VMware View-Architekturplanungsanleitung

View 4.5
View Manager 4.5
View Composer 2.5

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-000350-00

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 5

1 Einführung in VMware View 7
- Vorteile von VMware View 7
- VMware View-Funktionen 9
- Zusammenspiel der VMware View-Komponenten 10
- Integrieren und Anpassen von VMware View 14

2 Planen einer umfassenden Benutzerumgebung 17
- Übersicht der unterstützten Funktionen 17
- Auswählen eines Anzeigeprotokolls 18
- Verwenden eines View-Desktops ohne Netzwerkverbindung 20
- Zugreifen auf an einen lokalen Computer angeschlossene USB-Geräte 22
- Drucken auf einem View-Desktop 22
- Streaming von Multimediadaten auf einen View-Desktop 22
- Verwenden der Single Sign-On-Funktion zur Anmeldung an einem View-Desktop 23
- Verwenden mehrerer Monitore mit einem View-Desktop 23

3 Zentrales Verwalten von Desktop-Pools 25
- Vorteile von Desktop-Pools 25
- Reduzieren und Verwalten von Speicheranforderungen 26
- Anwendungsbereitstellung 28
- Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten 30

4 Architekturentwurfselemente und Planungsanleitungen 31
- Anforderungen virtueller Maschinen 32
- VMware View-ESX-Knoten 37
- Desktop-Pools für bestimmte Nutzertypen 38
- Konfigurieren virtueller Maschinen für View-Desktops 42
- vCenter und View Composer: Konfigurieren von Maximalwerten für virtuelle Maschinen und Desktop-Pools 43
- View Connection Server: Konfigurieren von Maximalwerten und virtuellen Maschinen 44
- View Transfer Server: Konfiguration und Speicher für virtuelle Maschinen 45
- vSphere-Cluster 46
- VMware View-Bausteine 47
- VMware View-Struktur 51

5 Planen von Sicherheitsfunktionen 53
- Grundlegendes zu Clientverbindungen 53
- Auswählen einer Benutzerauthentifizierungsmethode 55

Einschränken des Zugriffs auf View-Desktops 58
Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von View-Desktops 59
Implementieren empfohlener Vorgehensweisen zum Sichern von Clientsystemen 59
Zuweisen von Administratorrollen 60
Vorbereiten des Einsatzes eines Sicherheitsservers 60
Grundlegendes zu VMware View-Kommunikationsprotokollen 65

6 Überblick über die Schritte zum Einrichten einer VMware View-Umgebung 71

Index 73

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.

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?

Damit Sie Ihre VMware View-Installation schützen können, werden in diesem Handbuch auch Sicherheitsfunktionen behandelt.

Zielgruppe

Diese Anleitung richtet sich an IT-Entscheider, -Architekten, -Administratoren und andere Benutzer, 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 Benutzer erfüllt. Die Beispielarchitektur soll die Hardwareanforderungen und den Einrichtungsaufwand einer umfangreichen Bereitstellung von VMware View veranschaulichen.

VMware Technical Publications – Glossar

VMware® Technical Publications stellt ein Glossar mit Begriffen bereit, mit denen Sie möglicherweise noch nicht vertraut sind. Definitionen für Begriffe, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/de/support/pubs (möglicherweise in englischer Sprache).

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

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

Supportangebote

Um herauszufinden, wie VMware mithilfe seines Supportangebots 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. Kurse werden am Kundenstandort, in einer Kursraumumgebung und live im Internet angeboten. Zusätzlich zu Pilotprogrammen am Kundenstandort und empfohlenen Vorgehensweisen bei der Implementierung haben die VMware Consulting Services Angebote im Programm, mit deren Hilfe Sie Ihre virtuelle Umgebung bewerten, planen, erstellen und verwalten können. 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. Benutzer 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“, auf Seite 7
- „VMware View-Funktionen“, auf Seite 9
- „Zusammenspiel der VMware View-Komponenten“, auf Seite 10
- „Integrieren und Anpassen von VMware View“, auf Seite 14

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 Datencenter bietet die folgenden Vorteile:

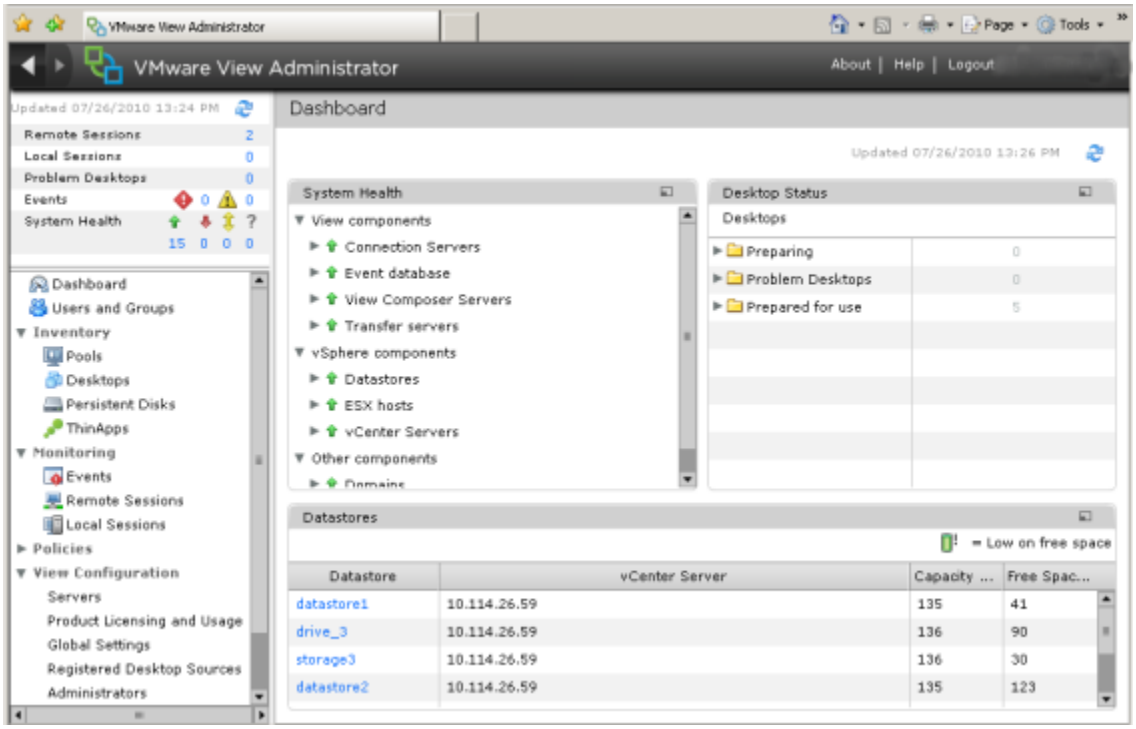
- Der Zugriff auf Daten kann mit einfachen Mitteln eingeschränkt werden. Das Kopieren vertraulicher Daten auf den Heimcomputer eines Remote-Mitarbeiters kann verhindert werden.
- Datensicherungen können geplant werden, ohne berücksichtigen zu müssen, dass die Systeme der Benutzer ggf. ausgeschaltet sind.
- Virtuelle Desktops, die in einem Datencenter 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

Für Skalierbarkeit wurde die vereinheitlichte Verwaltungskonsole auf Adobe Flex aufgebaut, damit selbst die größten View-Bereitstellungen von einer einzigen View Manager-Oberfläche aus effizient verwaltet werden können. Assistenten und Dashboards verbessern den Workflow und vereinfachen den Drilldown zum Anzeigen von Details oder zum Ändern von Einstellungen. Abbildung 1-1 bietet ein Beispiel für die browserbasierte Benutzeroberfläche von View Administrator.

Abbildung 1-1. View Manager-Verwaltungskonsole mit Dashboard-Anzeige



Eine weitere Funktion zum Verbessern des Komforts ist das VMware Remote-Anzeigeprotokoll PCoIP. Das PCoIP-Anzeigeprotokoll (PC-over-IP) bietet eine Benutzerumgebung, die der auf einem physischen PC entspricht:

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

Verwaltbarkeit

Die Bereitstellung von Desktops für Benutzer erfolgt schnell. Anwendungen müssen nicht einzeln auf den physischen PCs der Benutzer installiert werden. Benutzer verbinden sich mit einem virtuellen Desktop, auf dem die Anwendungen bereits vorhanden sind. Benutzer 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, Macs, 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 Benutzer eine vertraute Umgebung bereitgestellt:

- Drucken von einem virtuellen Desktop aus auf einem beliebigen lokalen oder Netzwerkdrucker, der auf dem Clientgerät definiert ist, oder Verwenden der ortsabhängigen Druckfunktion, um Drucker zuzuordnen, die sich in der Nähe des Clientsystems befinden. 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:

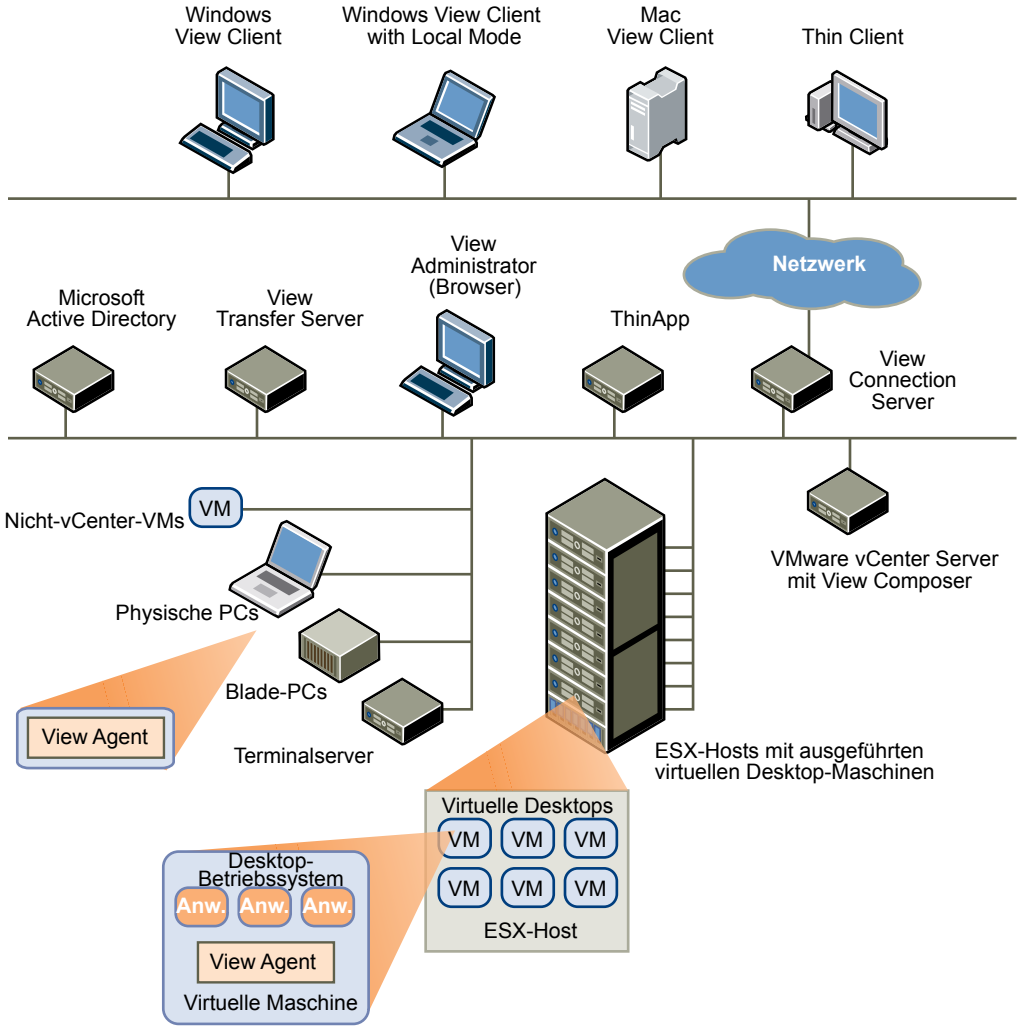
- Integration mit VMware vSphere zum Erzielen kostengünstiger Dichten, hoher Verfügbarkeitsgrade und einer erweiterten Steuerung der Ressourcenzuweisung für Ihre virtuellen Desktops
- Konfiguration von View Connection Server zum Vermitteln von Verbindungen zwischen Benutzern und den virtuellen Desktops, 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

Benutzer starten View Client, um sich bei View Connection Server anzumelden. 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 1-2 zeigt die Beziehung zwischen den Hauptkomponenten einer Bereitstellung von VMware View.

Abbildung 1-2. Allgemeines Beispiel einer VMware View-Umgebung



Clientgeräte

Ein Hauptvorteil von VMware View ist, dass Desktops dem Benutzer 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 Mac- und Windows-Laptops und -PCs öffnen die Benutzer View Client zum Anzeigen ihres View-Desktops. 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
- Zuweisen von Anwendungen, die mit VMware ThinApp für bestimmte Desktops und Pools verpackt wurden
- Verwalten von lokalen und Remote-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 2008, bevorzugt in einer virtuellen VMware-Maschine installiert.

View Client

Die Clientsoftware für den Zugriff auf View-Desktops wird entweder auf einem Windows- oder Mac-PC als systemeigene Anwendung oder auf 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 Benutzer ein Anzeigeprotokoll auswählen können. Zu den Protokollen zählen PCoIP, Microsoft RDP und HP RGS (für View-Desktops, die auf HP Blades gehostet werden). Geschwindigkeit und Anzeigequalität von PCoIP können es mit einem physischen PC aufnehmen.

View Client with Local Mode (früher Offline Desktop) ist eine erweiterte Version von View Client, mit der Benutzer virtuelle Maschinen herunterladen und auf ihren lokalen Systemen verwenden können. Dies gilt unabhängig davon, ob die Benutzer mit dem Netzwerk verbunden sind.

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

- 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 Windows-PC oder -Laptop können Benutzer einen Webbrowser öffnen und View Portal verwenden, um den Windows-basierten View Client herunterzuladen, zu installieren, zu aktualisieren und zu starten. Ab View-Version 4.5 installiert View Portal den vollständigen View Client für Windows mit oder ohne Local Mode.

Zum Verwenden von View Portal müssen Benutzer einen Internet Explorer-Browser öffnen und die URL einer View Connection Server-Instanz eingeben. View Portal stellt einen Link zum Herunterladen des Installationsprogramms für den vollständigen View Client für Windows bereit.

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 Benutzer.

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 Linked-Clone-Desktop-Pools 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 Benutzer sind nicht betroffen. Ab View-Version 4.5 können Sie die Linked-Clone-Technologie auch für View-Desktops einsetzen, die Sie herunterladen und für die Verwendung auf lokalen Systemen auschecken.

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 Linked-Clone-Desktop-Pools 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 2008, bevorzugt in einer virtuellen VMware-Maschine installiert.

View Transfer Server

Diese Software verwaltet und optimiert Datenübertragungen zwischen dem Rechenzentrum und View-Desktops, die für die Verwendung auf lokalen Systemen von Benutzern ausgecheckt wurden. View Transfer Server ist zur Unterstützung von Desktops erforderlich, auf denen View Client with Local Mode (früher Offline Desktop) ausgeführt wird.

Bei mehreren Operationen wird View Transfer Server zum Senden von Daten zwischen dem View-Desktop in vCenter Server und dem entsprechenden lokalen Desktop auf dem Clientsystem verwendet.

- Wenn ein Benutzer einen Desktop ein- oder auscheckt, wird diese Operation von View Manager autorisiert und verwaltet. View Transfer Server überträgt die Dateien zwischen dem Rechenzentrum und dem lokalen Desktop.
- View Transfer Server synchronisiert lokale Desktops mit den entsprechenden Desktops im Rechenzentrum, indem Benutzeränderungen im Rechenzentrum repliziert werden.

  Replikationen finden in Intervallen statt, die Sie in den Richtlinien für den lokalen Modus festlegen. Außerdem können Sie Replikationen in View Administrator starten. Sie können eine Richtlinie festlegen, die Benutzern das Starten von Replikationen von ihren lokalen Desktops aus ermöglicht.

- View Transfer Server hält lokale Desktops auf dem neuesten Stand, indem allgemeine Systemdaten vom Rechenzentrum an lokale Clients verteilt werden. View Transfer Server lädt View Composer-Basis-Images aus dem Image-Repository auf lokale Desktops herunter.
- Wenn ein lokaler Computer beschädigt wird oder verloren geht, kann View Transfer Server den lokalen Desktop bereitstellen und die Benutzerdaten wiederherstellen, indem die Daten und das System-Image auf den lokalen Desktop heruntergeladen werden.

Integrieren und Anpassen von VMware View

Zum Verbessern der Effektivität von VMware View in Ihrer Organisation können Sie mehrere Schnittstellen einsetzen, um VMware View in externe Anwendungen zu integrieren oder Verwaltungsskripts zu erstellen, die an der Befehlszeile oder im Batchmodus ausgeführt werden können.

Integrieren von View in Business Intelligence-Software

Sie können VMware View so konfigurieren, dass Ereignisse in einer Microsoft SQL Server- oder Oracle-Datenbank aufgezeichnet werden.

- Benutzeraktionen wie die Anmeldung und das Starten einer Desktop-Sitzung.
- Administratoraktionen wie das Hinzufügen von Berechtigungen und das Erstellen von Desktop-Pools.
- Warnungen, die über Systemausfälle und Fehler berichten.
- Statistische Abfragen wie die Aufzeichnung der Höchstzahl an Benutzern über einen Zeitraum von 24 Stunden.

Anhand von Business Intelligence-Berichterstellungsprogrammen wie Crystal Reports, IBM Cognos, MicroStrategy 9 und Oracle Enterprise Performance Management System können Sie auf die Ereignisdatenbank zugreifen und diese analysieren.

Weitere Informationen finden Sie im *VMware View Integration Guide (VMware View-Integrationshandbuch)*.

Verwenden von View PowerCLI zum Erstellen von Verwaltungsskripts

Windows PowerShell ist eine Befehlszeilen- und Skriptumgebung, die für Microsoft Windows entwickelt wurde. PowerShell verwendet das .NET-Objektmodell und stellt Verwaltungs- und Automatisierungsfunktionen für Administratoren bereit. Wie bei jeder anderen Konsolenumgebung erfolgt die Arbeit mit PowerShell über die Ausführung von Befehlen, die in PowerShell als Cmdlets bezeichnet werden.

View PowerCLI bietet eine benutzerfreundliche PowerShell-Schnittstelle in VMware View. Mithilfe der View PowerCLI-Cmdlets können Sie verschiedene Verwaltungsaufgaben an View-Komponenten ausführen.

- Erstellen und Aktualisieren von Desktop-Pools
- Hinzufügen von Rechenzentrumsressourcen zu einer vollständigen virtuellen Maschine oder zu einem Linked-Clone-Pool
- Durchführen von Vorgängen zur Neuverteilung, Aktualisierung oder Neuzusammenstellung für Linked-Clone-Desktops
- Analysieren der Nutzung bestimmter Desktops oder Desktop-Pools über einen Zeitraum
- Abfragen der Ereignisdatenbank
- Abfragen des Status von View-Diensten

Sie können die Cmdlets zusammen mit den vSphere PowerCLI-Cmdlets einsetzen, welche eine Verwaltungsoberfläche für das Produkt VMware vSphere bereitstellen.

Weitere Informationen finden Sie im *VMware View Integration Guide (VMware View-Integrationshandbuch)*.

Ändern von LDAP-Konfigurationsdaten in View

Wenn Sie die Konfiguration von VMware View mithilfe von View Administrator ändern, werden die entsprechenden LDAP-Daten im Repository aktualisiert. VMware View speichert Konfigurationsdaten in einem mit LDAP kompatiblen Repository. Wenn Sie beispielsweise einen Desktop-Pool hinzufügen, speichert VMware View Informationen über Benutzer, Benutzergruppen und Berechtigungen in LDAP.

Mithilfe der VMware- und Microsoft-Befehlsprogramme können Sie LDAP-Konfigurationsdaten in LDIF-Dateien (LDAP Data Interchange Format) aus VMware View exportieren und darin importieren. Diese Befehle sind für fortgeschrittene Administratoren bestimmt, die Konfigurationsdaten anhand von Skripts und nicht über View Administrator oder View PowerCLI aktualisieren möchten.

Mithilfe von LDIF-Dateien können Sie eine Reihe von Aufgaben durchführen.

- Übertragen von Konfigurationsdaten zwischen View Connection Server-Instanzen
- Definieren einer großen Anzahl an View-Objekten, z.B. Desktop-Pools, und Hinzufügen dieser Objekte zu Ihren View Connection Server-Instanzen ohne Einsatz von View Administrator oder View PowerCLI
- Sichern Ihrer View-Konfiguration, damit der Zustand einer View Connection Server-Instanz wiederhergestellt werden kann

Weitere Informationen finden Sie im *VMware View Integration Guide (VMware View-Integrationshandbuch)*.

Verwenden von SCOM zur Überwachung von View-Komponenten

Mithilfe von Microsoft SCOM (System Center Operations Manager) können Sie den Status und die Leistung von VMware View-Komponenten überwachen. Hierzu gehören View Connection Server-Instanzen und Sicherheitsserver sowie auf diesen Hosts ausgeführte View-Dienste.

Weitere Informationen finden Sie im *VMware View Integration Guide (VMware View-Integrationshandbuch)*.

Verwenden des Befehls „vdmadmin“ zur Verwaltung von View

Mithilfe der Befehlszeilenschnittstelle `vdmadmin` können Sie eine Vielzahl von Verwaltungsaufgaben auf einer View Connection Server-Instanz durchführen. Sie können `vdmadmin` zur Durchführung von Verwaltungsaufgaben einsetzen, die innerhalb der View Administrator-Benutzeroberfläche nicht möglich sind oder die automatisch über Skripts ausgeführt werden sollen.

Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.

Planen einer umfassenden Benutzerumgebung

2

VMware View bietet die vertraute, individuell angepasste Desktop-Umgebung, die Benutzer erwarten. Benutzer 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 Benutzern zur Verfügung stellen möchten. Bevor Sie entscheiden, welche Funktionen verwendet werden sollen, müssen Sie sich mit den Einschränkungen der einzelnen Funktionen vertraut machen.

Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht der unterstützten Funktionen“, auf Seite 17
- „Auswählen eines Anzeigeprotokolls“, auf Seite 18
- „Verwenden eines View-Desktops ohne Netzwerkverbindung“, auf Seite 20
- „Zugreifen auf an einen lokalen Computer angeschlossene USB-Geräte“, auf Seite 22
- „Drucken auf einem View-Desktop“, auf Seite 22
- „Streaming von Multimediadaten auf einen View-Desktop“, auf Seite 22
- „Verwenden der Single Sign-On-Funktion zur Anmeldung an einem View-Desktop“, auf Seite 23
- „Verwenden mehrerer Monitore mit einem View-Desktop“, auf Seite 23

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 Benutzern zur Verfügung stellen möchten, an Tabelle 2-1 und Tabelle 2-2, um zu bestimmen, welche Clientbetriebssysteme die jeweilige Funktion unterstützen.

Tabelle 2-1. Auf Windows-Clients unterstützte Funktionen

Funktion	Windows XP Home/Pro SP3, 32-Bit	Windows Vista SP1, SP2, 32-Bit	Windows 7, 32-Bit und 64-Bit
USB-Anschluss	X	X	X
RDP-Anzeigeprotokoll	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X
HP RGS-Anzeigeprotokoll	X	X	

Tabelle 2-1. Auf Windows-Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows XP Home/Pro SP3, 32-Bit	Windows Vista SP1, SP2, 32-Bit	Windows 7, 32-Bit und 64-Bit
Wyse MMR	X	X	
Virtuelle Druckfunktion	X	X	X
Smartcards	X	X	X
RSA SecurID	X	X	X
Single Sign-On	X	X	X
Mehrere Monitore	X	X	X
Lokaler Modus	X	X	X

Zu den Editionen von Windows Vista gehören Windows Vista Home, Enterprise, Ultimate und Business. Zu den Editionen von Windows 7 gehören Home, Professional, Enterprise und Ultimate.

Tabelle 2-2. Auf Mac-Clients unterstützte Funktionen

Funktion	Mac OS X (10.5,6)	Mac OS X (10.6)
USB-Anschluss		
RDP-Anzeigeprotokoll	X	X
PCoIP-Anzeigeprotokoll		
HP RGS-Anzeigeprotokoll		
Wyse MMR		
Virtuelle Druckfunktion		
Smartcards		
RSA SecurID	X	X
Single Sign-On	X	X
Mehrere Monitore		
Lokaler Modus		

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 Benutzern 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 um die Benutzer das Protokoll auswählen lassen, wenn sie sich am Desktop anmelden.

Hinweis Wenn Sie einen Desktop zur Verwendung auf einem lokalen Clientsystem auschecken, wird weder das RDP- noch das PCoIP-Remote-Anzeigeprotokoll verwendet.

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 Benutzer 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 2560 x 1600) 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.

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.

Verwenden eines View-Desktops ohne Netzwerkverbindung

Mit View Client with Local Mode können Benutzer einen View-Desktop auschecken und auf ein lokales System, beispielsweise einen Laptop, herunterladen. Administratoren können diese lokalen View-Desktops verwalten, indem sie Richtlinien für die Häufigkeit von Sicherungen und Serverkontakten, für den Zugriff auf USB-Geräte und für die Berechtigung zum Einchecken von Desktops festlegen.

Für Mitarbeiter in externen Büros mit schlechter Netzwerkverbindung werden Anwendungen schneller auf einem lokalen View-Desktop als auf einem Remote-Desktop ausgeführt. Außerdem können Benutzer die lokale Desktop-Version mit oder ohne Netzwerkverbindung nutzen.

Wenn auf dem Clientsystem eine Netzwerkverbindung besteht, kommuniziert der ausgescheckte Desktop weiterhin mit View Connection Server, um Richtlinienaktualisieren bereitzustellen und zu gewährleisten, dass lokal zwischengespeicherte Authentifizierungskriterien auf dem neuesten Stand sind. Standardmäßig wird alle fünf Minuten ein Kontaktversuch unternommen.

View Client with Local Mode ist eine vollständig unterstützte Funktion, die in früheren Versionen als experimentelle Funktion namens View Client with Offline Desktop zur Verfügung stand.

View-Desktops im lokalen Modus verhalten sich genauso wie die entsprechenden Remote-Desktops, können jedoch lokale Ressourcen nutzen. Wartezeiten werden vermieden und die Leistung wird verbessert. Benutzer können die Verbindung zu ihrem lokalen View-Desktop trennen und sich erneut anmelden, ohne sich mit View Connection Server zu verbinden. Sobald der Netzwerkzugriff wiederhergestellt oder der Benutzer bereit ist, kann die ausgecheckte virtuelle Maschine gesichert, per Rollback zurückgesetzt oder eingecheckt werden.

Nutzung lokaler Ressourcen

Nach dem Auschecken eines lokalen Desktops kann dieser den Arbeitsspeicher und die CPU des lokalen Systems nutzen. Beispielsweise wird Arbeitsspeicher, der über die Anforderungen für Host- und Gastbetriebssysteme hinaus zur Verfügung steht, normalerweise zwischen dem Host und dem lokalen View-Desktop aufgeteilt, unabhängig von den Arbeitsspeichereinstellungen, die in vCenter Server für die virtuelle Maschine festgelegt werden. In gleicher Weise kann der lokale View-Desktop automatisch bis zu zwei auf dem lokalen System verfügbare CPUs nutzen, und Sie können den lokalen Desktop für die Verwendung von bis zu vier CPUs konfigurieren.

Auch wenn ein lokaler Desktop lokale Ressourcen nutzen kann, kann ein Desktop unter Windows 7 oder Windows Vista View, der auf einem ESX 3.5-Host erstellt wurde, keine 3D- und Windows Aero-Effekte produzieren. Diese Einschränkung gilt auch dann, wenn der Desktop zur lokalen Verwendung auf einem Windows 7- oder Windows Vista-Host ausgecheckt wird. Windows Aero- und 3D-Effekte stehen nur dann zur Verfügung, wenn der View-Desktop mithilfe von vSphere 4.x erstellt wird.

Einsparen von Rechenzentrumsressourcen, indem die Verwendung des lokalen Modus als obligatorisch festgelegt wird

Sie können die Rechenzentrumskosten für Bandbreiten-, Arbeitsspeicher- und CPU-Ressourcen reduzieren, indem Sie festlegen, dass View-Desktops heruntergeladen und ausschließlich im lokalen Modus verwendet werden können. Mit dieser Strategie können Mitarbeiter und Auftragnehmer ihre eigenen Computer verwenden.

Auschecken

Wird der View-Desktop ausgecheckt, wird die vCenter Server-Version des Desktops gesperrt, damit kein anderer Benutzer darauf zugreifen kann. Bei einem gesperrten View-Desktop werden vCenter Server-Operationen deaktiviert. Hierzu gehören Operationen wie das Einschalten des Online-Desktops, das Erstellen von Snapshots und die Bearbeitung der Einstellungen der virtuellen Maschine. View-Administratoren können jedoch die lokale Sitzung dennoch überwachen und auf die vCenter Server-Version zugreifen, um den Zugriff zu entfernen oder ein Rollback für den Desktop durchzuführen.

Sicherungen

Während Sicherungsvorgängen wird der View-Desktop in vCenter Server mit allen neuen Daten und Konfigurationen aktualisiert, der lokale Desktop bleibt jedoch auf dem lokalen System ausgecheckt und die Sperre bleibt in vCenter Server erhalten.

Rollbacks

Während Rollback-Vorgängen wird der lokale View-Desktop verworfen und die Sperre wird in vCenter Server aufgehoben. Nachfolgende Clientverbindungen werden an den View-Desktop in vCenter Server weitergeleitet, bis der Desktop wieder ausgecheckt wird.

Einchecken

Beim Einchecken eines View-Desktops wird der lokale Desktop in vCenter Server hochgeladen und die Sperre wird aufgehoben. Nachfolgende Clientverbindungen werden an den View-Desktop in vCenter Server weitergeleitet, bis der Desktop wieder ausgecheckt wird.

Die Daten auf den einzelnen lokalen Systemen werden mit AES verschlüsselt. Die 128-Bit-Verschlüsselung wird standardmäßig verwendet, Sie können jedoch die 256-Bit-Verschlüsselung konfigurieren. Der Desktop besitzt eine über Richtlinien gesteuerte Lebenszeit. Wenn der Client den Kontakt mit View Connection Server verliert, entspricht die maximale Zeit ohne Serverkontakt dem Zeitraum, während dessen der Benutzer den Desktop weiterhin nutzen kann, bevor ihm der Zugriff verweigert wird. In ähnlicher Weise ist das Clientsystem nach Entfernen des Benutzerzugriffs nicht mehr zugänglich, wenn der Cache abläuft oder nachdem der Client diese Änderung durch View Connection Server ermittelt hat.

Für View Client with Local Mode gelten folgende Einschränkungen:

- Sie müssen eine View-Lizenz besitzen, die die Local Mode-Komponente umfasst.
- Benutzer können während Rollbacks und Vorgängen zum Auschecken nicht auf ihren lokalen Desktop zugreifen.
- Diese Funktion steht nur für virtuelle Maschinen zur Verfügung, die von vCenter Server verwaltet werden.
- Die Zuweisung von mit VMware ThinApp erstellten Anwendungspaketen wird auf lokalen Desktops nicht unterstützt.

- Aus Sicherheitsgründen können Sie innerhalb des View-Desktops nicht auf die Host-CD-ROM zugreifen.
- Ebenfalls aus Sicherheitsgründen können Sie keinen Text oder Systemobjekte wie Dateien und Ordner zwischen dem lokalen System und dem View-Desktop kopieren und einfügen.

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 auf Windows 2000-Systemen oder für View-Desktops, deren Quelle Microsoft Terminalserver sind, nicht unterstützt.

Drucken auf einem View-Desktop

Die virtuelle Druckfunktion ermöglicht Benutzern 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.

Um Druckaufträge an einen USB-Drucker zu senden, können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion nutzen.

Außerdem können IT-Organisationen mithilfe der standortbasierten Druckfunktionen von View 4.5 und höher View-Desktops dem Drucker zuordnen, der dem Endpunkt-Clientgerät am nächsten ist. Wenn ein Arzt im Krankenhaus sich beispielsweise von Raum zu Raum bewegt, wird der Druckauftrag bei jedem Ausdrucken eines Dokuments an den nächstgelegenen Drucker gesendet.

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 Mediendateiformate, die das Clientsystem unterstützt, da auf dem Client lokale Decoder vorhanden sein müssen. Diese Dateiformate sind unter anderen MPEG2, WMV, AVI und WAV.

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.
- MMR wird auf Clients oder virtuellen Desktops unter Windows 7 nicht unterstützt.

  Auch wenn MMR auf virtuellen Windows 7-Desktops nicht unterstützt wird, können Sie, wenn auf dem Windows 7-Desktop 1 GB RAM und zwei virtuelle CPUs verfügbar sind, mithilfe von PCoIP Videos im 480p- und 720p-Format in systemeigenen Auflösungen wiedergeben. Bei 1080p können Sie das Fenster möglicherweise nicht in Vollbildgröße anzeigen.

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 Benutzer nur einmalig zur Anmeldung aufgefordert werden.

Wenn Sie die Single Sign-On-Funktion nicht verwenden, werden Benutzer zweimal zur Anmeldung aufgefordert: einmal bei View Connection Server und anschließend an ihrem View-Desktop. Beim Verwenden von Smartcards müssen sich Benutzer 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.
- Wenn Sie einen View-Desktop im lokalen Modus verwenden, wird kein Remote-Anzeigeprotokoll eingesetzt. Sie können den Modus für die Anzeige auf mehreren Bildschirmen verwenden.

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 Images generieren. Mit VMware ThinApp können Sie Anwendungen ganz einfach in Pools installieren oder per Streaming übertragen.

Dieses Kapitel behandelt die folgenden Themen:

- „Vorteile von Desktop-Pools“, auf Seite 25
- „Reduzieren und Verwalten von Speicheranforderungen“, auf Seite 26
- „Anwendungsbereitstellung“, auf Seite 28
- „Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten“, auf Seite 30

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 vSphere-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 oder das Bereitstellen von Anwendungen auf allen virtuellen Desktops in einem Pool ermöglicht. Die folgenden Beispiele zeigen einige der verfügbaren Einstellungen:

- Geben Sie an, welches Remote-Anzeigeprotokoll als Standard für den View-Desktop verwendet werden soll und ob Benutzer die Standardeinstellung außer Kraft setzen dürfen.
- Konfigurieren Sie die Anzeigequalität und die 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.
- Wenn Sie vSphere 4.1 verwenden, geben Sie an, ob eine Microsoft Sysprep-Anpassungsspezifikation oder QuickPrep von VMware verwendet werden soll. Sysprep generiert eine eindeutige SID und GUID für jede virtuelle Maschine im Pool.
- Geben Sie an, ob der View-Desktop auf ein lokales Clientsystem heruntergeladen und ausgeführt werden kann oder muss.

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

Pools mit fester Zuweisung

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.

Pools mit dynamischer Zuweisung

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

Pools mit dynamischer Zuordnung 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 Server 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 26

  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 27

  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.

Mit View 4.5 und vSphere 4.1 können Sie jetzt auch die folgenden Funktionen verwenden:

- vStorage-Thin Provisioning – ermöglicht Ihnen, mit so wenig Festplattenspeicher wie nötig zu beginnen und die Festplatte später nach Bedarf zu vergrößern
- Mehrstufiger Speicher – ermöglicht Ihnen die Verteilung virtueller Festplatten in der View-Umgebung über Hochleistungsspeicher und kostengünstigere Speicherschichten, um die Leistung zu optimieren und Kosten zu senken
- Lokaler Speicher auf dem ESX-Server für die Auslagerungsdateien der virtuellen Maschine auf dem Gastbetriebssystem

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 Linked-Clone-Desktop-Pool 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, können im selben Datenspeicher bzw. derselben LUN (Logical Unit Number) abgelegt werden. Bei Bedarf können Sie mithilfe der Neuverteilungsfunktion das Replikat und die verknüpften Klone aus einer LUN in eine andere verschieben.

Alternativ dazu können Sie View Composer-Replikate und verknüpfte Klone in separaten Datenspeichern mit unterschiedlichen Leistungsmerkmalen ablegen. Beispielsweise können Sie die virtuellen Replikatmaschinen auf einer SSD (Solid-State Disk) speichern. Solid-State-Laufwerke besitzen eine niedrige Speicherkapazität und eine hohe Leseleistung, indem sie in der Regel Zehntausende E/As pro Sekunde (IOPS) unterstützen. Sie können verknüpfte Klone auf herkömmlichen, auf drehgelagerten Medien basierenden Datenspeichern speichern. Diese Datenträger bieten eine niedrigere Leistung, sind jedoch kostengünstig und stellen eine hohe Speicherkapazität bereit, wodurch sie zur Speicherung der zahlreichen verknüpften Klone in einem großen Pool geeignet sind. Konfigurationen des mehrstufigen Speichers können zur kosteneffektiven Verarbeitung intensiver E/A-Szenarios verwendet werden. Hierzu gehören gleichzeitige Neustarts vieler virtueller Maschinen oder die Ausführung geplanter Antivirenscans.

Bei der Erstellung eines Linked-Clone-Pools können Sie optional auch eine separate, temporäre virtuelle Festplatte konfigurieren, auf der die während der Benutzersitzungen generierten Auslagerungsdateien und temporären Dateien des Gastbetriebssystems gespeichert werden. Beim Ausschalten der virtuellen Maschine löscht View Manager die temporäre Festplatte. Durch die Verwendung temporärer Festplatten können Sie Speicherplatz sparen, da das Anwachsen verknüpfter Klone verlangsamt und der durch ausgeschaltete virtuelle Maschinen belegte Speicherplatz reduziert wird.

Wenn Sie Desktop-Pools mit fester Zuweisung erstellen, kann View Composer optional auch eine separate persistente virtuelle Festplatte für jeden virtuellen Desktop erstellen. Auf dieser persistenten Festplatte werden das Windows-Profil und die Anwendungsdaten des Benutzers gespeichert. Wird ein verknüpfter Klon aktualisiert, neu zusammengestellt oder neu verteilt, bleibt der Inhalt der persistenten virtuellen Festplatte erhalten. VMware empfiehlt, die persistenten View Composer-Festplatten in einem anderen Datenspeicher abzulegen. Sie können dann die gesamte LUN sichern, die die persistenten Festplatten enthält.

Weitere Informationen finden Sie im Handbuch mit empfohlenen Vorgehensweisen namens *Storage Considerations for VMware View* (Speicheraspekte bei VMware View).

Anwendungsbereitstellung

In VMware View stehen mehrere Optionen zur Anwendungsbereitstellung zur Verfügung: Sie können die herkömmlichen Methoden zur Anwendungsbereitstellung verwenden, mit VMware ThinApp erstellte Anwendungspakete verteilen oder Anwendungen als Bestandteil eines View Composer-Basis-Images bereitstellen.

- Bereitstellen von Anwendungen und System-Updates mit View Composer auf Seite 28

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

- Verwalten von VMware ThinApp-Anwendungen in View Administrator auf Seite 29

  VMware ThinApp™ ermöglicht das Verpacken einer Anwendung in 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 29

  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 Linked-Clone-Desktop-Pools 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)

Sie können eine persistente View Composer-Festplatte mit Benutzereinstellungen und anderen von Benutzern generierten Daten erstellen. Diese persistente Festplatte wird bei einer Neuzusammenstellung nicht berücksichtigt. Wenn ein verknüpfter Klon gelöscht wird, können Sie die Benutzerdaten erhalten. Verlässt ein Mitarbeiter das Unternehmen, kann ein anderer Mitarbeiter auf die Benutzerdaten dieses Mitarbeiters zugreifen. Ein Benutzer mit mehreren Desktops kann die Benutzerdaten auf einem einzigen Desktop konsolidieren.

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.

Verwalten von VMware ThinApp-Anwendungen in View Administrator

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

ThinApp ermöglicht die Anwendungsvirtualisierung, indem eine Anwendung von dem zugrunde liegenden Betriebssystem und dessen Bibliotheken und Framework entkoppelt und anschließend in eine ausführbare Datei gebündelt wird. Diese wird als Anwendungspaket bezeichnet. Ab View-Version 4.5 können Sie ThinApp-Anwendungen mithilfe von View Administrator an Desktops und Pools verteilen.

Nachdem Sie mithilfe von ThinApp eine virtualisierte Anwendung erstellt haben, können Sie die Anwendung entweder von einem freigegeben Dateiserver per Streaming übertragen oder auf den virtuellen Desktops installieren. Wenn Sie die virtualisierte Anwendung für das Streaming konfigurieren, müssen Sie die folgenden Architekturaspekte berücksichtigen:

- Den Zugriff für bestimmte Benutzergruppen auf bestimmte Anwendungs-Repositories, in denen das Anwendungspaket gespeichert ist
- Die Speicherkonfiguration für das Anwendungs-Repository
- Den beim Streaming generierten Netzwerkdatenverkehr, der stark vom Typ der Anwendung abhängt

Per Streaming übertragene Anwendungen werden von Benutzern über eine Desktop-Verknüpfung gestartet.

Wenn Sie ein ThinApp-Paket so zuweisen, dass es auf einem virtuellen Desktop installiert wird, müssen dieselben Architekturaspekte berücksichtigt werden wie bei der herkömmlichen Softwarebereitstellung mit MSI-Paketen. Die Speicherkonfiguration für das Anwendungs-Repository muss sowohl für per Streaming übertragene Anwendungen als auch für auf virtuellen Desktops installierte ThinApp-Pakete berücksichtigt werden.

HINWEIS Die Zuweisung von Anwendungspaketen, die mit VMware ThinApp erstellt wurden, wird für heruntergeladene und im lokalen Modus verwendete View-Desktops nicht unterstützt.

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, wie zum Beispiel dem Aktualisieren und Neuzusammenstellen des Desktops. 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 Gruppenrichtlinien-Verwaltungsvorlagen (ADM), mit deren Hilfe die Verwaltung und Konfiguration von View-Komponenten 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 ADM-Vorlagen verfügbaren Einstellungen finden Sie im *VMware View-Administratorhandbuch*.

Architekturentwurfselemente und Planungsanleitungen

4

Ein typischer VMware View-Architekturentwurf basiert zur Erzielung von Skalierbarkeit auf einem Bausteinmodell. Jede Bausteindefinition kann je nach Hardwarekonfiguration, den verwendeten View- und vSphere-Softwareversionen und anderen umgebungsspezifischen Entwurfsfaktoren variieren.

In diesem Kapitel wird ein geprüfter Beispielbaustein beschrieben, der aus Komponenten besteht, die mit vSphere 4.1 bis zu 2.000 virtuelle Desktops unterstützen. In der Gesamtbereitstellung werden fünf dieser Bausteine mit insgesamt 10.000 virtuellen Desktops in eine Struktur integriert.

Diese Architektur bietet einen skalierbaren Standardentwurf, den Sie an Ihre Unternehmensumgebung und besondere Anforderungen anpassen können. In diesem Kapitel finden Sie wichtige 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:

- „Anforderungen virtueller Maschinen“, auf Seite 32
- „VMware View-ESX-Knoten“, auf Seite 37
- „Desktop-Pools für bestimmte Nutzertypen“, auf Seite 38
- „Konfigurieren virtueller Maschinen für View-Desktops“, auf Seite 42
- „vCenter und View Composer: Konfigurieren von Maximalwerten für virtuelle Maschinen und Desktop-Pools“, auf Seite 43
- „View Connection Server: Konfigurieren von Maximalwerten und virtuellen Maschinen“, auf Seite 44
- „View Transfer Server: Konfiguration und Speicher für virtuelle Maschinen“, auf Seite 45
- „vSphere-Cluster“, auf Seite 46
- „VMware View-Bausteine“, auf Seite 47
- „VMware View-Struktur“, auf Seite 51

Anforderungen virtueller Maschinen

Beim Planen der Spezifikationen für View-Desktops besitzt die von Ihnen getroffene Auswahl in Bezug auf Arbeitsspeicher, CPU und Festplattenspeicher erhebliche Auswirkungen auf Ihre Auswahl von Server- und Speicherhardware und die damit verbundenen Kosten.

- Auf den Nutzertypen basierende Planung auf Seite 32

  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.

- Einschätzen der Arbeitsspeicheranforderungen für virtuelle Desktops auf Seite 33

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

- Einschätzen der CPU-Anforderungen für virtuelle Desktops auf Seite 35

  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 36

  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.

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.

Mitarbeiter, die Desktops nur im lokalen Modus verwenden	Diese Benutzer laden ihre View-Desktops herunter und führen sie nur auf ihren lokalen Systemen aus. Auf diese Weise werden die mit den Bandbreiten-, Arbeitsspeicher- und CPU-Ressourcen verbundenen Rechenzentrumskosten reduziert. Durch geplante Replikationen wird sichergestellt, dass Systeme und Daten gesichert werden. Administratoren konfigurieren, wie oft die Benutzersysteme mit View Manager Kontakt aufnehmen müssen, um nicht gesperrt zu werden.
Kioskbenutzer	Diese Benutzer müssen sich einen Desktop teilen, der öffentlich zur Verfügung gestellt wird. Beispiele für Kioskbenutzer sind Schüler, die sich in einem Klassenzimmer einen Computer teilen, Krankenschwestern auf einer Station oder Computer, die zur Stellenvermittlung verwendet werden. Diese Desktops erfordern eine automatische Anmeldung. Die Authentifizierung kann bei Bedarf über bestimmte Anwendungen erfolgen.

Einschätzen der Arbeitsspeicheranforderungen für virtuelle Desktops

Arbeitsspeicher (RAM) ist für Server kostspieliger als für PCs. Da die Arbeitsspeicherkosten einen hohen Prozentsatz der Gesamtkosten für Serverhardware und der erforderlichen Gesamtspeicherkapazität 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.

Hinweis Dieses Thema befasst sich mit Aspekten der Speicherzuweisung für den Remote-Zugriff auf View-Desktops. Wenn Benutzer View-Desktops im lokalen Modus auf ihren Clientsystemen ausführen, entspricht die Menge des beanspruchten Arbeitsspeichers einem bestimmten Anteil des auf dem Clientgerät verfügbaren Arbeitsspeichers.

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, legen Sie auf dem ESX-Server für die Einstellungen zur Arbeitsspeicherreservierung Werte ungleich null fest. Das Reservieren einer bestimmten Arbeitsspeichermenge stellt sicher, dass verwendete Desktops im Leerlauf nie vollständig auf die Festplatte ausgelagert werden. Außerdem kann dadurch der von ESX-Auslagerungsdateien beanspruchte Speicherplatz verringert 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. Verwenden Sie für den Zugriff auf die Dateien in der folgenden Liste das Windows-Gastbetriebssystem, um die Windows-Auslagerungs- und -Ruhezustandsdateien zu finden, und verwenden Sie das Dateisystem des ESX-Servers zum Finden der ESX-Auslagerungs- und Anhaltedateien.

Windows-Auslagerungsdatei
Die Größe dieser Datei beträgt standardmäßig das 1,5-fache des Gastarbeitsspeichers. Diese Datei, deren Pfad standardmäßig `C:\pagefile.sys` lautet, bewirkt, dass per Thin Provisioning bereitgestellter Speicher anwächst, da häufig darauf zugegriffen wird. Bei auf verknüpften Klonen basierenden virtuellen Maschinen können die Auslagerungsdatei und die temporären Dateien auf eine separate virtuelle Festplatte umgeleitet werden, die beim Ausschalten der virtuellen Maschinen gelöscht wird. Die Umleitung von Auslagerungsdateien auf temporäre Festplatten spart Speicherplatz, verlangsamt das Anwachsen verknüpfter Klone und kann außerdem die Leistung verbessern. 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 Local Mode 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. Diese Datei kann im lokalen Datenspeicher auf dem ESX-Host oder im Cluster gespeichert werden.

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 der vom ESX-Host benötigte zusätzliche Arbeitsspeicher teilweise von der Anzahl der Monitore, die für Benutzer konfiguriert sind, und von der Anzeigeauflösung ab. Tabelle 4-1 zeigt die Menge des Arbeitsspeicher-Overheads, 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.

Tabelle 4-1. Overhead für PCoIP-Clientanzeige

Standardanzeigeauflösung	Breite (in Pixel)	Höhe (in Pixel)	Overhead bei einem Monitor	Overhead bei zwei Monitoren	Overhead bei vier Monitoren
VGA	640	480	2,34 MB	4,69 MB	9,38 MB
SVGA	800	600	3,66 MB	7,32 MB	14,65 MB
720p	1280	720	7,03 MB	14,65 MB	28,13 MB
UXGA	1600	1200	14,65 MB	29,30 MB	58,59 MB
1080p	1920	1080	15,82 MB	31,64 MB	63,28 MB

Tabelle 4-1. Overhead für PCoIP-Clientanzeige (Fortsetzung)

Standardanzeige-auflösung	Breite (in Pixel)	Höhe (in Pixel)	Overhead bei einem Monitor	Overhead bei zwei Monitoren	Overhead bei vier Monitoren
WUXGA	1920	1200	17,58 MB	35,16 MB	70,31 MB
QXGA	2048	1536	24,00 MB	48,00 MB	96,00 MB
WQXGA	2560	1600	31,25 MB	62,50 MB	125,00 MB

Wenn Sie diese Anforderungen prüfen, beachten Sie, dass sich die Konfiguration für zugewiesenen Speicherplatz virtueller Maschinen nicht verändert. Sie müssen also nicht 1 GB Arbeitsspeicher für Anwendungen und weitere 31 MB für zwei 1080p-Monitore zuweisen. Berücksichtigen Sie stattdessen den Overhead-Arbeitsspeicher bei der Berechnung der Gesamtmenge an physischem Arbeitsspeicher, der für die einzelnen ESX-Server erforderlich ist. Addieren Sie den Arbeitsspeicher des Gastbetriebssystems zum Overhead-Arbeitsspeicher hinzu und multiplizieren Sie ihn mit der Anzahl virtueller Maschinen.

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 guter Ausgangspunkt ist, 1 GB für Windows XP-Desktops und 32-Bit-Desktops unter Windows Vista und Windows 7 sowie 2 GB für 64-Bit-Desktops unter Windows 7 zuzuweisen. 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.

Hinweis Dieses Thema behandelt Aspekte hinsichtlich der CPU-Anforderungen beim Remote-Zugriff auf View-Desktops. Wenn Benutzer einen View-Desktop im lokalen Modus auf ihren Clientsystemen ausführen, verwendet der View-Desktop bis zu zwei der auf dem Clientgerät verfügbaren CPUs.

Die CPU-Anforderungen variieren je nach Nutzertyp. Überprüfen Sie in der Pilotphase mit einem Systemüberwachungsprogramm, wie Perfmon in der virtuellen Maschine und ESX Top in ESX, die Durchschnitts- und Spitzennutzungsgrade der CPU für diese Nutzergruppen. Beachten Sie außerdem die folgenden Richtlinien:

- Softwareentwickler und andere Hauptbenutzer mit hohem Systemleistungsbedarf haben ggf. wesentlich höhere CPU-Anforderungen als Büroanwender und Sachbearbeiter. Zwei virtuelle CPUs werden für rechenintensive Aufgaben oder für Windows 7-Desktops verwendet, die über das PCoIP-Anzeigeprotokoll 720p-Video wiedergeben sollen.
- Einfache virtuelle CPUs werden im Normalfall empfohlen.

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 Faustregel zum Festlegen der Anfangsgröße nehmen Sie an, dass jede virtuelle Maschine 1/16 bis 1/8 eines CPU-Kerns als garantierte Mindestrechenleistung benötigt. Planen Sie daher eine Pilotumgebung mit 8 bis 16 virtuellen Maschinen pro Kern. Wenn Sie beispielsweise von 16 virtuellen Maschinen pro Kern ausgehen und einen Vier-Kern-ESX-Server mit 2 Sockets verwenden, können Sie während der Pilotphase 128 virtuelle Maschinen auf dem Server hosten. Überwachen Sie während dieser Phase die CPU-Gesamtauslastung auf dem Host und stellen Sie sicher, dass sie selten eine Sicherheitstoleranz von 80 Prozent überschreitet, um genügend Spielraum für Spitzenauslastungen zu geben.

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 persistenten View Composer-Festplatte 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 bzw. `.vmdk`-Datei muss das Betriebssystem, Anwendungen sowie künftige Anwendungen und Software-Updates aufnehmen können. Die virtuelle Festplatte 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, für View-Desktop-Pools eine Richtlinie für die Speichermehrfachvergabe festlegen und Windows-Auslagerungs- und temporäre Dateien auf eine separate, nicht persistente Festplatte umleiten.

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

VMware View-ESX-Knoten

Ein Knoten ist ein einzelner VMware ESX-Server, der als Host von Desktops auf Basis virtueller Maschinen in einer VMware View-Bereitstellung dient.

VMware View arbeitet am wirtschaftlichsten, wenn Sie das Konsolidierungsverhältnis, also die Anzahl der Desktops maximieren, die von einem ESX-Server gehostet werden. Auch wenn die Serverauswahl von vielen Faktoren beeinflusst wird, müssen Sie bei einer strikten Optimierung nach Einkaufspreis Serverkonfigurationen finden, die ein ausgewogenes Maß an Verarbeitungsleistung und Arbeitsspeicher bieten.

Es gibt keinen Ersatz für das Messen der Leistung unter realen Bedingungen wie in einem Pilotprojekt, um ein angemessenes Konsolidierungsverhältnis für Ihre Umgebung und Hardwarekonfiguration zu ermitteln. Konsolidierungsverhältnisse können je nach Nutzungsmustern und Umgebungsfaktoren erheblich variieren. Beachten Sie die folgenden Richtlinien:

- Als allgemeine Richtlinie empfiehlt es sich, die Rechenkapazität bezüglich der virtuellen Desktops pro CPU-Kern zu bedenken. Mit ESX 4.1 können Sie zwischen 8 und 16 virtuellen Desktops pro CPU-Kern verwenden. Informationen zum Berechnen der CPU-Anforderungen jeder virtuellen Maschine finden Sie unter „Einschätzen der CPU-Anforderungen für virtuelle Desktops“, auf Seite 35.
- Betrachten Sie die Arbeitsspeicherkapazität im Hinblick auf den Arbeitsspeicher für den virtuellen Desktop, den Hostarbeitsspeicher und die Speichermehrfachvergabe. Auch wenn Sie zwischen 8 und 16 virtuellen Maschinen pro CPU-Kern einsetzen können, müssen Sie die die physischen Arbeitsspeicheranforderungen genau untersuchen, insbesondere wenn virtuelle Desktops 1 GB oder mehr Arbeitsspeicher besitzen. Informationen zur Berechnung der erforderlichen Arbeitsspeichermenge pro virtuelle Maschine finden Sie unter „Einschätzen der Arbeitsspeicheranforderungen für virtuelle Desktops“, auf Seite 33.

  Beachten Sie, 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.
- Berücksichtigen Sie außerdem die Cluster-Anforderungen und eventuelle Failover-Anforderungen. Weitere Informationen finden Sie unter „Bestimmen der Hochverfügbarkeitsanforderungen“, auf Seite 46.

Informationen zu Spezifikationen von ESX-Hosts in vSphere finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere*.

Desktop-Pools für bestimmte Nutzertypen

VMware View bietet viele Funktionen, mit deren Hilfe Sie Speicherplatz sparen und die für verschiedene Anwendungsfälle erforderliche Verarbeitungsleistung reduzieren können. Viele dieser Funktionen stehen als Pool-Einstellung zur Verfügung.

Die wichtigste Frage lautet, ob ein bestimmter Nutzertyp ein zustandsbehaftetes Desktop-Image oder ein zustandsloses Desktop-Image benötigt. Benutzer, die ein zustandsbehaftetes Desktop-Image benötigen, haben möglicherweise Daten im Betriebssystem-Image abgelegt, die gespeichert, gewartet und gesichert werden müssen. Beispielsweise installieren diese Benutzer eigene Anwendungen oder verwenden Daten, die nicht außerhalb der virtuellen Maschine, also auf einem Dateiserver oder in einer Anwendungsdatenbank, gespeichert werden können.

Zustandslose Desktop-Images

Zustandslose Architekturen besitzen viele Vorteile. Beispielsweise sind sie einfacher zu unterstützen, ermöglichen eine auf View Composer basierende Image-Verwaltung und verursachen geringere Speicherkosten. Außerdem müssen virtuelle Maschinen auf der Basis verknüpfter Klone nur begrenzt gesichert werden, und die Disaster Recovery- und Business Continuity-Optionen sind weniger komplex und kostengünstiger.

Zustandsbehaftete Desktop-Images

Für diese Images sind herkömmliche Methoden zur Image-Verwaltung erforderlich. Zustandsbehaftete Images können in Verbindung mit bestimmten Speichersystemtechnologien geringe Speicherkosten verursachen. Sicherungs- und Wiederherstellungstechnologien wie VMware Consolidated Backup und VMware Site Recovery Manager sind bei der Erwägung von Sicherungs-, Disaster Recovery- und Business Continuity-Strategien von großer Bedeutung.

Sie können mit View Composer zustandslose Desktop-Images erstellen, indem Sie Pools mit dynamischer Zuweisung aus virtuellen Maschinen auf Basis verknüpfter Klone erstellen. Zustandsbehaftete Desktop-Images werden erstellt, indem Sie Pools mit fester Zuweisung aus vollständigen virtuellen Maschinen erstellen. Einige Speicherhersteller bieten kostengünstige Speicherlösungen für zustandsbehaftete Desktop-Images an. Diese Hersteller haben oft ihre eigenen empfohlenen Vorgehensweisen und Bereitstellungsdienstprogramme. Für den Einsatz eines dieser Produkte müssen Sie möglicherweise einen manuellen Pool mit fester Zuweisung erstellen.

- Pools für Sachbearbeiter auf Seite 39

  Sie können für Sachbearbeiter standardmäßig zustandslose Desktop-Images verwenden, damit das Image immer in einer bekannten und leicht unterstützbaren Konfiguration vorliegt und die Nutzer sich immer an einem beliebigen verfügbaren Desktop anmelden können.

- Pools für Büroanwender und Hauptbenutzer auf Seite 39

  Büroanwender müssen komplexe Dokumente erstellen und dauerhaft auf dem Desktop speichern können. Hauptbenutzer müssen ihre eigenen Anwendungen dauerhaft installieren können. Je nach Art und Menge der zu speichernden persönlichen Daten kann es sich um einen zustandslosen oder einen zustandsbehafteten Desktop handeln.

- Pools für mobile Benutzer auf Seite 40

  Diese Benutzer können einen View-Desktop auschecken und sogar ohne Netzwerkverbindung lokal auf ihrem Laptop oder Desktop ausführen.

- Pools für Kioskbenutzer auf Seite 41

  Zu Kioskbenutzern gehören zum Beispiel Kunden an Checkin-Schaltern von Fluggesellschaften, Schüler in Klassenräumen oder Bibliotheken, medizinisches Personal an Eingabestationen für medizinische Daten oder Kunden an öffentlichen Zugangspunkten. Konten, die eher mit Clientgeräten als mit Benutzern verknüpft sind, können diese Desktop-Pools verwenden, da Benutzer sich nicht anmelden müssen, um das Clientgerät oder den View-Desktop zu nutzen. Dennoch müssen Benutzer für manche Anwendungen Anmeldeinformationen zur Authentifizierung bereitstellen.

Pools für Sachbearbeiter

Sie können für Sachbearbeiter standardmäßig zustandslose Desktop-Images verwenden, damit das Image immer in einer bekannten und leicht unterstützbaren Konfiguration vorliegt und die Nutzer sich immer an einem beliebigen verfügbaren Desktop anmelden können.

Da Sachbearbeiter sich wiederholende Aufgaben in einer überschaubaren Anzahl an Anwendungen durchführen, können Sie zustandslose Desktop-Images erstellen. So benötigen Sie weniger Speicherplatz und Verarbeitungsleistung. Verwenden Sie folgende Pool-Einstellungen:

- Erstellen Sie einen automatisierten Pool, damit Desktops zusammen mit dem Pool erstellt oder je nach Pool-Auslastung nach Bedarf generiert werden können.
- Verwenden Sie die dynamische Zuweisung, damit Benutzer sich an jedem verfügbaren Desktop anmelden können. Durch diese Einstellung wird die Anzahl erforderlicher Desktops reduziert, wenn nicht alle gleichzeitig angemeldet sein müssen.
- Erstellen Sie View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Rechenzentrum beanspruchen als vollständige virtuelle Maschinen.
- Legen Sie gegebenenfalls die Aktion fest, die beim Abmelden des Benutzers ausgeführt werden soll. Festplatten werden mit der Zeit größer. Sie können Speicherplatz sparen, indem Sie den Desktop auf den ursprünglichen Zustand aktualisieren, sobald der Benutzer sich abmeldet. Außerdem können Sie einen Zeitplan zur regelmäßigen Aktualisierung von Desktops festlegen. Zum Beispiel können Sie einstellen, dass Desktops täglich, wöchentlich oder monatlich aktualisiert werden.

Pools für Büroanwender und Hauptbenutzer

Büroanwender müssen komplexe Dokumente erstellen und dauerhaft auf dem Desktop speichern können. Hauptbenutzer müssen ihre eigenen Anwendungen dauerhaft installieren können. Je nach Art und Menge der zu speichernden persönlichen Daten kann es sich um einen zustandslosen oder einen zustandsbehafteten Desktop handeln.

Da Hauptbenutzer und Büroanwender, zum Beispiel Buchhalter, Vertriebsleiter und Marktforscher, Dokumente und Einstellungen erstellen und speichern müssen, erstellen Sie für diese Benutzer Desktops mit fester Zuweisung. Da Büroanwender benutzerinstallierte Anwendungen höchstens vorübergehend benötigen, können Sie zustandslose Desktop-Images erstellen und alle persönlichen Daten außerhalb der virtuellen Maschine auf einem Dateiserver oder in einer Anwendungsdatenbank speichern. Für andere Büroanwender und für Hauptanwender können Sie zustandsbehaftete Desktop-Images erstellen. Verwenden Sie folgende Pool-Einstellungen:

- Verwenden Sie die feste Zuweisung, damit jeder Büroanwender oder Hauptbenutzer sich jedes Mal an demselben Desktop anmeldet.
- Verwenden Sie vStorage Thin Provisioning, damit jeder Desktop zunächst nur so viel Speicherplatz beansprucht wie die Festplatte für den anfänglichen Betrieb benötigt.

- Wenn Büroanwender benutzerinstallierte Anwendungen höchstens vorübergehend benötigen, können Sie View Composer-Linked-Clone-Desktops erstellen. Diese zustandslosen Desktop-Images nutzen dasselbe Basis-Image und benötigen weniger Speicherplatz als vollständige virtuelle Maschinen.
- Wenn Sie View Composer-Linked-Clone-Desktops einsetzen, implementieren Sie entweder eine Lösung mit servergespeichertem oder virtuellem Profil zur zentralen Speicherung von Benutzerdaten oder konfigurieren Sie eine persistente Festplatte für den Desktop. Beachten Sie jedoch, dass zwar die zentral gespeicherten Daten und die persistente Festplatte nach einer Aktualisierung oder Neuzusammenstellung eines Desktops beibehalten werden, die Festplatte mit dem Betriebssystem und den Anwendungen hingegen nicht.
- Für Hauptbenutzer und Büroanwender, die ihre eigenen Anwendungen installieren müssen und so der Festplatte mit dem Betriebssystem Daten hinzufügen, erstellen Sie Desktops mit vollständigen virtuellen Maschinen. Diese Benutzer benötigen zustandsbehaftete Desktop-Images.

Pools für mobile Benutzer

Diese Benutzer können einen View-Desktop auschecken und sogar ohne Netzwerkverbindung lokal auf ihrem Laptop oder Desktop ausführen.

View Client with Local Mode bietet Vorteile sowohl für Benutzer als auch für IT-Administratoren. Für Administratoren können durch den lokalen Modus View-Sicherheitsrichtlinien auf Laptops ausgeweitet werden, die zuvor nicht verwaltet wurden. Administratoren können die auf dem View-Desktop ausgeführten Anwendungen genau kontrollieren und den Desktop genau wie Remote-View-Desktops zentral verwalten. Mit dem lokalen Modus können alle Vorteile von VMware View auch auf externe Büros oder Niederlassungen mit langsamen oder unzuverlässigen Netzwerken ausgedehnt werden.

Für Benutzer ergibt sich der Vorteil, dass sie ihre eigenen Computer weiterhin flexibel online oder offline verwenden können. Der View-Desktop wird automatisch verschlüsselt und kann zur Wiederherstellung nach Ausfällen einfach mit einem Image im Rechenzentrum synchronisiert werden.

Allgemeine Empfehlungen

Benutzer im lokalen Modus müssen gelegentlich auf ihre Desktop-Anwendungen und Daten von ihrem Laptop aus zugreifen, wenn keine Netzwerkverbindung verfügbar ist. Außerdem müssen diese Daten regelmäßig und automatisch im Rechenzentrum gesichert werden für den Fall, dass der Laptop verloren geht, beschädigt oder gestohlen wird. Um diese Möglichkeiten bereitzustellen, können Sie die folgenden Pool-Einstellungen verwenden.

- Beim Erstellen einer virtuellen Maschine als Basis für den Pool konfigurieren Sie die Mindestmenge an Arbeitsspeicher und virtuellen CPUs, die für das Gastbetriebssystem erforderlich sind. Im lokalen Modus ausgeführte Desktops passen die Menge an Arbeitsspeicher und Prozessorleistung basierend auf der auf dem Clientcomputer verfügbaren Menge an.
- Erstellen Sie einen automatisierten Pool, damit Desktops zusammen mit dem Pool erstellt oder je nach Pool-Auslastung nach Bedarf generiert werden können.
- Verwenden Sie eine feste Zuweisung, da Benutzer im lokalen Modus sich jedes Mal an demselben Desktop anmelden müssen.
- Erstellen Sie View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Rechenzentrum beanspruchen als vollständige virtuelle Maschinen.

- Wenn Sie möchten, dass der Bereitstellungsprozess eine eindeutige lokale Computer-SID und GUID für jeden verknüpften Klon im Pool erstellt, wählen Sie beim Erstellen des Pools eine Sysprep-Anpassungsspezifikation aus. Sysprep erstellt neue SIDs und GUIDs während der anfänglichen Bereitstellung und nach Neuzusammenstellungen. Da Sie Pools im lokalen Modus normalerweise nicht neu zusammenstellen, werden sich die SIDs und GUIDs wahrscheinlich nicht verändern.
- Nehmen Sie nur Desktops in den Pool auf, die im lokalen Modus verwendet werden sollen. Virtuelle Maschinen im lokalen Modus können in Datenspeichern mit niedrigeren IOPS-Anforderungen platziert werden als Speicher, die große Mengen an Remote-View-Desktops unterstützen müssen.

Zusätzliche Empfehlungen für minimalen Investitionsaufwand

Sie können die Anzahl an ESX-Servern reduzieren, die für den Pool für den lokalen Modus erforderlich sind, indem Sie die Anzahl virtueller Maschinen pro ESX-Server erhöhen. Ein ESX 4.1-Server kann bis zu 500 virtuelle Maschinen hosten, wenn die meisten nicht gleichzeitig eingeschaltet sind, wie dies in Pools für den lokalen Modus häufig der Fall ist.

Beachten Sie die folgenden Empfehlungen zum Reduzieren der von den einzelnen virtuellen Maschinen beanspruchten Bandbreite und E/A-Operationen sowie zum Maximieren der Anzahl virtueller Maschinen auf einem ESX-Server.

- Legen Sie eine View-Richtlinie fest, damit Benutzer ihre View-Desktops im lokalen Modus verwenden müssen. Mit dieser Einstellung bleiben die virtuellen Maschinen im Rechenzentrum gesperrt und ausgeschaltet.
- Richten Sie Richtlinien für den lokalen Modus so ein, dass Benutzer keine Desktop-Rollbacks, Datensicherungen oder Eincheckvorgänge am Rechenzentrum initiieren können.
- Planen Sie keine automatischen Sicherungen.
- Aktivieren Sie kein SSL zum Bereitstellen oder Herunterladen von Desktops im lokalen Modus.
- Wenn die Leistung von View Connection Server durch die Anzahl lokaler Desktops beeinträchtigt wird, verlängern Sie das Taktsignalintervall. Das Taktsignal informiert View Connection Server darüber, dass der lokale Desktop mit dem Netzwerk verbunden ist. Das Standardintervall beträgt fünf Minuten.

Pools für Kioskbenutzer

Zu Kioskbenutzern gehören zum Beispiel Kunden an Checkin-Schaltern von Fluggesellschaften, Schüler in Klassenräumen oder Bibliotheken, medizinisches Personal an Eingabestationen für medizinische Daten oder Kunden an öffentlichen Zugangspunkten. Konten, die eher mit Clientgeräten als mit Benutzern verknüpft sind, können diese Desktop-Pools verwenden, da Benutzer sich nicht anmelden müssen, um das Clientgerät oder den View-Desktop zu nutzen. Dennoch müssen Benutzer für manche Anwendungen Anmeldeinformationen zur Authentifizierung bereitstellen.

View-Desktops, die für die Ausführung im Kioskmodus eingestellt sind, verwenden zustandslose Desktop-Images, weil Benutzerdaten nicht auf der Betriebssystemfestplatte gespeichert werden müssen. Desktops im Kioskmodus werden mit Thin Client-Geräten oder gesperrten PCs mit eingeschränkten Funktionen verwendet. Sie müssen sicherstellen, dass die Desktop-Anwendung den Authentifizierungsmechanismus für sichere Transaktionen implementiert, dass das physische Netzwerk vor Sabotage und Überwachung geschützt ist und dass alle mit dem Netzwerk verbundenen Geräte vertrauenswürdig sind.

Es hat sich bewährt, dedizierte View Connection Server-Instanzen für die Verwaltung von Clients im Kioskmodus einzusetzen und dedizierte Organisationseinheiten und Gruppen in Active Directory für die Konten dieser Clients zu erstellen. Diese Vorgehensweise gewährleistet nicht nur einen Schutz dieser Systeme vor unbefugten Eingriffen, sie vereinfacht auch die Konfiguration und Verwaltung der Clients.

Zum Einrichten des Kioskmodus müssen Sie die Befehlszeilenschnittstelle `vdmadmin` verwenden und mehrere Verfahren durchführen, die im *VMware View-Administratorhandbuch* unter den Themen zum Kioskmodus dokumentiert sind. Im Zuge dieser Einrichtung können Sie die folgenden Pool-Einstellungen verwenden.

- Erstellen Sie einen automatisierten Pool, damit Desktops zusammen mit dem Pool erstellt oder je nach Pool-Auslastung nach Bedarf generiert werden können.
- Verwenden Sie die dynamische Zuweisung, damit Benutzer auf jeden verfügbaren Desktop im Pool zugreifen können.
- Erstellen Sie View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Rechenzentrum beanspruchen als vollständige virtuelle Maschinen.
- Richten Sie eine Aktualisierungsrichtlinie ein, damit der Desktop häufig aktualisiert wird, beispielsweise bei jeder Benutzerabmeldung.
- Verwenden Sie ein Active Directory-Gruppenrichtlinienobjekt zum Konfigurieren der standortbasierten Druckfunktion, damit der Desktop den nächstgelegenen Drucker verwendet. Eine vollständige Liste und Beschreibung der über Gruppenrichtlinien-ADM-Vorlagen verfügbaren Einstellungen finden Sie im *VMware View-Administratorhandbuch*.
- Mit einem Gruppenrichtlinienobjekt können Sie die Standardrichtlinie außer Kraft setzen, die das Anschließen lokaler USB-Geräte am Desktop gestattet, wenn der Desktop gestartet wird oder wenn USB-Geräte an den Clientcomputer angeschlossen werden.

Konfigurieren virtueller Maschinen für View-Desktops

Da die Arbeits- und Festplattenspeichergröße und die CPU-Leistung, die von virtuellen Desktops benötigt wird, vom Gastbetriebssystem abhängt, werden nach Windows XP, Windows Vista und Windows 7 getrennte Konfigurationsbeispiele für virtuelle Desktops angegeben.

Die Beispieleinstellungen für virtuelle Maschinen in Bezug auf Arbeitsspeicher, Anzahl virtueller Prozessoren und Festplattenspeicher sind spezifisch für VMware View.

Die in Tabelle 4-2 angegebenen Vorgaben gelten für einen standardmäßigen virtuellen Desktop mit Windows XP, der im Remote-Modus ausgeführt wird.

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

Element	Beispiel
Betriebssystem	32-Bit-Windows XP (mit neuestem Service Pack)
Arbeitsspeicher (RAM)	1 GB (mindestens 512 MB, höchstens 2 GB)
Virtuelle CPU	1
Kapazität der Systemfestplatte	16 GB (mindestens 8 GB, höchstens 40 GB)
Benutzerdatenkapazität (als persistente Festplatte)	5 GB (Ausgangswert)
Virtueller SCSI-Adaptertyp	LSI Logic (nicht die Standardeinstellung)
Virtueller Netzwerkadapter	Flexibel (Standardeinstellung)

Die Speichergröße der Systemfestplatte hängt von der Anzahl der Anwendungen ab, die im Basis-Image benötigt werden. VMware hat eine Einrichtung mit 8 GB Festplattenspeicher geprüft. 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 Benutzers und den Unternehmensrichtlinien für die Datenspeicherung ab. Beim Verwenden von View Composer verbleiben diese Daten auf einer persistenten Festplatte.

Die in Tabelle 4-3 angegebenen Vorgaben gelten für einen standardmäßigen virtuellen Desktop mit Windows Vista, der im Remote-Modus ausgeführt wird.

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

Element	Beispiel
Betriebssystem	32-Bit-Windows Vista (mit neuestem Service Pack)
Arbeitsspeicher (RAM)	1 GB
Virtuelle CPU	1
Kapazität der Systemfestplatte	20 GB (Standardeinstellung)
Benutzerdatenkapazität (als persistente Festplatte)	5 GB (Ausgangswert)
Virtueller SCSI-Adaptertyp	LSI Logic (Standardeinstellung)
Virtueller Netzwerkadapter	E1000 (Standard)

Die in Tabelle 4-4 angegebenen Vorgaben gelten für einen standardmäßigen virtuellen Desktop mit Windows 7, der im Remote-Modus ausgeführt wird.

Tabelle 4-4. Beispiel für einen virtuellen Desktop für Windows 7, gehostet auf einem ESX 4.1-Server

Element	Beispiel
Betriebssystem	Windows 7, 32-Bit
Arbeitsspeicher (RAM)	1 GB
Virtuelle CPU	1
Kapazität der Systemfestplatte	20 GB (etwas weniger als Standard)
Benutzerdatenkapazität (als persistente Festplatte)	5 GB (Ausgangswert)
Virtueller SCSI-Adaptertyp	LSI Logic SAS (Standardeinstellung)
Virtueller Netzwerkadapter	E1000 (Standard)

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

vCenter Server 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 Server und View Composer auf einem physischen Computer installieren können, wird in diesem Beispiel eine virtuelle Maschine mit den in Tabelle 4-5 angegebenen technischen Daten verwendet. Der ESX-Server, der als Host dieser virtuelle Maschine dient, kann Teil eines VMware HA-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Dieses Beispiel geht davon aus, dass Sie VMware View mit vSphere 4.1 und vCenter Server 4.1 einsetzen.

Tabelle 4-5. vCenter Server: Beispiel für eine virtuelle Maschine und Festlegen der maximalen Poolgröße

Element	Beispiel
Betriebssystem	Windows Server 2008 R2 Enterprise, 64-Bit
Arbeitsspeicher (RAM)	4 GB
Virtuelle CPU	2
Kapazität der Systemfestplatte	40 GB
SCSI-Typ	LSI SAS Logic (Standardeinstellung für Windows Server 2008)

Tabelle 4-5. vCenter Server: Beispiel für eine virtuelle Maschine und Festlegen der maximalen Poolgröße (Fortsetzung)

Element	Beispiel
Netzwerkadapter	E1000 (Standard)
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. Richtlinien für die Datenbankdimensionierung finden Sie im *vCenter Server 4.x Database Sizing Calculator for Microsoft SQL Server* (Größenberechnung für die vCenter Server 4.x-Datenbank für Microsoft SQL Server) unter http://www.vmware.com/support/vsphere4/doc/vsp_4x_db_calculator.xls.

View Connection Server: Konfigurieren von Maximalwerten und virtuellen Maschinen

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

View Connection Server-Konfiguration

Wenngleich Sie View Connection Server auf einem physischen Computer installieren können, wird in diesem Beispiel eine virtuelle Maschine mit den in Tabelle 4-6 angegebenen technischen Daten verwendet. Der ESX-Server, der als Host dieser virtuelle Maschine dient, kann Teil eines VMware HA-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Tabelle 4-6. Beispiel einer virtuellen Maschine für View Connection Server

Element	Beispiel
Betriebssystem	Windows Server 2008 R2, 64-Bit
Arbeitsspeicher (RAM)	10 GB
Virtuelle CPU	4
Kapazität der Systemfestplatte	40 GB
SCSI-Typ	LSI SAS Logic (Standardeinstellung für Windows Server 2008)
Netzwerkadapter	E1000 (Standard)
1 Netzwerkadapter	1 Gigabit

Aspekte des Cluster-Aufbaus bei View Connection Server

Sie können mehrere replizierte View Connection Server-Instanzen in einer Gruppe bereitstellen, um Lastausgleich und hohe Verfügbarkeit zu unterstützen. Gruppen replizierter Instanzen sind auf die Unterstützung von Clustern innerhalb einer im LAN verbundenen Umgebung mit einem einzigen Rechenzentrum ausgelegt. Aufgrund des Kommunikationsdatenverkehrs zwischen den gruppierten Instanzen rät VMware von der Verwendung einer Gruppe replizierter View Connection Server-Instanzen über ein WAN ab. In Szenarios, in denen eine View-Bereitstellung sich über mehrere Rechenzentren erstreckt, erstellen Sie für jedes Rechenzentrum eine separate View-Bereitstellung.

Maximale Verbindungsanzahl für View Connection Server

Tabelle 4-7 bietet Informationen zu den getesteten Einschränkungen in Bezug auf die Anzahl gleichzeitiger Verbindungen, die eine VMware View-Bereitstellung unterstützen kann.

Dieses Beispiel geht davon aus, dass Sie VMware View mit vSphere 4.1 und vCenter Server 4.1 einsetzen.

Tabelle 4-7. View-Desktop-Verbindungen

Anzahl der Connection Server-Instanzen pro Bereitstellung	Verbindungstyp	Maximale Anzahl gleichzeitiger Verbindungen
1 Connection Server-Instanz	Direkte Verbindung, RDP oder PCoIP	2,000
7 Connection Server-Instanzen (5 + 2 Reserve)	Direkte Verbindung, RDP oder PCoIP	10.000
3 Connection Server-Instanzen	Tunnelverbindung, RDP	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.

View Transfer Server: Konfiguration und Speicher für virtuelle Maschinen

View Transfer Server ist zur Unterstützung von Desktops erforderlich, auf denen View Client with Local Mode (früher Offline Desktop) ausgeführt wird. Dieser Server beansprucht weniger Arbeitsspeicher als View Connection Server.

View Transfer Server – Konfiguration

Sie müssen View Transfer Server auf einer virtuellen und nicht auf einer physischen Maschine installieren, und die virtuelle Maschine muss von derselben vCenter Server-Instanz verwaltet werden wie die lokalen Desktops, die sie verwalten soll. Unter Tabelle 4-8 werden die Spezifikationen virtueller Maschinen für eine View Transfer Server-Instanz aufgeführt.

Tabelle 4-8. Beispiel für eine virtuelle View Transfer Server-Maschine

Element	Beispiel
Betriebssystem	Windows Server 2008 R2, 64-Bit
Arbeitsspeicher (RAM)	4 GB
Virtuelle CPU	2
Kapazität der Systemfestplatte	20 GB
SCSI-Typ	LSI Logic (nicht die Standardeinstellung, diese lautet SAS)
Netzwerkadapter	E1000 (Standard)
1 Netzwerkadapter	1 Gigabit

Speicher- und Bandbreitenanforderungen für View Transfer Server

Bei mehreren Operationen wird View Transfer Server zum Senden von Daten zwischen dem View-Desktop in vCenter Server und dem entsprechenden lokalen Desktop auf dem Clientsystem verwendet. Wenn ein Benutzer sich an einem Desktop anmeldet oder davon abmeldet, überträgt View Transfer Server die Dateien zwischen dem Rechenzentrum und dem lokalen Desktop. View Transfer Server synchronisiert außerdem lokale Desktops mit den entsprechenden Desktops im Rechenzentrum, indem Benutzeränderungen im Rechenzentrum repliziert werden.

Wenn Sie verknüpfte View Composer-Klone für lokale Desktops verwenden, muss das Festplattenlaufwerk, auf dem Sie das Transfer Server-Repository konfigurieren, genügend Speicherplatz für Ihre statischen Image-Dateien besitzen. Image-Dateien sind View Composer-Basis-Images. Je schneller die Netzwerkspeicherfestplatten sind, desto besser ist die erzielte Leistung. Informationen zum Ermitteln der Größe von Basis-Image-Dateien finden Sie im *VMware View-Administratorhandbuch*.

Jede Transfer Server-Instanz kann 60 gleichzeitige Festplattenvorgänge fassen, auch wenn die Netzwerkbandbreite wahrscheinlich bereits bei einer geringeren Anzahl ausgelastet ist. VMware hat 20 gleichzeitige Festplattenvorgänge getestet, beispielsweise 20 Clients, die gleichzeitig über eine Netzwerkverbindung mit 1 GB pro Sekunde einen lokalen Desktop herunterladen.

vSphere-Cluster

VMware View-Bereitstellungen können VMware HA-Cluster (High Availability) als Schutz gegen Ausfälle physischer Server nutzen. Aufgrund von View Composer-Beschränkungen darf das Cluster nicht mehr als 8 Server, oder 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 der Pool eines zustandslosen Desktop-Images (dynamische Zuweisung) andere RPO-Anforderungen (Recovery Point Objective) aufweisen als der Pool eines zustandsbehafteten Desktop-Images (feste Zuweisung). Bei einem Pool mit dynamischer Zuweisung 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: Beispiel der Konfiguration eines Clusters

Die Einstellungen in Tabelle 4-9 sind VMware View-spezifisch. Informationen zu den Grenzwerten von HA-Clustern in vSphere finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere*.

Tabelle 4-9. Beispiel eines HA-Clusters

Element	Beispiel
Knoten (ESX-Server)	8 (einschließlich einem in Reserve)
Cluster-Typ	DRS (Distributed Resource Scheduler)/HA
Netzwerkkomponente	Standard-ESX 4.1-Clusternetzwerk
Switch-Ports	80

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

VMware View-Bausteine

Ein Baustein für 2.000 Benutzer besteht aus physischen Servern, einer VMware vSphere-Infrastruktur, VMware View-Servern, gemeinsamem Speicher sowie 2.000 Desktops auf Basis virtueller Maschinen. Eine View-Struktur kann bis zu fünf Bausteine umfassen.

Tabelle 4-10. Beispiel eines LAN-basierten View-Bausteins

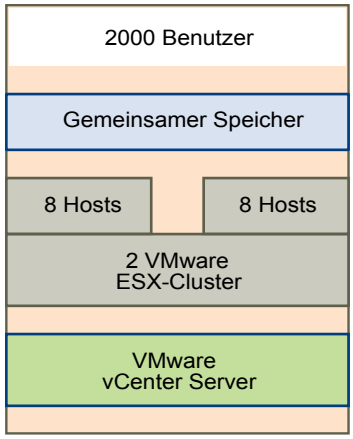
Element	Beispiel
vSphere-Cluster	Mindestens 2 (mit bis zu 8 ESX-Hosts pro Cluster)
Netzwerk-Switch mit 80 Ports	1
Gemeinsames Speichersystem	1
vCenter Server mit View Composer	1 (kann im Baustein selbst ausgeführt werden)
Datenbank	Microsoft SQL Server oder Oracle-Datenbankserver (kann im Baustein selbst ausgeführt werden)
VLANs	3 (jeweils ein 1 Gbit-Ethernet-Netzwerk: Verwaltungsnetzwerk, Speichernetzwerk und vMotion-Netzwerk)

Bei vCenter 4.1, das auf 10.000 virtuelle Maschinen pro vCenter beschränkt ist, können Sie möglicherweise vCenter Server-Instanzen verwenden, die virtuelle Desktops in mehreren Bausteinen verwalten. Zum Zeitpunkt der Drucklegung dieses Dokuments hat VMware einen solchen Ansatz in Verbindung mit VMware View noch nicht geprüft. Die Tests von vCenter Server 4.1 mit VMware View 4.5 waren auf das Testen von 2.000 virtuellen Desktops mit einem vCenter Server beschränkt.

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

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

Abbildung 4-1. VMware View-Baustein



Gemeinsamer Speicher für View-Bausteine

Die Planung des Speicherentwurfs ist eine der wichtigsten Voraussetzungen für eine erfolgreiche View-Architektur. Die Entscheidung mit dem größten Einfluss auf die Systemarchitektur ist die für den Einsatz von View Composer-Desktops, die mit der Linked-Clone-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 Sicht der Architektur erstellt View Composer 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 persistente View Composer-Festplatten oder freigegebene Dateiserver als primäre Speicherorte für die Profile und Dokumente der Benutzer einsetzen. Da View Composer das Trennen von Benutzerdaten vom Betriebssystem erlaubt, muss ggf. nur die persistente Festplatte gesichert oder repliziert werden, was die Speicheranforderungen weiter senkt. Weitere Informationen finden Sie unter „Reduzieren von Speicheranforderungen mit View Composer“, auf Seite 27.

Hinweis Die Entscheidung, ob Sie für jeden Baustein eine separate, dedizierte Speicherkomponente einsetzen möchten, können Sie während einer Pilotphase treffen. Das Hauptkriterium sind die E/A-Vorgänge pro Sekunde (IOPS). Sie können mit einer mehrere Bausteine umfassenden Strategie des mehrstufigen Speichers experimentieren, um die Leistung und die Kosteneinsparungen zu maximieren.

Weitere Informationen finden Sie im Handbuch mit empfohlenen Vorgehensweisen namens *Storage Considerations for VMware View* (Speicheraspekte bei VMware View).

Aspekte der Speicherbandbreite

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

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. Durch Speichern von View Composer-Replikaten in separaten Hochleistungs-Datenspeichern können Sie intensive, gleichzeitige Lesevorgänge beschleunigen, um E/A-Überlastungen zu bewältigen.

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.

Aspekte der Netzwerkbandbreite

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.

Wenn Sie ein Unternehmens-LAN mit 100 Mb oder ein vermitteltes Netzwerk mit 1 Gb verwenden, können Ihre Benutzer durch das PCoIP-Anzeigeprotokoll unter folgenden Umständen eine herausragende Leistung erwarten:

- Zwei Monitore (1920x1080)
- Starke Nutzung von Microsoft Office-Anwendungen
- Starke Nutzung von Webbrowsern mit eingebettetem Flash
- Häufige Multimedia-Nutzung bei begrenztem Einsatz des Vollbildmodus
- Starke Nutzung USB-basierter Peripheriegeräte
- Netzwerkbasiertes Drucken

Diese Informationen wurden dem Informationshandbuch *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide* (PCoIP-Anzeigeprotokoll: Handbuch und Leitfaden für die szenariobasierte Netzwerkdimensionierung) entnommen.

WAN-Unterstützung und PCoIP

Bei Weitbereichsnetzwerken (WAN) müssen Sie Bandbreiteneinschränkungen und Wartezeiten berücksichtigen. Das von VMware bereitgestellte PCoIP-Anzeigeprotokoll passt sich an wechselnde Wartezeit- und Bandbreitenbedingungen an.

Beim Verwenden des Anzeigeprotokolls RDP ist ein WAN-Optimierungsprodukt zum Beschleunigen von Anwendungen für Benutzer in Niederlassungen und kleinen Büroumgebungen erforderlich. Bei PCoIP sind viele WAN-Optimierungsmethoden in das Basisprotokoll integriert.

- Die WAN-Optimierung ist wertvoll für TCP-basierte Protokolle wie RDP, da diese Protokolle viele Handshakes zwischen Client und Server erfordern. Die Wartezeit für diese Handshakes kann recht lang sein. WAN-Beschleuniger geben Antworten auf Handshakes vor, sodass die Wartezeit im Netzwerk vor dem Protokoll verborgen wird. Da PCoIP auf UDP basiert, ist diese Art der WAN-Beschleunigung nicht notwendig.
- WAN-Beschleuniger komprimieren außerdem den Netzwerkdatenverkehr zwischen Client und Server. Diese Komprimierung ist jedoch in der Regel auf ein Komprimierungsverhältnis von 2:1 beschränkt. PCoIP kann Komprimierungsraten von bis zu 100:1 für Bild- und Audiodaten erzielen.

Im folgenden Beispiel wird dargestellt, welche Leistung PCoIP in verschiedenen WAN-Szenarios zeigt:

Arbeiten am Heimarbeitsplatz

Ein Benutzer mit dedizierter Kabel- oder DSL-Verbindung mit 4-8 MB Download und weniger als 300 ms Wartezeit kann unter folgenden Umständen eine herausragende Leistung erwarten:

- Zwei Monitore (1920x1080)
- Microsoft Office-Anwendungen
- Geringe Nutzung von Webbrowsern mit eingebettetem Flash
- Regelmäßige Multimedia-Nutzung
- Geringe Nutzung der Druckfunktion auf einem lokal angeschlossenen USB-Drucker

Mobiler Benutzer

Ein Benutzer mit einer dedizierten 3G-Verbindung mit 5-500 KB Download und weniger als 300 ms Wartezeit kann unter folgenden Umständen eine angemessene Bandbreite und tolerierbare Wartezeit erwarten:

- Einzelner Monitor
- Microsoft Office-Anwendungen
- Geringe Nutzung von Webbrowsern mit eingebettetem Flash
- Geringe Nutzung der Druckfunktion auf einem lokal angeschlossenen USB-Drucker

Halten Sie mobile Benutzer dazu an, lokale Anwendungen für den Zugriff auf Multimedia-Inhalte zu verwenden.

Niederlassung oder externes Büro

Planen Sie drei gleichzeitig aktive Benutzer pro 1 Mb Bandbreite. Benutzer in einem Büro mit einem dedizierten UDP-basierten 20-Mb-VPN von Standort zu Standort mit einer Wartezeit von weniger als 200 ms können unter folgenden Umständen eine akzeptable Leistung erwarten:

- Zwei Monitore (1920x1080)
- Microsoft Office-Anwendungen

- Geringe Nutzung von Webbrowsern mit eingebettetem Flash
- Geringe Nutzung der Druckfunktion auf einem lokal angeschlossenen USB-Drucker

Diese Informationen wurden dem Informationshandbuch *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide* (PCoIP-Anzeigeprotokoll: Handbuch und Leitfaden für die szenariobasierte Netzwerkdimensionierung) entnommen.

Informationen zum Einrichten von PCoIP finden Sie in den folgenden Lösungsübersichten, die auf der VMware-Website zur Verfügung stehen:

- *VMware View and Juniper Networks SA Series SSL VPN Solution* (VMware View und Juniper Networks SA Series – SSL-VPN-Lösung)
- *VMware View and F5 BIG-IP SSL VPN Solution* (VMware View und F5 BIG-IP – SSL-VPN-Lösung)
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution* (VMware View und Cisco Adaptive Security Appliances (ASA) – SSL-VPN-Lösung)

VMware View-Struktur

Eine VMware View-Struktur integriert fünf Bausteine mit je 2.000 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 4-11 zeigt die Komponenten einer View-Struktur.

Tabelle 4-11. Beispiel einer VMware View-Struktur

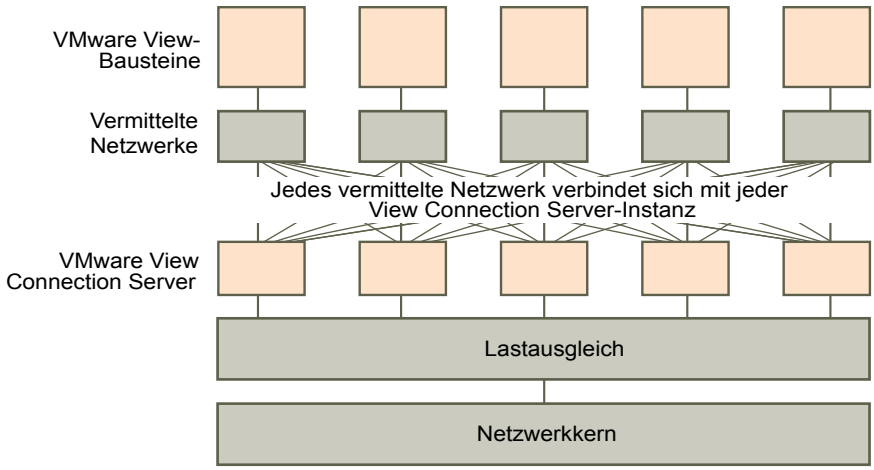
Element	Anzahl bzw. Größe
View-Bausteine	5
View Connection Server	7 (1 für jeden Baustein und 2 Reserve)
10-Gbit-Ethernet-Modul	1
Modularer Netzwerk-Switch	1
Lastausgleichsmodul	1
VPN für WAN	1 (optional)

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 10.000 View-Desktops



Planen von Sicherheitsfunktionen 5

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

Dieses Kapitel behandelt die folgenden Themen:

- „Grundlegendes zu Clientverbindungen“, auf Seite 53
- „Auswählen einer Benutzerauthentifizierungsmethode“, auf Seite 55
- „Einschränken des Zugriffs auf View-Desktops“, auf Seite 58
- „Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von View-Desktops“, auf Seite 59
- „Implementieren empfohlener Vorgehensweisen zum Sichern von Clientsystemen“, auf Seite 59
- „Zuweisen von Administratorrollen“, auf Seite 60
- „Vorbereiten des Einsatzes eines Sicherheitsservers“, auf Seite 60
- „Grundlegendes zu VMware View-Kommunikationsprotokollen“, auf Seite 65

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.

Während der View Connection Server-Installation wird ein Server-SSL-Standardzertifikat generiert. Clients werden standardmäßig mit diesem Zertifikat präsentiert, wenn sie eine sichere Seite wie die View Administrator-Seite besuchen.

Sie können das Standardzertifikat zu Testzwecken verwenden, sollten es jedoch so bald wie möglich durch ein eigenes Zertifikat ersetzen. Das Standardzertifikat wird nicht von einer kommerziellen Zertifizierungsstelle signiert. Die Verwendung nicht zertifizierter Zertifikate kann nicht vertrauenswürdigen Parteien das Abfangen von Datenverkehr ermöglichen, indem sie sich als ihr Server ausgeben.

- Getunnelte Clientverbindungen mit Microsoft RDP auf Seite 54

  Wenn Benutzer eine Verbindung mit einem View-Desktop mit dem Microsoft RDP-Anzeigeprotokoll herstellen, stellt View Client eine zweite HTTPS-Verbindung zum View Connection Server-Host her. Diese Verbindung wird als Tunnelverbindung bezeichnet, da sie einen Tunnel für den RDP-Datenverkehr darstellt.

- Direkte Clientverbindungen mit PCoIP und HP RGS auf Seite 54

  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 Local Mode – Clientverbindungen auf Seite 55

  View Client with Local Mode bietet mobilen Benutzern die Möglichkeit, View-Desktops auf ihren lokalen Computer auszuchecken.

Getunnelte Clientverbindungen mit Microsoft RDP

Wenn Benutzer eine Verbindung mit einem View-Desktop mit dem Microsoft RDP-Anzeigeprotokoll herstellen, stellt View Client eine zweite HTTPS-Verbindung zum View Connection Server-Host her. Diese Verbindung wird als Tunnelverbindung bezeichnet, da sie einen Tunnel für den RDP-Datenverkehr darstellt.

Die Tunnelverbindung bietet die folgenden Vorteile:

- RDP-Daten werden durch HTTPS getunnelt und über SSL verschlüsselt. Dieses leistungsstarke Sicherheitsprotokoll entspricht den Sicherheitsmaßnahmen, die auch für andere sichere Websites vorgenommen werden, wie z.B. für Online-Banking und Kreditkartenzahlungen.
- Ein Client kann über eine einzelne HTTS-Verbindung auf mehrere Desktops zugreifen, wodurch der gesamte Protokoll-Overhead reduziert wird.
- Da VMware View 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 60 finden Sie weitere Informationen zu Bereitstellungen mit Umkreisnetzwerk (DMZ) und Sicherheitsservern.

Clients mit den Anzeigeprotokollen PCoIP und HP RGS nutzen nicht die Tunnelverbindung.

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.

Clients, die die Anzeigeprotokolle PCoIP und HP RGS einsetzen, verwenden direkte Clientverbindungen. Sie können die Tunnelverbindung nicht nutzen.

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.

View Client with Local Mode – Clientverbindungen

View Client with Local Mode bietet mobilen Benutzern die Möglichkeit, View-Desktops auf ihren lokalen Computer auszuchecken.

View Client with Local Mode 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 lokalen Desktop auf dem Clientsystem und der virtuellen Maschine mit dem View-Desktop in vCenter Server übertragen.

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

Auswählen einer Benutzerauthentifizierungsmethode

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

- Active Directory-Authentifizierung auf Seite 55

  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.

- RSA SecurID-Authentifizierung auf Seite 56

  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 56

  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 57

  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 die Befehlszeilenschnittstelle `vdmadmin` können Administratoren eine Domänenfilterung konfigurieren, mit deren Hilfe die Domänen eingeschränkt werden, die eine View Connection Server-Instanz durchsucht und die den Benutzer angezeigt werden. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.

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.

VMware View 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.

Die Smartcard-Authentifizierung wird nur vom Windows-basierten View Client und von View Client with Local Mode unterstützt, nicht jedoch von View Administrator.

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.

Für den Einsatz von Smartcards müssen Clientcomputer über Smartcard-Middleware und einen Smartcard-Leser verfügen. Um Zertifikate auf Smartcards zu installieren, müssen Sie einen Computer einrichten, der als Registrierungsstelle fungiert.

Zur Verwendung von Smartcards auf lokalen Desktops müssen Sie bei der Smartcard-Registrierung eine Schlüsselgröße von 1024 Bit oder 2048 Bit auswählen. Zertifikate mit 512-Bit-Schlüsseln werden für lokale Desktops nicht unterstützt. Standardmäßig verwendet View Connection Server AES-128 für die Verschlüsselung der virtuellen Festplattendatei, wenn Benutzer einen lokalen Desktop ein- oder auschecken. Sie können die Verschlüsselungsmethode in AES-192 oder AES-256 ändern.

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 View 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. Administratoren können auch mithilfe der Gruppenrichtlinie festlegen, welche View Connection Server-Instanzen die Benutzeridentitäts- und Anmeldeinformationen akzeptieren, die bei Aktivierung des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** in View Client übergeben werden.

Für die Funktion **[Log in as current user (Anmelden als aktueller Benutzer)]** gelten folgende Einschränkungen und Anforderungen:

- Ist eine Smartcard-Authentifizierung auf einer View Connection Server-Instanz auf **[Required (Erforderlich)]** festgelegt, müssen Smartcard-Benutzer, die das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktivieren, sich bei der Anmeldung am View-Desktop dennoch erneut mit ihrer Smartcard und PIN authentifizieren.
- Benutzer können einen Desktop zur Verwendung im lokalen Modus nicht auschecken, wenn sie bei der Anmeldung das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktiviert haben.
- Die Zeit auf dem System, an dem der Client sich anmeldet, und die Zeit auf dem View Connection Server-Host müssen synchronisiert sein.
- Wenn die Standardzuweisungen des Benutzerrechts **[Access this computer from the network (Auf diesen Computer vom Netzwerk aus zugreifen)]** auf dem Clientsystem geändert werden, muss diese Änderung wie im VMware Knowledge Base-Artikel 1025691 beschrieben durchgeführt werden.

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.

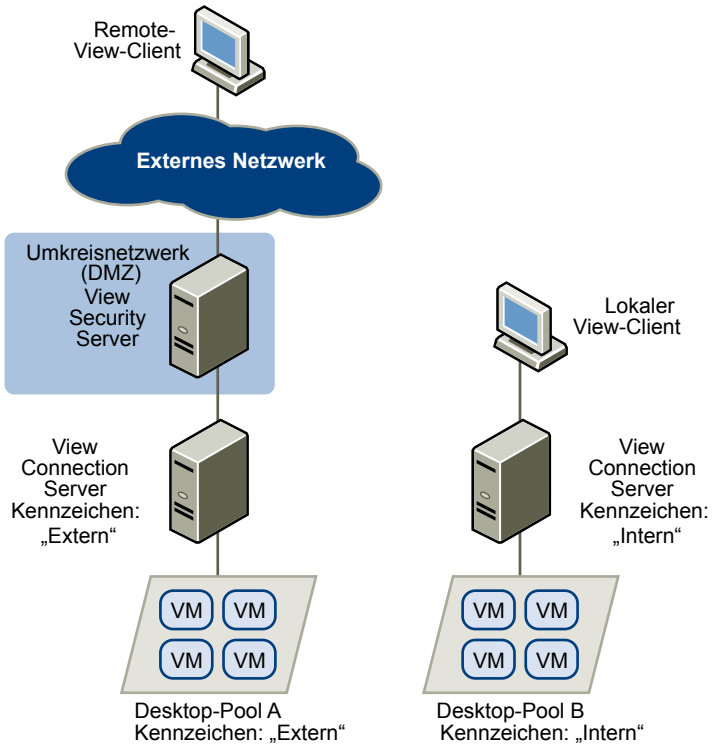
Zum Einschränken von Berechtigungen weisen Sie einer View Connection Server-Instanz ein oder mehrere Kennzeichen zu. Wenn Sie anschließend einen Desktop-Pool konfigurieren, wählen Sie die Kennzeichen der View Connection Server-Instanzen aus, auf die der Desktop-Pool zugreifen können soll. Wenn Benutzer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

Angenommen, Ihre VMware View-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 Desktop-Pools zu, auf die nur interne Benutzer zugreifen dürfen.
- Weisen Sie das Kennzeichen „Extern“ den Desktop-Pools zu, auf die nur externe Benutzer zugreifen dürfen.

Externen Benutzern werden keine als „Intern“ gekennzeichneten Desktop-Pools angezeigt, da sie sich an der als „Extern“ gekennzeichneten View Connection Server-Instanz anmelden. Hingegen können interne Benutzern keine als „Extern“ gekennzeichneten Desktop-Pools sehen, da sie sich an der als „Intern“ gekennzeichneten View Connection Server-Instanz anmelden. Abbildung 5-1 zeigt diese Konfiguration.

Abbildung 5-1. 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 Desktop-Pools 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.

Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von View-Desktops

VMware View umfasst Gruppenrichtlinien-Verwaltungsvorlagen (ADM) mit sicherheitsbezogenen Gruppenrichtlinieneinstellungen, mit deren Hilfe Sie Ihre View-Desktops sichern können.

Beispielsweise können Sie Gruppenrichtlinieneinstellungen zum Durchführen der folgenden Aufgaben verwenden.

- Angeben der View Connection Server-Instanzen, die Benutzeridentitäts- und Anmeldeinformationen akzeptieren können, die bei Aktivierung des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** in View Client übergeben werden.
- Aktivieren von Single Sign-On für die Smartcard-Authentifizierung in View Client.
- Konfigurieren der Server-SSL-Zertifikatprüfung in View Client.
- Verhindern, dass Benutzer Anmeldeinformationen über die View Client-Befehlszeilenoptionen bereitstellen.

Informationen zur Verwendung von View Client-Gruppenrichtlinieneinstellungen finden Sie im *VMware View-Administratorhandbuch*.

Implementieren empfohlener Vorgehensweisen zum Sichern von Clientsystemen

Sie sollten die empfohlenen Vorgehensweisen anwenden, um Clientsysteme zu sichern.

- Stellen Sie sicher, dass Clientsysteme so konfiguriert sind, dass sie nach einer bestimmten Leerlaufzeit in den Energiesparmodus wechseln. Benutzer müssen somit ein Kennwort eingeben, um den Computer wieder zu aktivieren.
- Verlangen Sie von Benutzern beim Starten von Clientsystemen die Eingabe eines Benutzernamens und eines Kennworts. Konfigurieren Sie Clientsysteme nicht so, dass automatische Anmeldungen zulässig sind.
- Für Mac-Clientsysteme sollten Sie erwägen, verschiedene Kennwörter für den Schlüsselbund und das Benutzerkonto festzulegen. Wenn die Kennwörter sich unterscheiden, werden Benutzer abgefragt, bevor das System Kennwörter in ihrem Namen eingibt. Ziehen Sie außerdem die Aktivierung des FileVault-Schutzes in Betracht.
- Clientsysteme im lokalen Modus besitzen möglicherweise mehr Netzwerkzugriff als Clientsysteme, die remote und mit dem Intranet verbunden sind. Setzen Sie Netzwerksicherheitsrichtlinien für Clientsysteme im lokalen Modus durch, oder deaktivieren Sie den Netzwerkzugriff für solche Clientsysteme, solange sie im lokalen Modus ausgeführt werden.

Zuweisen von Administratorrollen

Eine wichtige Verwaltungsaufgabe in einer VMware View-Umgebung besteht darin festzulegen, wer View Administrator verwenden kann und welche Aufgaben die betreffenden Benutzer ausführen dürfen.

Die Autorisierung zum Ausführen von Aufgaben in View Administrator wird durch ein Zugriffssteuerungssystem geregelt, das aus Administratorrollen und -berechtigungen besteht. Eine Rolle ist eine Sammlung von Berechtigungen. Berechtigungen ermöglichen die Durchführung bestimmter Aktionen wie das Erteilen einer Desktop-Pool-Berechtigung an einen Benutzer oder das Ändern einer Konfigurationseinstellung. Berechtigungen steuern außerdem, was einem Administrator in View Administrator angezeigt wird.

Ein Administrator kann Ordner erstellen, um Desktop-Pools zu unterteilen, und die Verwaltung bestimmter Desktop-Pools an andere Administratoren in View Administrator delegieren. Ein Administrator konfiguriert den Administratorzugriff auf die Ressourcen in einem Ordner, indem er einem Benutzer für diesen Ordner eine Rolle zuweist. Administratoren können nur auf die Ressourcen in Ordnern zugreifen, für die ihnen eine Rolle zugewiesen wurde. Die Rolle, die ein Administrator für einen Ordner besitzt, bestimmt die Zugriffsebene, mit der der Administrator auf die Ressourcen im jeweiligen Ordner zugreifen kann.

View Administrator umfasst eine Reihe vordefinierter Rollen. Administratoren können durch die Kombination ausgewählter Berechtigungen auch benutzerdefinierte Rollen erstellen.

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 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 Sicherheitsserverbereitstellung auf Basis eines Umkreisnetzwerks erfordert das Öffnen verschiedener Ports in der Firewall, damit sich Clients mit Sicherheitsservern im Umkreisnetzwerk verbinden können. Sie müssen ferner 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 64.

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.

Hinweis 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.

Informationen zum Einrichten von PCoIP finden Sie in den folgenden Lösungsübersichten, die auf der VMware-Website zur Verfügung stehen:

- *VMware View and Juniper Networks SA Series SSL VPN Solution* (VMware View und Juniper Networks SA Series – SSL-VPN-Lösung)
- *VMware View and F5 BIG-IP SSL VPN Solution* (VMware View und F5 BIG-IP – SSL-VPN-Lösung)
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution* (VMware View und Cisco Adaptive Security Appliances (ASA) – SSL-VPN-Lösung)

Empfohlene Vorgehensweisen für die Bereitstellung von Sicherheitsservern

Bei Verwendung eines Sicherheitsservers in einem Umkreisnetzwerk sollten Sie die empfohlenen Vorgehensweisen für Sicherheitsrichtlinien und -vorgänge befolgen.

Das Whitepaper *DMZ Virtualization with VMware Infrastructure* (Virtualisierung von Umkreisnetzwerken mit VMware Infrastructure) enthält Beispiele für empfohlene Vorgehensweisen für ein virtualisiertes Umkreisnetzwerk. Viele Empfehlungen in diesem Whitepaper gelten auch für ein physisches Umkreisnetzwerk.

Um den Geltungsbereich von Frame-Broadcasts einzuschränken, sollten View Connection Server-Instanzen, die mit Sicherheitsservern ein Paar bilden, in einem isolierten Netzwerk bereitgestellt werden. Mit dieser Topologie kann ein böswilliger Benutzer im internen Netzwerk daran gehindert werden, die Kommunikation zwischen den Sicherheitsservern und den View Connection Server-Instanzen zu überwachen.

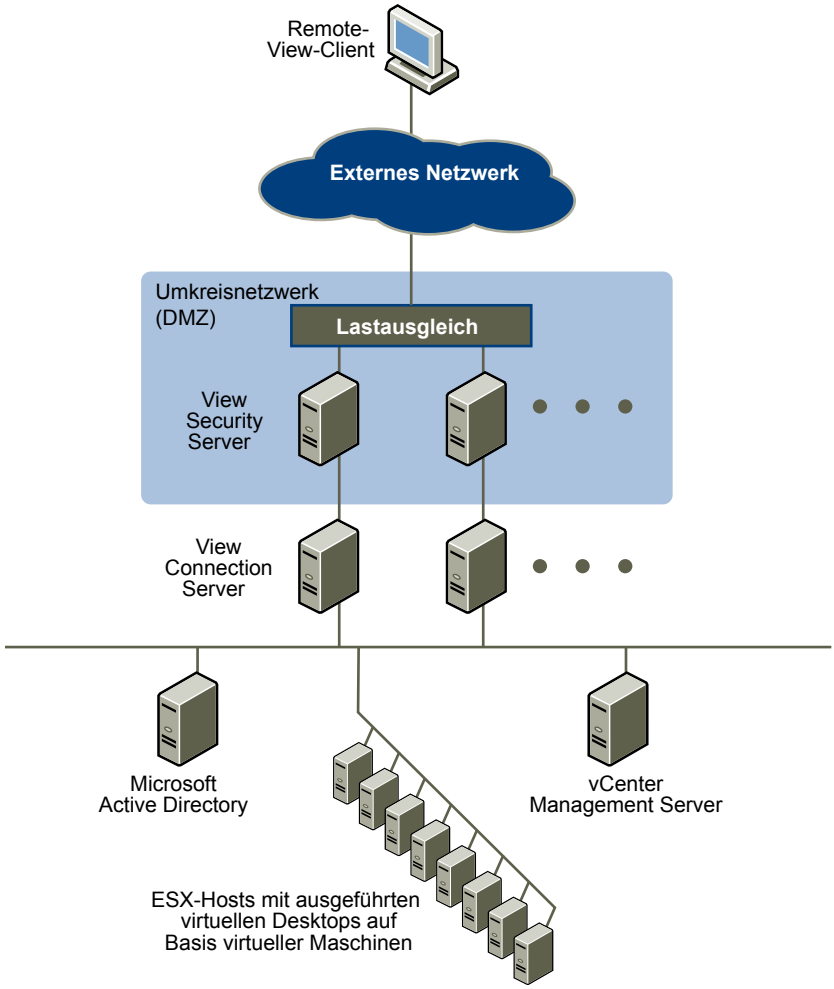
Alternativ dazu können Sie möglicherweise erweiterte Sicherheitsfunktionen in Ihrem Netzwerk-Switch einsetzen, um die böswillige Überwachung der Sicherheitsserver- und View Connection Server-Kommunikation zu verhindern und sich vor Überwachungsangriffen wie ARP Cache Poisoning zu schützen. Weitere Informationen finden Sie in der Administratordokumentation für Ihre Netzwerkausrüstung.

Topologien von Sicherheitsservern

Sie können mehrere verschiedene Topologien von Sicherheitsservern implementieren.

Die Topologie in Abbildung 5-2 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 5-2. Sicherheitsserver mit Lastausgleich in einem Umkreisnetzwerk

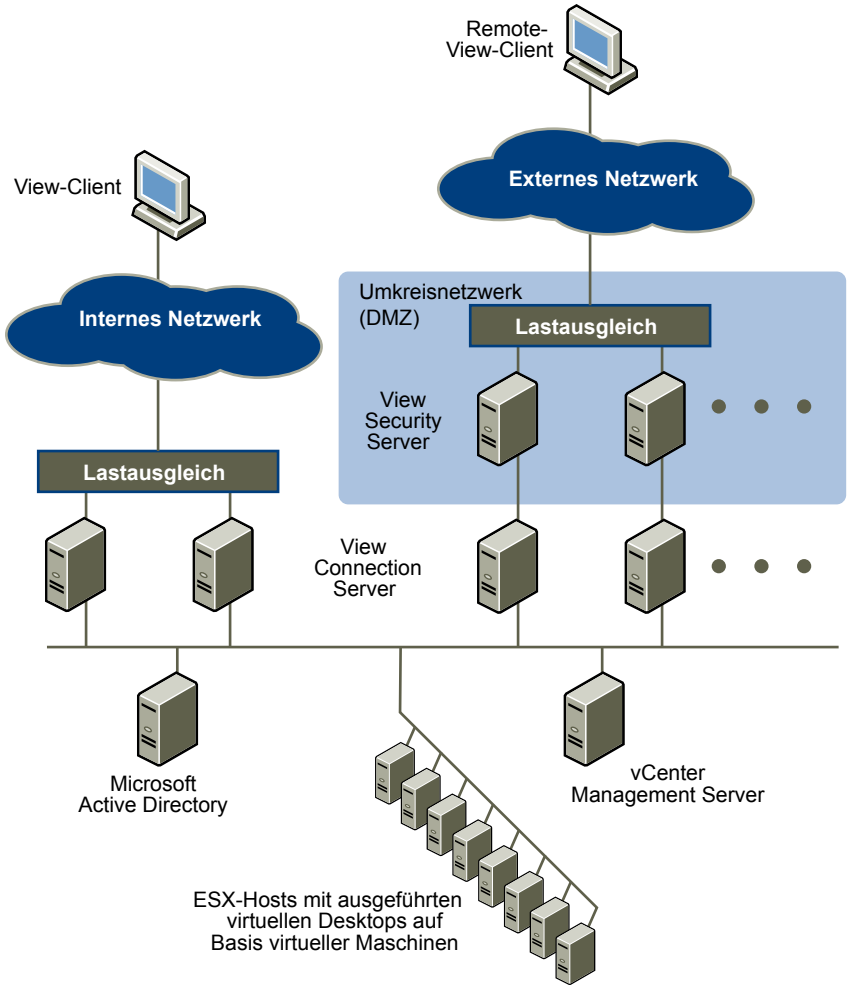


Wenn sich Remote-Benutzer mit einem Sicherheitsserver verbinden, müssen sie sich vor einem Zugriff auf View-Desktops erfolgreich authentifizieren. Bei entsprechenden Firewall-Regeln auf beiden Seiten des Umkreisnetzwerks eignet sich diese Topologie für die Zugriff auf View-Desktops auf Clientgeräten, 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 5-3 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 5-3. Mehrere Sicherheitsserver



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

Firewalls für Sicherheitsserver im Umkreisnetzwerk

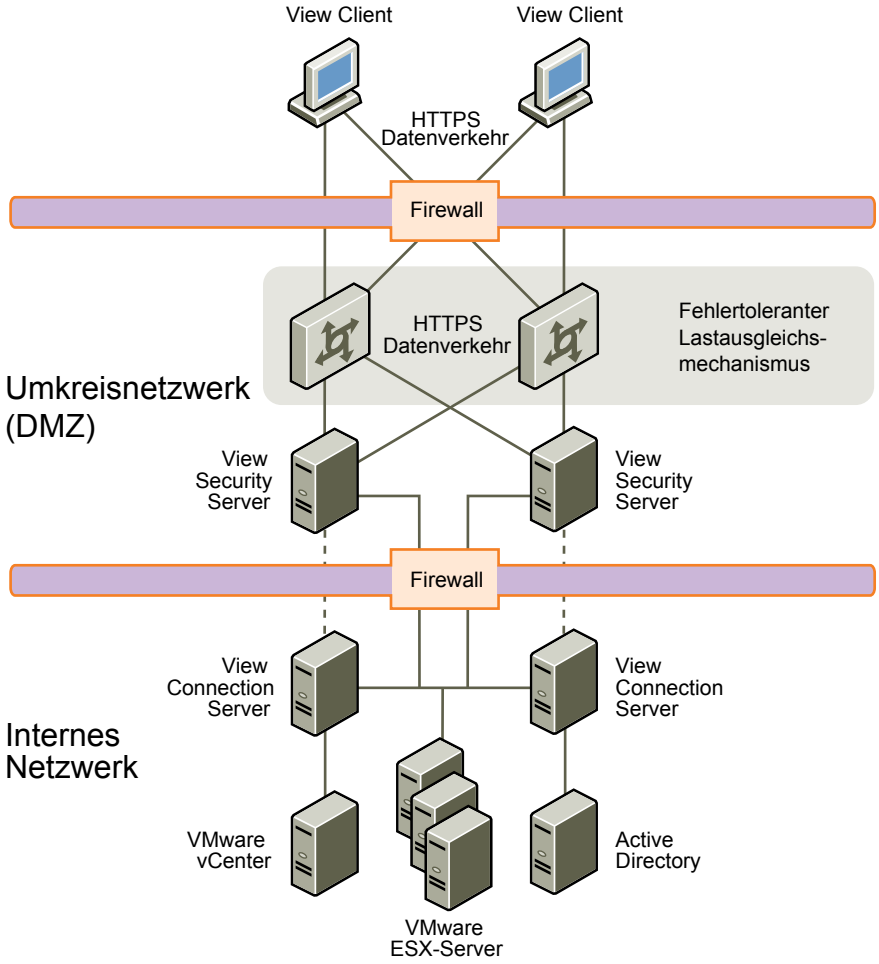
Eine Bereitstellung von Sicherheitsservern in einem Umkreisnetzwerk muss zwei Firewalls aufweisen.

- 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 5-4 zeigt eine Beispielkonfiguration mit Front-End- und Back-End-Firewall.

Abbildung 5-4. Zwei-Firewall-Topologie



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 5-1 enthält eine Übersicht der Regeln für die Front-End-Firewall.

Tabelle 5-1. 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 5-2 enthält eine Übersicht der Regeln für die Back-End-Firewall.

Tabelle 5-2. 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 die Kommunikation zwischen View Connection Server-Instanzen

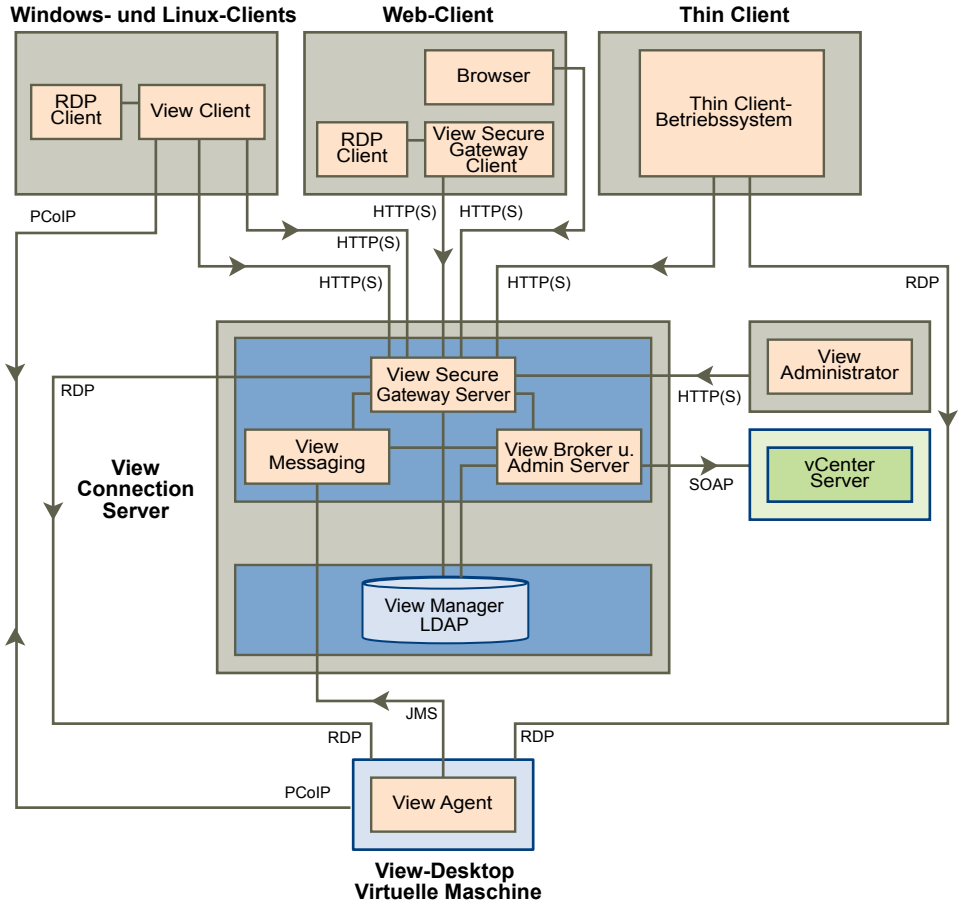
Gruppen von View Connection Server-Instanzen nutzen zusätzliche TCP-Ports für die Kommunikation untereinander. Zum Beispiel verwenden View Connection Server-Instanzen Port 4100 zum Übertragen von JMS-Datenverkehr (JMSIR) zwischen View Connection Server-Instanzen. Firewalls werden im Allgemeinen nicht zwischen den View Connection Server-Instanzen in einer Gruppe verwendet.

Grundlegendes zu VMware View-Kommunikationsprotokollen

VMware View-Komponenten tauschen Nachrichten mithilfe mehrerer Protokolle aus.

Abbildung 5-5 veranschaulicht die Protokolle, die die einzelnen Komponenten für die Kommunikation verwenden, wenn kein Sicherheitsserver konfiguriert ist.

Abbildung 5-5. VMware View-Komponenten und -Protokolle ohne Sicherheitsserver



Unter Tabelle 5-3 finden Sie die Standardports, die von den einzelnen Protokollen verwendet werden.

Abbildung 5-6 veranschaulicht die Protokolle, die die einzelnen Komponenten für die Kommunikation verwenden, wenn ein Sicherheitsserver konfiguriert ist.

Abbildung 5-6. VMware View-Komponenten und -Protokolle mit Sicherheitsserver

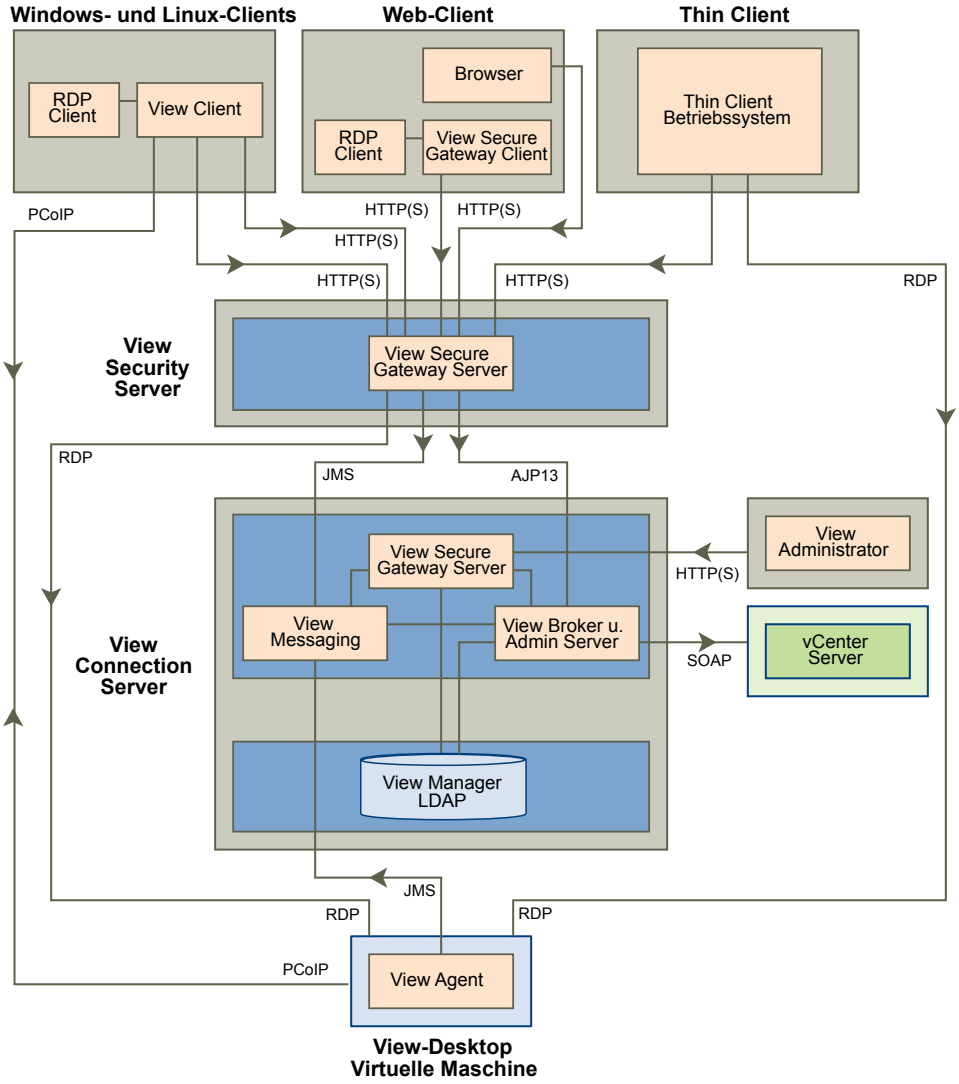


Tabelle 5-3 zeigt die Standardports, die von den einzelnen Protokollen verwendet werden.

Tabelle 5-3. 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 5-3. Standardports (Fortsetzung)

Protokoll	Port
SOAP	TCP-Port 80 oder 443
PCoIP	TCP-Port 4172 vom View Client zum View-Desktop. PCoIP nutzt auch UDP-Port 4172 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 VMware 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 VMware 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 VMware 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 VMware 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 VMware 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 VMware View verwendet wird.

Standardmäßig handelt es sich bei RSA-Schlüsseln, die zur komponentenübergreifenden Nachrichtenprüfung verwendet werden, um 512-Bit-Schlüssel. Die RSA-Schlüsselgröße kann auf 1024 Bit erhöht werden, wenn Sie eine stärkere Verschlüsselung bevorzugen.

Wenn Sie nur 1024-Bit-Schlüssel verwenden möchten, muss die RSA-Schlüsselgröße unmittelbar nach der Installation der ersten View Connection Server-Instanz und vor der Erstellung weiterer Server und Desktops geändert werden. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel 1024431.

Firewall-Regeln für View Connection Server

Bestimmte eingehende TCP-Ports müssen in der Firewall für View Connection Server-Instanzen und Sicherheitsserver geöffnet werden.

Bei der Installation von View Connection Server unter Windows Server 2008 kann das Installationsprogramm optional die erforderlichen Windows-Firewall-Regeln für Sie konfigurieren. Wenn Sie View Connection Server unter Windows Server 2003 installieren, müssen Sie die erforderlichen Windows-Firewall-Regeln manuell konfigurieren.

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

Protokoll	Ports	Typ der View Connection Server-Instanz
JMS	4001	Standard und Replikat
JMSIR	4100	Standard und Replikat
AJP13	8009	Standard und Replikat
HTTP	80	Standard-, Replikat- und Sicherheitsserver
HTTPS	443	Standard-, Replikat- und Sicherheitsserver

Firewall-Regeln für View Agent

Das View Agent-Installationsprogramm öffnet bestimmte TCP-Ports in der Firewall. Wenn nicht anders angegeben, handelt es sich hierbei um eingehende Ports.

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

Protokoll	Ports
RDP	3389
USB-Umleitung	32111
MMR	9427
PCoIP	4172 (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.

Wenn Sie im View Agent-Installationsprogramm angeben, dass die Remote-Desktop-Unterstützung nicht aktiviert werden soll, werden die Ports 3389 und 32111 nicht geöffnet und Sie müssen diese Ports manuell öffnen.

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 VMware 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 Local Mode

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

Überblick über die Schritte zum Einrichten einer VMware View-Umgebung

6

Führen Sie diese allgemeinen Aufgaben aus, um VMware View zu installieren und eine erste Bereitstellung zu konfigurieren.

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

Schritt	Aktion
1	Einrichten der benötigten Administrator- und Benutzergruppen in Active Directory. Anweisungen: *VMware View-Installationshandbuch* und vSphere-Dokumentation
2	Installieren und konfigurieren Sie VMware ESX-Server und vCenter Server gegebenenfalls. Anweisungen: vSphere-Dokumentation
3	Wenn Sie Linked-Clone-Desktops bereitstellen möchten, installieren Sie View Composer auf dem vCenter Server-System. Anweisungen: *VMware View-Installationshandbuch*
4	Installieren und konfigurieren Sie View Connection Server. Anweisungen: *VMware View-Installationshandbuch*
5	Wenn Sie Desktops im lokalen Modus verwenden möchten, installieren Sie Transfer Server. Anweisungen: *VMware View-Installationshandbuch*
6	Erstellen einer oder mehrerer virtueller Maschinen, die als Vorlage für Desktop-Pools auf Basis vollständiger Klone oder als übergeordnete virtuelle Maschinen von Linked-Clone-Desktop-Pools dienen. Anweisungen: *VMware View-Administratorhandbuch*
7	Erstellen Sie einen Desktop-Pool. Anweisungen: *VMware View-Administratorhandbuch*
8	Steuern Sie den Benutzerzugriff auf Desktops. Anweisungen: *VMware View-Administratorhandbuch*
9	Installieren Sie View Client auf den Computern der Benutzer und lassen Sie die Benutzer auf ihre View-Desktops zugreifen. Anweisungen: *VMware View-Installationshandbuch*
10	(Optional) Erstellen und konfigurieren Sie zusätzliche Administratoren, um verschiedene Zugriffsebenen auf bestimmte Bestandsobjekte und -einstellungen zu ermöglichen. Anweisungen: *VMware View-Administratorhandbuch*
11	(Optional) Konfigurieren Sie Richtlinien, um das Verhalten von View-Komponenten, Desktop-Pools und Desktop-Benutzern zu steuern. Anweisungen: *VMware View-Administratorhandbuch*
12	(Optional) Integrieren Sie zur zusätzlichen Sicherheit die Smartcard-Authentifizierung und die RSA SecurID-Lösung. Anweisungen: *VMware View-Administratorhandbuch*

Index

A

Active Directory **9, 30, 55**
ADM-Vorlagendateien **59**
Administration Server **68**
Administratorrollen **60**
Adobe Flash **25**
Agent, View **12**
AJP13-Protokoll **64, 65**
Aktualisierungsfunktion **28, 36**
Ältere PCs **11**
Anhaltedateien **33, 36**
Anmeldedaten, Benutzer **57**
Anmelden als aktueller Benutzer, Option **23, 57**
Anwendungsvirtualisierung und -bereitstellung **28, 29**
Anzeigeprotokolle
  Definition **18**
  HP RGS **17, 20, 54**
  Microsoft RDP **17, 19, 54**
  PCoIP **54, 60**
  View PCoIP **9, 17, 19**
Arbeitsspeicherzuweisung für virtuelle Maschinen **33, 42**
Architekturentwurfselemente **31**
Auslagerungsdateien **33**

B

Back-End-Firewall
  konfigurieren **63**
  Regeln **64**
Bandbreite **49, 50**
Basis-Image für virtuelle Desktops **26, 27**
Benutzerauthentifizierung
  Active Directory **55**
  Methoden **55**
  RSA SecurID **56**
  Smartcards **56**
Benutzertypen **32**
Berechtigungen, eingeschränkt **58**
Bereitstellen von Desktops **7**
Bestimmen der Datenbankgröße **43**
Browser, unterstützte **12**
Büroanwender **32, 33, 39**
Business Intelligence-Software **14**

C

Checkliste für die Einrichtung von VMware View **71**
Clientsysteme, Empfohlene Vorgehensweisen zur Sicherung **59**
Clientverbindungen
  direkt **54**
  Tunnel **54**
Cluster, vSphere **46**
CPU-Schätzwerte **35, 42**

D

Datenbanktypen **47**
Datenspeicher **27**
Delegierte Verwaltung **60**
Desktop **12**
Desktop als verwalteter Dienst (DaaS) **7**
Desktop-Pools **13, 25, 27, 38**
Desktop-Quellen **25**
Diagramm einer Bereitstellung von VMware View **10**
direkte Clientverbindungen **44, 54**
Distributed Resource Scheduler (DRS) **46**
drucken, virtuell **22**
Drucker **17**
Dynamische Zuweisung, Desktop-Pools **25**

E

E/A-Überlastungen **49**
eingeschränkte Berechtigungen **58**
Einmalige Anmeldung **12, 23, 57**
Einrichtung, VMware View **71**
ESX-Hosts **37**

F

Feste Zuweisung, Desktop-Pools **25, 27**
Festplattenspeicherzuweisung für virtuelle Desktops **36, 42**
Fibre Channel SAN-Arrays **26**
Firewall-Regeln
  Active Directory **70**
  View Agent **69**
  View Client with Local Mode **70**
  View Connection Server **69**
Firewalls
  Back-End **63**

Front-End **63**
Regeln **64**
Front-End-Firewall
konfigurieren **63**
Regeln **64**

G

Gateway-Server **68**
Gemeinsamer Speicher **26, 48**
getunnelte Kommunikation **55, 68**
Gruppenrichtlinienobjekte, Sicherheitseinstellungen für View-Desktops **59**

H

HA-Cluster **43, 44, 46**
Hauptbenutzer **32**
HP RGS **17, 20, 54**

I

iSCSI SAN-Arrays **26**

J

Java Message Service **68**
Java Message Service-Protokoll **64**
JMS-Protokoll **64, 65**

K

Kerne, Dichte virtueller Maschinen **35**
Kioskmodus **41**
Klone, verknüpfte **13, 28**
Kommunikationsprotokolle, Grundlegendes **65**

L

Lastausgleich, View Connection Server **51, 61**
LDAP-Konfigurationsdaten **14**
LDAP-Verzeichnis **11, 68**
Linux-Clients **12**
Lokale Desktops, View Transfer Server **13**
Lokaler Desktop, Verwendung, Vorteile **20**
lokaler Modus, , *siehe* Lokaler Desktop
Lokaler Modus, Benutzer **40**
LUNs **27**

M

Macintosh-Clients **11, 12**
mehrere Monitore **9, 19, 23**
Microsoft RDP **17, 19, 23, 54**
Microsoft Remotedesktopverbindung-Client für Mac **12**
Multimedia-Streaming **22**
Multimedia-Umleitung (MMR) **22**

N

Nachrichtenübermittlungs-Router **68**
NAS-Arrays **26**
Netzwerkbandbreite **49**
Neuverteilungsfunktion **27**
Neuzusammenstellungsfunktion **28**
Nutzertypen **32, 33, 35, 38**

O

Offline Desktop (Local Mode), , *siehe* Lokaler Desktop

P

PCoIP **7, 9, 17, 19, 54, 60**
persistente Festplatten **27**
Physische PCs **44**
Pools
Büroanwender **39**
Desktop **27, 38**
Kioskbenutzer **41**
lokaler Modus, Benutzer **40**
Sachbearbeiter **39**
Pools, Desktop **13, 25**
Professional Services **5**

R

RAM-Zuweisung für virtuelle Maschinen **33, 42**
Remote-Desktops, Vergleich mit lokalen Desktops **20**
Replikate **27**
Richtlinien, Desktop **30**
RSA SecurID-Authentifizierung **56**
RSA-Schlüsselgröße, ändern **68**

S

Sachbearbeiter **32, 33, 39**
SCOM **14**
SCSI-Adaptertypen **42**
Sicherheitsfunktionen, Planung **53**
Sicherheitsserver
empfohlene Vorgehensweisen zur Bereitstellung **61**
implementieren **60**
Lastausgleich **61**
Übersicht **11**
Skalierbarkeit, Planung **31**
Smartcard-Authentifizierung **56**
Smartcard-Leser **22, 56**
Snapshots **28**
Softwarebereitstellung **29**
Speicher, reduzieren, mit View Composer **26, 27**

Speicherbandbreite **49**
Speicherkonfigurationen **48**
Streaming von Anwendungen **29**
Streaming von Multimedia **22**

T

TCP-Ports
  Active Directory **70**
  View Agent **69**
  View Client with Local Mode **70**
  View Connection Server **69**
technischer Support **5**
Terminalserver **44**
Thin Client-Unterstützung **11, 17**
ThinApp **29**
Tunnelverbindung **44, 54**

U

übergeordnete virtuelle Maschine **27, 28**
Übersicht der unterstützten Funktionen **17**
Umkreisnetzwerk **60, 61, 63**
Umkreisnetzwerk (DMZ) **11, 60, 61, 63**
Unified Access **44**
unterstützte Mediendatenformate **22**
USB-Geräte, verwenden mit View-Desktops **9, 17, 22**
USB-Umleitung **22**

V

vCenter, Konfiguration **43**
vCenter Server **13, 25**
vdmadmin (Befehl) **14**
Verarbeitungsanforderungen **35**
Verbindungstypen
  Client **53**
  direkt **54**
  externer Client **60**
  Tunnel **54**
verknüpfte Klone **13, 27, 28, 44, 48**
Verschlüsselung
  unterstützt mit PCoIP **19**
  unterstützt von Microsoft RDP **19**
  von Benutzeranmeldedaten **57**
View Administrator **12, 30**
View Agent **12, 30**
View Broker **68**
View Client **11, 30**
View Client für Linux **11**
View Client with Local Mode, Verbindungen **55**
View Client with Offline Desktop (Local Mode), *, siehe* Lokaler Desktop
View Composer, Vorgänge **44, 48**
View Connection Server
  gruppieren **61**
  Konfiguration **12, 30, 44**
  Lastausgleich **61**
  RSA SecurID-Authentifizierung **56**
  Smartcard-Authentifizierung **56**
  Übersicht **11**
View Messaging **68**
View Open Client **11**
View Portal **11, 12**
View PowerCLI **14**
View Secure Gateway Server **68**
View Transfer Server
  Konfiguration **45**
  Synchronisieren lokaler Desktops **13**
View-Baustein **47, 48**
View-Bereitstellungsdiagramm **10**
View-Desktop-Konfigurationen **32**
View-Knotenkonfiguration **37**
View-Struktur **51**
virtuelle Druckfunktion **9, 17, 22**
virtuelle Maschine, Konfiguration
  für vCenter **43**
  für View Composer **43**
  für View Connection Server **44**
  für View Transfer Server **45**
  für View-Desktops **32**
virtuelle private Netzwerke **19, 60**
VMDK-Dateien **36**
vMotion **46**
VMware View with Local Mode, *, siehe* Lokaler Desktop
Vorlagen, Gruppenrichtlinienobjekt **30**
vSphere **7, 9, 26**
vSphere-Cluster **46, 47**

W

WAN-Konfigurationen **47**
WAN-Unterstützung **50**
Wartezeit **50**
Windows-Auslagerungsdatei **36**
Wyse MMR **17, 22**

Z

Zwei-Firewall-Topologie **63**