Introduction to Virtual Desktop Manager
You can find the most up-to-date technical documentation on our Web site at

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242,
6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022,
6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481,
7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999,
7,278,030, 7,281,102, and 7,290,253; patents pending.

VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or
trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names
mentioned herein may be trademarks of their respective companies.
Contents

Introduction to Virtual Desktop Manager 3
  Introduction 3
  Features 4
  VDM Overview 5
    VDM User Authentication 9
    VDM Extended USB Device Redirection 11
    VDM Secure Access 12
    VDM Virtual Desktop Pool Management 13
    VDM High Availability and Scalability 15
    VDM Connection Server DMZ Deployment 17
  VDM Connection Server Components 21
    VDM Broker 22
    VDM Secure Gateway Server 22
    VDM LDAP 23
    VDM Messaging 24
    VDM Security Server 24

Glossary 27
Introduction to Virtual Desktop Manager
Introduction to Virtual Desktop Manager

VMware Virtual Desktop Manager 2 (VDM) is a key component in the VMware Virtual Desktop Infrastructure (VDI) solution. VDM is an enterprise-class virtual desktop manager that securely connects authorized users to centralized virtual desktops. It works with VMware Virtual Infrastructure 3 to provide a complete, end-to-end VDI solution that improves control and manageability and provides a familiar desktop experience.

The benefits of VDI with VDM include the following:

- **Control and manageability in a single product** – Administrators can more easily provision, manage, and maintain desktops because the desktops are running in the datacenter.

- **Familiar end-user experience** – Users get flexible access to a personalized, virtual desktop that behaves just like their PC desktops.

- **VMware Infrastructure 3 integration** – VDI extends the benefits of VMware Infrastructure 3 to the desktop by leveraging the backup, failover, and disaster recovery capabilities of VMware Infrastructure 3.

- **Lower total cost of ownership (TCO)** – By reducing administration and energy costs and extending the useful life of PCs, VDI delivers lower TCO.
Features

The features of VDM in VDI include the following:

- **Enterprise-class connection brokering** – VDM manages the connections between users and their virtual desktops. When users log in to VDM, the virtual desktops they are authorized to access appear. After connecting to a virtual desktop, users access their applications as if the applications are running locally.

- **USB client device support** – USB devices can be locally connected to clients and accessed through a virtual desktop.

- **Web-based management user interface** – A Web-based management console allows virtual desktops to be managed from any location.

- **“Smart pooling” capabilities** – A range of persistent and non-persistent pooling capabilities simplifies the provisioning and management of centralized desktops.

- **Secure access** – Optional secure encapsulation capabilities allow all network connections to be encrypted.

- **Integration with Microsoft Active Directory** – Connection to Active Directory, which allows you to locate user and user group accounts and use the authentication features in Active Directory to control which users can access virtual desktops.

- **Support for two-factor authentication** – With RSA SecurID, access control is strengthened.

- **Seamless integration with VMware Virtual Infrastructure 3** – Works closely with VMware VirtualCenter to provide advanced virtual desktop management capabilities, such as automatic suspend and resume, which reduces the memory and processing power required to host virtual desktops. By leveraging the capabilities of VMware Virtual Infrastructure 3, desktops can run even when server hardware fails and recover quickly from unplanned outages without duplicate hardware.

- **Flexible deployment options** – Critical components can be deployed in a variety of configurations and to different parts of the network, which improve security, scalability, and reliability. Multiple VirtualCenter servers are supported, and VDM can scale horizontally to support many virtual desktops.

- **High availability** – Servers can be clustered for high availability and scalability with automatic failover. These servers can also leverage industry-standard load-balancing solutions.
VDM Overview

VDM includes the following key components:

- VDM Connection Server
- VDM Agent
- VDM Client
- VDM Web Access
- VDM Administrator
Figure 1 shows the physical topology of a VDI infrastructure with VDM and shows the relationship between the main VDM components.

**Figure 1. Physical Topology of VMware VDI Infrastructure with VDM**
VDM Connection Server

This component is the VDI connection broker that manages secure access to virtual desktops and works with VirtualCenter to provide advanced management capabilities. It is installed on a Microsoft Windows Server 2003 server that is part of an Active Directory domain.

VDM Connection Server is installed as one of the following instances:

- **Standard** – This instance appears in Figure 1. It provides stand-alone functionality and is used as the only VDM Connection Server (or the first of a group of VDM Connection Servers that act as part of a high-availability, fully replicated group).

- **Replica** – This instance is installed as a second or subsequent VDM server in a high-availability group. Configuration data is initialized from an existing VDM server and is automatically replicated between VDM group members.

- **Security Server** – This instance implements a subset of the VDM Connection Server functionality and is used in a demilitarized zone (DMZ) deployment. A VDM Security Server does not need to be in an Active Directory domain. The Standard and Replica instances automatically include the Security Server functionality.

The instance type is selected during VDM Connection Server installation.

High-availability and DMZ deployments of VDM Connection Server using Replica and Security Server instances are described in VDM Connection Server DMZ Deployment.

Configuration data is stored in an embedded LDAP directory on each Standard and Replica instance.
VDM Agent

This component runs on each virtual desktop and is used for session management and single sign-on. With VDM Client, this component supports optional USB device redirection. This agent can be installed on a virtual machine template so that virtual desktops created from that template automatically include the VDM Agent.

Place virtual desktops in an Active Directory domain that is one of the following:

- The same domain to which the VDM Connection Servers are joined
- A domain with a trust agreement with the VDM Connection Server domain

When users connect to their virtual desktops, they are automatically logged in using the same credentials they use to log in to their domain. The single sign-on capability can be disabled in VDM Agent which meant that users are always required to log on to the virtual desktop manually. If the virtual desktop is not part of a domain or is part of a domain with which no trust agreement exists, single sign-on is not available, and the user must manually log in to the virtual desktop.

VDM Client

This component runs on a Windows PC as a native Windows application and allows users to connect to their virtual desktops through VDM. This component connects to a VDM Connection Server and allows the user to log on using any of the supported authentication mechanisms. After logging in, users can select from the list of virtual desktops for which they are authorized. This step provides remote access to their virtual desktop and provides users with a familiar desktop experience.

VDM Client also works closely with VDM Agent to provide enhanced USB support. Basic USB support (such as USB drives and USB printers) is supported without VDM USB support, but VDM extends this support to include additional USB devices. You can specify VDM USB support in VDM Client during the installation.

VDM Web Access

This component is similar to VDM Client but provides a VDM user interface through a Web browser. VDM Web Access is included automatically during the VDM Connection Server installation. VDM Web Access is supported on Linux and Mac OS/X, but this Web access does not support VDM USB extensions. All necessary VDM software is installed automatically on the client through the Web browser. VDM Web Access on Linux uses rdesktop and on Mac OS/X uses Microsoft Remote Desktop Connection Client for Mac.
VDM Web Access can also be used on a Windows client with VDM Client. A user obtains the required software on their client device by accessing a VDM Connection Server with a Web browser. If the VDM Client software is installed with USB support by a user with administrative rights, VDM Web Access on Windows has complete VDM USB support.

**VDM Administrator**

This component provides VDM administration through a Web browser. It is used by VDM administrators to do the following:

- Make configuration settings
- Manage virtual desktops and entitlements of desktops of Windows users and groups

VDM Administrator also provides an interface to monitor log events on a VDM Server and is installed with VDM Connection Server. More information about the VDM Connection Server components and their relationship with other VDM components, see VDM Connection Server Components.

**VDM User Authentication**

Users need to log in to VDM first in order to prove their identity and to gain access to their virtual desktops. Normally, they do this by entering their Windows credentials at the login prompt.

As an added level of security, VDM can be configured to require RSA SecurID authentication. This requires the use of a SecurID token for each user. As part of the login process, users must enter their SecurID user names together with their SecurID PINs and tokencodes. After successful verification of the SecurID details entered, users are prompted for their Windows credentials.

**Active Directory Authentication**

Each VDM Connection Server must be joined to an Active Directory domain. This allows user authentication for VDM against Active Directory for the joined domain and for additional user domains with which a trust agreement exists. For example, if VDM Connection Server is a member of Domain A, and a trust agreement exists between Domain A and Domain B, users from either domain can log in to VDM.
By authenticating users against an existing Active Directory, an organization can simplify the operational management of VDM by ensuring that the management of user accounts is handled in one place. If a user account is disabled in Active Directory, that user cannot log in to VDM. Policies, such as restricting permitted hours of login and the expiration date for passwords, are also handled through existing Active Directory operational procedures.

**RSA SecurID Authentication**

VDM is certified through the RSA SecurID Ready program to operate with RSA SecurID authentication technology. Individual VDM Connection Servers can be enabled for RSA SecurID authentication. Users who access a VDM Connection Server that is enabled for RSA SecurID authentication are prompted for their RSA SecurID user names and passcodes (PINs and token codes). After authenticating against an RSA Authentication Manager, users can continue to log in.

Using RSA SecurID provides enhanced security with two-factor authentication. This requires knowledge of the user’s PIN and token code, which is only available on the physical SecurID token. As required for RSA SecurID certification, VDM supports the full range of SecurID capabilities, including New PIN Mode, Next Token Code Mode, RSA Authentication Manager, load balancing, and so on.
Figure 2 shows the physical topology diagram for VDM with an additional server used to authenticate RSA SecurID users. The RSA Authentication Manager is shown as a single server, but for high-availability deployments, you need multiple servers.

**Figure 2.** VDM RSA SecurID Authentication with RSA Authentication Manager

When users enter their RSA SecurID credentials, VDM Connection Server communicates with RSA Authentication Manager to verify the information. After the credentials are verified, VDM Connection Server requests Active Directory domain credentials from the user and communicates with Active Directory to continue the authentication process.

**VDM Extended USB Device Redirection**

VDM allows the redirection of a variety of locally attached USB devices for software that run on a user’s virtual desktop. Suitable devices, when attached, can be selected from a dynamic drop-down menu in VDM Client. Devices attached after the virtual desktop session starts will appear in the menu and are available for redirection after being initialized.
Introduction to Virtual Desktop Manager

Some devices, such as printers, local USB flash drives, and smart cards, can be forwarded to the virtual desktop using standard Microsoft Remote Desktop Protocol (RDP). But VDM Client USB redirection extends the range of usable devices and the functionality of some devices beyond that provided by RDP. For example, sound can be brought to the local machine using RDP, but disabling this feature and using VDM USB redirection allows you to use VoIP devices.

VDM USB redirection is initiated after the user is authenticated. Because of this, smart card forwarding is limited to RDP functionality so that smart cards can be used to authenticate the virtual desktop session. As a result, these devices do not appear in the VDM Client devices menu. Human interface devices (HIDs), such as a keyboard or a mouse, are also filtered from the USB device list because these devices are required locally and function without being forwarded or redirected.

RDP forwarding and VDM USB redirection can be governed through Active Directory Group Policy and VDM Administrator. Using VDM USB redirection requires VDM Client, VDM Agent, and the user to have administration rights on the VDM Client and the VDM Agent operating systems.

VDM Secure Access

VDM Connection Server with VDM Client and VDM Web Access provides security for the desktop protocols between the client device and the VDM Connection Server.

VDM encapsulates all protocols, such as the extended RDP in an HTTPS connection, which offers the following advantages:

- **The RDP Protocol is “tunneled” through HTTPS and is encrypted using SSL** – This is a powerful security protocol and is consistent with the security provided by other secure Web sites like those used for online banking, credit card payments, and so on.

- **One HTTPS connection is used for all client-server communication** – Multiple desktop connections are multiplexed over this HTTPS connection, which reduces the overall protocol overheads.

- **VDM controls both ends of this HTTPS connection, so the reliability of the underlying protocols is significantly improved** – If a user temporarily loses a network connection, after it is restored, the HTTPS connection is reestablished and the RDP connections automatically resume without having to reconnect and log in again.
VDM is accessed using standard Web protocols, so it can be easily accessed through corporate proxies – In a standard deployment of just VDM Connection Servers, the HTTPS secure connection terminates at the VDM Connection Server and in a DMZ deployment, at the VDM Security Server. See VDM Connection Server DMZ Deployment.

VDM Connection Server can be configured to not use a secure connection, so that RDP communication is direct from the client device to the virtual desktop.

**VDM Virtual Desktop Pool Management**

VDM includes integrated virtual desktop pool management capabilities that leverage the control provided by VirtualCenter to provision and manage the virtual desktops.

VDM provides the following types of desktops:

- **Individual desktops** – These are existing virtual desktops that are available through VDM. The pool manager can control the power state of these virtual desktops.

- **Persistent desktop pool** – This type is a pool of virtual desktops whose lifecycle and power state is controlled by the pool manager. Persistent virtual desktops are assigned to their user on the first use, so the user returns each time to the same virtual desktop. This type of pool is used when users want to customize their desktops by installing additional applications and storing local data.

- **Non-persistent desktop pool** – Similar to a persistent desktop pool, except in this case the virtual desktops are not permanently assigned to users. When a session is finished, the virtual desktop is returned to the pool and made available for other users.

  By deleting the virtual desktops after each use, this type of pool ensures that each user receives a newly provisioned virtual desktop each time the user connects (optional). Use this type of pool where a clean machine is needed for each user session or in highly controlled environments that has no requirement for customization to be stored on the virtual desktop.
The two pool desktops are sized using the following parameters:

- **Minimum** – The minimum number of virtual desktops to be created when the pool is first created. The pool manager continues to create virtual desktops until this minimum count is reached. This process ensures that a pool is appropriately sized when a user population is moved to VDM.

- **Maximum** – The maximum number of virtual desktops that can exist in the pool. Use this parameter to limit the number of virtual desktops in the pool to avoid overusing available resources.

- **Available** – The number of virtual desktops that are available for immediate use. For persistent pools, this parameter relates only to the unassigned virtual desktops. This is used to ensure that the pool manager creates enough virtual desktops in advance to cope with demand. Use a higher number for more volatile environments.

When a pool contains too few virtual desktops, the manager provisions new virtual desktops from a designated template. These virtual desktops can also be automatically customized (for example, named and become part of an Active Directory domain) or be left for an administrator to manually configure.

Power management is applied to all virtual desktops under VDM control, and the following policies are supported:

- **Remain on** – After being started, VDM does not power the machine down. If a virtual desktop is powered down, for example using the VirtualCenter client, VDM automatically starts it when it is needed.

- **Always powered on** – VDM ensures that any virtual desktop with this policy applied is powered on all the time. If a virtual desktop is powered down, VDM immediately powers it up again.

- **Suspend when not in use** – If a virtual desktop is not required, it is suspended. This policy is applied to individual and assigned persistent virtual desktops when the user logs off. It is also applied to nonpersistent virtual desktops when there are too many available virtual desktops. For example, this can be triggered by a virtual desktop being returned to the pool when a user logs out.
■ **Power off when not in use** – If a virtual desktop is not required, it is powered off. This is just like the “Suspend when not in use” policy, except that the virtual desktop is completely powered off.

VDM supports individual and pooled desktops on multiple VirtualCenter instances. A pool cannot span VirtualCenters, but VDM can manage multiple pools across multiple VirtualCenters. VDM limits the number of provisioning and power operations that can be concurrently active for each VirtualCenter to ensure that the rate of operations is not excessive. These limits are applied across all pools and desktops for each VirtualCenter. In a multi-broker environment, the VDM Connection Servers cooperate with each other to enforce these limits and to perform the pool management operations.

**VDM High Availability and Scalability**

To support high-availability and scalability requirements, VDM Connection Server can be deployed using multiple VDM Connection Servers. The first VDM Connection Server to be deployed is installed as a Standard instance. In this case, a new instance of the LDAP directory is installed and the VDM Connection Server supports full functionality using its local LDAP directory.

To extend the environment, a second server can be installed as a Replica instance. During this installation, the user references an existing VDM Connection Server and the Replica instance is joined to the Standard instance to form a VDM Connection Server group. The LDAP VDM configuration data from the Standard instance is copied to the Replica instance. A two-way replication agreement is established so that VDM configuration changes on either server are automatically and immediately made on the other.

Both servers offer identical functionality and in the event of server failure, the other server can continue to operate alone. When the failed server resumes, any changed LDAP VDM configuration data is reflected on the resumed server so that both servers remain up to date. Adding a third and subsequent VDM Connection Servers to the group is done by installing additional Replica instances. During the Replica instance installation, the user can reference any existing group member to join the new server to the group.

After installation, no differences exist between a Replica instance and a Standard instance. If the first Standard instance is decommissioned, additional Replicas can be added to the group by referencing any active VDM Connection Server in the group. All VDM configuration data can be backed up by backing up the LDAP directory instance.
Figure 3 shows two VDM Connection Servers operating as a group. To automatically use both VDM Connection Servers and support high-availability and scalability needs, deploy load balancing. This ensures that load is balanced evenly across the available VDM Connection Servers and that failed servers are automatically avoided. VDM Connection Server does not provide load-balancing functionality but works with standard third-party load-balancing solutions.

**Figure 3.** Multiple VDM Connection Servers
The load balancing requirements for VDM Connection Server are to support standard HTTP and HTTPS load-balancing with session affinity. Load balancing solutions for VDM Connection Server can include Microsoft Network Load Balancing (NLB), standard hardware-based load balancers, or virtual appliance load balancers that can operate on ESX Server.

Users in a load-balanced VDM Connection Server environment use a load-balanced URL to make the connection. This is an alias URL used by the load balancer to direct the connection to any of the available VDM Connection Servers in the group.

**VDM Connection Server DMZ Deployment**

In secure environments, particularly when VDM is being accessed from an insecure network such as the Internet, it is common practice to deploy servers in a DMZ.

VDM Connection Server functionality is split between servers in the secure network and the DMZ. VDM Connection Servers that operate in a DMZ are known as VDM Security Servers and are installed using the VDM Connection Server installer and specifying a Security Server instance type. VDM Security Servers in the DMZ operate with VDM Connection Servers (Standard or Replica) in the secure network.
Figure 4 shows a high-availability environment comprising two load-balanced VDM Security Servers in the DMZ working with two full VDM Connection Servers (Standard and Replica instance) in the secure network.

**Figure 4.** DMZ Deployment with Multiple VDM Connection Servers

![Diagram of DMZ deployment with multiple VDM Connection Servers.](image-url)
VDM Security Servers do not contain an LDAP configuration repository and do not access any authentication repositories (Active Directory or RSA Authentication Manager). When remote users connect using a VDM Security Server, they must successfully authenticate before a secure connection is established. This means they cannot attempt to access any virtual desktops until they are successfully authenticated. With appropriate firewall rules on both sides of the DMZ, this type of deployment is suitable for accessing virtual desktops from Internet-located client devices.

To support remote VDM Client and VDM Web Access connecting to the environment using HTTPS from an external network, the only TCP port that must be allowed in the DMZ is the HTTPS port (TCP port 443). VDM Security Servers do not need to be part of an Active Directory domain, and no communication occurs between VDM Security Servers and Active Directory.

Although Figure 4 shows a one-to-one relationship between VDM Security Servers and VDM Connection Servers, multiple VDM Security Servers can be connected to each VDM Connection Server. A DMZ deployment can be combined with a standard deployment to offer VDM access for internal users and external users.

Figure 5 shows a more complex environment where four VDM Connection Servers act as one group with the servers in the internal network dedicated to the users of that network, and the servers in the external network dedicated to users of that network. The servers on the right can be enabled for RSA SecurID authentication, so that all external network users are required to authenticate using RSA SecurID tokens.
Figure 5. DMZ Deployment with Internal Network Access
VDM Connection Server Components

Figure 6 shows the VDM Connection Server components and their relationship with the other VDM components and the protocols used for communication between the components.

The following default TCP ports are used for each protocol:

- JMS – 4001
- HTTP – 80
- HTTPS – 443
- RDP – 3389
- SOAP – 80 or 443
Figure 6. VDM Components
**VDM Broker**

VDM Broker is the core of VDM Connection Server. It is responsible for all user interaction between the client (VDM Client, VDM Web Access, and Thin Client) and the VDM Connection Server.

VDM Broker provides the following:

- User authentication
- User desktop entitlements with VDM LDAP
- Virtual desktop session management
- Coordination of the secure connection establishment, virtual desktop connection, and single sign-on
- Administration server used by VDM Administrator Web client
- Virtual desktop pool management

VDM Broker operates closely with VirtualCenter to provide advanced management of virtual desktops. This includes virtual desktop creation as part of pool management and power operations, such as automatic suspend and resume.

**VDM Secure Gateway Server**

VDM Secure Gateway Server provides the server-side component for the secure HTTPS connection between the VDM Client (or VDM Secure Gateway Client) and the VDM Connection Server. After the user is authenticated, a secure HTTPS connection is established between the client and the VDM Connection Server. For a Windows client, this connection is initiated by the native Windows VDM Client. On Linux or Mac OS/X, it is initiated by the Java VDM Secure Gateway Client using Java Web Start technology. After this secure connection is established, virtual desktop protocols (RDP) can securely and reliably connect.

When the VDM Secure Gateway Server sees an incoming RDP connection through the HTTPS connection, it forwards this connection to the appropriate virtual desktop. To ensure that all virtual desktops are only accessed through VDM Connection Server, firewall rules can be applied to each virtual desktop so that all RDP connections originate from a VDM Connection Server. This way, direct access to virtual desktops bypassing VDM Connection Server is not possible because VDM Connection Server acts as gatekeeper for all virtual desktop access. With VDM 2.1 and newer, the VDM Agent can be configured so that direct incoming RDP connections to virtual desktops are not allowed. This ensures that all remote access to virtual desktops must pass through a VDM Connection Server.
Introduction to Virtual Desktop Manager

VDM Secure Gateway Server is also responsible for forwarding other Web traffic (such as authentication traffic, user desktop selection traffic, and so on) to the VDM broker from the VDM clients. VDM Administrator Web traffic is passed by VDM Secure Gateway Server to the VDM Broker.

**VDM LDAP**

VDM LDAP is an embedded LDAP directory on each VDM Connection Server Standard and Replica instances. It is used as the configuration repository for all VDM configuration data. VDM LDAP for Windows Server 2003 uses Microsoft Active Directory Application Mode (ADAM). This is an embedded LDAP directory bundled with VDM. It installs the following components that are appropriate for VDM:

- Specific VDM schema definitions
- Directory information tree (DIT) definitions
- Access control lists (ACLs)

VDM LDAP also includes a set of VDM plug-in DLLs to provide automation and notification services for other VDM components.

VDM LDAP contains entries to represent the following configuration items:

- **Virtual desktop entries that represent each accessible virtual desktop** – This contains references to Foreign Security Principal entries of Windows users and Windows user groups in Active Directory who are authorized to use this desktop.
- **Virtual Desktop Pool entries that represent multiple virtual desktops managed together**
- **Virtual machine entries that represent each virtual desktop**
- **VDM component configuration entries used to store configuration settings**

When a Standard instance is installed during VDM Connection Server installation, a new, local stand-alone ADAM instance is created. The schema definitions, DIT definition, ACLs, and so on are loaded and initial data is added. Configuration data in VDM LDAP is mainly maintained from VDM Administrator, although VDM Broker also manages some parts automatically.
When a VDM Connection Server Replica instance is installed, an ADAM instance is also created locally, but the initial data is retrieved from an existing instance. This means that the initial data is a copy of an existing instance that includes all configuration settings. During a Replica instance installation, a replication agreement is set up so that all VDM Connection Servers in the group share the same configuration data. LDAP changes on any server are replicated to all other servers. This replication functionality is provided by ADAM, which uses the same replication technology as Active Directory.

**VDM Messaging**

This component provides the messaging router for communication between VDM Connection Server components and between VDM Agent and VDM Connection Server. It supports the Java Message Service (JMS) API, which is used for messaging in VDM.

**VDM Security Server**

VDM Security Server is an instance type that is selected when VDM Connection Server is installed. It has a subset of the functionality of a full VDM Connection Server and is used in a DMZ deployment. Figure 7 shows a VDM Security Server and shows the relationship with all other VDM components and the protocols used for communication between the components.

The following default TCP ports are used for each protocol:

- **JMS** – 4001
- **AJP13** – 8009
- **HTTP** – 80
- **HTTPS** – 443
- **RDP** – 3389
- **SOAP** – 80 or 443
Introduction to Virtual Desktop Manager

**Figure 7.** VDM Component Diagram with Security Server

For more information about VDM deployment within a DMZ, see VDM Connection Server DMZ Deployment.
Glossary

A

Active Directory
A Microsoft directory service that stores information about the network operating system and provides services. Active Directory configures and manages users and groups and enables administrators to set security policies, control resources, and deploy programs across an enterprise.

ADAM (Active Directory Application Mode)
An LDAP implementation based on Active Directory.

active session
A live connection from a client or Web Access user to a virtual desktop. An established connection to a virtual desktop that has not timed out.

administrator user interface
The Web-based administrator user interface used to perform configuration and management tasks in VDM. Also known as the VDM Administrator.

agent
See “VMware VDM Agent.”

B
broker
Also known as a connection broker. The VDM Connection Server is a type of connection broker. See also “VMware VDM Connection Server.”
Introduction to Virtual Desktop Manager

C

client
See “VMware VDM Client.”

connection broker
A server that allows connections between remote users and virtual desktops and provides authentication and session management. The VDM Connection Server is a type of connection broker. See also “VMware VDM Connection Server.”

connection server
See “VMware VDM Connection Server.”

D
desktop
See “virtual desktop.”

desktop virtual machine
See “virtual desktop.”

desktop pool
A pool of virtual machines that an administrator designates for users or groups of users. See also “persistent desktop pool,” “nonpersistent desktop pool.”

DMZ (demilitarized zone)
A logical or physical subnetwork that connects internal servers to a larger, untrusted network (usually the Internet) and provides an additional layer of security and gives administrators more control over who can access network resources.

DNS (Domain Name System)
An Internet data query service that translates host names into IP addresses. Also called “Domain Name Server” or “Domain Name Service.”

F

FQDN (fully qualified domain name)
The name of a host, including both the host name and the domain name. For example, the FQDN of a host named esx1 in the domain vmware.com is esx1.vmware.com.

G
guest
See “guest operating system.”

guest operating system
An operating system that runs inside a virtual machine.
H high availability
A system design approach that ensures a degree of operational continuity.

L load balancing
A technique used for distributing processes across servers so that the traffic load is spread more evenly and servers do not become overloaded.

N nonpersistent desktop pool
A desktop pool in which users are not assigned to a specific desktop. When users log off or are timed out of a desktop, their desktops are returned to the pool and made available to other users. Users should not save data or files to their desktops when using a nonpersistent pool.

P persistent desktop pool
A desktop pool in which users are assigned to a specific desktop. Users log on to the same desktop every time and their data is preserved when they log off. Users can save data and files to their desktops when using a persistent pool.

R RDP (remote desktop protocol)
A multichannel protocol that allows a user to connect to a computer remotely.

RSA SecurID
A product from RSA that provides strong two factor authentication using a password and an authenticator.

S security server
A VDM Connection Server deployment that adds a layer of security between the Internet and the internal network. Security Server is an option that you choose during VDM connection server installation. See also “DMZ (demilitarized zone).”

T thin client
A device that allows a user to access virtual desktops but requires little memory or disk drive space. Application software, data, and CPU power resides on a network computer and not on the client device.

V VMware VDM Agent
Installed on the guest, the VDM Agent enables communication between the desktop virtual machine, the VDM Connection Server, and end users who access virtual desktops by using VDM Web Access or VDM Clients.
VMware VDM Client
A Windows-based application used for accessing virtual desktops.

VMware VDM Connection Server
A connection broker that provides management and user authentication for virtual desktops. The VDM Connection Server directs incoming remote desktop user requests to the appropriate virtual desktop.

VMware VDM Web Access
Web browser-based application for accessing virtual desktops. End users who run supported Windows, Linux, or Macintosh operating systems can access virtual desktops by using VDM Web Access.

virtual desktop
A desktop operating system that runs on a virtual machine. A virtual desktop is indistinguishable from any other computer running the same operating system.

VMware Virtual Desktop Infrastructure
The VMware desktop infrastructure solution that consists of VMware ESX Server, VMware VirtualCenter, and VMware Virtual Desktop Manager. VDI provides an end-to-end virtual desktop solution that allows administrators to easily deploy and manage virtual desktop environments.

web access
See “VMware VDM Web Access.”