VMware View-Architekturplanungsanleitung

View 4.0.1

View Manager 4.0.1

View Composer 2.0.0

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-000241-02

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Informationen zu diesem Buch

Die *VMware View-Architekturplanungsanleitung* bietet eine Einführung in VMware® View, eine Beschreibung der wichtigsten Funktionen und Bereitstellungsoptionen und eine Übersicht, wie VMware View-Komponenten in einer Produktionsumgebung üblicherweise eingerichtet werden. Damit Sie Ihre VMware View-Installation schützen können, werden in diesem Buch auch Sicherheitsfunktionen behandelt. Diese Anleitung liefert Antworten auf die folgenden Fragen:

- Können mit VMware View die Probleme gelöst werden, die gelöst werden sollen?
- Kann eine VMware View-Lösung kostengünstig in Ihrem Unternehmen implementiert werden?

Zielgruppe

Diese Anleitung richtet sich u. a. an IT-Entscheider, -Architekten, -Administratoren, die sich mit den Komponenten und Funktionsmöglichkeiten von VMware View vertraut machen möchten. Anhand dieser Informationen können Architekten und Planer bestimmen, ob VMware View die Anforderungen ihres Unternehmens an eine effiziente und sichere Bereitstellung von Windows-Desktops und -Anwendungen für die Endbenutzer erfüllt. Die Beispielarchitektur soll die Hardwareanforderungen und den Einrichtungsaufwand einer umfangreichen Bereitstellung von VMware View veranschaulichen.

Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Bitte senden Sie Ihre Kommentare und Vorschläge an docfeedback@vmware.com.

Technischer Support und Schulungsressourcen

Die folgenden technischen Support-Ressourcen stehen Ihnen zur Verfügung. Die neueste Version dieses Buchs und andere Bücher finden Sie unter http://www.vmware.com/de/support/pubs.

Online- und telefonischer Support

Um beim Online-Support technische Unterstützung anzufordern, Ihre Produkt- und Vertragsdaten abzurufen und Produkte zu registrieren, besuchen Sie http://www.vmware.com/de/support.

Kunden mit entsprechenden Support-Verträgen erhalten über den telefonischen Support schnelle Hilfe bei Problemen der Prioritätsstufe 1. Besuchen Sie http://www.vmware.com/de/support/phone_support.html.

Support-Angebote

Um herauszufinden, wie VMware mithilfe seines Support-Angebots Ihre geschäftlichen Anforderungen erfüllen kann, besuchen Sie http://www.vmware.com/de/support/services.

VMware Professional Services

Die VMware Education Services-Kurse umfassen umfangreiche praktische Übungen, Fallbeispiele und Kursmaterialien, die bei der praktischen Arbeit als Referenz dienen. Die Kurse werden als Vor-Ort-Schulungen, Schulungen mit Kursleiter und als Online-Kurse bereitgestellt. Für Vor-Ort-Pilotprogramme und die Implementierung von empfohlenen Vorgehensweisen stellen die VMware Consulting Services Angebote zur Bewertung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung bereit. Unter http://www.vmware.com/de/services finden Sie Informationen zu Schulungen, Zertifizierungsprogrammen und Beratungsservices.

Einführung in VMware View 1

VMware View ermöglicht IT-Abteilungen die Ausführung virtueller Desktops im Rechenzentrum und stellt Mitarbeitern Desktops als verwalteten Dienst zur Verfügung. Endbenutzer erhalten eine vertraute, persönlich angepasste Umgebung, auf die sie auf einer Vielzahl von Geräten überall im Unternehmen oder von zu Hause aus zugreifen können. Administratoren werden dank Desktop-Daten im Rechenzentrum zentrale und effiziente Steuerungs- und Sicherheitsfunktionen geboten.

Dieses Kapitel behandelt die folgenden Themen:

Vorteile von VMware View

Das Verwalten von Unternehmens-Desktops mit VMware View bietet zahlreiche Vorteile: höhere Zuverlässigkeit, Sicherheit, Hardware-Unabhängigkeit und mehr Komfort.

Zuverlässigkeit und Sicherheit

Virtuelle Desktops können durch eine Integration mit VMware vSphere und Virtualisierung von Server-, Speicher- und Netzwerkressourcen zentral verwaltet werden. Das Platzieren von Desktopbetriebssystemen und Anwendungen auf einem Server im Rechenzentrum bietet die folgenden Vorteile:

- Der Zugriff auf Daten kann mit einfachen Mitteln eingeschränkt werden. Das Kopieren vertraulicher Daten auf den Heimcomputer eines Remote-Mitarbeiters kann verhindert werden.
- Datensicherungen können geplant werden, ohne berücksichtigen zu müssen, dass die Systeme der Endbenutzer ggf. ausgeschaltet sind.
- Virtuelle Desktops, die in einem Rechenzentrum gehostet werden, unterliegen nur kurzen oder keinen Ausfallzeiten. Virtuelle Maschinen können sich in hoch verfügbaren VMware-Server-Clustern befinden.

Virtuelle Desktops können sich auch mit physischen Back-End-Systemen und Servern mit Windows-Terminaldienste verbinden.

Komfort

Das PC-over-IP-Protokoll von VMware View bietet eine Endbenutzerumgebung, die der auf einem aktuellen physischen PC entspricht:

- In lokalen Netzwerken (LANs) ist die Anzeige schneller und schärfer als bei herkömmlichen Remote-Anzeigen.
- In Weitbereichsnetzen (WANs) kann das Protokoll längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können.

Verwaltbarkeit

Die Bereitstellung von Desktops für Endbenutzer erfolgt schnell. Anstatt Anwendungen nacheinander auf den physischen PCs der einzelnen Endbenutzer zu installieren, können sich die Endbenutzer mit einem virtuellen Desktop mit Anwendungen verbinden. Endbenutzer können unabhängig von Gerät und Standort auf denselben virtuellen Desktop zugreifen.

Das Hosten virtueller Desktops mit VMware vSphere bietet folgende Vorteile:

- Verwaltungsaufgaben und Routinearbeiten werden reduziert. Administratoren können Patches und Upgrades für Anwendungen und Betriebssysteme aufspielen, ohne sich an die physischen PCs der Benutzer begeben zu müssen.
- Auch die Speicherverwaltung wird mit VMware vSphere vereinfacht, da Sie Laufwerke und Dateisysteme virtualisieren können, um die Verwaltung getrennter Speichergeräte zu vermeiden.

Hardware-Unabhängigkeit

Virtuelle Maschinen sind unabhängig von der Hardware. Da ein View-Desktop auf einem Server im Rechenzentrum ausgeführt wird und der Zugriff nur über ein Clientgerät erfolgt, kann ein View-Desktop mit Betriebssystemen arbeiten, die ggf. nicht mit der Hardware des Clientgeräts kompatibel sind.

Obgleich Windows Vista beispielsweise nur auf für Vista aktivierten PCs ausgeführt werden kann, können Sie Windows Vista in einer virtuellen Maschine installieren und diese virtuelle Maschine auf einem PC nutzen, der nicht für Vista aktiviert ist. Virtuelle Desktops können auf PCs, Thin Clients und PCs ausgeführt werden, die als Thin Clients betrieben werden.

VMware View-Funktionen

Die benutzerfreundlichen Funktionen von VMware View bieten Sicherheit und ermöglichen eine zentrale Steuerung und Skalierbarkeit.

Mithilfe der folgenden Funktionen wird dem Endbenutzer eine vertraute Umgebung bereitgestellt:

- Die Druckausgabe eines virtuellen Desktops kann über einen beliebigen lokalen oder Netzwerkdrucker erfolgen, der auf dem Clientgerät definiert ist. Die virtuelle Druckerfunktion beseitigt Kompatibilitätsprobleme und erfordert nicht die Installation zusätzlicher Druckertreiber in einer virtuellen Maschine.
- Mehrere Monitore können eingesetzt werden. Dank der PCoIP-Unterstützung mehrerer Monitore können Sie die Anzeigeauflösung und -drehung für jeden Monitor getrennt einstellen.
- Zugriff auf USB-Geräte und andere Peripheriegeräte, die am lokalen Gerät angeschlossen sind, auf dem Ihr virtueller Desktop angezeigt wird.

VMware View bietet u. a. die folgenden Sicherheitsfunktionen:

- Zweistufige RSA SecurID-Authentifizierung oder Smartcards zur Anmeldung.
- Einrichtung eines SSL-Tunnels zum Sicherstellen, dass sämtliche Verbindungen vollständig verschlüsselt sind
- VMware High Availability zum Hosten von Desktops und Sicherstellen eines automatischen Failovers

Die folgenden Funktionen ermöglichen eine zentrale Verwaltung:

- Microsoft Active Directory zum Verwalten des Zugriffs auf virtuelle Desktops und von Richtlinien
- Die webbasierte Verwaltungskonsole zum ortsunabhängigen Verwalten virtueller Desktops
- Eine Vorlage bzw. ein Master-Image zum schnellen Erstellen und Bereitstellen von Desktops
- Übertragung von Updates und Patches auf virtuelle Desktops ohne Beeinträchtigung von Benutzereinstellungen, Daten oder Voreinstellungen

Skalierbarkeitsfunktionen hängen von der VMware-Virtualisierungsplattform zum Verwalten von sowohl Desktops als auch Servern ab:

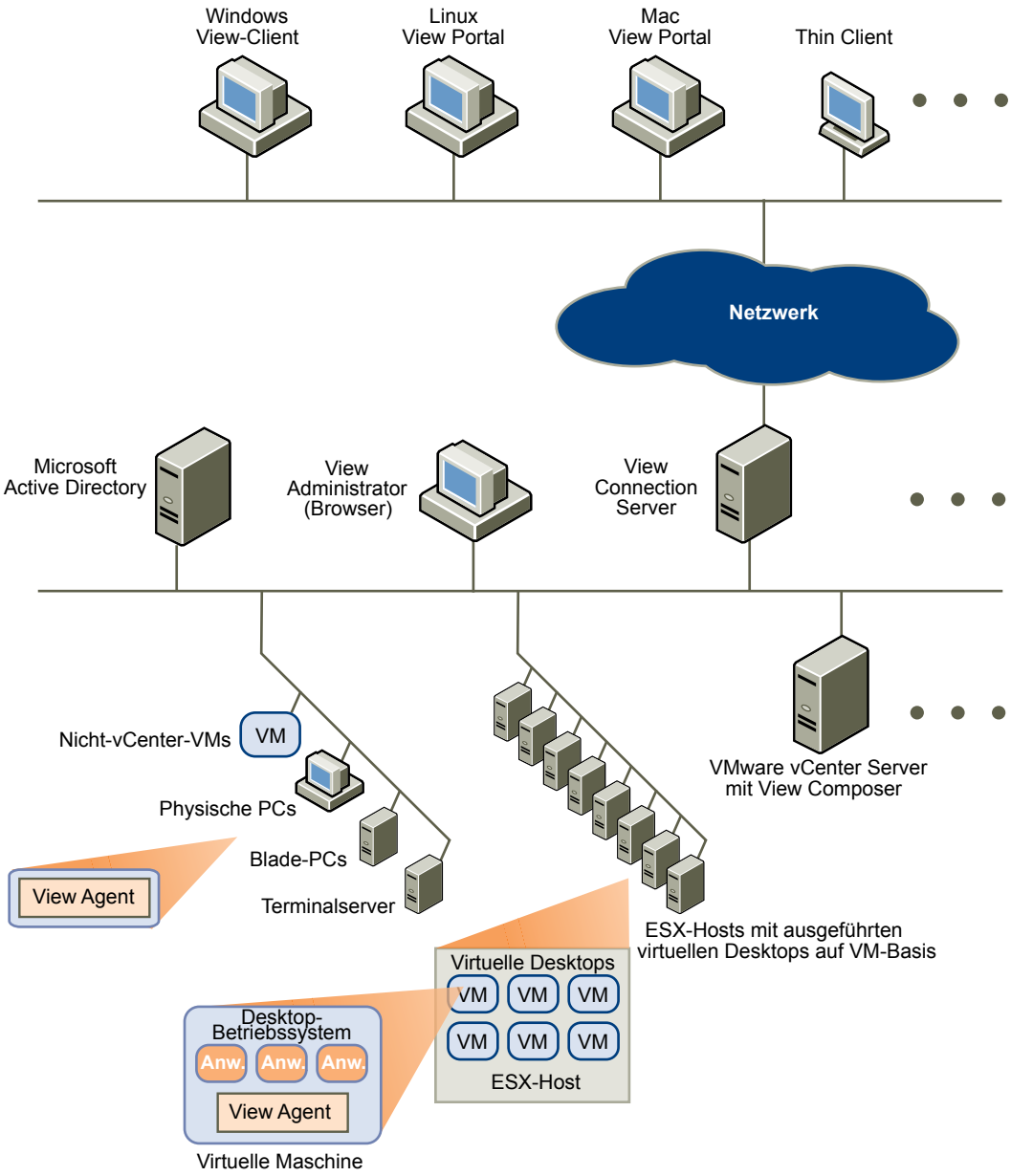
- Integration mit VMware vSphere zum Erzielen kostengünstiger Dichten, hoher Verfügbarkeitsgrade und einer erweiterten Steuerung der Ressourcenzuweisung für Ihre virtuellen Desktops
- Konfiguration von View Connection Server zum Vermitteln von Verbindungen zwischen Endbenutzern und den virtuellen Desktops, auf die sie zugreifen dürfen
- View Composer zum schnellen Erstellen von Desktop-Images, die virtuelle Festplatten mit einem Master-Image gemeinsam nutzen. Verwendung verknüpfter Klone dergestalt, dass Festplattenspeicher eingespart und die Update- und Patch-Verwaltung des Betriebssystems vereinfacht wird

Zusammenspiel der VMware View-Komponenten

Endbenutzer starten View Client oder verwenden View Portal zur Anmeldung an View Connection Server. Dieser Server, der mit Windows Active Directory integriert ist, bietet einen Zugriff auf einen virtuellen Desktop, der auf einem Server mit VMware ESX, einem Blade- oder physischen PC oder Server mit Windows-Terminaldienste gehostet wird.

Abbildung 1-1 zeigt die Beziehung zwischen den Hauptkomponenten einer Bereitstellung von VMware View.

Abbildung 1-1. Allgemeines Beispiel einer VMware View-Umgebung



Clientgeräte

Ein Hauptvorteil von VMware View ist, dass Desktops dem Endbenutzer unabhängig von Gerät oder Standort folgen. Benutzer können auf ihren individuell angepassten virtuellen Desktop auf einem Firmen-Laptop, ihrem Heim-PC, einem Thin Client-Gerät oder einem Macintosh zugreifen.

Auf Laptops und Windows-PCs öffnen die Benutzer View Client zum Anzeigen ihres View-Desktops. Auf einem Macintosh oder Linux-PC öffnen die Benutzer einen Web-Browser und View Portal zum Anzeigen ihres View-Desktops. Windows-Geräte können auch View Portal nutzen, wenngleich bestimmte Funktionen dann nicht unterstützt werden.

Thin Client-Geräte verwenden View Thin Client-Software und können so konfiguriert werden, dass die einzige Anwendung, die Benutzer direkt auf dem Gerät starten können, View Thin Client ist. Durch Umwandeln eines älteren PC in einen Thin Client-Desktop kann die Lebensdauer der Hardware um drei bis fünf Jahre verlängert werden. Beim Verwenden von VMware View auf einem Thin Client-Desktop können Sie beispielsweise ein neueres Betriebssystem wie Windows Vista auf älterer Desktop-Hardware verwenden.

View Connection Server

Diese Software dient als Vermittler für Clientverbindungen. View Connection Server authentifiziert Benutzer mittels Windows Active Directory und leitet die Anforderung an den/die entsprechende(n) virtuelle Maschine, physischen oder Blade-PC oder Server mit Windows-Terminaldienste weiter.

View Connection Server bietet die folgenden Verwaltungsfunktionen:

- Authentifizieren von Benutzern
- Erteilen von Benutzerberechtigungen für bestimmte Desktops und Pools
- Verwalten von Desktop-Sitzungen
- Einrichten sicherer Verbindungen zwischen Benutzern und Desktops
- Aktivieren der einmaligen Anmeldung
- Festlegen und Aktivieren von Richtlinien

Innerhalb der Firewall des Unternehmens installieren und konfigurieren Sie eine Gruppe mit zwei oder mehr Instanzen von View Connection Server. Deren Konfigurationsdaten werden in einem eingebetteten LDAP-Verzeichnis gespeichert und an die Mitglieder der Gruppe repliziert.

Außerhalb der Firewall des Unternehmens können Sie im Umkreisnetzwerk (DMZ) View Connection Server als Sicherheitsserver installieren und konfigurieren. Sicherheitsserver im Umkreisnetzwerk, die mit View Connection Server-Instanzen innerhalb der Firewall des Unternehmens kommunizieren, bieten eine eingeschränkte Funktionalität und müssen nicht in einer Active Directory-Domäne vorhanden sein.

View Connection Server wird auf einem Server mit Windows Server 2003 oder bevorzugt in einer virtuellen VMware-Maschine installiert.

View Client

Die Clientsoftware für den Zugriff auf View-Desktops wird entweder auf einem Windows-PC als systemeigene Windows-Anwendung oder einem Thin Client ausgeführt, wenn Sie mit View Client für Linux arbeiten.

Nach der Anmeldung treffen Benutzer eine Auswahl in einer Liste virtueller Desktops, die sie nutzen dürfen. Für die Autorisierung können Active Directory-Anmeldedaten, ein Benutzerprinzipalname (UPN), eine Smartcard-PIN oder ein RSA SecurID-Token erforderlich sein.

Ein Administrator kann View Client so konfigurieren, dass Endbenutzer ein Anzeigeprotokoll auswählen können. Zu den Protokollen zählen PCoIP, Microsoft RDP und HP RGS (für View-Desktops, die auf HP Blades gehostet werden). Das Anzeigeprotokoll PCoIP steht nun in VMware View 4 zur Verfügung. Geschwindigkeit und Anzeigequalität von PCoIP können es mit einem physischen PC aufnehmen.

View Client with Offline Desktop ist eine Version von View Client, die zur Unterstützung der experimentelle Offline Desktop-Funktion erweitert wurde. Diese Funktion ermöglicht Endbenutzern das Herunterladen virtueller Maschinen und deren Nutzung auf ihren lokalen Systemen.

Abhängig vom verwendeten View Client sind unterschiedliche Funktionen verfügbar. Der Schwerpunkt in diesem Handbuch liegt auf View Client und View Portal für Microsoft Windows. Die folgenden Arten von Clients werden in diesem Handbuch nicht im Detail beschrieben:

- View Portal für Linux (experimentell) und View Portal für Mac OS X (experimentell).
- View Client für Linux, nur über zertifizierte Partner erhältlich.

- Verschiedene Drittanbieterclients, nur über zertifizierte Partner erhältlich.
- View Open Client, der das VMware-Partnerzertifizierungsprogramm unterstützt. View Open Client ist kein offizieller View-Client und wird daher als solcher nicht unterstützt.

View Portal

Auf einem Macintosh, Windows- oder Linux-PC können Endbenutzer einen Web-Browser und View Portal zum Anzeigen ihres View-Desktops öffnen. Bei dieser webbasierten Version von View Client wird die erforderliche View-Software auf einem Clientgerät installiert, doch einige Erweiterungen, z. B. für den Anschluss von USB-Geräten, werden ggf. nicht installiert.

Zum Verwenden von View Portal müssen Endbenutzer einen Browser wie Firefox, Internet Explorer oder Safari öffnen und die URL einer View Connection Server-Instanz eingeben. View Portal fordert Benutzer zum Angeben von Berechtigungen für die Installation der benötigten View Client-Komponenten auf. Auf Linux-Clients erfordert View Portal `rdesktop` zum Anzeigen virtueller Desktops. Unter Mac OS/X erfordert View Portal den Microsoft Remotedesktopverbindung-Client für Mac zum Anzeigen virtueller Desktops.

View Agent

Sie installieren den View Agent-Dienst auf allen virtuellen Maschinen, physischen Systemen und Servern mit Terminaldienste, die Sie als Quellen für View-Desktops nutzen. Dieser Agent kommuniziert mit View Client, um Funktionen wie Verbindungsüberwachung, eine virtuelle Druckfunktion und Zugriff auf lokal angeschlossene USB-Geräte bereitzustellen.

Wenn die Desktop-Quelle eine virtuelle Maschine ist, installieren Sie den View Agent-Dienst zuerst auf dieser virtuellen Maschine und nutzen anschließend die virtuelle Maschine als Vorlage bzw. übergeordnetes Element verknüpfter Klone. Wenn Sie basierend auf dieser virtuellen Maschine einen Pool erstellen, wird der Agent automatisch in allen virtuellen Desktops installiert.

Sie können den Agent mit einer Option für die einmalige Anmeldung installieren. Bei der einmaligen Anmeldung werden die Benutzer nur zur Anmeldung aufgefordert, wenn sie sich mit View Connection Server verbinden, und nicht erneut aufgefordert, wenn sie eine Verbindung mit einem virtuellen Desktop herstellen.

View Administrator

Diese webbasierte Anwendung ermöglicht Administratoren das Konfigurieren von View Connection Server, das Bereitstellen und Verwalten von View-Desktops, das Steuern der Benutzerauthentifizierung und das Beheben von Problemen der Endbenutzer.

Bei Installation einer View Connection Server-Instanz wird die Anwendung View Administrator ebenfalls installiert. Diese Anwendung ermöglicht Administratoren das ortsunabhängige Verwalten von View Connection Server-Instanzen, ohne eine Anwendung auf ihrem lokalen Computer installieren zu müssen.

View Composer

Sie installieren diesen Softwaredienst in einer vCenter Server-Instanz, die zum Verwalten virtueller Maschinen dient. View Composer kann anschließend einen Pool verknüpfter Klone anhand einer angegebenen übergeordneten virtuellen Maschine erstellen, wodurch die Speicherkosten um bis zu 90 % reduziert werden.

Jeder verknüpfte Klon fungiert als unabhängiger Desktop (mit eindeutigem/r Hostnamen/IP-Adresse), aber dennoch benötigt der verknüpfte Klon wesentlich weniger Speicherplatz, da er mit der übergeordneten virtuellen Maschine ein Basis-Image gemeinsam nutzt.

Da Desktop-Pools auf Grundlage verknüpfter Klone ein Basis-Image gemeinsam nutzen, können Sie Updates und Patches schnell bereitstellen, indem nur die übergeordnete virtuelle Maschine aktualisiert wird. Die Einstellungen, Daten und Anwendungen der Endbenutzer sind nicht betroffen.

vCenter Server

Dieser Dienst dient zur zentralen Verwaltung von VMware ESX-Servern, die mit einem Netzwerk verbunden sind. vCenter Server, zuvor VMware VirtualCenter genannt, bildet die Zentrale für die Konfiguration, Bereitstellung und Verwaltung virtueller Maschine im Rechenzentrum.

Zusätzlich zur Verwendung dieser virtuellen Maschinen als Quellen von View-Desktop-Pools können Sie virtuelle Maschinen zum Hosten der Serverkomponenten von VMware View nutzen, einschließlich Connection Server-Instanzen, Active Directory-Servern und vCenter Server-Instanzen.

Sie können View Composer auf demselben Server wie vCenter Server installieren, um Desktop-Pools auf Basis verknüpfter Klone zu erstellen. vCenter Server verwaltet anschließend das Zuweisen der virtuellen Maschinen zu physischen Servern und Datenspeichern und verwaltet die Zuweisung von CPU- und Arbeitsspeicherressourcen zu virtuellen Maschinen.

vCenter Server wird auf einem Server mit Windows Server 2003 oder bevorzugt in einer virtuellen VMware-Maschine installiert.

Planen einer umfassenden Benutzerumgebung

2

VMware View bietet die vertraute, individuell angepasste Desktop-Umgebung, die Endbenutzer erwarten. Endbenutzer können auf an ihren lokalen Computer angeschlossene USB- und andere Geräte zugreifen, Dokumente an beliebige Drucker senden, die von ihrem lokalen Computer erkannt werden, eine Authentifizierung mithilfe von Smartcards durchführen und mehrere Anzeigemonitore verwenden.

VMware View bietet viele Funktionen, die Sie ggf. Ihren Endbenutzern zur Verfügung stellen möchten. Bevor Sie entscheiden, welche Funktionen verwendet werden sollen, müssen Sie sich jedoch mit den Einschränkungen der einzelnen Funktionen vertraut machen.

Dieses Kapitel behandelt die folgenden Themen:

Übersicht der unterstützten Funktionen

Die meisten Funktionen wie der Zugriff auf lokale USB-Geräte, die virtuelle Druckfunktion, Wyse Multimedia Redirection (MMR) und die Microsoft RDP- und PCoIP-Anzeigeprotokolle werden unter den meisten Clientbetriebssystemen unterstützt.

Halten Sie sich bei der Planung der Anzeigeprotokolle und Funktionen, die Sie Ihren Endbenutzern zur Verfügung stellen möchten, an Tabelle 2-1, um zu bestimmen, welche Clientbetriebssysteme die jeweilige Funktion unterstützen.

Tabelle 2-1. Von 32-Bit-Windows-Clients unterstützte Funktionen

Funktion	Windows 2000	Windows XP Pro	Windows XP Home	Vista Business SP1, SP2	Vista Ultimate SP1, SP2	Vista Enterprise SP2
USB-Anschluss		X	X	X	X	X
RDP-Anzeigeprotokoll	X	X	X	X	X	X
PCoIP-Anzeigeprotokoll		X	X	nur SP2	nur SP2	X

Tabelle 2-1. Von 32-Bit-Windows-Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows 2000	Windows XP Pro	Windows XP Home	Vista Business SP1, SP2	Vista Ultimate SP1, SP2	Vista Enterprise SP2
HP RGS-Anzeigeprotokoll		X		X	nur SP2	X
Wyse MMR		X	X		nur SP1	
Virtuelle Druckfunktion	X	X	X		nur SP1	
Offline Desktop		X				

Hinweis Die Anzeigeprotokolle HP RGS und PCoIP stehen nicht zur Verfügung, wenn Sie Web Portal anstelle des systemeigenen View Client verwenden. Informationen zu Clienthardwareanforderungen und View-Desktopanforderungen für PCoIP finden Sie in Abschnitt „VMware View mit PCoIP“, auf Seite 17.

Wie Tabelle 2-2 zeigt, sind die Optionen für Linux- und Macintosh-Clients eingeschränkt, die experimentell über Web Portal unterstützt werden.

Tabelle 2-2. Von Web Portal unterstützte Funktionen für Mac OS X- und 32-Bit-Linux-Clients

Funktion	Red Hat Enterprise Linux 5.1	SUSE Linux Enterprise Desktop 10	Ubuntu Linux 8.04	Mac OS X (10.5)	Mac OS X (10.4)
USB-Anschluss					
RDP-Anzeigeprotokoll	X	X	X	X	X
PCoIP-Anzeigeprotokoll					
HP RGS-Anzeigeprotokoll					
Wyse MMR					
Virtuelle Druckfunktion					
Offline Desktop					

Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für VMware View-Bereitstellungen. Die Funktionen, die für die einzelnen Thin Client-Geräte verfügbar sind, werden vom Hersteller und Modell sowie der vom jeweiligen Unternehmen gewählten Konfiguration bestimmt. Informationen zu den Herstellern und Modellen von Thin Client-Geräten finden Sie auf der VMware-Website unter *Thin Client Compatibility Guide* (Thin Client-Kompatibilitätsleitfaden).

Auswählen eines Anzeigeprotokolls

Ein Anzeigeprotokoll bietet Endbenutzern eine grafische Oberfläche für einen View-Desktop, der sich im Rechenzentrum befindet. Zur Auswahl stehen Microsoft RDP (Remote Desktop Protocol), HP RGS für physische HP-Computer und PCoIP (PC-over-IP).

Sie können Richtlinien festlegen, um zu steuern, welches Protokoll verwendet werden soll, oder die Endbenutzer das Protokoll auswählen lassen, wenn sie sich am Desktop anmelden.

VMware View mit PCoIP

PCoIP ist ein neues überaus leistungsfähiges Remote-Anzeigeprotokoll, das von VMware bereitgestellt wird. Dieses Protokoll ist verfügbar für View-Desktops, deren Quelle virtuelle Maschinen, Teradici-Clients und physische Computer mit für Teradici aktivierten Hostkarten sind.

PCoIP kann längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können. PCoIP ist für die Übermittlung von Bild-, Audio- und Videoinhalten für viele verschiedene Benutzer im LAN oder WAN optimiert. PCoIP bietet die folgenden Funktionen:

- Sie können bis zu vier Monitore einsetzen und die Auflösung jedes Monitors (bis zu 1920 x 1200) einzeln pro Anzeige festlegen.
- Sie können Text zwischen dem lokalen System und dem View-Desktop kopieren und einfügen, nicht aber Systemobjekte wie Ordner und Dateien zwischen Systemen.
- Sie können die von Adobe Flash belegte Bandbreite konfigurieren, um die allgemeine Web-Browser-Umgebung zu optimieren und andere Anwendungen schneller reagieren zu lassen.
- PCoIP unterstützt 32-Bit-Farben.
- PCoIP unterstützt die 128-Bit-Verschlüsselung.
- PCoIP unterstützt die AES-Verschlüsselung (Advanced Encryption Standard), die standardmäßig aktiviert ist.
- Sie können dieses Protokoll zusammen mit dem virtuellen privaten Netzwerk Ihres Unternehmens verwenden.

PCoIP hat die folgenden Einschränkungen:

- Das Betriebssystem auf dem View-Desktop muss Windows XP Professional SP 2 oder 3 bzw. Windows Vista SP 1 oder 2 sein.
- PCoIP unterstützt keine Smartcards.
- PCoIP kann nicht von Benutzern verwendet werden, die über View Portal auf ihre virtuellen Desktops zugreifen.

Folgende Clienthardwareanforderungen müssen erfüllt werden:

- Prozessorgeschwindigkeit: 800 MHz oder höher
- x86-basierter Prozessor mit SSE2-Erweiterungen

View-Clients, die PCoIP verwenden, können sich mit View-Sicherheitsservern verbinden, aber PCoIP-Sitzungen mit dem virtuellen Desktop ignorieren den Sicherheitsserver. PCoIP nutzt das User Datagram Protocol (UDP) für das Streaming von Audio und Video. Sicherheitsserver unterstützen jedoch nur TCP.

Microsoft RDP

Remote Desktop Protocol (RDP) entspricht dem Protokoll, das viele Benutzer bereits nutzen, um vom ihrem Heimcomputer aus auf ihren Firmencomputer zuzugreifen. RDP bietet Zugriff auf sämtliche Anwendungen, Dateien und Netzwerkressourcen auf einem Remote-Computer.

Microsoft RDP ermöglicht Folgendes:

- Sie können den Modus für die Anzeige auf mehreren Bildschirmen verwenden.
- Sie können Text zwischen dem lokalen System und dem View-Desktop kopieren und einfügen, nicht aber Systemobjekte wie Ordner und Dateien zwischen Systemen.

- Sie können die von Adobe Flash belegte Bandbreite konfigurieren, um die allgemeine Web-Browser-Umgebung zu optimieren und andere Anwendungen schneller reagieren zu lassen.
- RDP unterstützt 32-Bit-Farben.
- RDP unterstützt die 128-Bit-Verschlüsselung.
- Mithilfe dieses Protokolls können Sie im Umkreisnetzwerk (DMZ) des Unternehmens sichere, verschlüsselte Verbindungen mit einem View-Sicherheitsserver herstellen.

HP RGS-Protokoll

RGS ist ein Anzeigeprotokoll von HP, mit dem Benutzer über ein Standardnetzwerk auf einen Desktop auf einem physischen Remote-Computer zugreifen können.

Sie können HP RGS als Anzeigeprotokoll bei der Verbindungsherstellung mit HP Blade PCs, HP Workstations und HP Blade Workstations verwenden. Verbindungen zu virtuellen Maschinen, die auf VMware ESX-Servern ausgeführt werden, werden nicht unterstützt.

HP RGS ermöglicht Folgendes:

- Sie können den Modus für die Anzeige auf mehreren Bildschirmen verwenden.
- Sie können die von Adobe Flash belegte Bandbreite konfigurieren, um die allgemeine Web-Browser-Umgebung zu optimieren und andere Anwendungen schneller reagieren zu lassen.

HP RGS gehört nicht zum Lieferumfang von VMware View, und VMware bietet keine Lizenzen für HP RGS an. Wenden Sie sich an HP, um eine Kopie von HP RGS, Version 5.2.5, zur Verwendung mit VMware View zu lizenzieren. Informationen zur Installation und Konfiguration von HP RGS-Komponenten finden Sie in der HP RGS-Dokumentation unter http://www.hp.com.

Zugreifen auf an einen lokalen Computer angeschlossene USB-Geräte

Administratoren können einen View-Desktop so konfigurieren, dass USB-Geräte wie Flash-Laufwerke VoIP-Geräte und Drucker genutzt werden können. Diese Funktion wird als USB-Umleitung bezeichnet.

Bei Aktivierung dieser Funktion stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, in einem Menü in View Client zur Verfügung. Über das Menü können Sie die Geräte anschließen und trennen.

Zu USB-Geräten, die nicht im Menü angezeigt werden, aber in einem View-Desktop verfügbar sind, zählen Smartcard-Leser sowie Tastaturen und Zeigegeräte. Der View-Desktop und der lokale Computer verwenden diese Geräte gleichzeitig.

Diese Funktion hat die folgenden Einschränkungen:

- Wenn Sie in einem Menü in View Client auf ein USB-Gerät zugreifen und es in einem View-Desktop verwenden, können Sie auf dem lokalen Computer nicht auf das Gerät zugreifen.
- Die USB-Umleitung wird nicht von Systemen mit Windows 2000 unterstützt.
- Wenn Sie über View Portal auf einen View-Desktop zugreifen, steht diese Funktion nur auf Windows-Clients zur Verfügung, und auch nur dann, wenn Sie View Client zuerst auf dem lokalen Windows-System mit der optionalen USB-Umleitungskomponente installieren.
- Um einen USB-Drucker in einem View-Desktop verwenden zu können, müssen Sie die benötigten Druckertreiber im View-Desktop installieren.

Drucken auf einem View-Desktop

Die virtuelle Druckfunktion ermöglicht Endbenutzern das Verwenden von lokalen oder Netzwerkdruckern auf einem View-Desktop, ohne dass im View-Desktop zusätzliche Druckertreiber installiert werden müssen. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe usw. festlegen.

Nachdem ein Drucker dem lokalen Computer hinzugefügt wurde, fügt View diesen Drucker der Liste der verfügbaren Drucker auf dem View-Desktop hinzu. Keine weitere Konfiguration ist erforderlich. Benutzer mit Administratorrechten können weiterhin Druckertreiber auf dem View-Desktop installieren, ohne einen Konflikt mit der virtuellen Druckfunktionskomponente zu verursachen.

Die virtuelle Druckfunktion hat die folgenden Einschränkungen:

- Wenn Sie über View Portal auf einen View-Desktop zugreifen, steht diese Funktion nur auf Windows-Clients zur Verfügung, und auch nur dann, wenn Sie View Client zuerst auf dem lokalen Windows-System mit der optionalen USB-Umleitungskomponente installieren.
- Diese Funktion steht für USB-Drucker nicht zur Verfügung. Um einen USB-Drucker in einem View-Desktop verwenden zu können, müssen Sie die benötigten Druckertreiber im View-Desktop installieren.

Streaming von Multimediadaten auf einen View-Desktop

Wyse MMR (Multimedia Redirection) ermöglicht eine originalgetreue Wiedergabe, wenn Multimediadateien per Streaming an einen View-Desktop übertragen werden.

Die MMR-Funktion unterstützt die folgenden Mediendateiformate:

- AC3
- MP3
- MPEG-1, MPEG-2, MPEG-4-part2
- WMA
- WMV 7, 8 und 9

Diese Funktion hat die folgenden Einschränkungen:

- Arbeiten Sie zum Erzielen einer optimalen Qualität mit Windows Media Player 10 oder höher, und installieren Sie das Programm sowohl auf dem lokalen Computer als auch dem Clientzugriffsgerät sowie dem View-Desktop.
- Der Wyse MMR-Port (standardmäßig 9427) muss dem View-Desktop als Firewall-Ausnahme hinzugefügt werden.

Verwenden der Single Sign-On-Funktion zur Anmeldung an einem View-Desktop

Die Single Sign-On-Funktion (SSO oder einmalige Anmeldung) ermöglicht die Konfiguration von View Manager dergestalt, dass Endbenutzer nur einmalig zur Anmeldung aufgefordert werden.

Wenn Sie die Single Sign-On-Funktion nicht verwenden, werden Endbenutzer zweimal zur Anmeldung aufgefordert: einmal bei View Connection Server und anschließend an ihrem View-Desktop. Beim Verwenden von Smartcards müssen sich Endbenutzer dreimal anmelden, d. h. noch einmal, wenn der Smartcard-Leser zur Eingabe einer PIN auffordert.

Die einmalige Anmeldung wird als optionale Komponente implementiert, die Sie bei der View Agent-Installation für eine Desktop-Quelle installieren. Diese Funktion enthält die GINA-DLL (Graphical Identification and Authentication Dynamic-Link Library) für Windows XP und eine Anmeldedatenanbieter-DLL für Windows Vista.

Verwenden mehrerer Monitore mit einem View-Desktop

Unabhängig vom Anzeigeprotokoll können Sie mit einem View-Desktop mehrere Monitore verwenden.

Beim Verwenden von PCoIP, dem Anzeigeprotokoll von VMware, können Sie die Anzeigeauflösung und -drehung für jeden Monitor getrennt einstellen. PCoIP lässt eine echte Mehrfachmonitorsitzung anstatt nur eine Erweiterungsmodussitzung zu.

Eine Remote-Sitzung im Erweiterungsmodus ist tatsächlich nur eine Einzelmonitorsitzung. Die Monitore müssen dieselbe Größe und Auflösung aufweisen, und das Monitorlayout muss in ein Umgrenzungsfeld passen. Wenn Sie ein Anwendungsfenster maximieren, wird das Fenster auf alle Monitore erweitert.

Bei einer echten Mehrfachmonitorsitzung können die Monitore verschiedene Auflösungen und Größen haben, und ein Monitor kann schwenkbar sein. Wenn Sie ein Anwendungsfenster maximieren, wird das Fenster auf den vollständigen Bildschirm auf ausschließlich dem Monitor ausgedehnt, der es enthält.

Diese Funktion hat die folgenden Einschränkungen:

- Die maximale Anzahl von Monitoren, die Sie zum Anzeigen eines View-Desktops verwenden können, ist 10, wenn Sie das Anzeigeprototokoll RDP verwenden, und 4 bei Verwendung von PCoIP.
- Bei Einsatz des Anzeigeprotokolls Microsoft RDP muss Microsoft Remotedesktopverbindung 6.0 oder höher im View-Desktop installiert sein.

Zentrales Verwalten von Desktop-Pools 3

Sie können Pools einrichten, die einen oder hunderte virtueller Desktops enthalten. Als Quelle von Desktops können Sie virtuelle Maschinen, physische Computer und Server mit Windows-Terminaldienste verwenden. Wenn Sie eine virtuelle Maschine als Basis-Image erstellen, kann VMware View einen Pool virtueller Desktops anhand dieses Image generieren.

Dieses Kapitel behandelt die folgenden Themen:

Vorteile von Desktop-Pools

VMware View bietet als Grundlage eines zentralen Managements die Möglichkeit, Pools mit Desktops zu bilden und bereitzustellen.

Sie können einen Pool virtueller Desktops aus folgenden Quellen erstellen:

- Einem physischen System wie einem physischen Desktop-PC oder einem Server mit Windows-Terminaldienste
- Einer virtuellen Maschine, die auf einem ESX-Server gehostet und von vCenter Server verwaltet wird
- Einer virtuellen Maschine, die auf VMware Server oder einer anderen Virtualisierungsplattform ausgeführt wird, die View Agent unterstützt

Wenn Sie eine virtuelle vCenter-Maschine als Desktop-Quelle verwenden, können Sie den Prozess der Erstellung der gewünschten Anzahl identischer virtueller Desktops automatisieren. Sie können eine minimale und maximale Anzahl an virtuellen Desktops festlegen, die für den Pool erstellt werden soll. Das Festlegen dieser Parameter stellt sicher, dass Sie zur unmittelbaren Verwendung stets über eine ausreichende Anzahl von View-Desktops verfügen, ohne die verfügbaren Ressourcen zu überlasten.

Durch die Verwendung von Pools zur Verwaltung von Desktops wird das Anwenden von Einstellungen auf alle virtuellen Desktops in einem Pool ermöglicht. Die folgenden Beispiele zeigen einige der verfügbaren Einstellungen:

- Angeben, welches Anzeigeprotokoll als Standard für den View-Desktop verwendet werden soll und ob Endbenutzer die Standardeinstellung außer Kraft setzen dürfen.
- Konfigurieren der Anzeigequalität und Bandbreitendrosselung für Adobe Flash-Animationen.
- Geben Sie beim Verwenden einer virtuellen Maschine an, ob die virtuelle Maschine ausgeschaltet werden soll, wenn sie nicht verwendet wird, und ob sie vollständig gelöscht werden soll.

Darüber hinaus bietet das Verwenden von Desktop-Pools viele Vorteile.

Persistente Pools Jedem Benutzer wird ein bestimmter View-Desktop zugewiesen, und er kehrt bei jeder Anmeldung zum selben virtuellen Desktop zurück. Benutzer können ihre Desktops individuell anpassen, Anwendungen installieren und Daten speichern.

Nicht persistente Pools Der virtuelle Desktop wird nach jeder Verwendung optional gelöscht und erneut erstellt, wodurch eine hohe Kontrolle der Umgebung möglich ist. Ein nicht persistente Desktop entspricht einer Test- oder Kioskumgebung, in der die benötigten Anwendungen auf alle Desktops aufgespielt werden und alle Desktops Zugriff auf die benötigten Daten haben.

Nicht persistente Pools ermöglichen auch das Erstellen eines Pools mit Desktops, die von Benutzern in Schichten genutzt werden können. Ein Pool mit 100 Desktops kann beispielsweise von 300 Benutzern verwendet werden, wenn diese in drei Schichten mit je 100 Benutzern arbeiten.

Reduzieren und Verwalten von Speicheranforderungen

Das Verwenden virtueller Desktops, die von vCenter verwaltet werden, bietet sämtliche Speichervorteile, die zuvor nur für virtuelle Server möglich waren. Durch Verwenden von View Composer wird die Speichernutzung optimiert, da alle Desktops in einem Pool eine virtuelle Festplatte mit einem Basis-Image gemeinsam nutzen.

- Verwalten des Speichers mit vSphere auf Seite 22

  VMware vSphere ermöglicht eine Virtualisierung von Festplattenlaufwerken und Dateisystemen, sodass Sie den Speicher verwalten und konfigurieren können, ohne berücksichtigen zu müssen, wo die Daten physisch gespeichert sind.

- Reduzieren von Speicheranforderungen mit View Composer auf Seite 23

  Da View Composer Desktop-Images erstellt, die virtuelle Festplatten mit einem Basis-Image gemeinsam nutzen, kann die erforderliche Speicherkapazität um 50-90 % reduziert werden.

Verwalten des Speichers mit vSphere

VMware vSphere ermöglicht eine Virtualisierung von Festplattenlaufwerken und Dateisystemen, sodass Sie den Speicher verwalten und konfigurieren können, ohne berücksichtigen zu müssen, wo die Daten physisch gespeichert sind.

Fibre Channel SAN-, iSCSI SAN- und NAS-Arrays sind weit verbreitete Speichertechnologien, die von VMware vSphere zur Erfüllung verschiedener Speicheranforderungen von Rechenzentren unterstützt werden. Die Speicher-Arrays werden mithilfe von Speichernetzwerken (SANs) mit Gruppen von Servern verbunden, die diese dann gemeinsam nutzen. Diese Vorgehensweise erlaubt die Zusammenführung von Speicherressourcen und bietet mehr Flexibilität bei ihrer Bereitstellung für virtuelle Maschinen.

Reduzieren von Speicheranforderungen mit View Composer

Da View Composer Desktop-Images erstellt, die virtuelle Festplatten mit einem Basis-Image gemeinsam nutzen, kann die erforderliche Speicherkapazität um 50-90 % reduziert werden.

View Composer arbeitet mit einem Basis-Image (bzw. einer übergeordneten virtuellen Maschine) und erstellt einen Pool mit bis zu 512 virtuellen Maschinen auf Basis verknüpfter Klone. Jeder verknüpfte Klon fungiert als unabhängiger Desktop (mit eindeutigem/r Hostnamen/IP-Adresse), aber dennoch benötigt der verknüpfte Klon wesentlich weniger Speicherplatz.

Wenn Sie einen Desktop-Pool auf Basis verknüpfter Klone erstellen, wird von der übergeordneten virtuellen Maschine ein erster vollständiger Klon erstellt. Der vollständige Klon (bzw. das Replikat) und die Klone, die damit verknüpft sind, werden im selben Datenspeicher bzw. derselben LUN (Logical Unit Number) abgelegt. Bei Bedarf können Sie mithilfe der Neuverteilungsfunktion das Replikat und die verknüpften Klone aus einer LUN in eine andere verschieben.

Beim Erstellen persistenter Desktop-Pools erstellt View Composer für jeden virtuellen Desktop auch eine getrennte Festplatte für Benutzerdaten. Auf dieser Festplatte werden das Profil und die Anwendungsdaten des Endbenutzers gespeichert. VMware empfiehlt, die Festplatten mit Benutzerdaten in einem anderen Datenspeicher abzulegen. Sie können dann die gesamte LUN sichern, die die Festplatten mit Benutzerdaten enthält.

Anwendungsbereitstellung

Beim Verwenden von VMware View können Sie herkömmliche Bereitstellungstechniken nutzen, Anwendungen mithilfe von VMware ThinApp virtualisieren oder Anwendungen als Teil eines View Composer-Basis-Image bereitstellen.

- Bereitstellen von Anwendungen und System-Updates mit View Composer auf Seite 23

  Da Desktop-Pools auf Grundlage verknüpfter Klone ein Basis-Image gemeinsam nutzen, können Sie Updates und Patches schnell bereitstellen, indem die übergeordnete virtuelle Maschine aktualisiert wird.

- Virtualisieren von Anwendungen mit VMware ThinApp auf Seite 24

  ThinApp™ ermöglicht das Komprimieren einer Anwendung zu einer einzelnen Datei, die in einer virtualisierten Anwendungstestumgebung (auch „Sandbox oder Sandkasten“ genannt) ausgeführt wird. Diese Vorgehensweise führt zu einer flexiblen, problemlosen Anwendungsbereitstellung.

- Verwenden bestehender Prozesse für die Anwendungsbereitstellung auf Seite 24

  VMware View ermöglicht, dass Sie die aktuellen Prozesse für die Anwendungsbereitstellung in Ihrem Unternehmen weiter nutzen können. Zwei zu berücksichtigende Aspekte sind die Verwaltung der Nutzung der Server-CPU und der Speicher-E/A sowie die Festlegung, ob Benutzer Anwendungen installieren dürfen.

Bereitstellen von Anwendungen und System-Updates mit View Composer

Da Desktop-Pools auf Grundlage verknüpfter Klone ein Basis-Image gemeinsam nutzen, können Sie Updates und Patches schnell bereitstellen, indem die übergeordnete virtuelle Maschine aktualisiert wird.

Die Neuzusammenstellungsfunktion ermöglicht das Vornehmen von Änderungen an der übergeordneten virtuellen Maschine, das Erstellen eines Snapshots des neuen Status und das Übertragen der neuen Version des Image an alle oder eine Untermenge der Benutzer und Desktops. Sie können diese Funktion für die folgenden Aufgaben verwenden:

- Aufspielen von Patches und Upgrades für Betriebssysteme und Software
- Aufspielen von Service Packs
- Hinzufügen von Anwendungen

- Hinzufügen virtueller Geräte
- Ändern anderer Einstellungen virtueller Maschinen (z. B. verfügbarer Arbeitsspeicher)

Wenn Sie verhindern möchten, dass Benutzer Software hinzufügen oder entfernen bzw. Einstellungen ändern, können Sie den Desktop über die Aktualisierungsfunktion auf seine Standardeinstellungen zurücksetzen. Diese Funktion reduziert auch die Größe verknüpfter Klone, die meist mit der Zeit anwachsen.

Virtualisieren von Anwendungen mit VMware ThinApp

ThinApp™ ermöglicht das Komprimieren einer Anwendung zu einer einzelnen Datei, die in einer virtualisierten Anwendungstestumgebung (auch „Sandbox oder Sandkasten“ genannt) ausgeführt wird. Diese Vorgehensweise führt zu einer flexiblen, problemlosen Anwendungsbereitstellung.

Wenn Sie mithilfe von ThinApp eine virtualisierte Anwendung erstellen, können Benutzer entweder die Anwendung von einem freigegeben Dateiserver per Streaming übertragen oder sie auf ihre virtuellen Desktops kopieren. Wenn Sie die virtualisierte Anwendung für das Streaming konfigurieren, müssen Sie die folgenden Architekturaspekte berücksichtigen:

- Den Zugriff bestimmter Benutzergruppen auf bestimmte Anwendungen
- Die Konfiguration eines gemeinsamen Datenspeichers
- Den beim Streaming generierten Netzwerkdatenverkehr, der stark vom Typ der Anwendung abhängt

Bei per Streaming übertragenen Anwendungen können die Benutzer die Anwendungen direkt auf dem freigegebenen Dateiserver oder indirekt über eine Desktop-Verknüpfung starten.

Wenn Sie eine ThinApp-Paketdatei so konfigurieren, dass sie auf einen virtuellen Desktop kopiert und auf diesem ausgeführt wird, müssen dieselben Architekturaspekte berücksichtigt werden wie bei der herkömmlichen Softwarebereitstellung mit MSI-Paketen.

Verwenden bestehender Prozesse für die Anwendungsbereitstellung

VMware View ermöglicht, dass Sie die aktuellen Prozesse für die Anwendungsbereitstellung in Ihrem Unternehmen weiter nutzen können. Zwei zu berücksichtigende Aspekte sind die Verwaltung der Nutzung der Server-CPU und der Speicher-E/A sowie die Festlegung, ob Benutzer Anwendungen installieren dürfen.

Wenn Sie Anwendungen an viele virtuelle Desktops exakt zur gleichen Zeit verteilen, kommt es zu signifikanten Spitzen bei der CPU-Nutzung und Speicher-E/A. Diese Spitzenarbeitslasten können spürbare Auswirkungen auf die Desktop-Leistung haben. Es hat sich bewährt, Anwendungs-Updates gestaffelt und außerhalb der Spitzenzeiten an Desktops zu verteilen. Sie müssen ferner prüfen, ob Ihre Speicherlösung solche Arbeitslasten unterstützt.

Falls Ihr Unternehmen Benutzern die Installation von Anwendungen gestattet, können Sie weiter mit Ihren aktuellen Richtlinien arbeiten, kommen dann aber nicht in den Genuss der Vorteile der View Composer-Funktionen. Wenn beim Arbeiten mit View Composer eine Anwendung nicht virtualisiert oder auf sonstige Weise in den Profil- oder Dateneinstellungen des Benutzers enthalten ist, wird die Anwendung verworfen, sobald ein View Composer-Aktualisierungs-, Neuzusammenstellungs- oder Neuverteilungsvorgang erfolgt. In vielen Fällen ist die Möglichkeit einer strengen Kontrolle der installierten Anwendungen ein Vorteil. View Composer-Desktops können einfach unterstützt werden, da sie nahezu stets eine als funktionierend bekannte Konfiguration haben.

Wenn Benutzer unbedingt ihre eigenen Anwendungen installieren und diese dauerhaft über die Lebensdauer des virtuellen Desktops nutzen möchten, können Sie, anstatt View Composer für die Anwendungsbereitstellung zu verwenden, vollständige persistente Desktops erstellen und Benutzern das Installieren von Anwendungen erlauben.

Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten

VMware View bietet zahlreiche Vorlagen für Gruppenrichtlinienobjekte, mit deren Hilfe die Verwaltung und Konfiguration von View Manager und View-Desktops zentral erfolgen kann.

Nach dem Import in Active Directory können Sie diese Vorlagen zum Festlegen von Richtlinien für die folgenden Gruppen und Komponenten nutzen:

- Alle Systeme unabhängig vom sich anmeldenden Benutzer
- Alle Benutzer unabhängig vom System, an dem sie sich anmelden
- View Connection Server-Konfiguration
- View Client-Konfiguration
- View Agent-Konfiguration

Nach Aktivierung eines Gruppenrichtlinienobjekts werden Eigenschaften in der lokalen Windows-Registrierung der betreffenden Komponente gespeichert.

Mithilfe von Gruppenrichtlinienobjekten können Sie alle Richtlinien festlegen, die auf der Benutzeroberfläche von View Administrator zur Verfügung stehen. Sie können Gruppenrichtlinienobjekte auch nutzen, um Richtlinien festzulegen, die nicht auf der Benutzeroberfläche verfügbar sind. Eine vollständige Liste und Beschreibung der über Gruppenrichtlinienobjekt-Vorlagen verfügbaren Einstellungen finden Sie im *View Manager-Administratorhandbuch*.

Architekturentwurfselemente und Planungsanleitungen

4

Ein typischer VMware View-Architekturentwurf basiert zur Erzielung von Skalierbarkeit auf einem Bausteinmodell. Jeder Baustein besteht aus Komponenten, die bis zu 1000 virtuelle Desktops unterstützen. Der Gesamtentwurf integriert fünf dieser Bausteine.

Diese Architektur bietet einen skalierbaren Standardentwurf, den Sie an Ihre Unternehmensumgebung und besondere Anforderungen anpassen können. In diesem Kapitel finden Sie Einzelheiten zu den Anforderungen hinsichtlich Arbeitsspeicher, CPU, Speicherkapazität, Netzwerkkomponenten und Hardware, sodass sich IT-Architekten und -Planer einen Überblick verschaffen können, was bei der Bereitstellung einer VMware View-Lösung in der Praxis zu berücksichtigen ist.

Dieses Kapitel behandelt die folgenden Themen:

Konfigurieren virtueller Maschinen für View-Desktops

Virtuelle Maschinen, die für Endbenutzer als View-Desktops vorgesehen sind, benötigen weniger Festplattenspeicher und Verarbeitungsressourcen als VMware Server-basierte virtuelle Maschinen.

Wenn Sie eine virtuelle Maschine einrichten, die als View-Desktop verwendet werden soll, wirkt sich Ihre Auswahl bei Arbeitsspeicher, CPU und Festplattenspeicher wesentlich auf Ihre Optionen bei der Serverhardware und den Kosten aus.

- Einschätzen der CPU-Anforderungen für virtuelle Desktops auf Seite 31

  Beim Einschätzen der CPU-Anforderungen müssen Sie Informationen zur durchschnittlichen CPU-Nutzung der verschiedenen Nutzertypen in Ihrem Unternehmen sammeln. Darüber hinaus müssen Sie berücksichtigen, dass weitere 10-25 % der Verarbeitungsleistung für den Virtualisierungs-Overhead und Spitzennutzungszeiten erforderlich sind.

- Auswählen der geeigneten Systemfestplattengröße auf Seite 31

  Beim Zuweisen von Festplattenspeicher sollten Sie nur so viel Speicherplatz für Betriebssystem, Anwendungen und weitere Inhalte bereitstellen, die Benutzer ggf. installieren oder generieren, wie unbedingt nötig. In der Regel ist diese Menge kleiner als die Größe der Festplatte eines physischen PC.

- Beispielkonfiguration eines auf einer virtuellen Maschine basierenden Desktops auf Seite 32

  Da die Arbeits- und Festplattenspeichergröße und CPU-Leistung, die von virtuellen Desktops benötigt wird, vom Gastbetriebssystem abhängt, werden nach Windows XP und Windows Vista getrennte Konfigurationsbeispiele für virtuelle Desktops angegeben.

Auf den Nutzertypen basierende Planung

Bei vielen Konfigurationselementen, z. B. Arbeitsspeicher (RAM), CPU und Festplattenspeichergröße, hängen die Anforderungen größtenteils vom Typ des Nutzers, der mit dem virtuellen Desktop arbeitet, und den zu installierenden Anwendungen ab.

Zur Architekturplanung können Nutzer in verschiedene Kategorien eingeteilt werden.

Sachbearbeiter Sachbearbeiter führen in der Regel an einem stationären Computer mithilfe einer kleinen Gruppe von Anwendungen sich wiederholende Aufgaben aus. Die Anwendungen benötigen zumeist weniger CPU- und Arbeitsspeicherressourcen als die von Büroanwendern. Sachbearbeiter, die in bestimmten Schichten arbeiten, können sich alle gleichzeitig an ihren virtuellen Desktops anmelden. Zu Sachbearbeitern zählen Callcenter-Mitarbeiter, Filialkräfte, Lagerpersonal usw.

Büroanwender Zu den täglichen Aufgaben von Büroanwendern gehören der Zugriff auf das Internet, das Arbeiten mit E-Mail sowie das Anlegen komplexer Dokumente, Präsentationen und Kalkulationstabellen. Büroanwender sind Buchhalter, Verkaufsleiter, Marktforscher usw.

Hauptbenutzer Hauptbenutzer sind Anwendungsentwickler und Nutzer grafikintensiver Anwendungen.

Zuweisen von Arbeitsspeicher zu einem Gastbetriebssystem

Arbeitsspeicher (RAM) ist für Server kostspieliger als für PCs. Da die Arbeitsspeicherkosten einen hohen Prozentsatz der Gesamtkosten für Serverhardware ausmachen, ist das überlegte Zuweisen von Arbeitsspeicher für die Planung Ihrer Desktop-Umgebung besonders wichtig.

Wenn die Arbeitsspeicherzuweisung zu niedrig ist, kann die Speicher-E/A davon beeinträchtigt werden, da Arbeitsspeicher zu stark auf Festplatten ausgelagert wird. Wenn die Arbeitsspeicherzuweisung zu hoch ist, kann die Speicherkapazität beeinträchtigt werden, da die Auslagerungsdatei im Gastbetriebssystem sowie die Auslagerungs- und Anhaltedatei für die einzelnen virtuellen Maschinen zu groß werden.

Auswirkungen der Arbeitsspeichergröße auf die Systemleistung

Vermeiden Sie bei der Zuteilung von Arbeitsspeicher allzu konservative Einstellungen. Berücksichtigen Sie Folgendes:

- Eine unzureichende Arbeitsspeicherzuweisung kann übermäßig viele Auslagerungsvorgänge auf dem Gastsystem verursachen, wodurch E/A-Vorgänge generiert werden, die zu signifikanten Leistungseinbußen und einer Steigerung der Speicher-E/A-Last führen.
- VMware ESX unterstützt hoch entwickelte Algorithmen für das Management von Arbeitsspeicherressourcen, z. B. die transparente gemeinsame Nutzung von Arbeitsspeicher und das Anpassen der Größe des Gast-Arbeitsspeichers zur Laufzeit (das sog. Memory Ballooning), wodurch der zur Unterstützung einer gegebenen Arbeitsspeicherzuweisung zu einem Gastsystem erforderliche physische Arbeitsspeicher beträchtlich verringert werden kann. Auch wenn beispielsweise 2 GB einem virtuellen Desktop zugewiesen werden, wird nur ein Bruchteil dieser Menge im physischen Arbeitsspeicher belegt.
- Da für die Leistung virtueller Desktops schnelle Antwortzeiten sehr wichtig sind, müssen Sie auf dem ESX-Server für die Einstellungen zur Arbeitsspeicherreservierung Werte ungleich null festlegen. Das Reservieren einer bestimmten Arbeitsspeichermenge stellt sicher, dass verwendete Desktops im Leerlauf nie vollständig auf die Festplatte ausgelagert werden. Höhere Reservierungseinstellungen wirken sich jedoch auf die Fähigkeit aus, Arbeitsspeicher auf einem ESX-Server mehrfach zu vergeben, und können VMotion-Wartungsvorgänge beeinträchtigen.

Auswirkungen der Arbeitsspeichergröße auf die Speicherung

Die Größe des Arbeitsspeichers, den Sie einer virtuellen Maschine zuweisen, steht in direktem Zusammenhang mit der Größe bestimmter Dateien, welche die virtuelle Maschine verwendet.

Windows-Auslagerungsdatei	Die Größe dieser Datei beträgt standardmäßig das 1,5-fache des Gastarbeitsspeichers. Diese Datei, deren Pfad normalerweise `C:\pagefile.sys` lautet, bewirkt, dass auf verknüpften Klonen basierende virtuelle Maschinen und per Thin Provisioning bereitgestellter Speicher anwachsen, da häufig darauf zugegriffen wird. Die Verkleinerung der Auslagerungsdatei führt häufig zur Verkleinerung virtueller Festplatten (`.vmdk`-Dateien) für verknüpfte Klone. Wenngleich Sie die Größe unter Windows anpassen können, kann sich dies negativ auf die Anwendungsleistung auswirken.
Windows-Ruhezustandsdatei für Laptops	Die Größe diese Datei kann 100 % des Gastarbeitsspeichers entsprechen. Sie können diese Datei unbesorgt löschen, da sie in View-Bereitstellungen nicht benötigt wird, selbst wenn Sie View Client with Offline Desktop einsetzen.
ESX-Auslagerungsdatei	Diese Datei mit der Erweiterung `.vswp` wird angelegt, wenn Sie weniger als 100 % des Arbeitsspeichers einer virtuellen Maschine reservieren. Die Größe dieser Auslagerungsdatei entspricht dem nicht reservierten Anteil des Gastarbeitsspeichers. Wenn beispielsweise 50 % des Gastarbeitsspeichers reserviert sind und dieser eine Größe von 2 GB hat, ist die ESX-Auslagerungsdatei 1 GB groß.
ESX-Anhaltedatei	Diese Datei mit der Erweiterung `.vmss` wird erstellt, wenn Sie die Abmeldungsrichtlinie für den Desktop-Pool so festlegen, dass der virtuelle Desktop angehalten wird, wenn sich der Benutzer abmeldet. Die Größe dieser Datei entspricht der Größe des Gastarbeitsspeichers.

Festlegen der Arbeitsspeichergröße für bestimmte Monitorkonfigurationen bei der Verwendung von PCoIP

Wenn Sie PCoIP, das Anzeigeprotokoll von VMware, verwenden, hängt die benötigte Arbeitsspeichergröße teilweise von der Anzahl der Monitore, die für Endbenutzer konfiguriert sind, und von der Anzeigeauflösung ab. Tabelle 4-1 zeigt die Größe des Arbeitsspeichers, der für verschiedene Konfigurationen benötigt wird. Die in den Spalten angegebenen Arbeitsspeichergrößen sind als Zusatz zur Arbeitsspeichergröße zu verstehen, die für andere PCoIP-Funktionen benötigt wird.

Da Sie Arbeitsspeicher in Schritten zuweisen können, zeigt die Tabelle die zu wählenden Schritte. Eine Konfiguration mit einem Monitor, der VGA verwendet, benötigt 37,03 MB, die kleinste RAM-Schrittgröße ist jedoch 64 MB.

Tabelle 4-1. Overhead für PCoIP-Clientanzeige

Standardanzeige-auflösung	Breite (in Pixel)	Höhe (in Pixel)	Overhead bei 1 Monitoren (RAM-Schritt-größe)	Overhead bei 2 Monitoren (RAM-Schritt-größe)	Overhead bei 4 Monitoren (RAM-Schrittgröße)
VGA	640	480	37,03 MB (64 MB)	44,06 MB (64 MB)	58,13 MB (64 MB)
SVGA	800	600	40,06 MB (64 MB)	51,97 MB (64 MB)	73,95 MB (96 MB)
720p	1280	720	51,09 MB (64 MB)	72,19 MB (96 MB)	114,38 MB (128 MB)
UXGA	1600	1200	73,95 MB (96 MB)	117,89 MB (128 MB)	205,78 MB (256 MB)
1080p	1920	1080	77,46 MB (96 MB)	124,92 MB (128 MB)	219,84 MB (256 MB)
WUXGA	1920	1200	82,73 MB (96 MB)	135,47 MB (196 MB)	240,94 MB (256 MB)
QXGA	2048	1536	102,00 MB (128 MB)	174,00 MB (196 MB)	318,00 MB (384 MB)
WQXGA	2560	1600	123,75 MB (128 MB)	217,50 MB (256 MB)	405,00 MB (512 MB)

Bestimmen der Arbeitsspeichergröße für bestimmte Arbeitslasten und Betriebssysteme

Da die Größe des erforderlichen Arbeitsspeichers je nach Nutzertyp stark variieren kann, führen viele Unternehmen eine Pilotphase durch, um die ordnungsgemäße Einstellung für die verschiedene Nutzergruppen in ihrem Unternehmen zu bestimmen.

Ein empfohlener Ausgangswert ist 1024 MB für Windows XP-Desktops und 1536 MB für Windows Vista-Desktops. Überwachen Sie in der Pilotphase die Leistung und den durch verschiedene Nutzertypen belegten Speicherplatz, und nehmen Sie so lange Anpassungen vor, bis Sie die optimale Einstellung für jede Nutzergruppe ermittelt haben.

Einschätzen der CPU-Anforderungen für virtuelle Desktops

Beim Einschätzen der CPU-Anforderungen müssen Sie Informationen zur durchschnittlichen CPU-Nutzung der verschiedenen Nutzertypen in Ihrem Unternehmen sammeln. Darüber hinaus müssen Sie berücksichtigen, dass weitere 10-25 % der Verarbeitungsleistung für den Virtualisierungs-Overhead und Spitzennutzungszeiten erforderlich sind.

Die CPU-Anforderungen variieren je nach Nutzertyp. Softwareentwickler und andere Hauptbenutzer mit hohem Systemleistungsbedarf haben ggf. wesentlich höhere CPU-Anforderungen als Büroanwender. Büroanwender können wiederum höhere CPU-Anforderungen als Sachbearbeiter haben, die hauptsächlich mit der Dateneingabe beschäftigt sind. Überprüfen Sie in der Pilotphase mit einem Systemüberwachungsprogramm wie Perfmon die Durchschnitts- und Spitzennutzungsgrade der CPU für diese Nutzergruppen.

Da viele virtuelle Maschinen auf einem einzigen Server ausgeführt werden, kann es zu CPU-Spitzen kommen, wenn Agents, z. B. von Antivirusprogrammen, alle zugleich eine Überprüfung auf Updates durchführen. Bestimmen Sie, welche bzw. wie viele Agents Leistungsprobleme verursachen können, und wählen Sie eine Strategie, um diesen Problemen zu begegnen. Die folgenden Strategien können sich beispielsweise in Ihrem Unternehmen als hilfreich erweisen:

- Setzen Sie View Composer zum Aktualisieren von Images ein, anstatt Softwareverwaltungs-Agents Software-Updates auf jeden einzelnen virtuellen Desktop herunterladen zu lassen.
- Planen Sie die Ausführung von Antivirus- und Software-Updates außerhalb der Spitzenzeiten ein, wenn meist nur wenige Benutzer angemeldet sind.
- Staffeln Sie Updates, und lassen Sie die Zeitpunkte nach dem Zufallsprinzip auswählen.

Als Größenvorschlag empfiehlt VMware, dass Sie ermitteln, wie viele virtuelle Desktops pro CPU-Kern unterstützt werden können. Ein geeigneter Ausgangswert für den Pilottest sind acht virtuelle Maschinen pro Kern. Wenn Sie z. B. einen physischen PC mit einem Kern und 2,2 GHz-Prozessor überwachen und feststellen, dass die durchschnittlich CPU-Nutzung bei 2,79 % liegt, beträgt der CPU-Wert 130 MHz. Wenn Sie einen ESX-Server mit zwei Sockets und vier Kernen haben, können Sie in der Pilotphase 64 virtuelle Maschinen auf dem Server hosten. Das Zuweisen von 130 MHz zu jeder der 64 virtuellen Maschinen bedeutet, dass der gesamte durchschnittlich benötigte CPU-Wert 8,3 GHz beträgt.

Neben der CPU-Leistung, die für das Gastbetriebssystem und Anwendungen erforderlich ist, müssen Sie auch die zusätzliche Verarbeitungsleistung berücksichtigen, die für die Virtualisierung des Desktops und für Nutzungsspitzen benötigt wird. Dieser Overhead beläuft sich auf 10-25 % der durchschnittlichen CPU-Leistung. Bei diesem Beispiel beträgt eine konservative CPU-Schätzung 25 % von 8,3 GHz. Demzufolge muss die CPU-Gesamtleistung des ESX-Servers 10,38 GHz betragen.

Auswählen der geeigneten Systemfestplattengröße

Beim Zuweisen von Festplattenspeicher sollten Sie nur so viel Speicherplatz für Betriebssystem, Anwendungen und weitere Inhalte bereitstellen, die Benutzer ggf. installieren oder generieren, wie unbedingt nötig. In der Regel ist diese Menge kleiner als die Größe der Festplatte eines physischen PC.

Da Festplattenspeicher im Rechenzentrum pro Gigabyte meist mehr kostet als der Festplattenspeicher von Desktops bzw. Laptops in einer herkömmlichen PC-Bereitstellung, müssen Sie die Image-Größe des Betriebssystems optimieren. Befolgen Sie hierzu die folgenden Anweisungen:

- Entfernen Sie überflüssige Dateien. Reduzieren Sie z. B. die Kontingente für temporäre Internetdateien.
- Wählen Sie eine virtuelle Festplattengröße, die künftiges Wachstum zulässt, aber nicht unrealistisch groß ist.
- Arbeiten Sie mit zentralen Dateifreigaben oder einer VMware View-Benutzerdatenfestplatte für von Benutzern generierte Inhalte und installierte Anwendungen.

Bei der Größe des benötigten Speicherplatzes müssen für jeden virtuellen Desktop die folgenden Dateien berücksichtigt werden:

- Die Größe der ESX-Anhaltedatei entspricht der Größe des Arbeitsspeichers, der der virtuellen Maschine zugewiesen ist.
- Die Größe der Windows-Auslagerungsdatei entspricht 150 % der Arbeitsspeichergröße.
- Protokolldateien belegen für jede virtuelle Maschine ca. 100 MB.
- Die virtuelle Festplatte oder `.vmdk`-Datei muss ferner lokale Benutzerdaten und vom Benutzer installierte Anwendungen aufnehmen, wenn sich diese auf dem virtuellen Desktop und nicht auf Dateifreigaben befinden.

  Beim Verwenden von View Composer wachsen die `.vmdk`-Dateien mit der Zeit an. Sie können dieses Anwachsen jedoch kontrollieren, indem Sie View Composer-Aktualisierungsvorgänge planen und für View-Desktop-Pools eine Richtlinie für die Speichermehrfachvergabe festlegen.

Sie können auch diesem Schätzwert 15 % hinzufügen, um sicherzustellen, dass Speicherplatz nicht knapp wird.

Beispielkonfiguration eines auf einer virtuellen Maschine basierenden Desktops

Da die Arbeits- und Festplattenspeichergröße und CPU-Leistung, die von virtuellen Desktops benötigt wird, vom Gastbetriebssystem abhängt, werden nach Windows XP und Windows Vista getrennte Konfigurationsbeispiele für virtuelle Desktops angegeben.

Die Beispieleinstellungen für virtuelle Maschinen (Arbeitsspeicher, Anzahl virtueller Prozessoren und Festplattenspeicher) sind VMware View-spezifisch und basieren auf Informationen, die bei der Ausarbeitung von *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments* (VMware View-Referenzarchitektur: Anleitung für umfangreiche VMware View-Bereitstellungen in Unternehmen) gesammelt wurden. Bei dieser Architektur wurde VMware Infrastructure 3.5 zum Hosten und Verwalten virtueller Maschinen verwendet. Weitere Informationen zu den Einschränkungen virtueller Maschinen in vSphere finden Sie im Dokument *VMware vSphere Configuration Maximums* (Maximalwerte bei der Konfiguration von VMware vSphere).

Die in Tabelle 4-2 angegebenen Vorgaben gelten für einen standardmäßigen virtuellen Desktop mit Windows XP.

Tabelle 4-2. Beispiel eines virtuellen Desktops für Windows XP

Element	Beispiel
Betriebssystem	32-Bit-Windows XP (mit neuestem Service Pack)
Arbeitsspeicher (RAM)	1024 MB (mindestens 512 MB, höchstens 2048 MB)
Virtuelle CPU	1
Kapazität der Systemfestplatte	16 GB (mindestens 8 GB, höchstens 40 GB)
Benutzerdatenkapazität (entweder als Benutzerdatenfestplatte oder umgeleitetes Profil)	5 GB (Ausgangswert)
Virtueller SCSI-Adaptertyp	LSI Logic (nicht die Standardeinstellung)
Virtueller Netzwerkadapter	Betriebssystemabhängige Standardeinstellung

Die Speichergröße der Systemfestplatte hängt von der Anzahl der Anwendungen ab, die im Basis-Image benötigt werden. Die View-Referenzarchitektur arbeitet mit einer Einrichtung, die 8 GB Festplattenspeicher vorsieht. Zu den Anwendungen gehören Microsoft Word, Excel, PowerPoint, Adobe Reader, Internet Explorer, McAfee Antivirus und PKZIP.

Die Größe des Festplattenspeichers, der für Benutzerdaten benötigt wird, hängt von der Aufgabe des Endbenutzers und den Unternehmensrichtlinien für die Datenspeicherung ab. Beim Verwenden von View Composer verbleiben diese Daten auf einer Benutzerdatenfestplatte. Beim Verwenden eines Profilverwaltungsprodukts eines anderen Anbieters können diese Daten in einem servergespeicherten Windows-Profil an ein CIFS-Dateisystem umgeleitet werden.

Die in Tabelle 4-3 angegebenen Vorgaben gelten für einen standardmäßigen virtuellen Desktop mit Windows Vista.

Tabelle 4-3. Beispiel eines virtuellen Desktops für Windows Vista

Element	Beispiel
Betriebssystem	32-Bit-Windows Vista (mit neuestem Service Pack)
Arbeitsspeicher (RAM)	1,536MB (Standardeinstellung)
Virtuelle CPU	1
Kapazität der Systemfestplatte	20 GB (Standardeinstellung)
Benutzerdatenkapazität (entweder als Benutzerdatenfestplatte oder umgeleitetes Profil)	5 GB (Ausgangswert)
Virtueller SCSI-Adaptertyp	LSI Logic (Standardeinstellung)
Virtueller Netzwerkadapter	Betriebssystemabhängige Standardeinstellung

vCenter und View Composer: Konfigurieren von Maximalwerten für virtuelle Maschinen und Desktop-Pools

vCenter und View Composer werden in derselben virtuellen Maschine installiert. Da diese virtuelle Maschine ein Server ist, benötigt sie wesentlich mehr Arbeitsspeicher und Verarbeitungsleistung als eine virtuelle Maschine für einen Desktop.

View Composer kann bis zu 512 Desktops pro Pool erstellen und bereitstellen. View Composer kann ferner einen Neuzusammenstellungsvorgang auf bis zu 512 Desktops gleichzeitig anwenden.

Wenngleich Sie vCenter und View Composer auf einem physischen Computer installieren können, werden in diesem Beispiel virtuelle Maschinen mit den in Tabelle 4-4 angegebenen technischen Daten verwendet. Der ESX-Server, der als Host dieser virtuellen Maschinen dient, kann Teil eines VMware High Availability-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Tabelle 4-4. vCenter: Beispiel einer virtuellen Maschine und Festlegen der maximalen Poolgröße

Element	Beispiel
Betriebssystem	32-Bit-Windows Server 2003 (mit neuestem Service Pack)
Arbeitsspeicher (RAM)	4 GB
Virtuelle CPU	2
Kapazität der Systemfestplatte	20 GB
SCSI-Typ	LSI Logic (Standardeinstellung für Windows Server 2003)
Netzwerkadapter	VM Network (Standardeinstellung)
Maximale View Composer-Poolgröße	512 Desktops

WICHTIG Legen Sie die Datenbank, mit der sich vCenter und View Composer verbinden, auf einer getrennten virtuellen Maschine ab. Anweisungen zum Bestimmen der Datenbankgröße finden Sie unter http://www.vmware.com/support/vi3/doc/vc_db_calculator.xls.

View Connection Server: Konfigurieren von virtuellen Maschinen und Maximalwerten

Bei Installation von View Connection Server wird die Anwendung View Administrator ebenfalls installiert. Dieser Server benötigt dieselben Arbeitsspeicher- und Verarbeitungsressourcen wie eine vCenter Server-Instanz.

View Connection Server-Konfiguration

Wenngleich Sie View Connection Server auf einem physischen Computer installieren können, werden in diesem Beispiel virtuelle Maschinen mit den in Tabelle 4-5 angegebenen technischen Daten verwendet. Der ESX-Server, der als Host dieser virtuellen Maschinen dient, kann Teil eines VMware High Availability-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Tabelle 4-5. Beispiel einer virtuellen Maschine für View Connection Server

Element	Beispiel
Betriebssystem	32-Bit-Windows Server 2003 (mit neuestem Service Pack)
Arbeitsspeicher (RAM)	4GB
Virtuelle CPU	2 oder 4
Kapazität der Systemfestplatte	20 GB
SCSI-Typ	LSI Logic (Standardeinstellung für Windows Server 2003)
Netzwerkadapter	VM Network (Standardeinstellung)
1 Netzwerkadapter	1 Gigabit

Maximale Verbindungsanzahl für View Connection Server

Tabelle 4-6 bietet Informationen zur maximalen Anzahl gleichzeitiger Verbindungen, die eine VMware View-Bereitstellung unterstützen kann.

Tabelle 4-6. View-Desktop-Verbindungen

Anzahl der Connection Server-Instanzen pro Bereitstellung	Verbindungstyp	Maximale Anzahl gleichzeitiger Verbindungen
1 Connection Server-Instanz	Direktverbindung, RDP	2,000
5 Connection Server-Instanzen	Direktverbindung, RDP	5,000
3 Connection Server-Instanzen	Tunnelverbindung, RDP	2,000
1 Connection Server-Instanz	Direktverbindung, PCoIP	2,000
1 Connection Server-Instanz	Unified Access auf physische PCs	100
1 Connection Server-Instanz	Unified Access auf Terminalserver	200

Tunnelverbindungen sind erforderlich, wenn Sie für RDP-Verbindungen, deren Anfangspunkt sich außerhalb des internen Firmennetzwerks befinden, Sicherheitsserver verwenden.

VMware View-Knoten

Ein Knoten ist ein einzelner VMware ESX-Server, der als Host von Desktops auf Basis virtueller Maschinen in einer VMware View-Bereitstellung dient. Ein Knoten kann acht virtuelle Maschinen pro Kern und 64 virtuelle Maschinen pro LUN hosten.

VMware View arbeitet am wirtschaftlichsten, wenn Sie die Anzahl der Desktops maximieren, die von einem ESX-Server gehostet werden. Obgleich sich zahlreiche Faktoren auf die Serverauswahl auswirken, müssen Sie, wenn Sie bei der Beschaffung sparen möchten, Serverkonfigurationen finden, die weder bei CPU-Kernen noch Arbeitsspeicher wesentlich eingeschränkt sind.

Im Allgemeinen sind acht virtuelle Maschinen pro CPU-Kern möglich, doch müssen Sie auch die physischen Arbeitsspeicheranforderungen berücksichtigen. Nachdem Sie bestimmt haben, wie viel Arbeitsspeicher jeder virtuellen Maschine zugewiesen werden soll, können Sie ermitteln, ob eine gegebene ESX-Serverkonfiguration kern- oder arbeitsspeicherbezogen eingeschränkt ist. Wenn ein Server kernbezogen eingeschränkt ist, verfügt er bei Ausführung mit der maximalen Anzahl virtueller Maschinen pro Kern über überschüssigen Arbeitsspeicher. Ist ein Server arbeitsspeicherbezogen eingeschränkt, ist der physische Arbeitsspeicher belegt, bevor die Zielanzahl virtueller Maschinen pro Kern erreicht ist.

Informationen zum Berechnen der CPU-Anforderungen jeder virtuellen Maschine finden Sie unter „Einschätzen der CPU-Anforderungen für virtuelle Desktops“, auf Seite 31. Informationen zum Berechnen der Arbeitsspeicheranforderungen jeder virtuellen Maschine finden Sie unter „Zuweisen von Arbeitsspeicher zu einem Gastbetriebssystem“, auf Seite 28. Berücksichtigen Sie ferner, dass physische Arbeitsspeicherkosten nicht linear sind und dass es in einigen Situationen wirtschaftlicher sein kann, mehr kleinere Server ohne teure DIMM-Chips zu beschaffen. In anderen Fällen können die Rack-Dichte, Speicheranbindung, Verwaltbarkeit und andere Aspekte dafür ausschlaggebend sein, die Anzahl der Server in einer Bereitstellung zu minimieren.

Empfehlungen für ESX 3.5-Knotenkomponenten in Tabelle 4-7 sind VMware View-spezifisch. Allgemeine Informationen zu Einschränkungen von ESX-Hosts in vSphere finden Sie im Dokument *VMware vSphere Configuration Maximums* (Maximalwerte bei der Konfiguration von VMware vSphere).

Tabelle 4-7. VMware View-Knoten: Beispiel für einen ESX-Server

Element	Beispiel
ESX-Version	ESX 3.5 U4 oder ESX 4.0 U1
Gehäusetyp	Blade oder Rack
CPU	Vier Kerne mit zwei oder vier Sockets
CPU-Geschwindigkeit	3,0 GHz pro Kern
Arbeitsspeicher (RAM)	128 GB
Ethernet-Anschlüsse	1 Gigabit
Virtuelle Maschinen pro Kern	8
Kerne pro Knoten	8 bei ESX 3.5, 16 bei ESX 4.0 U1
Netzwerkadapter	4 (32 virtuellen Maschine pro Netzwerkadapter)
Speicherdichte von View-Desktop, in virtuellen Maschinen pro LUN	64
Fiber Channel-Adapteranschlüsse	0 oder mehr

HINWEIS VMware View 3.x kann nicht unter vSphere 4 ausgeführt werden.

vSphere-Cluster

VMware View-Bereitstellungen können VMware HA-Cluster (High Availability) als Schutz gegen Ausfälle physischer Server nutzen. Da jeder ESX-Server in einem View-Cluster mehr als 40 virtuelle Maschinen hostet und View Composer-Einschränkungen vorliegen, darf das Cluster nicht mehr als acht Server bzw. Knoten enthalten.

VMware vSphere und vCenter bieten zahlreiche Funktionen zum Verwalten von Clustern mit Servern, die View-Desktops hosten. Die Cluster-Konfiguration ist auch von Bedeutung, da jeder View-Desktop-Pool einem vCenter-Ressourcenpool zugeordnet sein muss. Deshalb hängt die maximale Anzahl der Desktops pro Pool von der Anzahl der Server und virtuellen Maschinen ab, die Sie pro Cluster ausführen möchten.

Bei sehr großen VMware View-Bereitstellungen kann die Leistung und Reaktionsschnelligkeit von vCenter durch das Beschränken auf ein einziges Cluster-Objekt pro Rechenzentrumsobjekt verbessert werden, was nicht die Standardeinstellung ist. Standardmäßig erzeugt VMware vCenter neue Cluster innerhalb desselben Rechenzentrumsobjekts.

Bestimmen der Hochverfügbarkeitsanforderungen

VMware vSphere ermöglicht dank seiner effizienten Ressourcenverwaltung eine optimale Anzahl virtueller Maschinen pro Server. Doch eine höhere Dichte virtueller Maschinen pro Server bedeutet, dass bei einem Serverausfall mehr Benutzer betroffen sind.

Je nach Zweck des Desktop-Pools können sich die Hochverfügbarkeitsanforderungen wesentlich unterscheiden. Beispielsweise kann ein nicht persistenter Pool andere RPO-Anforderungen (Recovery Point Objective) haben als ein persistenter Pool. Bei einem nicht persistenter Pool kann eine akzeptable Lösung darin bestehen, dass sich die Benutzer an einem anderen Desktop anmelden, sobald der Desktop, den sie ansonsten nutzen, nicht verfügbar ist.

Sofern die Verfügbarkeitsanforderungen hoch sind, ist eine ordnungsgemäße Konfiguration von VMware HA wesentlich. Wenn Sie VMware HA einsetzen und eine feste Anzahl an Desktops pro Server einplanen, müssen Sie jeden Server mit reduzierter Kapazität ausführen. Sollte ein Server ausfallen, wird die Kapazität von Desktops pro Server nicht überschritten, wenn die Desktops auf einem anderen Host neu gestartet werden.

Beispiel: Wenn für ein Cluster mit acht Hosts, in dem jeder Host 128 Desktops unterstützen kann, das Ziel die Tolerierung des Ausfalls eines einzelnen Servers ist, sorgen Sie dafür, dass nicht mehr als 128 x (8-1) = 896 Desktops in diesem Cluster ausgeführt werden. Sie können auch mit VMware DRS (Distributed Resource Scheduler) arbeiten, um die Desktops gleichmäßig auf alle acht Hosts zu verteilen. Sie können die zusätzliche Serverkapazität vollständig nutzen, ohne dass in Reserve gehaltene Ressourcen ungenutzt bleiben. Darüber hinaus unterstützt DRS die Neuverteilung im Cluster, nachdem ein ausgefallener Server wieder den Betrieb aufgenommen hat.

Sie müssen außerdem sicherstellen, dass die Datenspeicherung ordnungsgemäß konfiguriert ist, um die E/A-Last zu unterstützen, die sich aus dem gleichzeitigen Neustart vieler virtueller Maschinen als Reaktion auf einen Serverausfall ergibt. Die Anzahl der E/A-Vorgänge pro Sekunden (IOPS) des Speichersystems hat den größten Einfluss darauf, wie schnell Desktops nach einem Serverausfall wiederhergestellt werden.

Beispiel 4-1. Beispiel der Konfiguration eines Clusters

Die Einstellungen in Tabelle 4-8 sind VMware View-spezifisch. Informationen zu den Grenzwerten von HA-Clustern in vSphere finden Sie im Dokument *VMware vSphere Configuration Maximums* (Maximalwerte bei der Konfiguration von VMware vSphere).

Tabelle 4-8. Beispiel eines HA-Clusters

Element	Beispiel
Knoten (ESX-Server)	8 (einschließlich einem in Reserve)
Cluster-Typ	DRS (Distributed Resource Scheduler)/HA

Tabelle 4-8. Beispiel eines HA-Clusters (Fortsetzung)

Element	Beispiel
Netzwerkkomponente	Standardmäßiges ESX 3.5 oder 4-Cluster-Netzwerk
Switch-Ports	48 verwaltete GigE für ESX 3.5 bzw. 80 für ESX 4

Die Netzwerkanforderungen hängen vom Servertyp, der Anzahl der Netzwerkadapter und der Konfiguration von vMotion ab.

VMware View-Bausteine

Ein Baustein für 1000 Benutzer besteht aus physischen Servern, einer VMware vSphere-Infrastruktur, VMware View-Servern, gemeinsamem Speicher sowie 1000 Desktops auf Basis virtueller Maschinen. Eine View-Struktur kann bis zu fünf Bausteine umfassen.

Tabelle 4-9. Beispiel eines LAN-basierten View-Bausteins

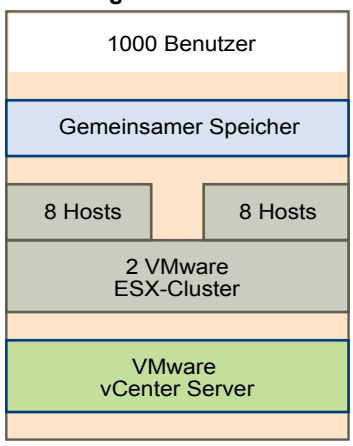
Element	Beispiel
vSphere-Cluster	2 (mit 8 ESX-Hosts pro Cluster)
Netzwerk-Switch mit 48 Ports	1
Gemeinsame Netzwerkspeicherkomponente	1
vCenter-Server mit View Composer	1 (kann im Baustein selbst ausgeführt werden)
Datenbank	Microsoft SQL Server 2005 oder Oracle-Datenbankserver (kann im Baustein selbst ausgeführt werden)
Gemeinsame Speicherkomponente	1 (mit 64 virtuellen Maschine pro LUN)
Netzwerke	3 (jeweils ein 1 Gbit-Ethernet-Netzwerk: Verwaltungsnetzwerk, Speichernetzwerk und VMotion-Netzwerk)

Wenn die View-Struktur nur einen Baustein enthält, können Sie zu Redundanzzwecken zwei View Connection Server-Instanzen einsetzen.

Diese Informationen stammen aus *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments* (VMware View-Referenzarchitektur: Anleitung für umfangreiche VMware View-Bereitstellungen in Unternehmen).

Abbildung 4-1 zeigt die Komponenten eines View-Bausteins.

Abbildung 4-1. VMware View-Baustein



Gemeinsamer Speicher für View-Bausteine

Die Speicherung von Daten ist einer der Hauptgründe, warum sich Unternehmen der Virtualisierungstechnologie zuwenden. Die Entscheidung mit dem größten Einfluss auf die Systemarchitektur ist die für den Einsatz von View Composer-Desktops, die mit einer auf verknüpften Klonen basierenden Technologie arbeiten.

Das externe Speichersystem, das von VMware vSphere verwendet wird, kann ein Fibre-Channel oder iSCSI-SAN-(Storage Area Network) oder ein NFS (Network File System)- oder CIFS (Common Internet File System)-NAS-System (Network-Attached Storage) sein. Die ESX-Binärdateien, die Auslagerungsdateien virtueller Maschinen und View Composer-Replikate übergeordneter virtueller Maschinen werden in diesem System gespeichert.

Aus Architektursicht hat die Entscheidung für den Einsatz von View Composer die größte Auswirkung auf die Speicherplanung. View Composer erstellt Desktop-Images, die ein Basis-Image gemeinsam nutzen, wodurch die Speicheranforderungen um 50 % und mehr gesenkt werden können. Sie können die Speicheranforderungen weiter reduzieren, indem Sie eine Aktualisierungsrichtlinie festlegen, die den Desktop regelmäßig in den Originalzustand zurückversetzt, wodurch Speicherplatz freigegeben wird, der zum Nachverfolgen von Änderungen seit dem letzten Aktualisierungsvorgang verwendet wird.

Sie können auch den Festplattenspeicher des Betriebssystems verkleinern, indem Sie View Composer-Datenfestplatten oder freigegebene Dateiserver als primäre Speicherorte für die Profile und Dokumente der Benutzer einsetzen. Da View Composer das Trennen von Benutzerdaten vom Betriebssystem erlaubt, müssen ggf. nur die Benutzerdatenfestplatten gesichert oder repliziert werden, was die Speicheranforderungen weiter senkt. Weitere Informationen finden Sie unter „Reduzieren von Speicheranforderungen mit View Composer“, auf Seite 23.

Beispiel 4-2. Speicherbeispiel

Als Speicherbeispiel enthält Tabelle 4-10 die in *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments* (VMware View-Referenzarchitektur: Anleitung für umfangreiche VMware View-Bereitstellungen in Unternehmen) veröffentlichten Speicherkomponenten. Mit dieser Tabelle können Sie sich einen Überblick verschaffen, welche Speicherkonfiguration für einen View-Baustein für maximale 1000 Benutzer erforderlich ist.

Tabelle 4-10. Beispiel einer EMC NS20FC-Speicherkonfiguration

Element	Anzahl bzw. Größe
Celerra NS20FC mit einem CLARiiON CX3-10F-Back-End-Array	1
CLARiiON-Schreib-Cache	259 MB
X-Blade 20-Konfigurationen	2
Pentium IV-CPUs mit 2,8 GHz	2
Double-Data-Rate-RAM (266 MHz)	4
Fibre Channel-Ports für Back-End-Speicherverbindungen	2
10/100/1000 BaseT-Ethernet-Ports	4
300 GB/15 K 2/4-GB Fibre Channel-Festplatten	30

Hardware-Beispiele für View-Bausteine und -Strukturen

Die virtuelle Infrastruktur einer Struktur von VMware View-Bausteinen befindet sich auf physischen Servern. VMware setzt Blade-Server-Gehäuse zum Überprüfen seiner Bausteinarchitektur ein. Sie können aber auch einen beliebigen anderen Servertyp mit denselben technischen Daten nutzen.

Beispiel 4-3. Hardware für die VMware View-Infrastruktur

Der Hardware in Tabelle 4-11 ähnliche Hardware eignet sich zum Hosten der Infrastrukturkomponenten eines View-Bausteins. Zu Infrastrukturkomponenten zählen Server auf Basis virtueller Maschinen, die als Hosts für Active Directory, DNS, DHCP, View Connection Server-Instanzen, vCenter mit View Composer und der Datenbank für vCenter dienen.

Tabelle 4-11. Beispiel der Hardware eines Bausteins mit Infrastrukturkomponenten

Element	Anzahl bzw. Größe
Blade-Gehäuse mit 16 Einschüben	1
Blade-Server	4
Vier-Kern-Prozessoren mit 2,66 GHz	4
Arbeitsspeicher (RAM)	32GB
72 GB-SAS-Laufwerk	1
Broadcom Gb Ethernet-Adapter	4

Von den vier Blade-Servern sind zwei zum Laden von Clients, einer für eine View Connection Server-Instanz und einer für Active Directory, DNS und DHCP vorgesehen.

Beispiel 4-4. Hosting-Hardware für VMware View-Desktops

Der Hardware in Tabelle 4-12 ähnliche Hardware eignet sich zum Hosten der virtuellen Desktops für einen View-Baustein mit maximal 1000 Benutzern.

Tabelle 4-12. Beispiel der Hardware für einen VMware View-Baustein

Element	Anzahl bzw. Größe
Blade-Gehäuse mit 16 Einschüben	1 für 2 Bausteine
Blade-Server	16 (8 pro Cluster)
Vier-Kern-Prozessoren mit 2,66 GHz	4
Arbeitsspeicher (RAM)	64 GB (32 GB pro Cluster)
72 GB-SAS-Laufwerk	2
Broadcom Gb Ethernet-Adapter	12 (6 pro Cluster)
Gigabit-Uplink-Module mit vier Ports	12 (6 pro Cluster)
Cisco 6500 Kern-Netzwerk-Switch	1

Sowohl die Infrastrukturkomponenten als auch die View-Desktops sind Teil von VMware HA-Clustern zu deren Schutz gegen den Ausfall physischer Server.

Diese Informationen stammen aus *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments* (VMware View-Referenzarchitektur: Anleitung für umfangreiche VMware View-Bereitstellungen in Unternehmen).

Aspekte bei der Bandbreite eines VMware View-Bausteins

Wenngleich viele Elemente beim Entwurf eines Speichersystems zur Unterstützung einer VMware View-Umgebung wichtig sind, ist das Planen einer ordnungsgemäßen Bandbreite aus Sicht der Serverkonfiguration besonders wesentlich. Außerdem müssen die Auswirkungen von Hardware zur Portkonsolidierung berücksichtigt werden.

Spitzenarbeitslasten

In VMware View-Umgebungen kann es gelegentlich zu E/A-Überlastungen kommen, wenn alle virtuellen Maschinen gleichzeitig eine Aktivität ausführen. E/A-Überlastungen können einerseits durch gastbasierte Agenten wie Antivirussoftware oder Software-Update-Agenten, andererseits durch menschliches Verhalten ausgelöst werden, z. B. wenn sich alle Mitarbeiter morgens nahezu zeitgleich anmelden.

Sie können diese Überlastungen durch Befolgen empfohlener Vorgehensweisen minimieren, z. B. durch Staffelung von Updates für unterschiedliche virtuellen Maschinen. Sie können im Rahmen einer Pilotphase auch verschiedene Abmeldungsrichtlinien testen, um zu bestimmen, ob virtuelle Maschinen angehalten oder ausgeschaltet werden sollen, wenn Benutzerabmeldungen zu einer E/A-Überlastung führen.

Zusätzlich zum Befolgen empfohlener Vorgehensweisen empfiehlt VMware die Bereitstellung einer Bandbreite von 1 Gbit/s pro 100 virtuellen Maschinen, auch wenn die durchschnittliche Bandbreite ggf. zehnmal niedriger ist. Eine solch konservative Planung stellt bei Spitzenarbeitslasten stets genügend Speicherverbindungen bereit.

Datenverkehr für Bildschirmanzeigen

Beim Datenverkehr für Bildschirmanzeigen können sich viele Elemente auf die Netzwerkbandbreite auswirken, z. B. das verwendete Protokoll, die Monitorauflösung und Konfiguration sowie der Umfang multimedialer Inhalte in der Arbeitslast. Der gleichzeitige Start per Streaming übertragener Anwendungen kann auch zu Nutzungsspitzen führen.

Da sich die Auswirkungen dieser Aspekte stark unterscheiden können, messen viele Unternehmen die Bandbreitenbelegung im Rahmen eines Pilotprojekts. Als Ausgangswert für ein Pilotprojekt bietet sich eine Kapazität von 150-200 Kbit/s für einen typischen Büroanwender an.

WAN-Unterstützung

Bei Weitbereichsnetzwerken (WAN) müssen Sie Bandbreiteneinschränkungen und Wartezeiten berücksichtigen.

Beim Verwenden des Anzeigeprotokolls RDP ist ein WAN-Optimierungsprodukt zum Beschleunigen von Anwendungen für Benutzer in Niederlassungen und kleinen Büroumgebungen erforderlich.

Tabelle 4-13. Unterstützen kleiner und mittelgroßer Büroumgebungen mithilfe der WAN-Optimierung

Element	Kleinbüro	Niederlassung
Anzahl der Benutzer	Bis zu 15	Bis zu 100
Verbindungstyp	T1	10 Mbit/s
Bandbreite	1544 Mbit/s	10 Mbit/s
Wartezeit	Bis zu 100 ms	Bis zu 100 ms

Benutzer, die von zu Hause aus über ein DSL- oder Kabelmodem auf einen View-Desktop mit dem Anzeigeprotokoll RDP zugreifen, benötigen ggf. keine WAN-Optimierung. In diesem Fall kann das Netzwerk drei bis fünf Benutzer unterstützen.

Diese Informationen stammen aus *VMware View WAN Reference Architecture* (VMware View – WAN-Referenzarchitektur).

VMware View-Struktur

Eine VMware View-Struktur integriert fünf Bausteine mit je 1000 Benutzern in einer View Manager-Installation, die Sie als Einheit verwalten können.

Eine Struktur ist eine Organisationseinheit, die durch Einschränkungen der Skalierbarkeit von VMware View bestimmt wird. Tabelle 4-14 zeigt die Komponenten einer View-Struktur.

Tabelle 4-14. Beispiel einer VMware View-Struktur

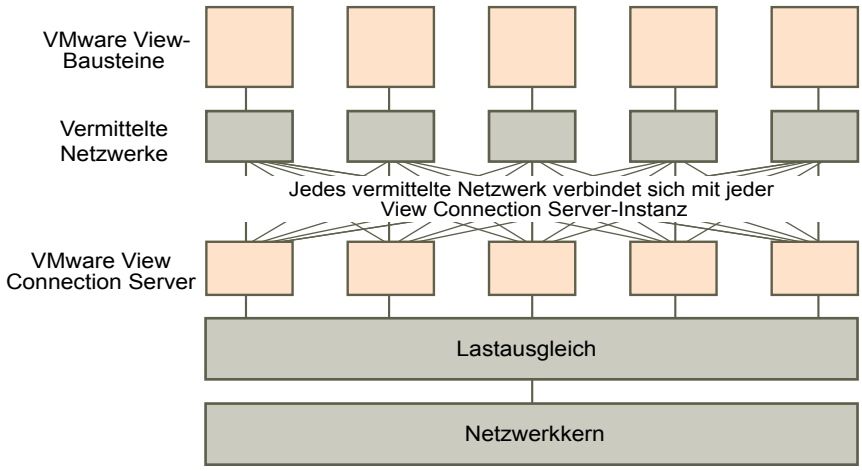
Element	Anzahl bzw. Größe
View-Bausteine	5
View Connection Server	5 (einer pro Baustein)
View Security Server	2 - 5 (mit Lastausgleich im Umkreisnetzwerk [DMZ])
10-Gbit-Ethernet-Modul	1
Modularer Kern-Netzwerk-Switch	1
Lastausgleichsmodul	1
VPN für WAN	1 (optional)
WAN-Beschleuniger bei Verwendung von RDP	1 (optional)

Der Netzwerkkern sorgt für eine gleichmäßige Verteilung eingehender Anforderungen auf die View Connection Server-Instanzen. Durch Unterstützung eines Redundanz- und Failover-Mechanismus, zumeist auf Netzwerkebene, wird verhindert, dass das Lastausgleichsmodul selbst zu einer Fehlerquelle wird. Das Virtual Router Redundancy Protocol (VRRP) kommuniziert beispielsweise mit dem Lastausgleichsmodul, um Redundanz- und Failover-Funktionen hinzuzufügen.

Wenn eine View Connection Server-Instanz während einer aktiven Sitzung ausfallen oder nicht mehr reagieren sollte, verlieren die Benutzer keine Daten. Der Desktop-Status wird im virtuellen Desktop gespeichert, sodass sich Benutzer mit einer anderen View Connection Server-Instanz verbinden und ihre Desktop-Sitzung an der Stelle fortsetzen können, an der es zum Ausfall gekommen war.

Abbildung 4-2 zeigt, wie alle Komponenten zu einer einzelnen verwaltbaren Einheit integriert werden können.

Abbildung 4-2. Abbildung einer Struktur für 5000 View-Desktops



Planen von Sicherheitsfunktionen 5

View Manager bietet leistungsstarke Netzwerksicherheitsfunktionen zum Schutz vertraulicher Unternehmensdaten. Zur Optimierung der Sicherheit können Sie View Manager mit verschiedenen Authentifizierungslösungen anderer Anbieter integrieren, einen Sicherheitsserver einsetzen und die Einschränkungsfunktion für Berechtigungen implementieren.

Dieses Kapitel behandelt die folgenden Themen:

Grundlegendes zu Clientverbindungen

View Client und View Administrator kommunizieren mit einem View Connection Server-Host über sichere HTTPS-Verbindungen.

Die einleitende View Client-Verbindung zur Benutzerauthentifizierung und View-Desktop-Auswahl wird eingerichtet, wenn ein Benutzer in View Client eine IP-Adresse angibt. Die View Administrator-Verbindung wird hergestellt, wenn ein Administrator die View Administrator-URL in einen Web-Browser eingibt.

View Manager bietet standardmäßig ein selbst signiertes SSL-Zertifikat, das Clients verwenden, wenn sie sich mit einem View Connection Server-Host verbinden. Clients werden standardmäßig mit diesem selbst signierten SSL-Zertifikat präsentiert, wenn sie eine sichere Seite wie die View Administrator-Seite besuchen.

Sie können das SSL-Standardzertifikat für Tests verwenden. Da es für Clients nicht vertrauenswürdig ist und nicht den für den Dienst ordnungsgemäßen Namen enthält, müssen Sie das SSL-Standardzertifikat ersetzen. Sie können ein eigenes selbst signiertes Zertifikat erstellen, ein signiertes Zertifikat von einer Zertifizierungsstelle beziehen oder ein bereits vorhandenes SSL-Zertifikat nutzen.

- Getunnelte Clientverbindungen mit Microsoft RDP auf Seite 44

  Wenn Benutzer sich mit einem View-Desktop mit dem Anzeigeprotokoll RDP verbinden, baut View Client eine zweite HTTPS-Verbindung mit dem View Connection Server-Host auf. Diese Verbindung wird als „Tunnelverbindung“ bezeichnet, da sie einen Tunnel für die Übertragung von RDP-Daten bereitstellt.

- Direkte Clientverbindungen mit PCoIP und HP RGS auf Seite 44

  Administratoren können View Connection Server-Einstellungen so konfigurieren, dass View-Desktop-Sitzungen zwischen dem Clientsystem und der virtuellen Maschine mit dem View-Desktop unter Umgehung des View Connection Server-Hosts direkt aufgebaut werden. Dieser Verbindungstyp wird als „direkte Clientverbindung“ bezeichnet.

- View Client with Offline Desktop-Clientverbindungen auf Seite 45

  View Client with Offline Desktop ist eine experimentelle Funktion, die mobilen Benutzern die Möglichkeit bietet, ein geklonte Instanz verschiedener Typen von View-Desktops auf ihren lokalen Computern zu überprüfen.

Getunnelte Clientverbindungen mit Microsoft RDP

Wenn Benutzer sich mit einem View-Desktop mit dem Anzeigeprotokoll RDP verbinden, baut View Client eine zweite HTTPS-Verbindung mit dem View Connection Server-Host auf. Diese Verbindung wird als „Tunnelverbindung“ bezeichnet, da sie einen Tunnel für die Übertragung von RDP-Daten bereitstellt.

Die Tunnelverbindung bietet die folgenden Vorteile:

- RDP-Daten werden über HTTPS getunnelt übertragen und mit SSL verschlüsselt. Dieses leistungsstarke Sicherheitsprotokoll stellt auch die Grundlage der Sicherheit anderer Websites dar, z. B. für das Onlinebanking oder Zahlungen per Kreditkarte.
- Ein Client kann über eine einzelne HTTS-Verbindung auf mehrere Desktops zugreifen, wodurch der gesamte Protokoll-Overhead reduziert wird.
- Da View Manager die HTTPS-Verbindung verwaltet, wird die Zuverlässigkeit der zugrunde liegenden Protokolle wesentlich verbessert. Wird bei einem Benutzer eine Netzwerkverbindung vorübergehend unterbrochen, wird die HTTPS-Verbindung wieder aufgebaut, nachdem die Netzwerkverbindung wiederhergestellt wurde, und die RDP-Verbindung automatisch fortgesetzt, ohne dass sich der Benutzer erneut verbinden und anmelden muss.

Bei einer Standardbereitstellung von View Connection Server-Instanzen endet die sichere HTTPS-Verbindung beim View Connection Server. In einer Bereitstellung mit Umkreisnetzwerk (DMZ) endet die sichere HTTPS-Verbindung beim Sicherheitsserver. Unter „Vorbereiten des Einsatzes eines Sicherheitsservers“, auf Seite 48 finden Sie weitere Informationen zu Bereitstellungen mit Umkreisnetzwerk (DMZ) und Sicherheitsservern.

Clients mit den Anzeigeprotokollen PCoIP und HP RGS nutzen nicht die Tunnelverbindung. Weitere Informationen finden Sie unter „Direkte Clientverbindungen mit PCoIP und HP RGS“, auf Seite 44.

Direkte Clientverbindungen mit PCoIP und HP RGS

Administratoren können View Connection Server-Einstellungen so konfigurieren, dass View-Desktop-Sitzungen zwischen dem Clientsystem und der virtuellen Maschine mit dem View-Desktop unter Umgehung des View Connection Server-Hosts direkt aufgebaut werden. Dieser Verbindungstyp wird als „direkte Clientverbindung“ bezeichnet.

Auch bei direkten Clientverbindungen wird zur Authentifizierung von Benutzern und Auswahl von View-Desktops eine HTTPS-Verbindung zwischen dem Client und View Connection Server-Host aufgebaut, ohne dass jedoch die zweite HTTPS-Verbindung (die Tunnelverbindung) verwendet wird.

Wenn Clients mit den Anzeigeprotokollen PCoIP und HP RGS arbeiten, müssen Sie direkte Clientverbindungen aktivieren.

Für PCoIP-Verbindungen gibt es die folgenden vordefinierten Sicherheitsfunktionen:

- PCoIP unterstützt die AES-Verschlüsselung (Advanced Encryption Standard), die standardmäßig aktiviert ist.
- Die Hardware-Implementierung von PCoIP verwendet sowohl AES als auch IPsec (IP Security).
- PCoIP arbeitet mit VPN-Clients anderer Anbieter zusammen.

Bei Clients, die mit dem Microsoft-Anzeigeprotokoll RDP arbeiten, dürfen direkte Clientverbindungen nur verwendet werden, wenn sich die VMware View-Bereitstellung innerhalb eines Firmennetzwerks befindet. Bei direkten Clientverbindungen wird RDP-Datenverkehr unverschlüsselt über die Verbindung zwischen dem Client und der virtuellen Maschine mit dem View-Desktop gesendet. Weitere Informationen finden Sie unter „Getunnelte Clientverbindungen mit Microsoft RDP“, auf Seite 44.

View Client with Offline Desktop-Clientverbindungen

View Client with Offline Desktop ist eine experimentelle Funktion, die mobilen Benutzern die Möglichkeit bietet, ein geklonte Instanz verschiedener Typen von View-Desktops auf ihren lokalen Computern zu überprüfen.

View Client with Offline Desktop unterstützt für Datenübertragungen im LAN sowohl eine getunnelte als auch nicht getunnelte Kommunikation. Bei der getunnelten Kommunikation wird der gesamte Datenverkehr durch den View Connection Server-Host geleitet, und Sie können angeben, ob die Kommunikation und Datenübertragungen verschlüsselt werden sollen. Bei der nicht getunnelten Kommunikation werden Daten unverschlüsselt direkt zwischen dem Offline Desktop-Clientsystem und der virtuellen Maschine mit dem View-Desktop übertragen.

Offline-Daten werden stets auf dem Computer des Benutzers unabhängig davon verschlüsselt, ob Sie eine getunnelte oder nicht getunnelte Kommunikation konfigurieren.

Auswählen einer Benutzerauthentifizierungsmethode

View Manager nutzt standardmäßig die vorhandene Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Zur Optimierung der Sicherheit können Sie View Manager mit RSA SecurID- und Smartcard-Authentifizierungslösungen integrieren.

- Active Directory-Authentifizierung auf Seite 46

  Jede View Connection Server-Instanz tritt einer Active Directory-Domäne bei, und die Benutzer werden für diese Domäne im Abgleich mit Active Directory authentifiziert.

- RSA SecurID-Authentifizierung auf Seite 46

  RSA SecurID bietet eine optimierte Sicherheit mit zweistufiger Authentifizierung, bei der der Benutzer PIN und Token-Code kennen muss. Der Token-Code wird nur auf dem SecurID-Token-Gerät angezeigt.

- Smartcard-Authentifizierung auf Seite 47

  Eine Smartcard ist eine kleine Kunststoffkarte, auf der sich ein Computerchip befindet. Viele Behörden und Großunternehmen statten ihre Benutzer zu Authentifizierungszwecken für den Zugriff auf ihre Computernetzwerke mit Smartcard aus. Eine Smartcard wird auch als „Common Access Card (CAC)“ bezeichnet.

- Die Funktion „Anmelden als aktueller Benutzer“ auf Seite 47

  Wenn View Client-Benutzer das Kontrollkästchen **[Log in as current User (Anmelden als aktueller Benutzer)]** aktivieren, werden die Anmeldedaten, die sie bei der Anmeldung am Clientsystem eingegeben haben, zur Authentifizierung bei der View Connection Server-Instanz und beim View-Desktop verwendet. Keine weitere Benutzerauthentifizierung ist erforderlich.

Active Directory-Authentifizierung

Jede View Connection Server-Instanz tritt einer Active Directory-Domäne bei, und die Benutzer werden für diese Domäne im Abgleich mit Active Directory authentifiziert.

Benutzer werden ferner im Abgleich mit beliebigen weiteren Benutzerdomänen authentifiziert, zu denen eine Vertrauensstellung besteht.

Beispiel: Wenn eine View Connection Server-Instanz zur Domäne A gehört und eine Vertrauensstellung zwischen Domäne A und Domäne B besteht, können sich Benutzer in sowohl Domäne A als auch Domäne B über View Client mit der View Connection Server-Instanz verbinden.

Wenn gleichsam eine Vertrauensstellung zwischen Domäne A und einem MIT-Kerberos-Bereich in einer heterogenen Domänenumgebung besteht, können Benutzer im Kerberos-Bereich beim Verbinden mit der View Connection Server-Instanz mittels View Client den Kerberos-Bereichsnamen auswählen.

View Connection Server bestimmt, auf welche Domänen zugegriffen werden kann, indem beginnend mit der Domäne, in der sich der Host befindet, Vertrauensbeziehungen durchlaufen werden. Bei einer kleinen, vielfach verbundenen Gruppe von Domänen kann View Connection Server rasch eine vollständige Liste mit Domänen bestimmen, doch die Zeit nimmt mit einer ansteigenden Zahl von Domänen oder bei Abnahme der Verbindungen zwischen den Domänen zu. Die Liste kann auch Domänen enthalten, die Sie Benutzern nicht anbieten möchten, wenn sie sich mit ihren Desktops verbinden.

Über den Befehl `vdmadmin` können Administratoren eine Domänenfilterung konfigurieren, mit deren Hilfe die Domänen eingeschränkt werden, die eine View Connection Server-Instanz oder ein Sicherheitsserver durchsucht und die den Benutzer angezeigt werden. Im technischen Hinweis *Befehlszeilenprogramm für View Manager* finden Sie weitere Informationen.

Richtlinien, z. B. zum Einschränken der Zeiten, in denen eine Anmeldung möglich ist, und zum Festlegen des Ablaufdatums von Kennwörtern, werden ebenfalls mithilfe von Active Directory verwaltet.

RSA SecurID-Authentifizierung

RSA SecurID bietet eine optimierte Sicherheit mit zweistufiger Authentifizierung, bei der der Benutzer PIN und Token-Code kennen muss. Der Token-Code wird nur auf dem SecurID-Token-Gerät angezeigt.

Administratoren können einzelne View Connection Server-Instanzen für die RSA SecurID-Authentifizierung aktivieren, indem die RSA SecurID-Software auf dem View Connection Server-Host installiert wird und die View Connection Server-Einstellungen geändert werden.

Wenn sich Benutzer über eine View Connection Server-Instanz anmelden, die für die RSA SecurID-Authentifizierung aktiviert ist, müssen sie sich zuerst mit ihrem RSA-Benutzernamen und -Passcode authentifizieren. Wenn auf dieser Stufe keine Authentifizierung erfolgt, wird der Zugriff verweigert. Wenn sie ordnungsgemäß bei RSA SecurID authentifiziert werden, können sie wie gewohnt fortfahren und müssen anschließend ihre Active Directory-Anmeldedaten eingeben.

Wenn es mehrere View Connection Server-Instanzen gibt, können Sie die RSA SecurID-Authentifizierung für einige Instanzen konfigurieren und für andere eine andere Benutzerauthentifizierungsmethode einrichten. Sie können beispielsweise die RSA SecurID-Authentifizierung nur für Benutzer konfigurieren, die remote über das Internet auf View-Desktops zugreifen.

View Manager ist gemäß dem RSA SecurID Ready-Programm zertifiziert und unterstützt die vollständige Palette von SecurID-Funktionen, einschließlich New PIN Mode, Next Token Code Mode, RSA Authentication Manager und Lastenausgleich.

Smartcard-Authentifizierung

Eine Smartcard ist eine kleine Kunststoffkarte, auf der sich ein Computerchip befindet. Viele Behörden und Großunternehmen statten ihre Benutzer zu Authentifizierungszwecken für den Zugriff auf ihre Computernetzwerke mit Smartcard aus. Eine Smartcard wird auch als „Common Access Card (CAC)“ bezeichnet.

Administratoren können einzelne View Connection Server-Instanzen für die Smartcard-Authentifizierung konfigurieren. Die Aktivierung einer View Connection Server-Instanz für den Einsatz der Smartcard-Authentifizierung erfordert zumeist das Hinzufügen Ihres Stammzertifikats zu einer Vertrauensspeicherdatei und das anschließende Ändern der View Connection Server-Einstellungen.

Clientverbindungen, die die Smartcard-Authentifizierung verwenden, müssen für SSL aktiviert sein. Administratoren können SSL für Clientverbindungen aktivieren, indem ein globaler Parameter in View Administrator festgelegt wird.

Jedes Clientsystem, das mit der Smartcard-Authentifizierung arbeitet, benötigt einen mit Windows kompatiblen Smartcard-Leser und produktspezifische Anwendungstreiber.

Die Smartcard-Authentifizierung wird nur von View Client und nicht von View Client with Offline Desktop, View Portal with Offline Desktop, View Portal oder View Administrator unterstützt.

Die Smartcard-Authentifizierung wird nicht für Clients unterstützt, die das PCoIP-Anzeigeprotokoll verwenden.

Die Funktion „Anmelden als aktueller Benutzer“

Wenn View Client-Benutzer das Kontrollkästchen **[Log in as current User (Anmelden als aktueller Benutzer)]** aktivieren, werden die Anmeldedaten, die sie bei der Anmeldung am Clientsystem eingegeben haben, zur Authentifizierung bei der View Connection Server-Instanz und beim View-Desktop verwendet. Keine weitere Benutzerauthentifizierung ist erforderlich.

Zur Unterstützung dieser Funktion werden Benutzeranmeldedaten sowohl in der View Connection Server-Instanz als auch auf dem Clientsystem gespeichert.

- In der View Connection Server-Instanz werden Benutzeranmeldedaten verschlüsselt und in der Benutzersitzung zusammen mit dem Benutzernamen, der Domäne und optional dem Benutzerprinzipalnamen gespeichert. Die Anmeldedaten werden hinzugefügt, wenn eine Authentifizierung erfolgt, und gelöscht, wenn das Sitzungsobjekt endgültig gelöscht wird. Das Sitzungsobjekt wird endgültig gelöscht, wenn sich der Benutzer abmeldet, das Zeitlimit der Sitzung überschritten wird oder die Authentifizierung fehlschlägt. Das Sitzungsobjekt befindet sich im flüchtigen Speicher und wird nicht im LDAP-Verzeichnis oder in einer Datei auf der Festplatte gespeichert.
- Auf dem Clientsystem werden die Anmeldedaten von Benutzern verschlüsselt in einer Tabelle im Authentication Package, einer View Client-Komponente, gespeichert. Die Anmeldedaten werden der Tabelle hinzugefügt, wenn sich der Benutzer anmeldet, und aus der Tabelle entfernt, wenn er sich abmeldet. Die Tabelle verbleibt im flüchtigen Speicher.

Administratoren können mithilfe von View Client-Gruppenrichtlinieneinstellungen die Verfügbarkeit des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** steuern und seine Standardeinstellung festlegen.

Hinweis Wird die Smardcard-Authentifizierung verlangt, misslingt die Authentifizierung von Benutzern, die das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktivieren. Diese Benutzer müssen sich beim Anmelden an einem View-Desktop mithilfe ihrer Smartcard und PIN erneut authentifizieren.

Vorbereiten des Einsatzes eines Sicherheitsservers

Ein Sicherheitsserver ist eine spezielle View Connection Server-Instanz, in der eine Teilmenge der View Connection Server-Funktionen ausgeführt wird. Mithilfe eines Sicherheitsservers können Sie eine weitere Sicherheitsebene zwischen dem Internet und Ihrem internen Netzwerk einführen.

Ein Sicherheitsserver befindet sich in einem Umkreisnetzwerk (auch demilitarisierte Zone [DMZ] genannt) und fungiert als Proxy-Host für Verbindungen innerhalb Ihres vertrauenswürdigen Netzwerks. Jeder Sicherheitsserver bildet mit einer Instanz von View Connection Server ein Paar und leitet den gesamten Datenverkehr an diese Instanz weiter. Dieses Konzept bietet eine weitere Sicherheitsebene, indem die View Connection Server-Instanz vor dem öffentlichen Internet abgeschirmt wird und alle ungeschützten Sitzungsanforderungen zwangsweise durch den Sicherheitsserver geleitet werden.

Eine Umkreisnetzwerkbereitstellung erfordert das Öffnen verschiedener Ports in der Firewall, damit sich Clients mit Sicherheitsservern im Umkreisnetzwerk verbinden können. Sie müssen ferner verschiedene Ports für die Kommunikation zwischen Sicherheitsservern und den View Connection Server-Instanzen im internen Netzwerk konfigurieren. Weitere Informationen zu verschiedenen Ports finden Sie unter „Firewall-Regeln für Sicherheitsserver im Umkreisnetzwerk“, auf Seite 55.

Da sich bei einer Bereitstellung im lokalen Netzwerk Benutzer in ihrem internen Netzwerk direkt mit einer beliebigen View Connection Server-Instanz verbinden können, müssen Sie keinen Sicherheitsserver implementieren.

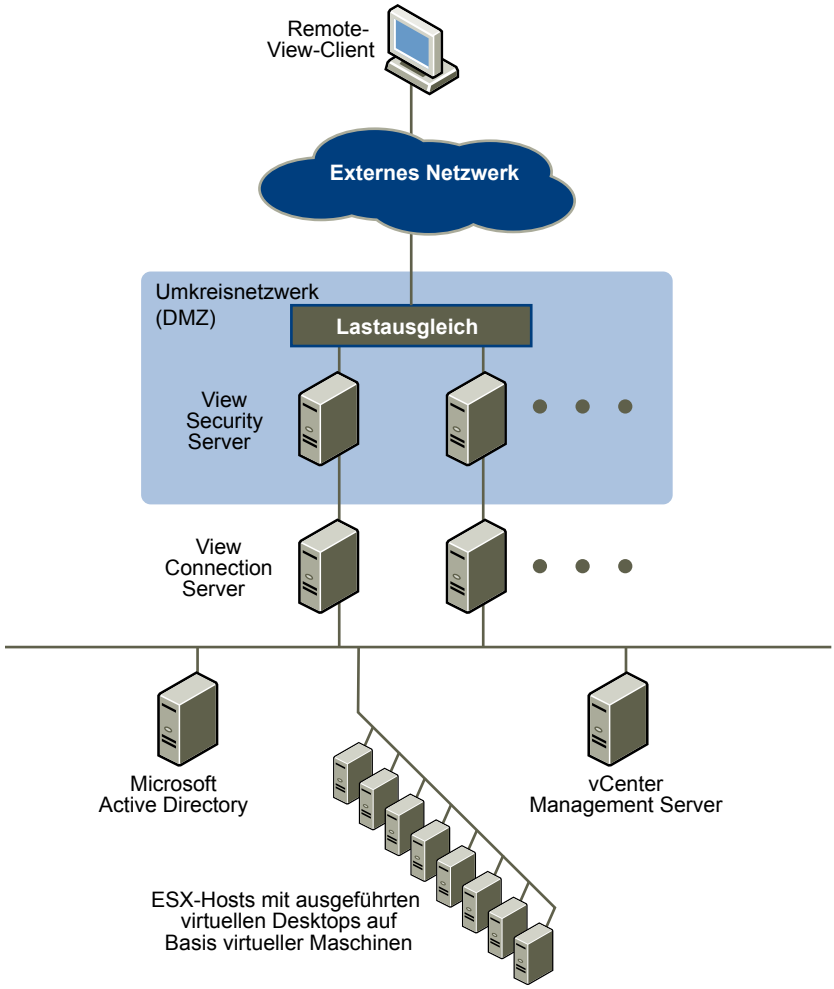
View-Clients, die PCoIP verwenden, können sich mit View-Sicherheitsservern verbinden, aber PCoIP-Sitzungen mit dem virtuellen Desktop ignorieren den Sicherheitsserver. PCoIP nutzt das User Datagram Protocol (UDP) für das Streaming von Audio und Video. Sicherheitsserver unterstützen jedoch nur TCP.

Topologien von Sicherheitsservern

Sie können mehrere verschiedene Topologien von Sicherheitsservern implementieren.

Die Topologie in Abbildung 5-1 zeigt eine hoch verfügbare Umgebung mit zwei mit Lastausgleich arbeitenden Sicherheitsservern in einem Umkreisnetzwerk. Die Sicherheitsserver im Umkreisnetzwerk kommunizieren mit zwei View Connection Server-Instanzen innerhalb des internen Netzwerks.

Abbildung 5-1. Sicherheitsserver mit Lastausgleich in einem Umkreisnetzwerk

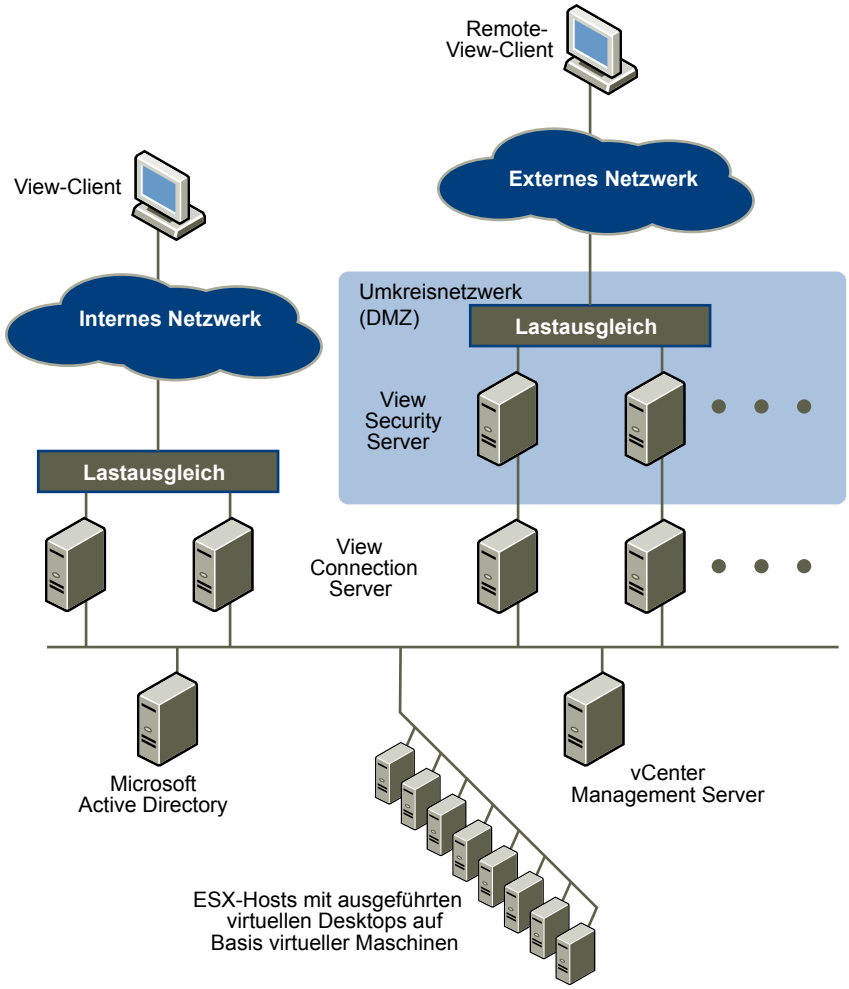


Wenn sich Remote-Benutzer mit einem Sicherheitsserver verbinden, müssen sie sich vor einem Zugriff auf View-Desktops erfolgreich authentifizieren. Bei entsprechenden Firewall-Regeln auf beiden Seiten des Umkreisnetzwerks eignet sich diese Topologie für die Zugriff auf View-Desktops auf Clientgeräten, die mit dem Internet verbunden sind.

Sie können mit jeder Instanz von View Connection Server mehrere Sicherheitsserver verbinden. Sie können auch eine Umkreisnetzwerkbereitstellung mit einer Standardbereitstellung kombinieren, um internen und externen Benutzern einen Zugriff zu bieten.

Die Topologie in Abbildung 5-2 zeigt eine Umgebung, in der vier Instanzen von View Connection Server als eine Gruppe fungieren. Die Instanzen im internen Netzwerk werden von Benutzern im internen Netzwerk, die Instanzen im externen Netzwerk von externen Benutzern verwendet. Wenn die View Connection Server-Instanzen, die mit den Sicherheitsservern Paare bilden, für die RSA SecurID-Authentifizierung aktiviert werden, müssen sich alle Netzwerkbenutzer über RSA SecurID-Token authentifizieren.

Abbildung 5-2. Mehrere Sicherheitsserver



Bei Installation mehrerer Sicherheitsserver müssen Sie eine hardware- oder softwarebasierte Lastausgleichslösung implementieren. View Connection Server arbeitet mit standardmäßigen Lastausgleichslösungen von Drittanbietern zusammen, bietet jedoch keine eigene Lastausgleichsfunktionalität.

Firewalls für Sicherheitsserver im Umkreisnetzwerk

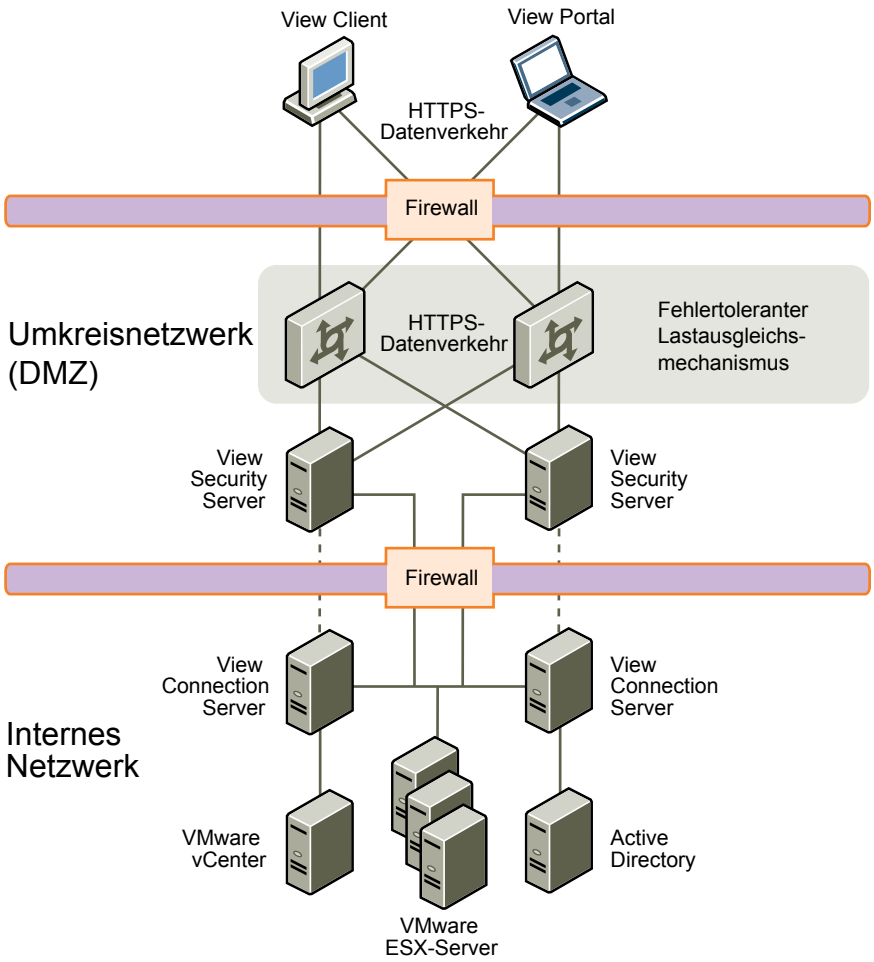
Eine Bereitstellung von Sicherheitsservern in einem Umkreisnetzwerk muss zwei Firewalls aufweisen.

- Eine externe, dem Netzwerk vorgelagerte Front-End-Firewall ist erforderlich, um sowohl das Umkreisnetzwerk als auch das interne Netzwerk zu schützen. Diese Firewall wird so konfiguriert, dass externer Netzwerkdatenverkehr das Umkreisnetzwerk erreichen kann.
- Eine Back-End-Firewall zwischen dem Umkreisnetzwerk und dem internen Netzwerk dient zum Bereitstellen einer zweiten Schutzschicht. Diese Firewall wird so konfiguriert, dass nur Datenverkehr zugelassen wird, der von Diensten innerhalb des Umkreisnetzwerks stammt.

Mithilfe von Firewall-Richtlinien wird die von Diensten im Umkreisnetzwerk eingehende Kommunikation streng kontrolliert, wodurch das Risiko einer Gefährdung des internen Netzwerks stark vermindert wird.

Abbildung 5-3 zeigt eine Beispielkonfiguration mit Front-End- und Back-End-Firewall.

Abbildung 5-3. Zwei-Firewall-Topologie

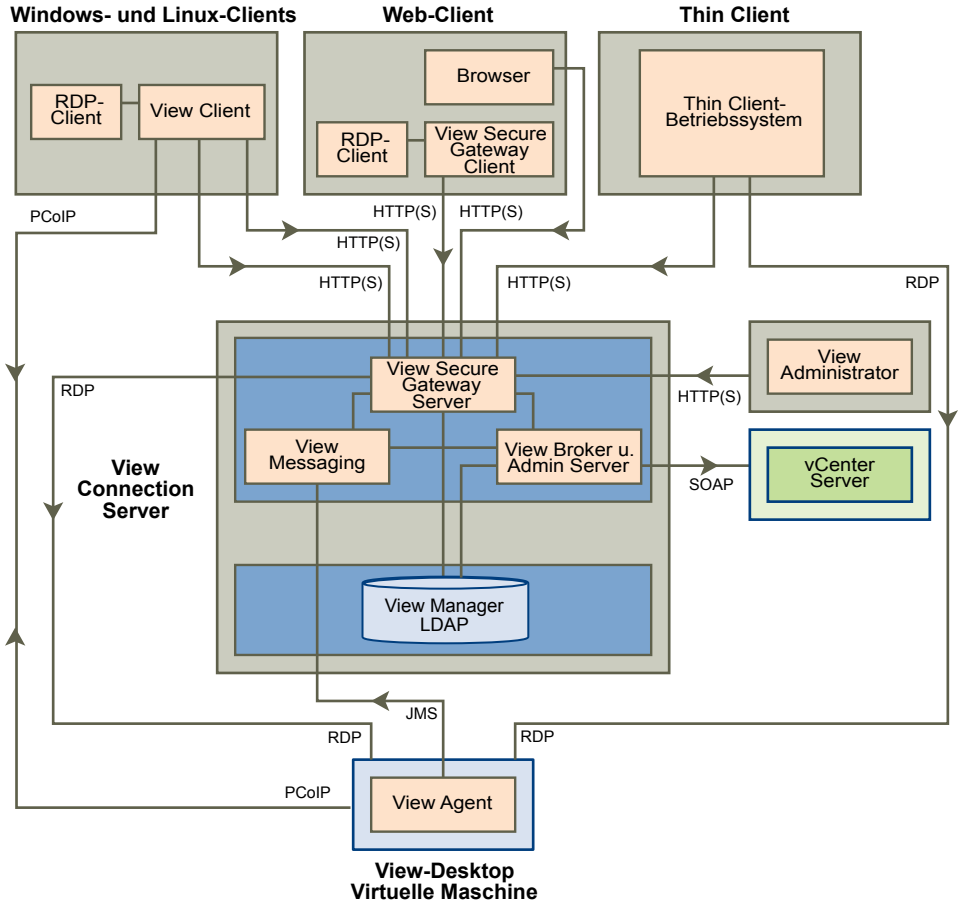


View Manager-Komponenten und -Protokolle

View Manager-Komponenten tauschen Nachrichten mithilfe mehrerer Protokolle aus.

Abbildung 5-4 veranschaulicht die Beziehungen zwischen den View Manager-Komponenten, einschließlich der Protokolle, welche die einzelnen Komponenten zur Kommunikation verwenden, wenn kein Sicherheitsserver konfiguriert ist.

Abbildung 5-4. View Manager-Komponenten und -Protokolle ohne Sicherheitsserver



Unter Tabelle 5-1 finden Sie die Standardports, die von den einzelnen Protokollen verwendet werden.

Abbildung 5-5 veranschaulicht die Beziehungen zwischen dem Sicherheitsserver und allen anderen View Manager-Komponenten, einschließlich der Protokolle, welche die einzelnen Komponenten zur Kommunikation verwenden, wenn ein Sicherheitsserver konfiguriert ist.

Abbildung 5-5. View Manager-Komponenten und -Protokolle mit Sicherheitsserver

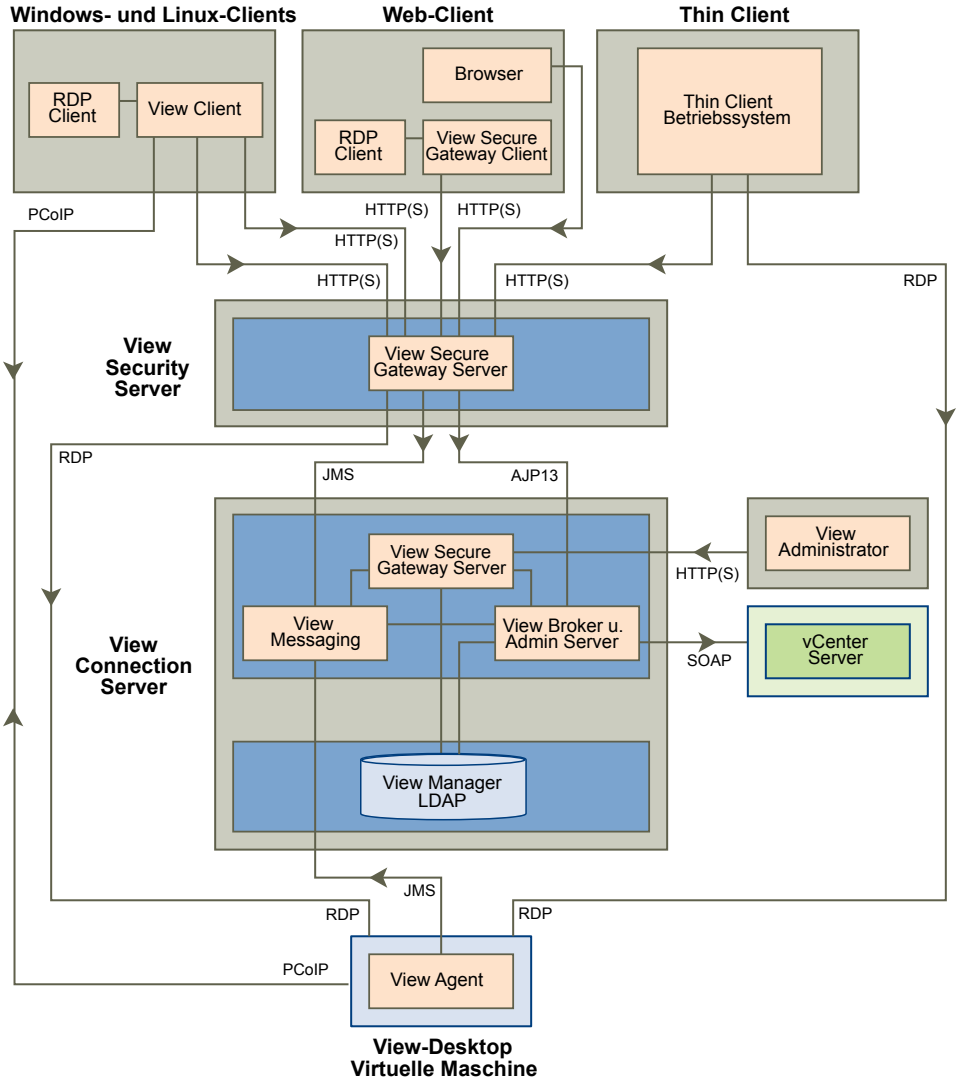


Tabelle 5-1 zeigt die Standardports, die von den einzelnen Protokollen verwendet werden.

Tabelle 5-1. Standardports

Protokoll	Port
JMS	TCP-Port 4001
AJP13	TCP-Port 8009 **Hinweis** AJP13 wird nur in einer Sicherheitsserverkonfiguration verwendet.
HTTP	TCP-Port 80
HTTPS	TCP-Port 443
RDP	TCP-Port 3389 Für die USB-Umleitung wird neben RDP der TCP-Port 32111 verwendet. Für MMR wird neben RDP der TCP-Port 9427 verwendet. **Hinweis** Wenn die View Connection Server-Instanz für direkte Clientverbindungen konfiguriert ist, können sich diese Protokolle direkt vom Client aus mit dem View-Desktop verbinden, ohne getunnelt durch die View Secure Gateway Server-Komponente übertragen zu werden.

Tabelle 5-1. Standardports (Fortsetzung)

Protokoll	Port
SOAP	TCP-Port 80 oder 443
PCoIP	TCP-Port 50002 vom View Client zum View-Desktop. PCoIP nutzt auch UDP-Port 50002 in beiden Richtungen. Für die USB-Umleitung vom Client zum View-Desktop wird neben PCoIP der TCP-Port 32111 genutzt.

View Broker und Administration Server

Die Komponente View Broker, die Hauptkomponente von View Connection Server, ist für die gesamte Benutzerinteraktion zwischen View-Clients und View Connection Server zuständig. Zu View Broker gehört auch die Komponente Administration Server, die vom View Administrator-Web-Client verwendet wird.

View Broker arbeitet eng mit vCenter Server zusammen, um eine erweiterte Verwaltung von View-Desktops zu ermöglichen, einschließlich der Erstellung virtueller Maschinen und Vorgänge zum Ändern des Betriebsstatus.

View Secure Gateway Server

View Secure Gateway Server ist die serverseitige Komponente der sicheren HTTPS-Verbindung zwischen View-Clients und einem Sicherheitsserver oder einer View Connection Server-Instanz.

Wenn Sie die Tunnelverbindung für View Connection Server konfigurieren, wird von RDP, USB und MMR (Multimedia Redirection) stammender Datenverkehr getunnelt durch die Komponente View Secure Gateway übertragen. Wenn Sie direkte Clientverbindungen konfigurieren, können sich diese Protokolle direkt vom Client aus mit dem View-Desktop verbinden, ohne getunnelt durch die View Secure Gateway Server übertragen zu werden.

Hinweis PCoIP und HP RGS verwenden nicht die Tunnelverbindung.

View Secure Gateway Server ist ferner zuständig für die Weiterleitung von anderem Web-Datenverkehr, z. B. dem bei Benutzerauthentifizierung und Desktop-Auswahl generiertem Datenverkehr, von View-Clients zu View Broker. View Secure Gateway Server leitet darüber hinaus Web-Datenverkehr vom View Administrator-Client zur Komponente Administration Server weiter.

View LDAP

View LDAP ist ein in View Connection Server eingebettetes LDAP-Verzeichnis und der Konfigurationsspeicher aller View-Konfigurationsdaten.

View LDAP enthält Einträge, die alle View-Desktops, alle View-Desktops, auf die zugegriffen werden kann, mehrere View-Desktops, die gemeinsam verwaltet werden, und die Konfigurationseinstellungen von View-Komponenten darstellen.

View LDAP bietet ferner eine Gruppe von Plug-In-DLLs für View, um anderen View-Komponenten Automatisierungs- und Benachrichtigungsdienste bereitzustellen.

View Messaging

Die Komponente View Messaging stellt den Nachrichtenvermittlungs-Router für die Kommunikation zwischen View Connection Server-Komponenten sowie zwischen View Agent und View Connection Server zur Verfügung.

Diese Komponente unterstützt die JMS-API (Java Message Service), die für die Nachrichtenvermittlung in View verwendet wird.

Firewall-Regeln für Sicherheitsserver im Umkreisnetzwerk

Für die Front-End- und Back-End-Firewall der Sicherheitsserver im Umkreisnetzwerk müssen bestimmte Firewall-Regel aktiviert sein.

Regeln für die Front-End-Firewall

Damit sich externe Clientgeräte mit einem Sicherheitsserver im Umkreisnetzwerk verbinden können, muss die Front-End-Firewall eingehenden Datenverkehr an bestimmten TCP-Ports zulassen. Tabelle 5-2 enthält eine Übersicht der Regeln für die Front-End-Firewall.

Tabelle 5-2. Regeln für die Front-End-Firewall

Quelle	Protokoll	Port	Ziel	Hinweise
Beliebig	HTTP	80	Sicherheitsserver	Externe Clientgeräte nutzen Port 80 für eine Verbindung mit einem Sicherheitsserver im Umkreisnetzwerk, wenn SSL deaktiviert ist.
Beliebig	HTTPS-	443	Sicherheitsserver	Externe Clientgeräte nutzen Port 443 für eine Verbindung mit einem Sicherheitsserver im Umkreisnetzwerk, wenn SSL aktiviert ist (Standardeinstellung).

Regeln für die Back-End-Firewall

Um einem Sicherheitsserver die Kommunikation mit den einzelnen View Connection Server-Instanzen im internen Netzwerk zu ermöglichen, muss die Back-End-Firewall eingehenden Datenverkehr an bestimmten TCP-Ports zulassen. Hinter der Back-End-Firewall müssen interne Firewalls ähnlich konfiguriert sein, damit View-Desktops und View Connection Server-Instanzen miteinander kommunizieren können. Tabelle 5-3 enthält eine Übersicht der Regeln für die Back-End-Firewall.

Tabelle 5-3. Regeln für die Back-End-Firewall

Quelle	Protokoll	Port	Ziel	Hinweise
Sicherheitsserver	AJP13	8009	View Connection Server	Sicherheitsserver nutzen Port 8009 zum Übertragen von Web-Datenverkehr an View Connection Server-Instanzen, der vom AJP13-Protokoll weitergeleitet wurde.
Sicherheitsserver	JMS	4001	View Connection Server	Sicherheitsserver nutzen Port 4001 zum Übertragen von JMS-Datenverkehr (Java Message Service) an View Connection Server-Instanzen.
Sicherheitsserver	RDP	3389	View-Desktop	Sicherheitsserver nutzen Port 3389 zum Übertragen von RDP-Datenverkehr an View-Desktops. **Hinweis** Für die USB-Umleitung wird neben RDP der TCP-Port 32111 verwendet. Für MMR wird neben RDP der TCP-Port 9427 verwendet.

TCP-Ports für View Connection Server-Kommunikation

Gruppen von View Connection Server-Instanzen nutzen zusätzliche TCP-Ports für die Kommunikation untereinander. Zum Beispiel verwenden View Connection Server-Instanzen Port 4100 zum Übertragen von JMS-Datenverkehr zwischen View Connection Server-Instanzen.

Da Firewalls in der Regel nicht zwischen den View Connection Server-Instanzen in einer Gruppe verwendet werden, wird hier nicht weiter auf diese TCP-Ports eingegangen.

Allgemeine Firewall-Regeln für View Manager-Komponenten

Bei jeder Firewall-Konfiguration müssen TCP-Ports geöffnet sein, um Datenverkehr zwischen bestimmten View Manager-Komponenten zuzulassen.

Unter „Firewall-Regeln für Sicherheitsserver im Umkreisnetzwerk“, auf Seite 55 finden Sie Informationen zu Firewall-Regeln, die spezifisch für Implementierungen von Sicherheitsservern gelten.

Firewall-Regeln für View Agent

Tabelle 5-4 zeigt die TCP-Ports, die in der Firewall durch das View Agent-Installationsprogramm geöffnet werden. Wenn nicht anders angegeben, handelt es sich bei den Ports um eingehende TCP-Ports. Weitere Informationen zur Protokollrichtung finden Sie unter „View Manager-Komponenten und -Protokolle“, auf Seite 51.

Tabelle 5-4. Während der View Agent-Installation geöffnete TCP-Ports

Protokoll	Ports
RDP	3389
USB-Umleitung	32111
MMR	9427
PCoIP	50002 (TCP und UDP)
HP RGS	42966

Das View Agent-Installationsprogramm konfiguriert die lokale Firewall-Regel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389). Wenn Sie die RDP-Portnummer ändern, müssen Sie die dazugehörigen Firewall-Regeln ändern.

HP RGS Sender ist die serverseitige Komponente des Remote-Anzeigeprotokolls HP RGS und nutzt standardmäßig Port 42966.

Bei Verwendung einer Vorlage einer virtuellen Maschine als Desktop-Quelle werden Firewall-Ausnahmen auf bereitgestellten Desktops nur dann übernommen, wenn die Vorlage eine virtuelle Maschine der Desktop-Domäne ist. Sie können Microsoft-Gruppenrichtlinieneinstellungen verwenden, um lokale Firewall-Ausnahmen zu verwalten. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 875357.

Firewall-Regeln für Active Directory

Wenn zwischen der View-Umgebung und dem Active Directory-Server eine Firewall vorhanden ist, müssen Sie sicherstellen, dass alle erforderlichen Ports geöffnet sind. Zum Beispiel muss View Connection Server auf den globalen Katalog von den Active Directory- und LDAP-Servern (Lightweight Directory Access Protocol) zugreifen können. Wenn die Ports für den globalen Katalog und LDAP von Ihrer Firewall-Software gesperrt werden, haben Administratoren Probleme bei der Konfiguration von Benutzerberechtigungen.

In der Dokumentation von Microsoft zu Ihrer Active Directory-Serverversion finden Sie weitere Informationen zu den Ports, die für eine ordnungsgemäße Funktionsweise von Active Directory in der Firewall geöffnet sein müssen.

Firewall-Regeln für View Client with Offline Desktop

View Client with Offline Desktop-Daten werden über Port 902 herunter- und hochgeladen. Wenn Sie View Client with Offline Desktop nutzen möchten, muss Ihr ESX-Host auf diesen Port zugreifen können.

Einschränken des Zugriffs auf View-Desktops

Mithilfe der Einschränkungsfunktion für Berechtigungen können Sie den Zugriff auf View-Desktops basierend auf der View Connection Server-Instanz einschränken, mit der sich ein Benutzer verbindet.

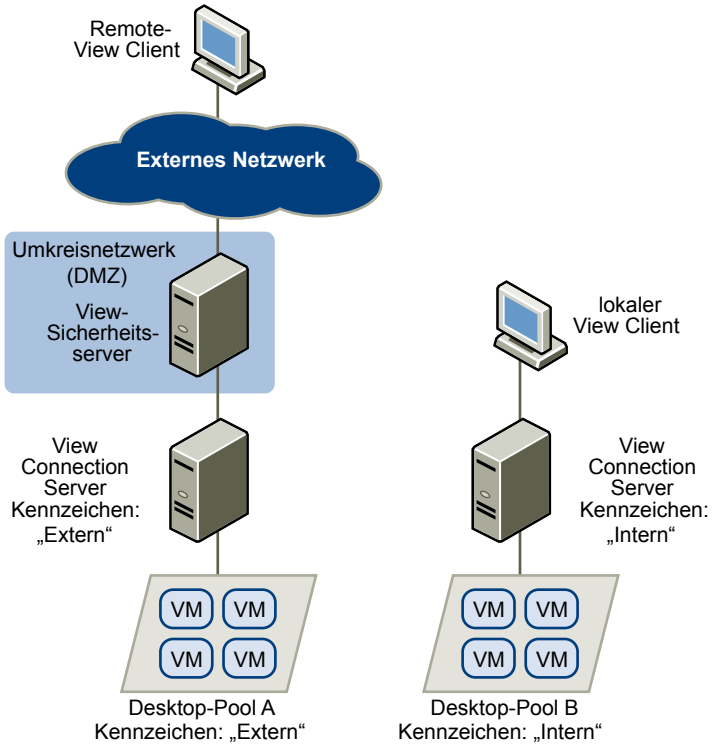
Zum Einschränken von Berechtigungen weisen Sie einer View Connection Server-Instanz ein oder mehrere Kennzeichen zu. Wenn Sie anschließend einen Desktop oder einen Desktop-Pool konfigurieren, wählen Sie die Kennzeichen der View Connection Server-Instanzen aus, auf die der Desktop oder Desktop-Pool zugreifen können soll. Wenn Benutzer sich an einer so konfigurieren View Connection Server-Instanz anmelden, können sie nur auf die Desktops oder Desktop-Pools zugreifen, die mindestens ein übereinstimmendes Kennzeichen oder keine Kennzeichen aufweisen.

Angenommen, Ihre Bereitstellung umfasst zwei View Connection Server-Instanzen. Die erste Instanz unterstützt Ihre internen Benutzer. Die zweite Instanz bildet ein Paar mit einem Sicherheitsserver und unterstützt Ihre externen Benutzer. Um externe Benutzer am Zugriff auf bestimmte Desktops zu hindern, können Sie eingeschränkte Berechtigungen wie folgt einrichten:

- Weisen Sie das Kennzeichen „Intern“ der View Connection Server-Instanz zu, die die internen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Extern“ der View Connection Server-Instanz zu, die ein Paar mit dem Sicherheitsserver bildet und die externen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Intern“ den Desktops und Desktop-Pools zu, auf die nur interne Benutzer zugreifen dürfen.
- Weisen Sie das Kennzeichen „Extern“ den Desktops und Desktop-Pools zu, auf die nur externe Benutzer zugreifen dürfen.

Externe Benutzern werden keine als „Intern“ gekennzeichneten Desktops und Desktop-Pools angezeigt, da sie sich an der als „Extern“ gekennzeichneten View Connection Server-Instanz anmelden. Hingegen können interne Benutzern keine als „Extern“ gekennzeichneten Desktops und Desktop-Pools sehen, da sie sich an der als „Intern“ gekennzeichneten View Connection Server-Instanz anmelden. Abbildung 5-6 zeigt diese Konfiguration.

Abbildung 5-6. Beispiel für eingeschränkte Berechtigungen



Außerdem können Sie mithilfe eingeschränkter Berechtigungen den Desktop-Zugriff basierend auf der Benutzerauthentifizierungsmethode steuern, die Sie für eine bestimmte View Connection Server-Instanz konfigurieren. Sie können beispielsweise bestimmte Desktops nur Benutzern zur Verfügung stellen, die sich mit einer Smartcard authentifiziert haben.

Die Einschränkungsfunktion für Berechtigungen erzwingt nur die Übereinstimmung mit Kennzeichen. Sie müssen Ihre Netzwerktopologie ändern, um bestimmte Clients zu zwingen, sich über eine bestimmte View Connection Server-Instanz anzumelden.

Überblick über die Schritte zum Einrichten einer VMware View-Umgebung

6

Die Checkliste für Installation und Einrichtung von VMware View enthält alle übergeordneten Aufgaben zum Erstellen einer View-Bereitstellung, gibt die Reihenfolge ihrer Ausführung an und nennt die Dokumente, die Anweisungen bieten.

Tabelle 6-1. Checkliste für die Installation und Einrichtung von VMware View

Schritt	Aufgabe
1	Einrichten der benötigten Administrator- und Benutzergruppen in Active Directory. Anweisungen: *VMware View Manager-Administratorhandbuch* und vSphere-Dokumentation
2	(Optional) Installieren und Einrichten von VMware ESX-Servern und vCenter Server Anweisungen: vSphere-Dokumentation, Dokumentationsübersicht (Documentation Roadmap)
3	(Optional) Installieren von View Composer unter vCenter Server Anweisungen: *VMware View Manager-Administratorhandbuch*
4	Installieren von View Connection Server. Anweisungen: *VMware View Manager-Administratorhandbuch*
5	Kopieren der Active Directory-Vorlagen für Gruppenrichtlinienobjekte vom Computer mit View Connection Server auf den Server mit Active Directory und deren anschließender Import. Anweisungen: *VMware View Manager-Administratorhandbuch*
6	Erstellen einer Ausgangskonfiguration von View Connection Server. Anweisungen: *VMware View Manager-Administratorhandbuch*
7	Erstellen einer oder mehrerer virtueller Maschinen, die als Vorlage für Desktop-Pools auf Basis vollständiger Klone oder als übergeordnete virtuelle Maschinen von Desktop-Pools auf Basis verknüpfter Klone dienen. Installieren der gewünschten Anwendung bzw. VMware ThinApp-Anwendungen. Anweisungen: vSphere-Dokumentation, Dokumentationsübersicht und *Windows XP Deployment Guide* (Windows XP-Bereitstellungsanleitung) für VMware View
8	Installieren von View Agent in den virtuellen Maschinen und auf den physischen Computern, die Sie als Desktop-Quellen nutzen möchten. Anweisungen: *VMware View Manager-Administratorhandbuch*
9	Erstellen eines einzelnen View-Desktops oder View-Desktop-Pools oder von beidem. Anweisungen: *VMware View Manager-Administratorhandbuch*
19	Erteilen von Benutzer- und/oder Benutzergruppenberechtigungen für Desktops. Anweisungen: *VMware View Manager-Administratorhandbuch*
11	Festlegen von Desktop-Richtlinien. Anweisungen: *VMware View Manager-Administratorhandbuch*
12	Installieren von View Client auf den Computern der Endbenutzer und diese instruieren, die benötigten Komponenten über View Portal zu installieren. Anweisungen: *VMware View Manager-Administratorhandbuch*

Tabelle 6-1. Checkliste für die Installation und Einrichtung von VMware View (Fortsetzung)

Schritt	Aufgabe
13	Ermöglichen des Benutzerzugriffs auf ihre View-Desktops. Anweisungen: *VMware View Manager-Administratorhandbuch*
14	Verwalten und Überwachen von Benutzern und Desktops. Anweisungen: *VMware View Manager-Administratorhandbuch*

Index

W

Z