

Introduction to VMware View Manager

View Manager 3.0

Introduction to VMware View Manager

Item: EN-000091-00

You can find the most up-to-date technical documentation on the VMware 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 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, 7,290,253, 7,356,679, 7,409,487, 7,412,492, 7,412,702, 7,424,710, 7,428,636, 7,433,951, 7,434,002, and 7,447,854; 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.

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

Contents

Introduction to VMware View Manager	5
Features	6
VMware View Overview	7
View User Authentication	11
View Extended USB Device Redirection	13
View Secure Access	14
View Virtual Desktop Pool Management	14
View High Availability and Scalability	16
View Connection Server DMZ Deployment	17
View Connection Server Components	20
View Broker	22
View Secure Gateway Server	22
View LDAP	23
View Messaging	24
View Security Server	24
Deployment Options	26
Offline Desktop	26
Linked Clones	27
Unified Access	28
Glossary	31

Introduction to VMware View Manager

VMware View is an enterprise-class virtual desktop manager that securely connects authorized users to centralized virtual desktops. It provides a complete, end-to-end solution that improves control and manageability and provides a familiar desktop experience.

The benefits of VMware View 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 desktop integration** – View extends the benefits of virtualization 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, VMware View Manager delivers lower TCO.

Features

The features of VMware View include the following:

- **Enterprise-class connection brokering** – VMware View Manager manages the connections between users and their virtual desktops. When users log in to View Manager, the virtual desktops they are authorized to access appears. 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 VMware View can scale 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.

- **VMware View Composer** – Dramatically reduces the amount of storage consumed. Images can be provisioned in a few seconds and in a fully automated manner by View Manager for rapid rollouts or as an immediate response to everyday support issues.
- **Support for non-VI systems** – physical machines or terminal services systems can be also managed by View Manager, ensuring a seamless integration of existing architectures into the View environment.
- **Scalable virtual infrastructure** – linked clone technology allows multiple desktops to be deployed from a single base image. Subsequent changes to this image can be automatically proliferated amongst all desktops in linked clone pool.
- **Simplified Printing** – Enables View Client and View Portal users to print using any printer configured for use by the View Client or View Portal host.

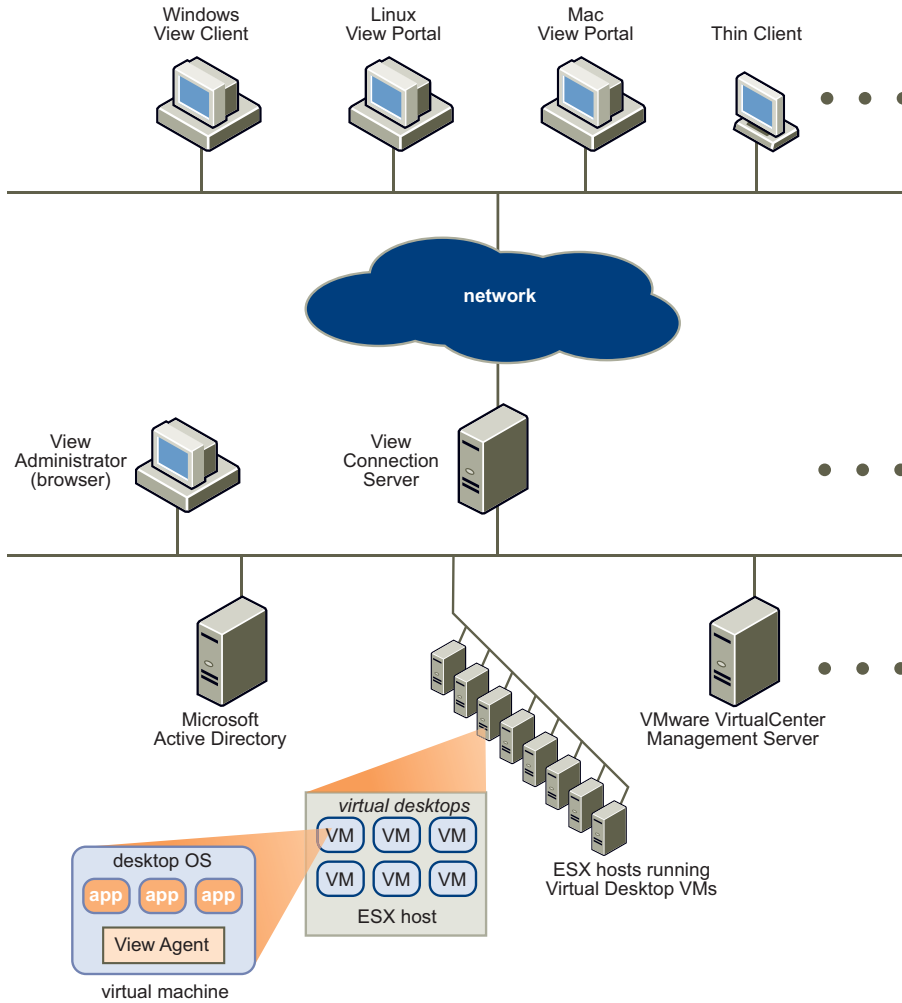
VMware View Overview

VMware View includes the following key components:

- View Connection Server
- View Agent
- View Client
- View Client with Offline Desktop
- View Portal
- View Administrator
- View Composer

Figure 1 shows the physical topology of VMware View infrastructure and shows the relationship between the main VMware View components.

Figure 1. Physical Topology of VMware View Infrastructure



View Connection Server

This component is the 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.

View 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 View Connection Server (or the first of a group of View Connection Servers that act as part of a high-availability, fully replicated group).
- **Replica** – This instance is installed as a second or subsequent ViewConnection Server in a high-availability group. Configuration data is initialized from an existing ViewConnection Server server and is automatically replicated between View group members.
- **Security Server** – This instance implements a subset of the View Connection Server functionality and is used in a demilitarized zone (DMZ) deployment. A View 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 View Connection Server installation.

High-availability and DMZ deployments of View Connection Server using Replica and Security Server instances are described in [View Connection Server DMZ Deployment](#).

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

View Agent

This component runs on each virtual desktop and is used for session management and single sign-on. With View 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 View Agent.

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

- The same domain to which the View Connection Servers are joined
- A domain with a trust agreement with the View 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 View Agent which means 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.

View Client

This component runs on a Windows PC as a native Windows application and allows users to connect to their virtual desktops through View. This component connects to a View 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.

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

View Client with Offline Desktop

Offline Desktop offers mobile users the ability to check out a cloned instance of certain types of View Manager desktop onto a local system such as a laptop. Once checked out, the local copy behaves like a standalone desktop system and can be used with or without a network connection; the desktop is now considered to be "offline".

Once downloaded, Offline desktops behave in the same way as their online equivalents yet can take advantage of local resources; latency is minimized and performance is enhanced. The presence of a downloaded virtual machine has no effect on the existing operating system of the client system, which users can continue to utilize if they wish.

View Portal

This component is similar to View Client but provides a View user interface through a Web browser. View Portal is included automatically during the View Connection Server installation. View Portal is supported on Linux and Mac OS/X, but this Web access does not support View USB extensions. All necessary View software is installed automatically on the client through the Web browser. View Portal on Linux uses rdesktop and on Mac OS/X uses Microsoft Remote Desktop Connection Client for Mac.

View Portal can also be used on a Windows client with View Client. A user obtains the required software on their client device by accessing a View Connection Server with a Web browser. If the View Client software is installed with USB support by a user with administrative rights, View Portal on Windows has complete View USB support.

View Administrator

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

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

View Administrator also provides an interface to monitor log events and is installed with View Connection Server. More information about the View Connection Server components and their relationship with other View components, see [View Connection Server Components](#).

View Composer

View Composer is used by View to create and deploy linked clone desktops from VirtualCenter. The linked clone feature enables View administrators to rapidly clone and deploy multiple desktops from a single centralized base image, called a Parent VM. Once the desktops have been created they remain indirectly linked to a snapshot residing on the Parent VM.

The link is indirect because the first time one or more desktop clones are created, a uniquely identified copy of the Parent VM—called a replica—is also created. All the desktop clones are anchored directly to the replica and not to the Parent VM.

View User Authentication

Users need to log in to View 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, View 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 token codes. After successful verification of the SecurID details entered, users are prompted for their Windows credentials.

Active Directory Authentication

Each View Connection Server must be joined to an Active Directory domain. This allows user authentication for View against Active Directory for the joined domain and for additional user domains with which a trust agreement exists. For example, if View 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 View.

By authenticating users against an existing Active Directory, an organization can simplify the operational management of View 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 View. Policies, such as restricting permitted hours of login and the expiration date for passwords, are also handled through existing Active Directory operational procedures.

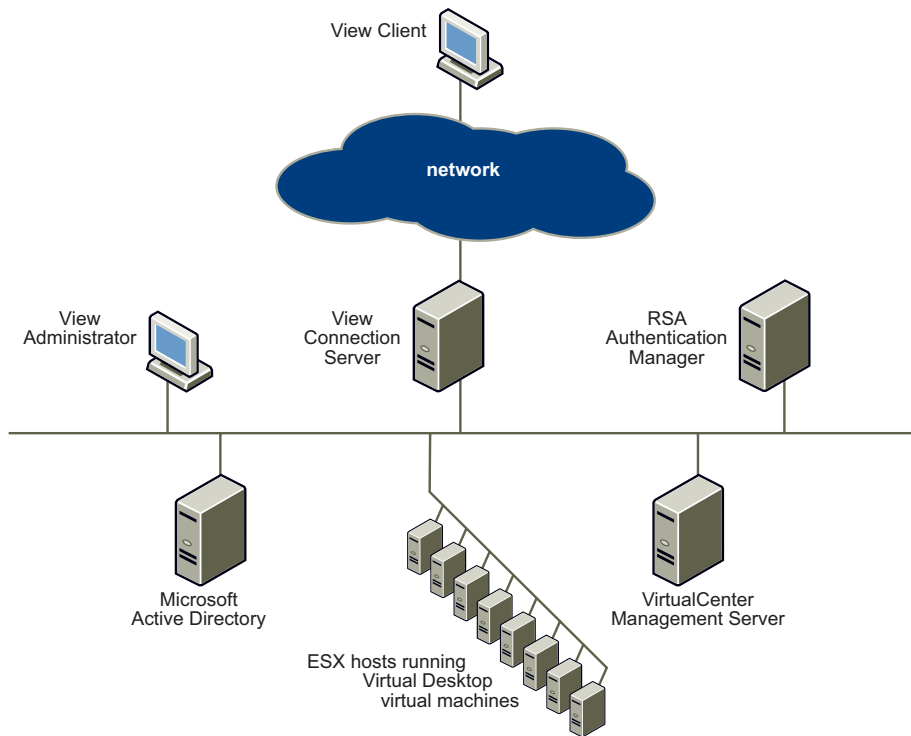
RSA SecurID Authentication

View is certified through the RSA SecurID Ready program to operate with RSA SecurID authentication technology. Individual View Connection Servers can be enabled for RSA SecurID authentication. Users who access a View 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, View 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 View 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. View RSA SecurID Authentication with RSA Authentication Manager



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

View Extended USB Device Redirection

View 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 View Client. Devices attached after the virtual desktop session starts will appear in the menu and are available for redirection after being initialized.

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 View 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 View USB redirection allows you to use VoIP devices.

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

View Secure Access

View Connection Server with View Client and View Portal provides security for the desktop protocols between the client device and the View Connection Server.

View 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.
- **View 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.
- **View is accessed using standard Web protocols, so it can be easily accessed through corporate proxies** – In a standard deployment of just View Connection Servers, the HTTPS secure connection terminates at the View Connection Server and in a DMZ deployment, at the View Security Server. See [View Connection Server DMZ Deployment](#).

View 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.

View Virtual Desktop Pool Management

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

View provides the following types of desktops:

- **Individual desktops** – These are existing virtual desktops that are available through View. 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 View.
- **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 View control, and the following policies are supported:

- **Do nothing (VM remains on)** – VMs that are powered off will be started when required and will remain on, even when not in use, until they are shut down.
- **Ensure VM is always powered on** – All VMs in the pool remain powered on, even when they are not in use. If they are shut down, they will immediately restart.
- **Suspend** – All VMs in the pool enter a suspended state when not in use.
- **Power off** – All VMs in the pool shut down when not in use..

View supports individual and pooled desktops on multiple VirtualCenter instances. A pool cannot span VirtualCenters, but View can manage multiple pools across multiple VirtualCenters. View 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 View Connection Servers cooperate with each other to enforce these limits and to perform the pool management operations.

View High Availability and Scalability

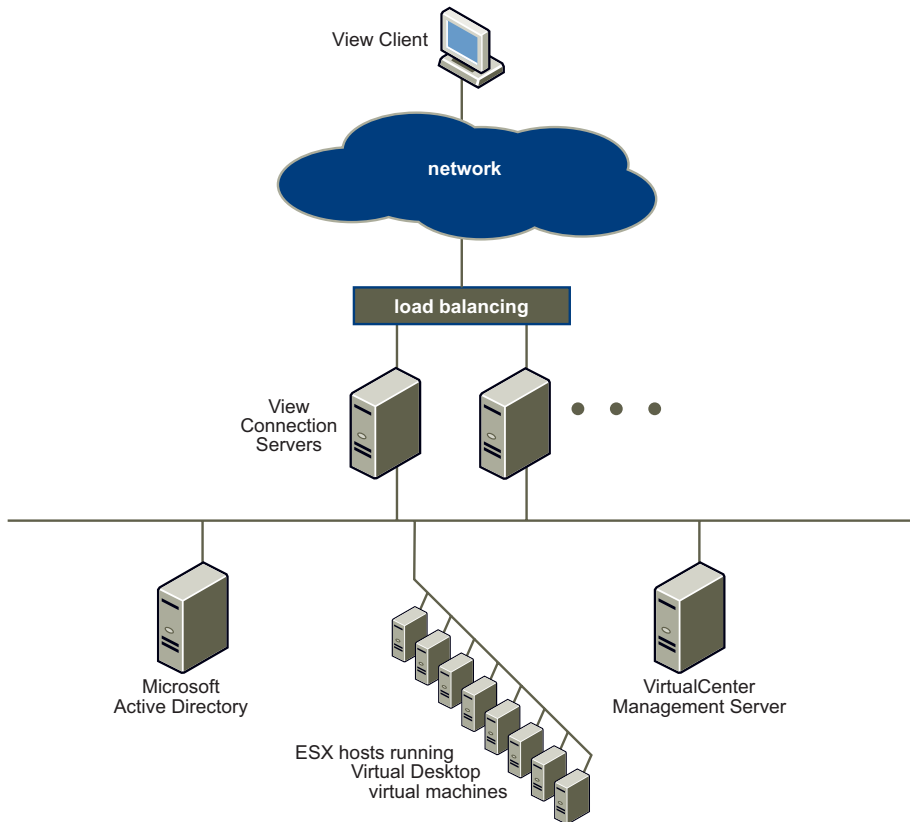
To support high-availability and scalability requirements, View can be deployed using multiple View Connection Servers. The first View Connection Server to be deployed is installed as a Standard instance. In this case, a new instance of the LDAP directory is installed and the View Connection Server supports 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 View Connection Server and the Replica instance is joined to the Standard instance to form a View Connection Server group. The LDAP View configuration data from the Standard instance is copied to the Replica instance. A two-way replication agreement is established so that View 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 View configuration data is reflected on the resumed server so that both servers remain up to date. Adding a third and subsequent View 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 View Connection Server in the group. All View configuration data can be backed up by backing up the LDAP directory instance.

Figure 3 shows two View Connection Servers operating as a group. To automatically use both View Connection Servers and support high-availability and scalability needs, deploy load balancing. This ensures that load is balanced evenly across the available View Connection Servers and that failed servers are automatically avoided. View Connection Server does not provide load-balancing functionality but works with standard third-party load-balancing solutions.

Figure 3. Multiple View Connection Servers

The load balancing requirements for View Connection Server are to support standard HTTP and HTTPS load-balancing with session affinity. Load balancing solutions for View 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 View 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 View Connection Servers in the group.

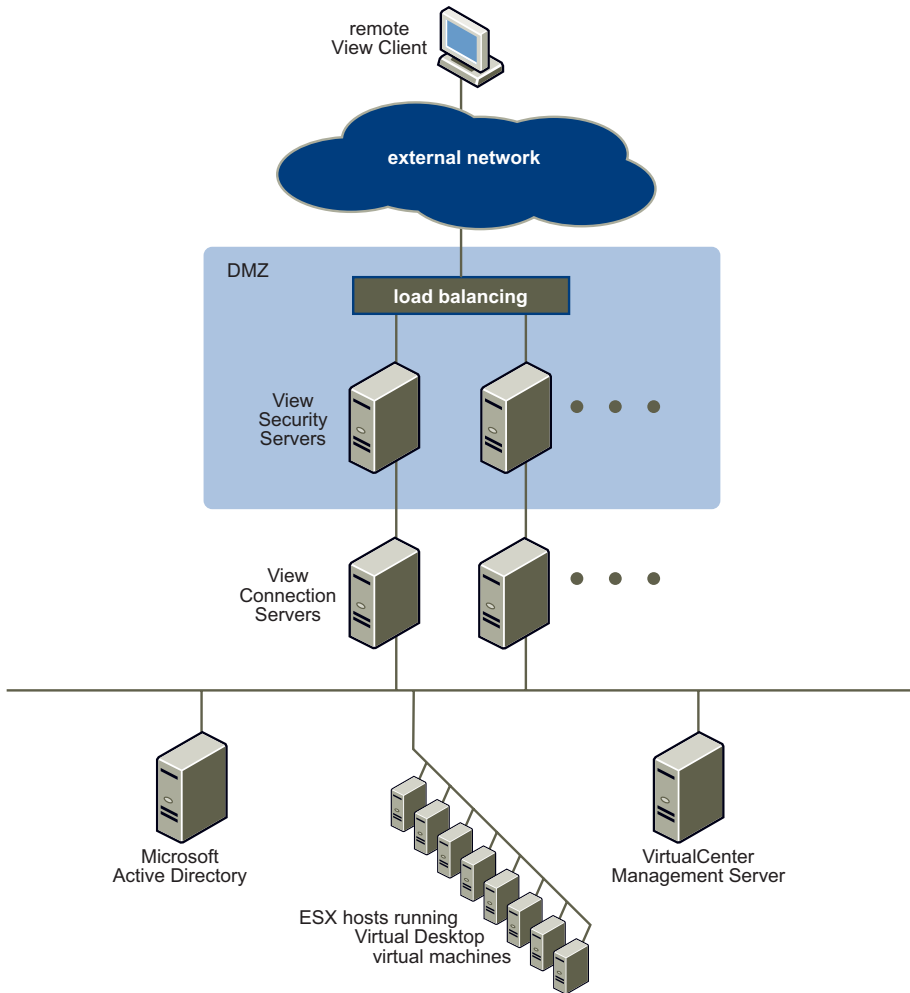
View Connection Server DMZ Deployment

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

View Connection Server functionality is split between servers in the secure network and the DMZ. View Connection Servers that operate in a DMZ are known as View Security Servers and are installed using the View Connection Server installer and specifying a Security Server instance type. View Security Servers in the DMZ operate with View Connection Servers (Standard or Replica) in the secure network.

Figure 4 shows a high-availability environment comprising two load-balanced View Security Servers in the DMZ working with two full View Connection Servers (Standard and Replica instance) in the secure network.

Figure 4. DMZ Deployment with Multiple View Connection Servers



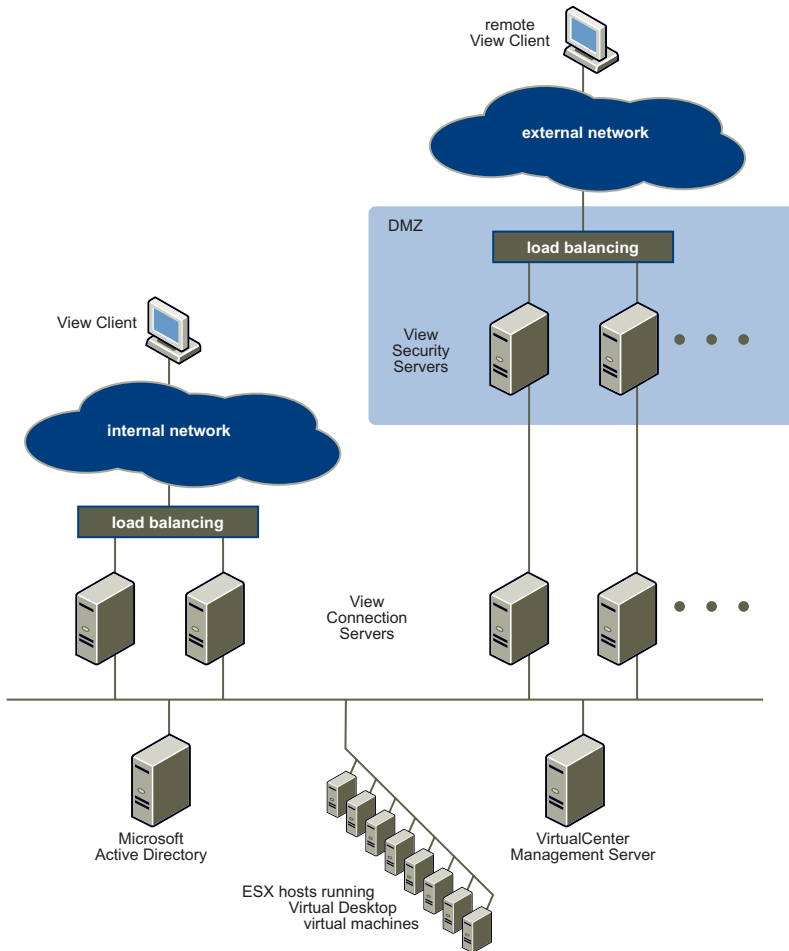
View Security Servers do not contain an LDAP configuration repository and do not access any authentication repositories (Active Directory or RSA Authentication Manager). When remote users connect using a View Security Server, they must successfully authenticate before a secure connection is established. 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 View Client and View Portal 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). View Security Servers do not need to be part of an Active Directory domain, and no communication occurs between View Security Servers and Active Directory.

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

[Figure 5](#) shows a more complex environment where four View 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



View Connection Server Components

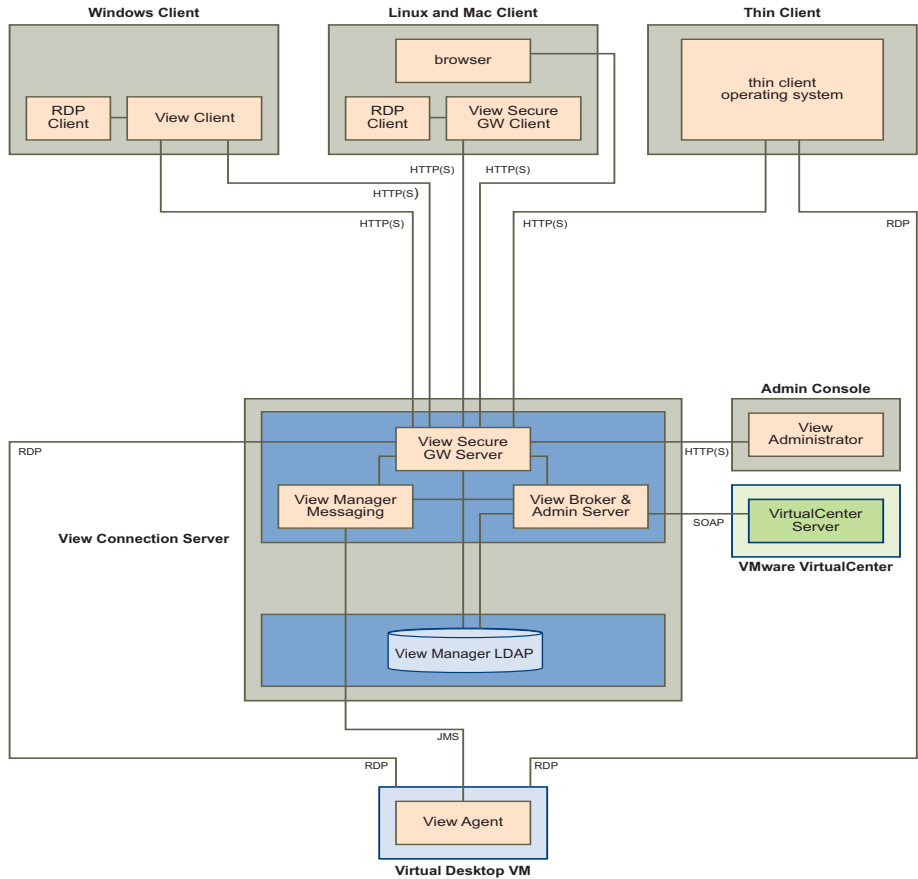
Figure 6 shows the View Connection Server components and their relationship with the other View components and the protocols used for communication between the components.

The following default TCP ports are used for each protocol:

- JMS – 4001
- HTTP – 80

- HTTPS – 443
- RDP – 3389
- SOAP – 80 or 443

Figure 6. View Components



View Broker

The View Connection Broker is the core of View Connection Server. It is responsible for all user interaction between the client (View Client, View Portal, and Thin Client) and the View Connection Server.

View Broker provides the following:

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

View 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.

View Secure Gateway Server

View Secure Gateway Server provides the server-side component for the secure HTTPS connection between the View Client (or View Secure Gateway Client) and the View Connection Server. After the user is authenticated, a secure HTTPS connection is established between the client and the View Connection Server. For a Windows client, this connection is initiated by the native Windows View Client. On Linux or Mac OS/X, it is initiated by the Java View 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 View 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 View Connection Server, firewall rules can be applied to each virtual desktop so that all RDP connections originate from a View Connection Server. This way, direct access to virtual desktops bypassing View Connection Server is not possible because View Connection Server acts as gatekeeper for all virtual desktop access. With VDM 2.1 and newer, the View 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 View Connection Server

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

View LDAP

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

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

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

View 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**
- **View component configuration entries used to store configuration settings**

When a Standard instance is installed during View 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 View LDAP is mainly maintained from View Administrator, although View Broker also manages some parts automatically.

When a View 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 View 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.

View Messaging

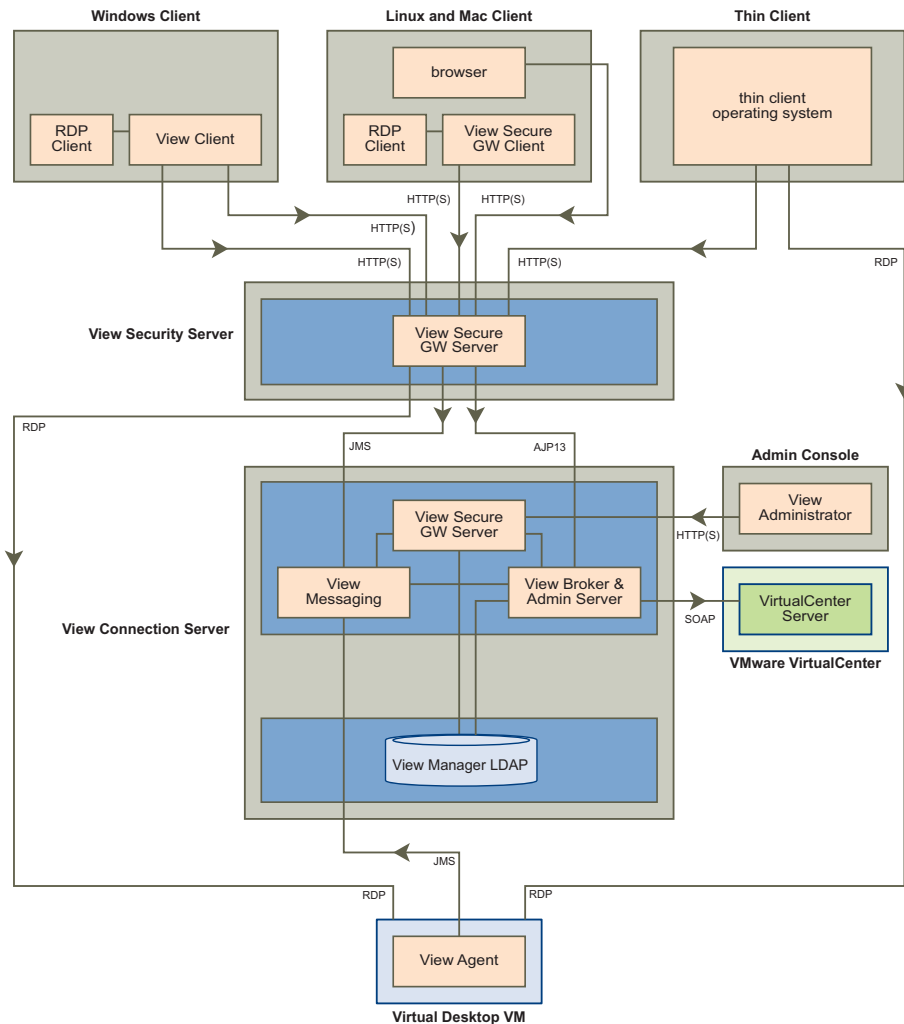
This component provides the messaging router for communication between View Connection Server components and between View Agent and View Connection Server. It supports the Java Message Service (JMS) API, which is used for messaging in View.

View Security Server

View Security Server is an instance type that is selected when View Connection Server is installed. It has a subset of the functionality of a full View Connection Server and is used in a DMZ deployment. [Figure 7](#) shows a View Security Server and shows the relationship with all other View 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

Figure 7. View Component Diagram with Security Server

For more information about View deployment within a DMZ, see [View Connection Server DMZ Deployment](#).

Deployment Options

VMware View offers several deployment options.

- Offline Desktop
- View Composer
- Unified Access

Offline Desktop

Offline Desktop offers mobile users the ability to check out a cloned instance of certain types of View desktop onto a local system such as a laptop. Once checked out, the local copy behaves like a standalone desktop system and can be used with or without a network connection; the desktop is now considered to be “offline”.

Once downloaded, Offline desktops behave in the same way as their online equivalents yet can take advantage of local resources; latency is minimized and performance is enhanced. The presence of a downloaded virtual machine has no effect on the existing operating system of the client system, which users can continue to utilize if they wish.

A consistent user experience is ensured through use of the View Client application for both online and offline sessions. In addition, users can disconnect from their offline desktop and then log in again without connecting to the View Connection Server.

Once network access is restored (or when the user is ready) the checked out VM can be:

- Backed up—the online system is updated with all new data and configurations, but the offline desktop remains checked out on the local system and the online lock remains in place.
- Rolled back—the offline desktop is discarded and the online lock is released. Future client connections will be directed to the online system until the desktop is checked out again
- Checked in—the offline desktop is uploaded to the online host and the online lock released. Future client connections will be directed to the online system until the desktop is checked out again.

The ability of users to download an online desktop for use on their local system is conferred through View entitlement and Offline VDI access policy. While a desktop is checked out, View administrators are still able to access the online system while monitoring the offline equivalent

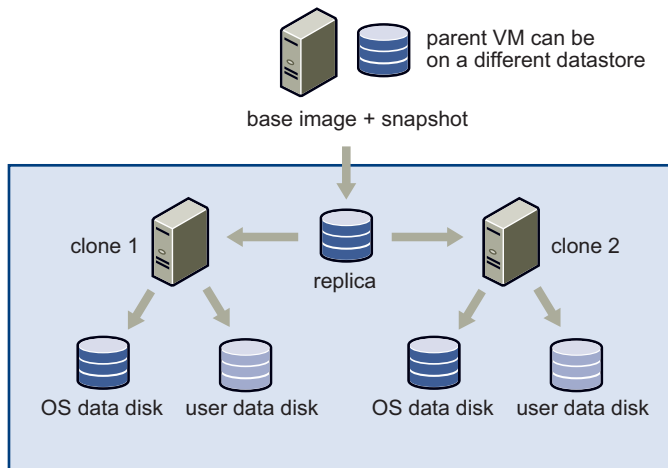
Linked Clones

The Linked Clone feature enables View administrators to clone and deploy multiple desktops from a single centralized base image, called a Master VM. Once the desktops have been created they remain indirectly linked to a snapshot residing on this master image.

The link is indirect because the first time one or more desktop clones are created, a uniquely identified copy of the Master VM—called a replica—is also created. All the desktop clones are anchored directly to the replica and not to the Master VM.

The Master VM can be updated or replaced without directly affecting the anchored clones and can therefore be viewed as a standalone VM. This set of relationships is illustrated in [Figure 8](#).

Figure 8. Master VM, Linked Replica, and Desktop Clones



Because all clones in this environment are connected to a common source, Linked Clone permits the centralized management of desktops while maintaining a seamless user experience. Tasks such as resetting each system to its default configuration, balancing storage, installing software and applying service packs are greatly accelerated by this type of deployment.

View administrators can simultaneously update (or change) the operating systems of all desktops, install or update client applications, or modify the desktop hardware settings by carrying out these activities on the Master VM and then anchoring the desktop clones to a new snapshot of this configuration. This action is called desktop recomposition.

NOTE Desktop clones can also be anchored to a completely different Master VM.

Administrators can also return the OS data of each desktop, which may have expanded through ongoing usage, to its original state (that of the Master VM) by carrying out an action called desktop refresh.

The administrative interface provided by View delivers a high-level overview of what actions are being carried out. Policies can control what actions are executed and at what time in order to minimize disruption to the user base. Connected users can be notified with custom messages if an update that will affect their session is about to take place.

Unified Access

Large enterprises use a mix of physical PCs, server-based desktops or applications that are published using terminal services; virtual desktops; and blade PCs. Users requiring access to more than one platform must use several different interfaces. Unified Access enables View to provide a unified interface through which users can access their desktops being delivered by multiple back-ends.

The desktop deployment paradigm in large enterprises is a mix of various back-end platforms. View support for back-end platforms has been limited to virtual machines managed by the VC server. Unified Access enables View to deliver and manage virtual machines that are not managed by the VC server.

The term “desktop source” refers to an individual desktop resource provided to pool users. This can be a provisioned or non-provisioned virtual machine, a terminal server session or a physical computer.

Unified Access supports different desktop delivery models which characterize the way a desktop is created, entitled, delivered, and used. The desktop delivery models supported by View are:

- **Individual Desktop** - a desktop that allows a single, pre-existing back-end source and can be entitled to many users or groups.
- **Manual Pool** - a manually-provisioned pool of desktop sources that allows multiple users to be mapped to multiple desktops.

- **Automated Pool** - an automatically provisioned pool of desktop sources that allows multiple users to be mapped to multiple desktops.
- **Terminal Server Pool** - a pool of terminal server (TS) desktop sources served by one or more terminal servers. A terminal server desktop source can deliver multiple desktops.

Administrators should deploy a roaming profile solution to enable user settings and personalization to be propagated to the currently accessed desktop.

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 View Portal 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 View. Also known as the View Administrator.

agent

See [“VMware View Agent.”](#)

B

broker

Also known as a connection broker. The View Connection Server is a type of connection broker. *See also* [“VMware View Connection Server.”](#)

C **client**

See “[VMware View Client.](#)”

connection broker

A server that allows connections between remote users and virtual desktops and provides authentication and session management. The View Connection Server is a type of connection broker. *See also “[VMware View Connection Server.](#)”*

connection server

See “[VMware View 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 View 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 View 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 View Agent**
Installed on the guest, the View Agent enables communication between the desktop virtual machine, the View Connection Server, and end users who access virtual desktops by using View View Portal or View Clients.

VMware View Client

A Windows-based application used for accessing virtual desktops.

VMware View Connection Server

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

VMware View Portal

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 View Portal.

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.