID

VDM では、追加のユーザー認証方法として RSA SecurID をサポートしています。RSA SecurID は、AD 認証情報を使用するときに提供される認証に加えて、仮想デスクトップへのアクセス時に、強力な 2 要素認証を提供します。

RSA SecurID を使用する場合は、まず VDM サーバ設定を編集してこれを有効にする必要があります。VDM サーバに RSA SecurID ソフトウェアをインストールした後、VDM 管理者のユーザー インターフェイスで RSA 設定を編集できます。

RSA SecurID を有効または編集するには、次の手順に従ってください。

- 1 [構成] タブをクリックします。
- 2 [VDM Servers] で、[編集] をクリックします。
- 3 [RSA SecurID] ダイアログ ボックスで、目的の RSA 設定を構成します。
  - › [有効にする] を選択すると、仮想デスクトップにアクセスするエンド ユーザーに対する RSA SecurID 認証が有効になります。
  - › [SecurID と Windows ユーザー名の一致を強制] を選択すると、SecurID によって名前が Windows ユーザー名と照合され、一致しない名前へのアクセスは拒否されます。
  - › [ノードの秘密をクリアする] は VDM Agent 上のノードの秘密のことです。  
この設定の詳細は、RSA Authentication Manager のユーザー マニュアルを参照してください。
- 4 [RSA 認証エージェントの設定ファイル (sdconf.rec) をアップロードする] フィールドで、sdconf.rec ファイルの場所を入力するか、[参照] をクリックしてファイルを検索します。  
  
sdconf.rec ファイルの詳細は、RSA Authentication Manager のユーザー マニュアルを参照してください。
- 5 [OK] をクリックします。

## VDM オブジェクトの削除

VDM オブジェクト (VirtualCenter、VDM サーバ、およびデスクトップ) は、管理者ユーザー インターフェイスを使用して削除してください。

VDM サーバから VirtualCenter サーバを削除するには、次の手順に従ってください。

- 1 [構成] タブをクリックします。
- 2 [VirtualCenter Servers] で、[削除] をクリックします。  
  
デスクトップでこの VirtualCenter サーバが使用されている場合、VirtualCenter を削除する前に、まずはこの VirtualCenter を使用しているデスクトップを削除する必要があることを知らせるエラー メッセージが表示されます。

デスクトップでこの VirtualCenter サーバが使用されていない場合は、この仮想センターで管理されている仮想マシンにはアクセスできなくなっていることを知らせる警告メッセージが表示されます。

- 3 [OK] をクリックします。

VirtualCenter サーバが削除されます。

VDM サーバからデスクトップを削除するには、次の手順に従ってください。

- 1 [インベントリ] タブをクリックします。
- 2 [すべてのデスクトップ] で、[デスクトップ] タブをクリックします。
- 3 削除するデスクトップを選択して、[削除] をクリックします。

コネクション ブローカーのみから、仮想マシンを削除するオプションも選択できます。この場合、仮想マシンは引き続き VirtualCenter に表示されます。ディスクから削除することを選択した場合、仮想マシンは VirtualCenter で表示されなくなります。

デスクトップにアクティブなセッションが存在する場合、ユーザーの切断を選択することもできます。この場合、ユーザーは接続しているデスクトップを失います。ユーザーを接続したままにすることを選択した場合、ユーザーは接続しているデスクトップを失わないこととなります。

VDM デスクトップから仮想マシンを削除するには、次の手順に従ってください。

- 1 [インベントリ] タブをクリックします。
- 2 [すべてのデスクトップ] で、削除する仮想マシンを含むデスクトップを選択します。
- 3 [仮想マシン] タブをクリックします。
- 4 [削除] をクリックします。

コネクション ブローカーのみから、仮想マシンを削除するオプションも選択できます。この場合、仮想マシンは引き続き VirtualCenter に表示されます。ディスクから削除することを選択した場合、仮想マシンは VirtualCenter で表示されなくなり、データストアから削除されます。

デスクトップにアクティブなセッションが存在する場合、ユーザーの切断を選択することもできます (コネクション ブローカーからの削除を選択している場合)。この場合、ユーザーは接続しているデスクトップを失います。ユーザーを接続したままにすることを選択した場合、ユーザーは接続しているデスクトップを失わないこととなります。

## SSL 証明書のインストール

VDM Connection Server には、最初の接続で使用できる自己署名入り SSL 証明書が含まれています。この証明書は、クライアントから信頼されず、サービスに対して正しい名前を持ちませんが、接続が可能になります。

これらの初期証明書は、そのサービス用に適切に構築された証明書と置き換えてください。これによって、ユーザーに表示される証明書確認メッセージが削除され、シングルクライアント デバイスが接続できるようになります。

証明書をインストールするには、次の高水準の手順に従ってください。

- 1 適切な証明書の署名要求 (CSR) を作成します。
- 2 要求を証明機関 (CA) に送信し、新しい証明書を受け取ります。
- 3 その証明書を VDM Connection Server のキーストアにインポートします。
- 4 この新しい証明書を使用するように VDM Connection Server を構成します。

### CSR の作成

CSR にバインドする名前を決定することは、重要な考慮事項です。証明書はサービス名を暗号化キー ペアにバインドし、これによってサービスとキーの所有権があると見なされます。所有権を主張する組織によってそのキーが要求されたことを CA が独自に判断したため、クライアントはそのサーバ (およびその暗号化キー) を信頼できません。

CSR の最も重要な部分は、共通名 (CN) 属性です。クライアント コンピュータが使用する名前を使用して VDM Connection Server に接続してください。通常、シングルサーバ環境では、この名前はサーバ名です。ロードバランシングが使用されている場合は、ロードバランスされた名前を使用してください。

CSR を作成するには、次の手順に従ってください。

- 1 Windows のコマンド プロンプトを使用して、キー ペア (公開キーと秘密キー) を含む新しいキーストアを作成します。

```
%JAVA_HOME%\bin\keytool -genkey -keyalg "RSA" -keystore keys.p12
-storetype pkcs12 -storepass <secret> -validity 360
```

- 2 以下の質問に答えます。

▷ 氏名は何ですか。

これは CN 属性です。たとえば、server.vmware.com のようなサーバ名またはロードバランスされた名前を入力してください。

- 2. 組織単位の名称は何ですか。  
これは、このサーバが展開される組織に関する情報です。CAはこのフィールドへの入力に要件を設定している場合があります。たとえば、会社のドメイン名 (vmware.com など) が要求される場合があります。
- 3. 組織の名称は何ですか。  
これには部署名または会社名を指定します。
- 4. 市町村名または地域名は何ですか。  
所在地を入力するか、空白のまま (不明) にしておいてください。
- 5. 州名または都道府県名は何ですか。  
州や都道府県の情報を入力するか、空白のまま (不明) にしておいてください。
- 6. この組織単位の2桁の国コードは何ですか。  
国コードを入力してください (GB など)。

3 フルネームを確認し、「Yes」と入力して、< Enter > キーを押します。

現在のディレクトリに keys.p12 ファイルが作成されます。

4 次のキーペアを使用して CSR を作成します。

```
%JAVA_HOME%\bin\keytool -certreq -keyalg "RSA" -file certificate.csr  
-keystore keys.p12 -storetype pkcs12 -storepass secret
```

certificate.csr ファイルが同じ場所に作成されます。ファイルの内容は、次の例のようになります。

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIBuDCCASECAQAwDELMAkGA1UEBhMCR0IxEDA0BgNV  
BAAgTB1Vua25vd24xEDA0BgNVBACjTB1Vua25vd24x  
FDASBgNVBAoTC1ZNd2FyZSBjb250bWwEQYDVQQL  
Ewp2bXdhcmUuY29tMR0wGAYDVQQDExFzZXJ2ZXIu  
dm13YXJlLmNvYmTCBnzANBjkqhkig9w0BAQEFAA  
OBjQAwYkCgYEA85iM2G4J695Nh3Lfu0S7eAdXHG51  
MtRcfr397jj0sjFk2TH0T8Xkeue6pCAG0E9vs  
RSKiFZiMQL0TSkg0Vwd+bYDMzMXUam/baSq7z7  
JF8irTHXYB/1PXDwdykUI7jYSRVxhjbHmXU8/2  
jEUL5DocLDLnygsUD2g7cUMYdz/HeECAwEAAaAA  
MA0GCSqGSIb3DQEBAQUAA4GBALq2e5FWHQIE26J  
01IdRFLQqlsu78IsuGF19nvJSxrdnHFUpUvTaT  
a3auGsz+UJG/vdHqFt49oSrIhd7NALLumBo0q4t  
EywvE3vq0ytUvIEimJCKsAiAeyWZUydJps+zhV  
KKhiscgFh60AZp1bmTJguAeHnsPs7a1Q0JH6  
0ZvdU-----END NEW CERTIFICATE REQUEST-----
```

- 5 (オプション)ある時点で、サーバ構成の再構築が必要となった場合は、証明書がインポートされた後で、keys.p12 ファイルのバックアップを作成してください。

CSRを送信して証明書をインポートするには、次の手順に従ってください。

- 1 CAに問い合わせ、「CSRを作成するには、次の手順に従ってください。(P.65)」で生成された関連情報とCSRのコピーを提供します。
- 2 証明書をPKCS#7形式で要求します。

無償のCA (<https://www.thawte.com/cgi/server/try.exe>) がテスト用としてThawte社から提供されています。このCAは信頼されていないルートに基づいて21日間のSSL証明書を生成します。正しい名前を使うことになるため、VDMから提供される最初の証明書よりもわずかですが優れています。ただし、クライアントはこのサービスが信頼されていないことを伝える警告を発行します。

- 3 生成されたファイルのコンテンツをテキストエディタにコピーし、certificate.p7として保存します。

ファイルは、次の例のようになります。

```
-----BEGIN PKCS7-----
MIIF+AYJKoZIhvcNAQcCoIIIF6TCCBeUCAQExADALBgkqhkiG9w0BBwGgggXNMIID
LDCCApWgAwIBAgIQTPY7DsV1n1HeMGgMjMR2PzANBgkqhkiG9w0BAQUFADCbhzEL
...
i7coVx71/LCB0lFmx66NyKlZK5mObgvd2dlnsAP+nnStyhVHFIPky3nsD04JqrIg
EhCsdpikSpbtDo18jUubV6z1kQ71CrRQtbi/WtdqxQEETgZCJO2lPoIWMQA=
-----END PKCS7-----
```

- 4 次のコマンドを使用して証明書をキーストアにインポートします (`secret`を別のパスワードと置き換えてください)。

```
%JAVA_HOME%\bin\keytool -import -keystore keys.p12 -storetype pkcs12
-storepass secret -keyalg "RSA" -trustcacerts -file certificate.p7
```

この操作では、次のメッセージが表示される場合があります。

```
... is not trusted. Install reply anyway?
```

このメッセージは、提供されたルート証明書がテスト用の証明書であって本稼動用ではないため、Javaによって信頼されないことから生成されます。この証明書のインストールは可能ですが、最初の証明書よりもユーザーエクスペリエンスが優れていない場合があります。

新しい証明書を使用するように VDM Connection Server を構成するには、次の手順に従ってください。

- 1 各 VDM Connection Server (標準、レプリカ、またはセキュリティ サーバ) の以下の場所に新しい証明書ファイルを配置します。

```
C:%Program Files%VMware%VMware VDM%Server%sslgateway%conf
```

- 2 各サーバで次のファイルを作成または編集します。

```
C:%ProgramFiles%VMware%VMwareVDM%Server%sslgateway%conf%  
locked.properties
```

- 3 次のプロパティを追加します。

```
> keyfile=keys.p12  
> keypass=secret
```

これによって、前述の手順で作成した内容と合うように、必要に応じて値が変更されます。

- 4 VDM サービスを再起動します。

環境内で SSL を使用するように設定されていると仮定すると、次のようなログメッセージが表示されます。

```
13:57:40,676 INFO <Thread-1> [NetHandler] Using SSL certificate store:  
keys.p12 with password of 6 characters
```

このメッセージはその構成が使用中であることを示します。

## ロード バランシング

VDM 用のサーバをセットアップして構成する場合、設計上ロード バランシングを考慮することが重要となります。ロード バランシングは、最も高い拡張性を実現し、単一点障害の回避に役立ちます。ロード バランシングによって VDM ソリューションの拡張およびフォルト トレランスに対応します。

VDM Connection Server は VDM のコア コンポーネントです。VDM Connection Server は、コネクション サーバとセキュリティ サーバのどちらとしても展開できます。VDM Connection Server にはセッション管理が用意されていて、すべての着信クライアント要求を処理して、これらを適切な仮想デスクトップセッションにダイレクトします。VDM Security Server はクライアント デバイスと VDM Connection Server との間の安全な通信を確保します。

現在のビジネス アプリケーションとサービスをサポートする、適切なロードバランシングソリューションをすでに設定している場合もあります。VDM がロードバランシング インフラストラクチャで使用する負荷は最小であるため、その既存のロードバランシング サービスを活用できます。また、通常のハードウェアベースのロードバランシング アプリケーションに加えて、安価な、あるいは無償のソフトウェアベースの製品をロードバランシングソリューションの候補として検討することもできます。

DMZ 内に展開されたセキュリティ サーバを持つ DMZ 展開と、エンド ユーザーが VDM Connection Server に直接接続する非セキュリティ サーバ展開のいずれを使用している場合、ロードバランシングを導入できます。「[DMZ 展開でのロードバランシング](#) (P.74)」を参照してください。

## 非 DMZ 展開でのロードバランシング

LAN ベースの展開など、場合によってユーザーは VDM Connection Server に直接接続できます。この場合、VDM Security Server は展開されません。LAN ベースの接続に使用できるトンネリングされた、またはトンネリングされない展開を使用できます。トンネリングを有効にした場合、すべての VDM トラフィックが暗号化され、VDM Connection Server を介してトンネリングされます。トンネリングを有効にしていない場合、セッション トラフィックは VDM Connection Server を介してルーティングされず、そのため SSL による暗号化は行われません。使用している仮想デスクトップにクライアントが接続した後、すべての通信がクライアントと仮想デスクトップとの間で実行されます。

## セッションのセットアップとロードバランシング

ロードバランシングを構成するには、セッションをセットアップする方法およびクライアントとコネクション サーバとの間で接続情報をやりとりする方法を理解することが重要です。

最初の HTTP または HTTPS TCP セッションは、クライアントと VDM Security Server との間、またはクライアントと VDM Connection Server との間で確立されます。ユーザーは最初の接続中に認証されます。認証に成功した場合、制御情報がクライアントに返されます。制御情報には、ユーザーが接続資格を付与されている仮想デスクトップのリスト、および VDM Connection Server または VDM Security Server の完全修飾ドメイン名 (FQDN) が含まれます。

クライアントは接続情報を受け取ると、(コネクション サーバの) FQDN へのトンネリングに対して 2 回目の TCP セッションを開始します。2 回目の TCP セッションとは、クライアントとセキュリティ サーバ、またはクライアントと VDM Connection Server との間の SSL トンネリングです。この TCP セッションが開始されると、クライアントマシン上の RDP クライアントがローカル ホスト リスナーへの接続を開始し、トラフィックはトンネルからセキュリティ サーバへとルーティングされ、その後仮想デスクトップにルーティングされます。

VDM の安全な接続は、RDP セッション内の通信に使用されます。クライアントは、選択された仮想デスクトップで RDP セッションを確立する準備ができると、ローカル TCP リスナーを起動します。起動された後、VDM Connection Server と、ESX サーバ上で実行している仮想デスクトップとの間に TCP セッションが確立されます。次にクライアントマシン上の RDP クライアントがローカルホストに接続し、以前確立された VDM の安全な接続を使用して通信が処理されます。

ロードバランスされた構成では、クライアントが TCP セッションを確立した場合に、その TCP セッションを別のホストで確立できます。たとえば、クライアントからロードバランサへのクライアントの最初の接続は、<https://vdi-yourcompany.com> などのグローバル DNS 名に設定されます。ロードバランシングインフラストラクチャは、この要求を VDM Security Server ファームのサーバの 1 つである <https://vdm1.example.com> に転送します。いくつかの一般的なロードバランシング方法（プロキシ、HTTP リダイレクト、NLB クラスタ、ラウンドロビン DNS など）のいずれかを使用して、どの VDM サーバがセッションを処理するかを決定できます。

VDM クライアントは VDM サーバで認証すると、特定の指示を受け取って <https://vdm1.example.com> に直接接続し、SSL トンネリングを確立します。

## ロードバランスされたソリューションの DNS 要件

使用しているロードバランシングメカニズムに関係なく、クライアントは自身の FQDN によって各 VDM サーバに直接接続する必要があります。つまり、クライアントはロードバランシングをまとめてバイパスする必要があります。VDM Security Server が DMZ 内に展開されている場合、または VDM Connection Server にローカルエリアネットワークからアクセスする場合は、すべてのサーバが有効な DNS 名を持っている必要があります。

ロードバランサは、最初の TCP セッションを選択された VDM Connection Server に指示することで、どの VDM Connection Server がクライアントセッションを処理するかという最初の決定を行います。安全なトンネル接続は、クライアントから VDM Connection Server に直接確立されます。そのため、この接続に対してロードバランシングインフラストラクチャは使用されません。クライアントとサーバ間でネットワークトラフィックが一括処理されます。

## ロードバランシングソリューション

VDM サーバにロードバランシングソリューションを実装する場合、いくつかの方法があります。たとえば、ラウンドロビン DNS は、技術的に実装が最も単純なロードバランシングソリューションですが、フェイルオーバーの面では大きな欠点があります。サーバの1つに障害が発生した場合、そのサーバを、ロードバランスされたドメイン名に対応する DNS レコードリストから削除しなければなりません。ラウンドロビン DNS によるアプローチのもう1つの問題は、VDM クライアントが VDM Security Server を介して自身の仮想デスクトップにインターネット経由でアクセスするという、リモートアクセスを使用した場合です。この場合、マスター DNS サーバの応答は、上流の DNS サーバでキャッシュされます。削除された DNS 名をすべてのインターネット DNS サーバに複製するには数時間かかることがあります。サーバがサービス停止状態であるとき、クライアントがそのサーバにダイレクトされている場合、クライアント接続が確立できないことがあります。これは、その間にキャッシュされたレコードがすべてのインターネット DNS サーバ上で期限切れとなるためです。

通常はネットワークレベルでの冗長性とフェイルオーバーメカニズムをサポートすることによって、ロードバランサが単一障害点となることを防止します。たとえば、Virtual Router Redundancy Protocol (VRRP) を使用してロードバランサと通信すると、冗長性とフェイルオーバーが付加されます。メインのロードバランサに障害が発生した場合は、グループ内の別のロードバランサが自動的に接続処理を開始します。

ある程度のフォルトトレランスを提供するには、障害の発生した VDM サーバノードをロードバランスされたグループから削除できるロードバランシングソリューションが必要です。障害が発生したノードが検出される方法は、ソリューションごとに異なります。ソリューションでは、新しい着信セッションが応答のないサーバにダイレクトされないようにする必要があります。

アクティブなセッション中に VDM サーバに障害が発生したり、応答がなくなった場合、ユーザはデータを失わず、デスクトップの状態が仮想デスクトップに保持されます。ユーザがグループ内の別の VDM サーバに再接続すると、ユーザのデスクトップセッションは障害が発生した時点から続行されます。

クライアントと VDM Connection Server との間の Web セッションの親和性をサポートするロードバランシングソリューションを選択する必要があります。Web セッションの親和性とは、特定の Web セッションが常に同じサーバにダイレクトされることを意味します。

VMware VDM で使用できる安価な、および無償のロードバランシングソリューションは数多くあります。セッションの親和性に対応した、標準に基づくロードバランサであれば、どのバランサでもお使いいただけます。

ソフトウェアベースのロードバランサの例として、Hercules と Windows Network Load Balancing (NLB) の 2 つが挙げられます。Hercules は無償の Linux ベースの仮想アプライアンスで、Pen と呼ばれるオープンソースのロードバランサを備えています。Windows NLB は、Windows Server 2003 で使用できる機能です。

## DMZ の展開

VDM は、DMZ (セキュリティサーバ) の展開にも対応しています。DMZ では、インターネットから仮想デスクトップにアクセスする際のセキュリティを強化することができます。DMZ 内のサーバは、VDM Connection Server の全機能のサブセットを実行します。DMZ の展開では、セキュリティを補足するレイヤが追加され、認証されたユーザのみがインターネットから内部ネットワークに接続を試みるすることができます。

## DMZ のインストール

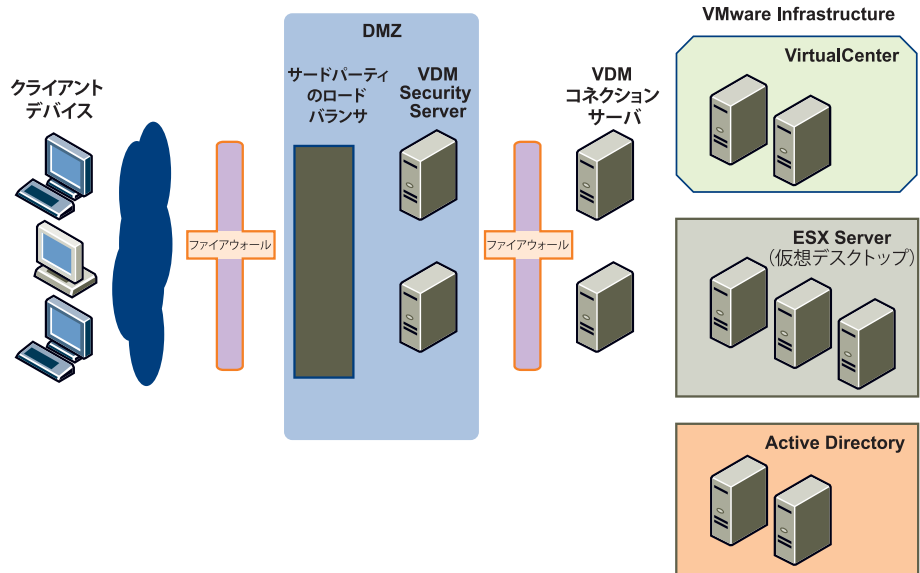
DMZ の展開には、インターネット、DMZ、および内部ネットワークというエンティティ、つまり場所があります。仮想デスクトップにアクセスする必要があるクライアントは、インターネット上に常駐します。仮想デスクトップは、仮想デスクトップインフラストラクチャを構成する残りのコンポーネントとともに内部ネットワーク上にあります。DMZ はインターネットと内部ネットワークとの間に存在し、内部ネットワークが侵害されるリスクを軽減します。

特定のサーバ構成によっては、ロードバランシングが必要な場合もあります。セキュリティサーバが複数ある場合は、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が必要です。

ファイアウォールを検討する場合は、2 つのファイアウォールを使用して、間に DMZ を設定し、これを両方のファイアウォールに接続する方法をとると、よりセキュリティを強化できます。この構成では、1 つのファイアウォールが内部ネットワークに接続され、もう 1 つのファイアウォールが外部ネットワークに接続されます。

**図 3-3** は、ユーザーがインターネットからそれぞれのデスクトップにアクセスできる DMZ の展開を示したものです。これには、DMZ の両側にロードバランサとファイアウォールが含まれます。

図 3-3 VDM DMZ の展開



セキュリティサーバ用にDMZのインストールを行うには、次の手順に従ってください。

- 1 VMware-vdmconnectionserver-2.1.0-<xxx>.exe を実行します。  
 <xxx> には、インストールするソフトウェア コンポーネントのビルド番号を指定します。  
 インストールウィザードが開きます。
- 2 [次へ] をクリックします。
- 3 ライセンス条件に同意して、[次へ] をクリックします。
- 4 インストール先フォルダを受け入れるか、変更して、[次へ] をクリックします。
- 5 [Security Server] を選択します。
- 6 セキュリティサーバが通信するコネクションサーバ（標準とレプリカのいずれか）の FQDN を入力します。  
 各セキュリティサーバは VDM Connection Server と対になっていて、すべてのトラフィックを VDM Connection Server サーバに転送します。
- 7 [次へ]-[インストール]-[完了] をクリックします。

## DMZ 展開でのロード バランシング

DMZ 内に VDM Connection Server を展開する場合、インストール プロセス中に専用 VDM Connection Server とのリンクが確立されます。VDM Connection Server が DMZ 内に展開されている場合、これらのサーバに DMZ 内でロード バランシングを行って、拡張性とフォルト トレランスを提供する必要があります。

## DMZ 展開のためのファイアウォールポートの構成

DMZ 展開でファイアウォールをセットアップする場合、通過する必要のある TCP プロトコルトラフィックがファイアウォールを通過できるようにファイアウォールルールを設定する必要があります。ここで説明する設定は、ファイアウォールルールが外部ネットワーク（インターネットなど）から、および DMZ から内部ネットワークに設定されている DMZ 展開に基づいています。また、この設定は、クライアントが外部ネットワークから VDM にアクセスし、DMZ 内にある VDM Security Server を使用して接続すること、および VDM はプロトコルごとにデフォルトの TCP ポートを使用してセットアップされることを前提としています。

外部ネットワークから DMZ にアクセスして、クライアントデバイスが DMZ 内の VDM Security Server に接続できるようにするには、TCP ポート 80 と 443 を許可します。

DMZ 内の VDM Security Server を使用して DMZ から内部ネットワークに接続し、内部ネットワークの VDM Connection Server（標準またはレプリカのインスタンス）に接続する場合は、AJP13 によって転送された Web トラフィック用に TCP ポート 8009 を、JMS メッセージングトラフィック用に TCP ポート 4001 を許可してください。

VDM Security Server を使用して DMZ から内部ネットワークに接続し、デスクトップ仮想マシンに接続するには、VDM によって保護された RDP トラフィック用に TCP ポート 3389 を許可してください。

各プロトコルには、次のデフォルトの TCP ポートが使用されます。プロトコルおよび関連ポートのリストは、[図 3-4](#) の参照用として使用してください。

- › JMS — 4001
- › AJP13 — 8009
- › HTTP — 80
- › HTTPS — 443
- › RDP — 3389
- › SOAP — 80 または 443











































