

Planung der View-Architektur

VMware Horizon 6 6.0



vmware®

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

<https://docs.vmware.com/de/>

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2009–2014 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Planung der View-Architektur 6

1 Einführung in View 7

- Vorteile der Verwendung von View 7
- Funktionen von View 11
- Zusammenspiel der Komponenten 13
 - Clientgeräte 14
 - View-Verbindungsserver 15
 - Horizon Client 16
 - VMware Horizon-Webportal für Benutzer 16
 - View Agent 17
 - View Administrator 17
 - View Composer 17
 - vCenter Server 18
- Integrieren und Anpassen von View 18

2 Planen einer umfassenden Benutzerumgebung 24

- Funktionsunterstützungs-Matrix für View Agent 24
- Auswählen eines Anzeigeprotokolls 26
 - PCoIP 26
 - Microsoft RDP 29
- Verwenden von gehosteten Anwendungen 29
- Verwendung von View Persona Management zur Speicherung von Benutzerdaten und -einstellungen 30
- Verwenden von USB-Geräten mit Remote-Desktops 33
- Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone 33
- Verwenden von 3D-Grafikanwendungen 34
- Streaming von Multimediadaten auf einen Remote-Desktop 35
- Drucken von einem Remote-Desktop aus 35
- Verwenden der Single Sign-On-Funktion zur Anmeldung bei einem Remote-Desktop 36
- Verwendung mehrerer Monitore 36

3 Zentrales Verwalten von Desktop- und Anwendungspools 38

- Vorteile von Desktop-Pools 38
- Vorteile von Anwendungspools 39
- Reduzieren und Verwalten von Speicheranforderungen 40
 - Verwalten des Speichers mit vSphere 41
 - Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung 42

| | |
|--|-----------|
| Reduzieren von Speicheranforderungen mit View Composer | 44 |
| Anwendungsbereitstellung | 47 |
| Bereitstellen von individuellen Anwendungen mithilfe eines RDS-Hosts | 47 |
| Bereitstellen von Anwendungen und System-Updates mit View Composer | 48 |
| Verwalten von VMware ThinApp-Anwendungen in View Administrator | 48 |
| Verwenden von bestehenden Prozessen oder VMware Mirage für die Anwendungsbereitstellung | 49 |
| Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten | 50 |
| 4 Architekturentwurfselemente und Planungsanleitungen für Remote-Desktop-Bereitstellungen | 51 |
| Anforderungen virtueller Maschinen für Remote-Desktops | 52 |
| Auf den Nutzertypen basierende Planung | 52 |
| Einschätzen der Arbeitsspeicheranforderungen für Desktops auf virtuellen Maschinen | 53 |
| Einschätzen der CPU-Anforderungen für Desktops auf virtuellen Maschinen | 56 |
| Auswählen der geeigneten Systemfestplattengröße | 57 |
| View ESXi-Knoten | 58 |
| Desktop-Pools für bestimmte Nutzertypen | 59 |
| Pools für Sachbearbeiter | 61 |
| Pools für Büroanwender und Hauptbenutzer | 62 |
| Pools für Kioskbenutzer | 63 |
| Konfigurieren virtueller Maschinen für View-Desktops | 64 |
| Konfiguration von virtuellen Maschinen als RDS-Hosts | 66 |
| vCenter Server- und View Composer-Konfiguration für virtuelle Maschinen | 66 |
| View-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen | 68 |
| vSphere-Cluster | 70 |
| Speicher- und Bandbreitenanforderungen | 73 |
| Beispiel für gemeinsamen Speicher | 73 |
| Aspekte der Speicherbandbreite | 76 |
| Aspekte der Netzwerkbandbreite | 77 |
| Ergebnisse von View Composer-Leistungstests | 79 |
| WAN-Unterstützung und PCoIP | 81 |
| View-Bausteine | 83 |
| View-Pods | 84 |
| Cloud Pod Architecture – Übersicht | 86 |
| Vorteile bei Verwendung mehrerer vCenter Server-Instanzen in einer Struktur | 87 |
| 5 Planen von Sicherheitsfunktionen | 90 |
| Grundlegendes zu Clientverbindungen | 90 |
| Clientverbindungen unter Verwendung des PCoIP Secure Gateway | 91 |
| Getunnelte Clientverbindungen mit Microsoft RDP | 92 |
| Direkte Clientverbindungen | 92 |

| | |
|--|------------|
| Auswählen einer Benutzerauthentifizierungsmethode | 93 |
| Active Directory-Authentifizierung | 94 |
| Verwenden der zweistufigen Authentifizierung | 94 |
| Smartcard-Authentifizierung | 95 |
| Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist | 95 |
| Einschränken des Zugriffs auf Remote-Desktops | 97 |
| Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von Remote-Desktops und -Anwendungen | 98 |
| Implementieren empfohlener Vorgehensweisen zum Sichern von Clientsystemen | 99 |
| Zuweisen von Administratorrollen | 99 |
| Vorbereiten des Einsatzes eines Sicherheitsservers | 100 |
| Empfohlene Vorgehensweisen für die Bereitstellung von Sicherheitsservern | 100 |
| Topologien von Sicherheitsservern | 101 |
| Firewalls für Sicherheitsserver im Umkreisnetzwerk | 103 |
| Grundlegendes zu View-Kommunikationsprotokollen | 107 |
| View Broker und Administration Server | 110 |
| View Secure Gateway Server | 110 |
| PCoIP Secure Gateway | 111 |
| View LDAP | 111 |
| View Messaging | 111 |
| Firewall-Regeln für View-Verbindungsserver | 112 |
| Firewall-Regeln für View Agent | 113 |
| Firewall-Regeln für Active Directory | 113 |
| 6 Überblick über die Schritte zum Einrichten einer View-Umgebung | 114 |

Planung der View-Architektur

Das Dokument zur *Planung der View-Architektur* bietet eine Einführung in VMware Horizon™ mit View™, eine Beschreibung der wichtigsten Funktionen und Bereitstellungsoptionen und eine Übersicht darüber, wie die Komponenten in einer Produktionsumgebung üblicherweise eingerichtet werden.

Diese Anleitung liefert Antworten auf die folgenden Fragen:

- Werden mit View die Probleme behoben, die Sie lösen müssen?
- Ist die Implementierung einer View-Lösung in Ihrem Unternehmen möglich und kosteneffektiv?

Nicht alle Funktionen und Merkmale von VMware Horizon mit View stehen in allen Editionen zur Verfügung. Einen Funktionsvergleich der einzelnen Editionen finden Sie unter <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

In diesem Handbuch werden zudem einige Sicherheitsfunktionen beschrieben, mit denen Sie Ihre Installation schützen können.

Zielgruppe

Diese Informationen richten sich an IT-Entscheider, -Architekten, -Administratoren und andere Benutzer, die sich mit den Komponenten und Funktionsmöglichkeiten von View vertraut machen möchten. Anhand dieser Informationen können Architekten und Planer bestimmen, ob 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 Aufwand für die Einrichtung einer umfangreichen Bereitstellung veranschaulichen.

Einführung in View

Mit View können IT-Abteilungen Remote-Desktops und -anwendungen im Rechenzentrum ausführen und die Desktops und Anwendungen den Mitarbeitern als verwalteten Dienst zur Verfügung stellen. 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 enthält die folgenden Themen:

- [Vorteile der Verwendung von View](#)
- [Funktionen von View](#)
- [Zusammenspiel der Komponenten](#)
- [Integrieren und Anpassen von View](#)

Vorteile der Verwendung von View

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

Zuverlässigkeit und Sicherheit

Desktops und Anwendungen können durch Integration in VMware vSphere[®] und Virtualisierung von Server-, Speicher- und Netzwerkressourcen zentralisiert werden. Das Platzieren von Desktopbetriebssystemen und Anwendungen auf einem Server im Datacenter 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.
- Die Unterstützung von RADIUS ermöglicht Flexibilität bei der Wahl verschiedener Anbieter für Zwei-Faktor-Authentifizierung. Zu den unterstützten Anbietern gehören unter anderem RSA SecureID, VASCO DIGIPASS, SMS Passcode und SafeNet.
- Durch die Integration in Workspace erhalten Endbenutzer über denselben Web-basierten Anwendungskatalog, den sie auch für den Zugriff auf SaaS-, Web- und Windows-Anwendungen verwenden, nach Bedarf Zugriff auf Remote-Desktops. Innerhalb eines Remote-Desktops können Benutzer zudem Workspace Catalog verwenden, um auf Anwendungen zuzugreifen.

- Durch die Fähigkeit zur Bereitstellung von Remote-Desktops mit vorerstellten Active Directory-Konten können die Anforderungen von gesperrten Active Directory-Umgebungen, in denen nur der Lesezugriff gestattet ist, erfüllt werden.
- Datensicherungen können geplant werden, ohne berücksichtigen zu müssen, dass die Systeme der Benutzer ggf. ausgeschaltet sind.
- Remote-Desktops und -anwendungen, die in einem Rechenzentrum gehostet werden, haben nur kurze oder keine Ausfallzeiten. Virtuelle Maschinen können sich in hoch verfügbaren VMware-Server-Clustern befinden.

Virtuelle Desktops können auch eine Verbindung mit physischen Back-End-Systemen und Microsoft-Remotedesktopdienste-Hosts (RDS) herstellen.

Komfort

Für Skalierbarkeit wurde die vereinheitlichte Verwaltungskonsole entwickelt, damit selbst die größten View-Bereitstellungen von einer einzigen Verwaltungsschnittstelle aus effizient verwaltet werden können. Assistenten und Dashboards verbessern den Workflow und vereinfachen den Drilldown zum Anzeigen von Details oder Ändern von Einstellungen. [Abbildung 1-1. Verwaltungskonsole mit Dashboard-Anzeige](#) bietet ein Beispiel der Browser-basierten Benutzeroberfläche für View Administrator.

Abbildung 1-1. Verwaltungskonsole mit Dashboard-Anzeige

VMware Horizon View Administrator

Aktualisiert 24.07.2014 12:03

Sitzungen 1

Problematische vCenter-VMs 0

Problematische RDS-Hosts 0

Ereignisse 2 4

Systemzustand 9 2 0 0

Bestandsliste

- Dashboard
- Benutzer und Gruppen
- Katalog
- Ressourcen
 - Farmen
 - Computer
 - Persistente Festplatten
- Überwachung
 - Ereignisse
 - Sitzungen
- Richtlinien
- View-Konfiguration
 - Server
 - Produktlizenzierung und -verwendu
 - Globale Einstellungen
 - Registrierte Computer
 - Administratoren
 - ThinApp-Konfiguration
 - Ereigniskonfiguration

Dashboard

Systemzustand

- View-Komponenten
 - Verbindungsserver
 - Ereignisdatenbank
 - Sicherheitsserver
 - View Composer Server-Instanzen
- RDS-Farmen
 - RDS-2008-APPs
 - RDS-2008-Desktop
- vSphere-Komponenten
 - Datenspeicher
 - ESX-Hosts
 - vCenter Server
- Andere Komponenten
 - Domänen
 - SAML 2.0-Authentifikatoren

Datenspeicher

| Datenspeicher | vCenter Server | Pfad |
|---------------|----------------|------------------|
| DatastoreT1 | 172.16.27.241 | /式而采鹁CEé停B這Üßàùあ |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Eine weitere Funktion für mehr Komfort 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 und Anwendungen für Endbenutzer erfolgt schnell. Anwendungen müssen nicht einzeln auf den physischen PCs der Benutzer installiert werden. Endbenutzer stellen eine Verbindung mit einer Remoteanwendung oder einem Remote-Desktop mit allen Anwendungen her. Endbenutzer können unabhängig von Gerät und Standort auf denselben Remote-Desktop oder dieselbe Remoteanwendung zugreifen.

Die Verwendung von VMware vSphere zum Hosten virtueller Desktops und RDS-Hostserver 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.
- Durch die Integration in Workspace können IT-Manager die Web-basierte Workspace-Verwaltungsoberfläche verwenden, um Benutzer- und Gruppenberechtigungen für Remote-Desktops zu überwachen.
- Mit View Persona Management können physische und virtuelle Desktops zentral verwaltet werden, unter anderem Benutzerprofile, Zugriffsberechtigungen für Anwendungen, Richtlinien, Systemleistung und andere Einstellungen. View Persona Management kann für Benutzer von physischen Desktops vor der Umwandlung in virtuelle Desktops bereitgestellt werden.
- Auch die Speicherverwaltung wird mit VMware vSphere vereinfacht, da Sie Laufwerke und Dateisysteme mit VMware vSphere virtualisieren können, um die Verwaltung getrennter Speichergeräte zu vermeiden.
- Mit vSphere 5.5 Update 1 oder einer neueren Version können Sie Virtual SAN verwenden, um die lokalen physischen Solid-State-Disks und Festplattenlaufwerke, die auf ESXi™-Hosts vorhanden sind, in einen, von allen Hosts in einem Cluster gemeinsam genutzten Datenspeicher zu virtualisieren. Sie geben bei der Erstellung eines Desktop-Pools nur einen Datenspeicher an. Die unterschiedlichen Komponenten wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Betriebssystemdateien werden auf den geeigneten Solid-State-Drive-Festplatten (SSD) oder direkt angeschlossene Festplatten (HDD) platziert.

Sie verwalten die Speicheranforderungen von virtuellen Maschinen wie Kapazität, Leistung und Verfügbarkeit in Form von Standardspeicherrichtlinienprofilen, die automatisch bei der Erstellung eines Desktop-Pools erstellt werden.

- Mit dem View-Speicherbeschleuniger wird die IOPS-Speicherbelastung erheblich verringert. Damit werden Logins von Endnutzern in größerem Umfang möglich, ohne dass dafür eine spezielle Speicher-Array-Technologie erforderlich wäre.
- Wenn Remote-Desktops das mit vSphere 5.1 und höher verfügbare platzsparende Diskformat nutzen, wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen.

Hardware-Unabhängigkeit

Remote-Desktops und Remoteanwendungen sind hardwareunabhängig. Beispiel: Da ein Remote-Desktop auf einem Server im Rechenzentrum ausgeführt wird und nur über ein Clientgerät auf ihn zugegriffen werden kann, kann ein Remote-Desktop ein Betriebssystem verwenden, das möglicherweise nicht mit der Hardware des Clientgeräts kompatibel ist.

Obwohl Windows 8 beispielsweise nur auf für Windows 8 aktivierten PCs ausgeführt werden kann, können Sie Windows 8 in einer virtuellen Maschine installieren und diese auf einem PC verwenden, der nicht für Windows 8 aktiviert ist.

Remote-Desktops können auf PCs, Macs, Thin Clients und PCs ausgeführt werden, die als Thin Clients, Tablets und Telefone betrieben werden. Remoteanwendungen wurden auf einer Teilmenge dieser Geräte ausgeführt. Unterstützung für neue Geräte wird vierteljährlich hinzugefügt.

Bei Verwendung von HTML Access können Endbenutzer einen Remote-Desktop in einem Webbrowser öffnen, ohne auf dem Clientsystem oder -gerät eine Clientanwendung installieren zu müssen.

Funktionen von View

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

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

- Auf Microsoft Windows-Clientgeräten kann von einem virtuellen Desktop auf alle lokalen oder über das Netzwerk verbundenen Drucker gedruckt werden, die auf dem Windows-Clientgerät definiert sind. Diese virtuelle Druckerfunktion beseitigt Kompatibilitätsprobleme und erfordert nicht die Installation zusätzlicher Druckertreiber in einer virtuellen Maschine.
- Verwenden Sie auf den meisten Clientgeräten für die Zuordnung zu Druckern in physischer Nähe des Clientsystems die standortbasierte Druckfunktion. Das standortbasierte Drucken erfordert die Installation von Druckertreibern in der 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.

Sie können angeben, mit welchen USB-Gerät-Typen die Endbenutzer eine Verbindung herstellen dürfen. Für aus mehreren Gerätetypen zusammengesetzte Gerätegruppen, die etwa aus einem Videoeingabegerät und einem Speichergerät bestehen, können Sie die Gerätegruppe so aufgliedern, dass zum Beispiel ein Gerät (wie etwa das Videoeingabegerät) zulässig ist, das andere Gerät (etwa das Speichergerät) jedoch nicht.

- Verwenden Sie View Persona Management, um die Benutzereinstellungen und -Daten zwischen den Sitzungen beizubehalten, auch wenn der Desktop aktualisiert oder neu zusammengestellt wurde. View Persona Management kann die Benutzerprofile in einem Remote-Profil-Speicher (CIFS-Freigabe) in konfigurierbaren Intervallen replizieren.

Sie können auch eine eigenständige Version von View Persona Management auf physischen Computern und virtuellen Maschinen, die nicht von View verwaltet werden, verwenden.

View bietet u. a. die folgenden Sicherheitsfunktionen:

- Verwendung der Zwei-Faktor-Authentifizierung wie etwa RSA SecurID oder RADIUS (Remote Authentication Dial-In User Service, Fernauthentifizierung über Anwahl-Nutzerdienst) oder Smartcards zum Anmelden.
- Verwendung von vorab erstellten Active Directory-Konten bei der Bereitstellung von Remote-Desktops und -Anwendungen in Umgebungen mit Nur-Lesen-Zugriff für Active Directory.
- Einrichtung eines SSL-Tunnels zum Sicherstellen, dass sämtliche Verbindungen vollständig verschlüsselt sind
- Verwenden von VMware High Availability zum Sicherstellen eines automatischen Failovers.

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

- Integration in VMware vSphere zum Erzielen kostengünstiger Dichten, einer hohen Verfügbarkeit und einer erweiterten Steuerung der Ressourcenzuweisung für Ihre Remote-Desktops und -Anwendungen.
- Mithilfe der Speicherbeschleunigungsfunktion von View können Endbenutzeranmeldungen in größerem Umfang mit den gleichen Speicherressourcen abgewickelt werden. Diese Speicherbeschleunigungsfunktion nutzt Funktionen der vSphere 5-Plattform zur Erstellung eines Host-Speichercaches für gewöhnliche Blockleseroutinen.
- Konfiguration von View-Verbindungsservern zum Vermitteln von Verbindungen zwischen Endbenutzern und den Remote-Desktops und -Anwendungen, 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

Die folgenden Funktionen ermöglichen eine zentrale Verwaltung:

- Microsoft Active Directory zum Verwalten des Zugriffs auf Remote-Desktops und -Anwendungen und zum Verwalten von Richtlinien.

- View Persona Management zur Vereinfachung und Vereinheitlichung der Migration von physischen auf virtuelle Desktops.
- Die webbasierte Verwaltungskonsole zum ortsunabhängigen Verwalten von Remote-Desktops und -Anwendungen.
- Verwendung von View Administrator zum Verteilen und Verwalten von Anwendungen, die mit VMware ThinApp™ verpackt wurden.
- 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
- Integration in Workspace™, sodass Endbenutzer über das Workspace-Webportal für Benutzer auf Remote-Desktops zugreifen und das Workspace-Webportal für Benutzer innerhalb eines Remote-Desktops verwenden können.
- Integration in Mirage™ zur Verwaltung von lokal installierten Desktops auf virtuellen Maschinen und zum Bereitstellen und Aktualisieren von Anwendungen auf dedizierten Full-Clone-Remote-Desktops, ohne dass die vom Benutzer installierten Anwendungen überschrieben werden.

Zusammenspiel der Komponenten

Endbenutzer starten Horizon Client, um sich am View-Verbindungsserver anzumelden. Dieser Server, der in Windows Active Directory integriert ist, bietet Zugriff auf Remote-Desktops, die auf einem VMware vSphere Server, einem physischen PC oder einem Microsoft RDS-Host gehostet werden. Horizon Client bietet auch Zugriff auf Remoteanwendungen auf einem Microsoft RDS-Host.

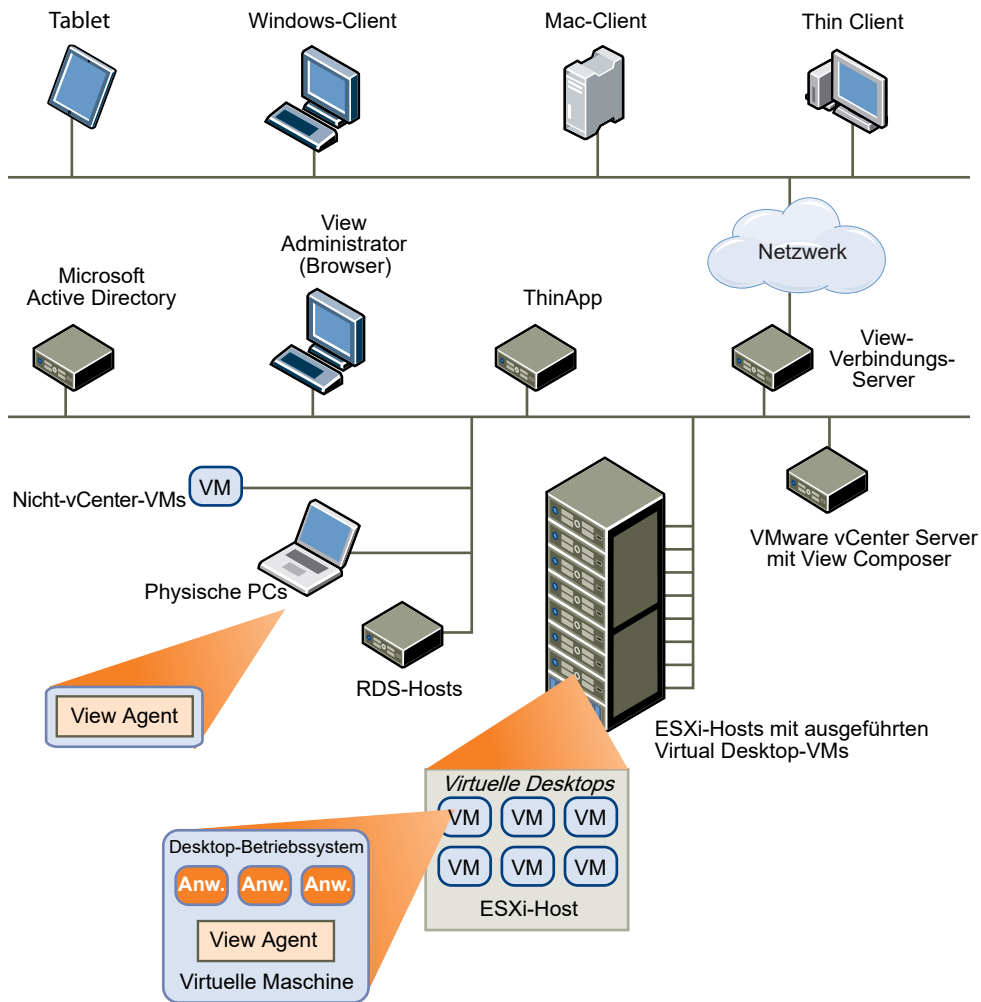
Hinweis View unterstützt folgende Domänenfunktionsebenen von Active Directory-Domänendiensten (AD DS):

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

View unterstützt Novell DSFW (Domain Services For Windows) nicht.

Abbildung 1-2. Allgemeines Beispiel einer View-Umgebung zeigt die Beziehung zwischen den Hauptkomponenten einer Bereitstellung von View.

Abbildung 1-2. Allgemeines Beispiel einer View-Umgebung



Clientgeräte

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

Endbenutzer öffnen Horizon Client, um ihre Remote-Desktops und -anwendungen anzuzeigen. 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. Bei Verwendung von View auf einem Thin Client-Desktop können Sie beispielsweise ein neueres Betriebssystem wie Windows 7 auf älterer Desktop-Hardware verwenden.

Bei Verwendung von HTML Access können Endbenutzer einen Remote-Desktop in einem Webbrowser öffnen, ohne auf dem Clientsystem oder -gerät eine Clientanwendung installieren zu müssen.

View-Verbindungsserver

Diese Software dient als Vermittler für Clientverbindungen. Der View-Verbindungsserver authentifiziert Benutzer mittels Windows Active Directory und leitet die Anforderung an die entsprechende virtuelle Maschine, den entsprechenden physischen PC oder den entsprechenden Microsoft RDS-Host weiter.

View-Verbindungsserver 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 Remote-Desktop-Sitzungen und Remote-Anwendungssitzungen
- Einrichten von sicheren Verbindungen zwischen Benutzern und Remote-Desktops und -Anwendungen
- 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-Verbindungsserver. 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-Verbindungsserver als Sicherheitsserver installieren und konfigurieren. Sicherheitsserver im Umkreisnetzwerk, die mit View-Verbindungsserver-Instanzen innerhalb der Firewall des Unternehmens kommunizieren, Mithilfe von Sicherheitsservern wird gewährleistet, dass im Unternehmensrechenzentrum nur Datenverkehr von Remote-Desktops und -Anwendungen der Benutzer verarbeitet wird, die authentifiziert wurden. Benutzer können nur auf Ressourcen zugreifen, für deren Zugriff sie berechtigt sind.

bieten eine eingeschränkte Funktionalität und müssen nicht in einer Active Directory-Domäne vorhanden sein. Der View-Verbindungsserver wird auf einem Server mit Windows Server 2008, Windows Server 2012 oder Windows Server 2012 R2 installiert, und zwar vorzugsweise auf einer virtuellen VMware-Maschine.

Wichtig Es ist möglich, eine View-Konfiguration ohne einen View-Verbindungsserver zu erstellen. Wenn Sie das View Agent Direct Connect-Plug-In auf dem Remote-Desktop einer virtuellen Maschine installieren, kann der Client eine direkte Verbindung mit der virtuellen Maschine herstellen. Alle Remote-Desktop-Funktionen, wie PCoIP, HTML Access, RDP, USB-Umleitung und die Sitzungsverwaltung, funktionieren genau wie bei einer Verbindung über View-Verbindungsserver. Weitere Informationen finden Sie unter *Verwaltung des View Agent Direct-Connection-Plug-Ins*.

Horizon Client

Die Client-Software für den Zugriff auf Remote-Desktops und -Anwendungen kann auf Tablets, Telefonen, Windows-, Linux- oder Mac-PCs und -Laptops, Thin Clients und vielen weiteren Geräten ausgeführt werden.

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

Ein Administrator kann Horizon Client so konfigurieren, dass Endbenutzer ein Anzeigeprotokoll auswählen können. Die Protokolle umfassen PCoIP und Microsoft RDP für Remote-Desktops. Geschwindigkeit und Anzeigequalität von PCoIP können es mit einem physischen PC aufnehmen.

Abhängig vom verwendeten Horizon Client sind unterschiedliche Funktionen verfügbar. Dieses Handbuch konzentriert sich auf Horizon Client für Windows. Die folgenden Arten von Clients werden in diesem Handbuch nicht im Detail beschrieben:

- Details zu Horizon Client für Tablets, Linux- und Mac-Clients. Einzelheiten finden Sie in der Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- Details zu HTML Access Web client mit der Möglichkeit, einen Remote-Desktop innerhalb eines Browsers zu öffnen. Auf dem Clientsystem oder -gerät ist keine Horizon Client-Anwendung installiert. Einzelheiten finden Sie in der Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- Verschiedene Thin Clients und Zero-Clients von Drittanbietern sind nur über zertifizierte Partner erhältlich.
- View Open Client, der das VMware-Partnerzertifizierungsprogramm unterstützt. View Open Client ist keine offizielle Client-Anwendung und wird daher als solche nicht unterstützt.

VMware Horizon-Webportal für Benutzer

Über einen Webbrowser auf einem Clientgerät können Endbenutzer eine Verbindung mit Remote-Desktops und -Anwendungen herstellen, Horizon Client automatisch starten, sofern installiert, oder das Horizon Client-Installationsprogramm herunterladen.

Wenn Sie einen Browser öffnen und die URL einer View-Verbindungsserver-Instanz eingeben, wird eine Webseite geöffnet, die Links zur [VMware Downloads-Website](#) enthält, von der Sie Horizon Client herunterladen können. Die Links auf der Webseite können jedoch konfiguriert werden. Zum Beispiel können Sie die Links so konfigurieren, dass sie zu einem internen Webserver führen oder Sie können einschränken, welche Client-Versionen auf Ihrem eigenen View-Verbindungsserver zur Verfügung stehen.

Wenn Sie die HTML Access-Funktion verwenden, enthält die Webseite auch einen Link zum Zugriff auf Remote-Desktops innerhalb eines unterstützten Browsers. Mit dieser Funktion wird keine Horizon Client-Anwendung auf dem Clientsystem oder -gerät installiert. Weitere Informationen finden Sie in der Dokumentation zu Horizon Client unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

View Agent

Sie installieren den View Agent-Dienst auf allen virtuellen Maschinen, physischen Systemen und Microsoft RDS-Hosts, die Sie als Quellen für Remote-Desktops und -anwendungen verwenden. Auf virtuellen Maschinen kommuniziert dieser Agent mit Horizon Client, um Funktionen wie Verbindungsüberwachung, virtuelles Drucken, View Persona Management 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 auf allen Remote-Desktops installiert.

Sie können den Agent mit einer Option für die einmalige Anmeldung installieren. Beim Single Sign-On (SSO) werden die Benutzer nur dann zur Anmeldung aufgefordert, wenn sie eine Verbindung mit dem View-Verbindungsserver herstellen. Sie werden nicht erneut aufgefordert, um eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herzustellen.

View Administrator

Mit dieser webbasierten Anwendung können Administratoren View-Verbindungsserver konfigurieren, Remote-Desktops und -Anwendungen bereitstellen und verwalten, die Benutzerauthentifizierung steuern und Probleme der Benutzer beheben.

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

View Composer

Sie können diesen Softwaredienst auf einer vCenter Server-Instanz installieren, die virtuelle Maschinen verwaltet, oder auf einem getrennten Server. 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.

Wenngleich Sie View Composer auf einem separaten Serverhost installieren können, kann ein View Composer-Dienst nur mit einer vCenter Server-Instanz ausgeführt werden. Gleichmaßen kann eine vCenter Server-Instanz mit nur einem View Composer-Dienst verknüpft werden.

vCenter Server

Dieser Dienst dient zur zentralen Verwaltung von VMware ESXi-Servern, die mit einem Netzwerk verbunden sind. vCenter Server ist die zentrale Komponente für die Konfiguration, Bereitstellung und Verwaltung virtueller Maschinen im Rechenzentrum.

Sie können diese virtuellen Maschinen nicht nur als Quellen von VM-Desktop-Pools verwenden, sondern virtuelle Maschinen auch zum Hosten der Serverkomponenten von View, darunter View-Verbindungsserver-Instanzen, Active Directory-Server, Microsoft-RDS-Hosts und vCenter Server-Instanzen, verwenden.

Sie können View Composer auf demselben Server wie vCenter Server oder auf einem anderen Server installieren. vCenter Server verwaltet anschließend die Zuweisung der virtuellen Maschinen zu physischen Servern und Datenspeichern und der CPU- und Arbeitsspeicherressourcen zu virtuellen Maschinen.

Sie können vCenter Server als virtuelle VMware-Appliance installieren oder vCenter Server auf einem Windows Server 2008 R2-Server, einem Windows Server 2012-Server oder einem Windows Server 2012 R2-Server installieren, was bevorzugt auf einer virtuellen VMware-Maschine erfolgen sollte.

Integrieren und Anpassen von View

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

Integrieren in andere VMware Horizon-Komponenten

VMware Workspace

Sie können Workspace in View integrieren, damit IT-Manager und Endbenutzer von den folgenden Vorteilen profitieren:

- Endbenutzer können nach Bedarf mit demselben Single Sign-On-Komfort über dasselbe Benutzerportal im Web, über das sie auch auf SaaS-, Web- und Windows-Anwendungen zugreifen, auch auf Remote-Desktops und -anwendungen zugreifen.
- Endbenutzer können von einem Remote-Desktop aus auf das Workspace-Benutzerportal zugreifen, um die benötigten Anwendungen zu verwenden.
- Bei Verwendung von HTML Access können Endbenutzer zudem einen Remote-Desktop in einem Webbrowser öffnen, ohne auf dem Clientsystem oder -gerät eine Clientanwendung installieren zu müssen.

- IT-Manager können die Administrator-Web-Oberfläche von Workspace verwenden, um Benutzer- und Gruppenberechtigungen für Remote-Desktops zu überwachen.

VMware Mirage

Mithilfe von Mirage können Sie Anwendungen auf dedizierten Full-Clone-Remote-Desktops bereitstellen und aktualisieren, ohne vom Benutzer installierte Anwendungen oder Daten zu überschreiben.

Mirage bietet eine bessere virtuelle Offline-Desktoplösung als die Funktion „Lokaler Modus“, die früher Bestandteil von View war. Mirage bietet folgende Sicherheits- und Verwaltungsfunktionen für Offline-Desktops:

- Verschlüsselt die lokal installierte virtuelle Maschine und verhindert, dass ein Benutzer Einstellungen der virtuellen Maschine ändert, die Auswirkungen auf die Integrität des sicheren Containers haben.
- Bietet Richtlinien, einschließlich Ablauf, in VMware Fusion™ Professional und VMware® Player Plus™, die mit den von der früheren Funktion „Lokaler Modus“ bereitgestellten vergleichbar sind. Fusion Pro und Player Plus sind in Mirage inbegriffen.
- Benutzer müssen ihre Desktops nicht mehr ein- oder auschecken, um Updates zu erhalten.
- Ermöglicht Administratoren, die Ebenenfunktion, Sicherungsfunktionen und das Dateiportal von Mirage zu verwenden.

Horizon vCenter Orchestrator-Plug-In

Das Horizon vCenter Orchestrator-Plug-In ermöglicht die Interaktion zwischen vCenter Orchestrator und VMware Horizon (mit View). Sie können dieses Plug-in verwenden, um die Einstellungen und Methoden zur Bereitstellung von Remote-Desktops und -Anwendungen zu erweitern.

Das Plug-In enthält eine Reihe von Standardarbeitsabläufen für die Automatisierung, den Self-Service basierend auf einem Anforderungs- und Genehmigungsmodell sowie für die skalierbare delegierte Verwaltung in mandantenfähigen oder hochgradig verteilten Umgebungen. Sie können diese vordefinierten Arbeitsabläufe auch verwenden, um eigene Arbeitsabläufe zu erstellen.

Integrieren in gängige Videokonferenzsoftware

Flash URL-Umleitung

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf Clientendpunkte wird die Datenlast auf dem ESXi-Host im Rechenzentrum gesenkt, das zusätzliche Routing über das Rechenzentrum vermieden und die erforderliche Bandbreite zum simultanen Streaming von Live-Video-Ereignissen an mehrere Clientendpunkte verringert.

Die Flash-URL-Umleitung verwendet ein JavaScript, das durch den Webseitenadministrator in eine Webseite eingebettet wird. Immer dann, wenn ein Benutzer eines virtuellen Desktops aus einer Webseite auf den festgelegten URL-Link klickt, fängt das JavaScript die ShockWave-Datei (SWF) von der virtuellen Desktop-Sitzung ab und leitet sie an den Clientendpunkt um. Der Endpunkt kann anschließend außerhalb der virtuellen Desktop-Sitzung einen lokalen VMware Flash Projector öffnen und den Medienstream lokal abspielen.

Hinweis Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die ShockWave Flash-Datei (SWF) zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

Diese Funktion ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungs-Matrix im Dokument „Verwenden von VMware Horizon Client“ für den spezifischen Typ von Desktop- oder mobilem Clientgerät. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Microsoft Lync

Sie können einen Microsoft Lync 2013-Client auf Remote-Desktops einsetzen, um an Unified Communications (UC) VoIP (Voice over IP) und Video-Chats mit Lync-zertifizierten USB-Audio- und -Videogeräten teilzunehmen. Ein spezielles IP-Telefon ist nicht länger erforderlich.

Für diese Architektur ist die Installation eines Microsoft Lync 2013-Clients auf dem Remote-Desktop und eines Microsoft Lync VDI-Plug-Ins auf dem Windows 7- oder 8-Clientendpunkt erforderlich. Kunden können den Microsoft Lync 2013-Client für Präsenz, Instant Messaging, Webkonferenz und Microsoft Office-Funktionen verwenden.

Sobald ein Lync VoIP-Anruf oder Video-Chat eintrifft, nimmt das Lync-VDI-Plug-In die gesamte Medienverarbeitung vom Rechenzentrumsserver auf den Clientendpunkt und codiert alle Medien in Lync-optimierten Audio- und Videocodecs. Diese optimierte Architektur ist äußerst skalierbar, was zu einer geringeren Nutzung der Netzwerkbandbreite führt und Unterstützung

für qualitativ hochwertige VoIP- und Video-Übertragung von Punkt zu Punkt in Echtzeit bietet. Weitere Informationen finden Sie im Blogeintrag „End-User Computing Blog“ unter <http://blogs.vmware.com/euc/2013/06/the-abcs-of-deploying-vmware-horizon-view-5-2-with-microsoft-lync-2013.html>.

Hinweis Die Aufnahme von Audio wird noch nicht unterstützt. Diese Integration wird nur mit dem PCoIP-Anzeigeprotokoll unterstützt.

Integrieren von View in Business Intelligence-Software

Sie können den View-Verbindungsserver 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 Dokument *Integration von View*.

Alternativ können Sie View-Ereignisse im Syslog-Format generieren, sodass eine Analysesoftware auf die Ereignisdaten zugreifen kann. Wenn Sie die dateibasierte Protokollierung von Ereignissen aktivieren, werden Ereignisse in einer lokalen Protokolldatei gesammelt. Bei Angabe einer Dateifreigabe werden die Protokolldateien auf diese Freigabe verschoben. Weitere Informationen finden Sie im Dokument *Installation von View*.

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 View. Mithilfe der View PowerCLI-Cmdlets können Sie verschiedene Verwaltungsaufgaben für View-Komponenten ausführen.

- Erstellen und Aktualisieren von Desktop-Pools

- Durch die Konfiguration mehrerer Netzwerkbezeichnungen können Sie die Anzahl der IP-Adressen erheblich erhöhen, die den virtuellen Maschinen in einem Pool zugewiesen sind.
- 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 Diensten

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

Weitere Informationen finden Sie im Dokument *Integration von View*.

Ändern von LDAP-Konfigurationsdaten in View

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

Mithilfe der VMware- und Microsoft-Befehlszeilenprogramme können Sie LDAP-Konfigurationsdaten in LDIF-Dateien (LDAP Data Interchange Format) aus und nach View exportieren. Diese Befehle sind für fortgeschrittene Administratoren bestimmt, die Konfigurationsdaten anhand von Skripten 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-Verbindungsserver-Instanzen
- Definieren einer großen Anzahl von View-Objekten, z. B. Desktop-Pools, und Hinzufügen dieser Objekte zu Ihren View-Verbindungsserver-Instanzen ohne Einsatz von View Administrator oder View PowerCLI
- Sichern einer Konfiguration, damit der Zustand einer View-Verbindungsserver-Instanz wiederhergestellt werden kann

Weitere Informationen finden Sie im Dokument *Integration von View*.

Verwenden von SCOM zur Überwachung von View-Komponenten

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

Weitere Informationen finden Sie im Dokument *Integration von View*.

Verwenden des Befehls „vdmadmin“

Über die Befehlszeilenschnittstelle `vdmadmin` kann eine Vielzahl von Verwaltungsaufgaben für eine View-Verbindungsserver-Instanz ausgeführt werden. 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 Dokument *Verwaltung von View*.

Planen einer umfassenden Benutzerumgebung

2

View bietet die vertraute, individuell angepasste Desktop-Umgebung, die Benutzer erwarten. Beispielsweise können Benutzer auf einigen Clientsystemen 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.

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 enthält die folgenden Themen:

- [Funktionsunterstützungs-Matrix für View Agent](#)
- [Auswählen eines Anzeigeprotokolls](#)
- [Verwenden von gehosteten Anwendungen](#)
- [Verwendung von View Persona Management zur Speicherung von Benutzerdaten und -einstellungen](#)
- [Verwenden von USB-Geräten mit Remote-Desktops](#)
- [Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone](#)
- [Verwenden von 3D-Grafikanwendungen](#)
- [Streaming von Multimediadaten auf einen Remote-Desktop](#)
- [Drucken von einem Remote-Desktop aus](#)
- [Verwenden der Single Sign-On-Funktion zur Anmeldung bei einem Remote-Desktop](#)
- [Verwendung mehrerer Monitore](#)

Funktionsunterstützungs-Matrix für View Agent

Ermitteln Sie bei der Planung des Anzeigeprotokolls und der Funktionen, die für Ihre Endbenutzer verfügbar sein sollen, mithilfe der folgenden Informationen die Agent-Betriebssysteme (Remote-Desktop und -anwendung), die die Funktion unterstützen.

Die Arten und Editionen der unterstützten Gastbetriebssysteme richten sich nach der Windows-Version.

Tabelle 2-1. Betriebssysteme für Linked-Clone- und Full-Clone-Remote-Desktops

| Gastbetriebssystem | Version | Edition | Service Pack |
|------------------------|-------------------|-----------------------------|-------------------|
| Windows 8.1 | 64 Bit und 32 Bit | Enterprise und Professional | Keines und Update |
| Windows 8 | 64 Bit und 32 Bit | Enterprise und Professional | – |
| Windows 7 | 64 Bit und 32 Bit | Enterprise und Professional | Keine und SP1 |
| Windows Vista | 32 Bit | Business und Enterprise | SP2 |
| Windows XP | 32 Bit | Professional | SP3 |
| Windows Server 2008 R2 | 64 Bit | Datacenter | SP1 |

Tabelle 2-2. Betriebssysteme für RDS-Hosts, mit denen Remote-Desktops oder Anwendungen bereitgestellt werden

| Gastbetriebssystem | Edition | Service Pack |
|------------------------|-------------------------------------|--------------|
| Windows Server 2008 R2 | Standard, Enterprise und Datacenter | SP1 |
| Windows Server 2012 | Standard und Datacenter | – |
| Windows Server 2012 R2 | Standard und Datacenter | – |

Tabelle 2-3. Auf Windows-Betriebssystemen mit installiertem View Agent unterstützte Funktionen

| Funktion | Windows XP-Desktop | Windows Vista-Desktop | Windows 7-Desktop | Windows 8.x-Desktop | Windows Server 2008 R2-Desktop | Microsoft RDS-Host |
|-----------------------------|--------------------|-----------------------|-------------------|---------------------|--------------------------------|--|
| USB-Zugriff | X | X | X | X | X | |
| Echtzeit-Audio/Video (RTAV) | X | X | X | X | X | |
| RDP-Anzeigeprotokoll | X | X | X | X | X | Nur sitzungsbasierte Desktops |
| PCoIP-Anzeigeprotokoll | X | X | X | X | X | Gehostete Anwendungen und sitzungsbasierte Desktops |
| Persona-Verwaltung | X | X | X | X | X | |
| Wyse MMR | X | X | | | | |
| Windows 7 MMR | | | X | | | |
| Standortbasiertes Drucken | X | X | X | X | | |
| Virtuelles Drucken | X | X | X | X | | |

| Funktion | Windows XP-Desktop | Windows Vista-Desktop | Windows 7-Desktop | Windows 8.x-Desktop | Windows Server 2008 R2-Desktop | Microsoft RDS-Host |
|-------------------------|--------------------|-----------------------|-------------------|---------------------|--------------------------------|--------------------|
| Smartcards | X | X | X | X | X | |
| RSA SecurID oder RADIUS | X | X | X | X | X | X |
| Einmaliges Anmelden | X | X | X | X | X | X |
| Mehrere Monitore | X | X | X | X | X | X |

Hinweis Informationen darüber, welche Funktionen auf den verschiedenen Typen von Clientgeräten unterstützt werden, finden Sie in der Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html

Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für View-Bereitstellungen an. 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 Herstellern und Modellen für Thin Client-Geräte finden Sie im *Thin Client Compatibility Guide* (Thin Client-Kompatibilitätsleitfaden), der auf der VMware-Website zur Verfügung steht.

Auswählen eines Anzeigeprotokolls

Ein Anzeigeprotokoll bietet Endbenutzern eine grafische Oberfläche für einen Remote-Desktop oder eine Remoteanwendung, der/die sich im Rechenzentrum befindet. Abhängig vom Typ Ihres Clientgeräts können Sie zwischen dem von VMware bereitgestellten PCoIP (PC-over-IP) und Microsoft RDP (Remote Desktop Protocol) wählen.

Sie können Richtlinien festlegen, um zu steuern, welches Protokoll verwendet werden soll, oder um den Benutzern die Auswahl des Protokolls zu ermöglichen, wenn sie sich am Desktop anmelden.

Hinweis Bei einigen Clienttypen kann weder das Remote-Anzeigeprotokoll PCoIP noch RDP verwendet werden. Beispiel: Wenn Sie den HTML Access-Client verwenden, der mit der HTML Access-Funktion verfügbar ist, wird anstelle von PCoIP oder RDP das Blast-Protokoll verwendet.

PCoIP

PCoIP (PC over IP) ermöglicht ein optimiertes Desktoperlebnis bei der Bereitstellung einer Remoteanwendung oder einer gesamten Desktopumgebung, einschließlich der Anwendungen, Bilder und Audio- und Videoinhalte, für eine Vielzahl von Benutzern im LAN oder über das WAN. PCoIP kann längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können.

PCoIP wird als Anzeigeprotokoll für die Remoteanwendung und für Remote-Desktops, die virtuelle Maschinen verwenden, physische Computer, die Teradici-Hostkarten verwenden, oder Desktops mit freigegebenen Sitzungen auf einem RDS-Host verwendet.

PCoIP-Funktionen

Zu den wichtigsten Funktionen von PCoIP zählen:

- Benutzer außerhalb der Unternehmensfirewall können dieses Protokoll mit dem Virtual Private Network (VPN) Ihrer Firma verwenden, oder Benutzer können sichere, verschlüsselte Verbindungen mit einem Sicherheitsserver in der Unternehmens-DMZ herstellen.
- AES (Advanced Encryption Standard) 128 Bit-Verschlüsselung wird unterstützt und ist standardmäßig aktiviert. Sie können jedoch jederzeit die Verschlüsselungsmethode auf AES-192 oder AES-256 ändern.
- Verbindungen von allen Arten von Clientgeräten.
- Optimierungssteuerungen zur Reduzierung der Bandbreitennutzung im LAN und WAN.
- Unterstützung von 32 Bit-Farben für virtuelle Anzeigegeräte.
- ClearType-Schriftarten werden unterstützt.
- Audioumleitung mit dynamischer Anpassung der Audioqualität für LAN und WAN.
- Echtzeit-Audio-Video für die Verwendung von Webcams und Mikrofonen auf einigen Clienttypen.
- Kopieren und Einfügen von Text und auf einigen Clients von Bildern zwischen dem Client-Betriebssystem und einer Remoteanwendung oder einem Remote-Desktop. Bei anderen Clienttypen wird nur das Kopieren und Einfügen von Klartext unterstützt. Sie können jedoch keine Systemobjekte wie Ordner und Dateien zwischen den Systemen kopieren und einfügen.
- Mehrere Monitore werden für einige Client-Typen unterstützt. Auf Windows-basierten Clients beispielsweise können Sie bis zu vier Monitore einsetzen und die Auflösung jedes Monitors einzeln festlegen, wobei eine Auflösung von bis zu 2560 x 1600 pro Monitor möglich ist. Drehung des Monitors (Pivot-Funktion) und automatische Anpassung werden ebenfalls unterstützt.

Wenn die 3D-Funktion aktiviert ist, werden bis zu zwei Monitore mit einer Auflösung von bis zu 1920 x 1200 unterstützt.

- USB-Umleitung wird für einige Client-Typen unterstützt.
- MMR-Umleitung wird für einige Windows Clientbetriebssysteme und einige Remote-Desktop-Betriebssysteme (mit installiertem View Agent) unterstützt.

Informationen darüber, welche Desktop-Betriebssysteme bestimmte PCoIP-Funktionen unterstützen, finden Sie unter [Funktionsunterstützungs-Matrix für View Agent](#).

Informationen darüber, welche Client-Geräte spezifische PCoIP-Funktionen unterstützen, finden Sie unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Empfohlene Einstellungen für das Gastbetriebssystem

Für Remote-Desktops werden u. a. die folgenden Betriebssystemeinstellungen empfohlen:

- Für Windows XP-Desktops: 768 MB RAM oder mehr und eine einzelne CPU.

- Für Windows 7- oder 8-Desktops oder Windows Server 2012- oder R2-Desktops: 1 GB RAM oder mehr und eine Dual-CPU wird für die Wiedergabe in High-Definition, Vollbildmodus oder 720p oder höher Video empfohlen. Für die Verwendung von vDGA (Virtual Dedicated Graphics Acceleration, virtuelle zugeordnete Grafikbeschleunigung) für grafikintensive Anwendungen wie CAD-Anwendungen sind 4 GB RAM erforderlich.

Videoqualitätsanforderungen

| | |
|---------------------------------|---|
| 480p-formatiertes Video | Die Videowiedergabe mit 480p oder niedriger bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über eine virtuelle CPU verfügt. Wenn Sie unter Windows 7 oder höher eine Videowiedergabe in hoch auflösendem Flash- oder im Vollbildmodus wünschen, benötigt der Desktop eine duale virtuelle CPU. Selbst mit einem dualen virtuellen CPU-Desktop kann ein 360p-Video, das im Vollbildmodus abgespielt wird, hinter der Audioausgabe zurückbleiben, insbesondere auf Windows-Clients. |
| 720p-formatiertes Video | Die Videowiedergabe mit 720p bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über zwei virtuelle CPUs verfügt. Bei der 720p-Videowiedergabe in hoch auflösendem oder Vollbildmodus könnte die Leistung beeinträchtigt sein. |
| 1080p-formatiertes Video | Wenn der Remote-Desktop über zwei virtuelle CPUs verfügt, können Sie 1080p-formatiertes Video wiedergeben, wobei der Media Player allerdings möglicherweise auf eine kleinere Fenstergröße angepasst werden muss. |
| 3D-Rendering | <p>Sie können Remote-Desktops für die Verwendung von software- oder hardwarebeschleunigter Grafik konfigurieren. Die softwarebeschleunigte Grafikfunktion ermöglicht es Ihnen, ohne eine physische GPU (Grafikverarbeitungseinheit) DirectX 9- und OpenGL 2.1-Anwendungen auszuführen. Die hardwarebeschleunigten Grafikfunktionen ermöglicht es virtuellen Maschinen, die physischen GPU (Grafikverarbeitungseinheit) auf einem vSphere-Host freizugeben oder eine physische GPU für einen VM-Desktop zu reservieren.</p> <p>Für 3D-Anwendungen werden bis zu zwei Monitore unterstützt, und die maximale Bildschirmauflösung beträgt 1920 x 1200. Das Gastbetriebssystem auf den Remote-Desktops muss Windows 7 oder höher sein.</p> <p>Weitere Informationen zu 3D-Funktionen finden Sie unter Verwenden von 3D-Grafikanwendungen.</p> |

Hardwareanforderungen für Clientsysteme

Informationen über Prozessor- und Speicheranforderungen für die spezifische Art von Desktop oder mobilen Clientgeräten finden Sie im Dokument „Verwenden von VMware Horizon Client“. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Microsoft RDP

Remote Desktop Protocol (RDP) entspricht dem Mehrkanalprotokoll, das viele Benutzer bereits nutzen, um vom ihrem Heimcomputer aus auf ihren Firmencomputer zuzugreifen. Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP.

Microsoft RDP ist ein unterstütztes Anzeigeprotokoll für Remote-Desktops, die virtuelle Maschinen, physische Maschinen oder Desktops mit gemeinsamen Sitzungen auf einem RDS-Host verwenden. (Nur das PCoIP-Anzeigeprotokoll wird für Remoteanwendungen unterstützt.) Microsoft RDP ermöglicht Folgendes:

- Mit RDP 6 können Sie den Modus für die Anzeige auf mehreren Monitoren verwenden. RDP 7 lässt eine echte Mehrfachmonitorunterstützung für bis zu 16 Monitore zu.
- Texte und Systemobjekte wie Ordner und Dateien können zwischen dem lokalen System und dem Remote-Desktop kopiert und eingefügt werden.
- Unterstützung von 32 Bit-Farben für virtuelle Anzeigegeräte.
- RDP unterstützt die 128 Bit-Verschlüsselung.
- Benutzer außerhalb der Unternehmens-Firewall können dieses Protokoll mit dem Virtual Private Network (VPN) Ihrer Firma benutzen, oder Benutzer können sichere, verschlüsselte Verbindungen zu einem View-Sicherheitsserver in der Unternehmens-DMZ herstellen.

Hinweis Für virtuelle Windows XP-Desktop-Maschinen müssen Sie die RDP-Patches installieren, die in den Knowledgebase-Artikeln 323497 und 884020 aufgeführt sind. Wenn Sie die RDP-Patches nicht installieren, wird möglicherweise ein Windows Socket-Fehler auf dem Client angezeigt.

Hardwareanforderungen für Clientsysteme

Informationen zu Prozessor- und Arbeitsspeichieranforderungen finden Sie im Dokument „Verwendung von VMware Horizon Client“ für den jeweiligen Typ des Clientsystems. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Hinweis Mobile Clientgeräte verwenden ausschließlich das PCoIP-Anzeigeprotokoll.

Verwenden von gehosteten Anwendungen

Sie können Horizon Client verwenden, um nicht nur auf Remote-Desktops, sondern auch auf Windows-basierte Remoteanwendungen sicher zuzugreifen.

Dank dieser Funktion sehen Benutzer nach dem Start von Horizon Client und der Anmeldung bei einem View Server zusätzlich zu den Remote-Desktops alle Remoteanwendungen, zu deren Verwendung sie berechtigt sind. Durch Auswahl einer Anwendung wird ein Fenster für die Anwendung auf dem lokalen Clientdienst geöffnet. Die Anwendung sieht so aus und verhält sich so, als wäre sie lokal installiert.

Wenn Sie beispielsweise das Anwendungsfenster auf einem Windows-Clientcomputer minimieren, verbleibt ein Element für diese Anwendung in der Taskleiste und sieht so aus, wie es aussehen würde, wenn es auf dem lokalen Windows-Computer installiert wäre. Sie können auch eine Verknüpfung für die Anwendung erstellen, die wie Verknüpfungen lokal installierter Anwendungen auf Ihrem Clientdesktop angezeigt wird.

Unter folgenden Voraussetzungen ist es möglicherweise sinnvoller, auf diese Weise Remoteanwendungen anstelle von vollständigen Remote-Desktops bereitzustellen:

- Wenn eine Anwendung mit einer Multi-Tier-Architektur eingerichtet ist, wobei die Komponenten besser arbeiten, wenn sie sich geografisch nahe beieinander befinden, ist die Verwendung von gehosteten Remoteanwendungen eine gute Lösung.

Wenn beispielsweise ein Benutzer remote auf eine Datenbank zugreifen muss und große Datenmengen über das WAN übermittelt werden müssen, wird die Leistung normalerweise beeinträchtigt. Bei gehosteten Anwendungen können sich alle Teile der Anwendung im selben Rechenzentrum befinden wie die Datenbank, sodass der Datenverkehr isoliert ist und nur die Bildschirmaktualisierungen über das WAN übertragen werden.

- Von einem mobilen Endgerät aus ist es einfacher, auf eine einzelne Anwendung zuzugreifen, als einen Remote-Windows-Desktop zu öffnen und dann zur Anwendung zu navigieren.

Um diese Funktion zu verwenden, installieren Sie Anwendungen auf einem Microsoft-RDS-Host. In dieser Hinsicht arbeiten gehostete View-Anwendungen ähnlich wie andere Lösungen für die Remote-Ausführung von Anwendungen. Gehostete View-Anwendungen werden für ein optimiertes Benutzererlebnis mithilfe des Anzeigeprotokolls PCoIP bereitgestellt.

Verwendung von View Persona Management zur Speicherung von Benutzerdaten und -einstellungen

Sie können View Persona Management mit Remote-Desktops und mit physischen Computern und virtuellen Maschinen, die nicht von View verwaltet werden, verwenden. View Persona Management speichert Änderungen, die Benutzer an ihren Profilen vornehmen. Ein Benutzerprofil umfasst verschiedene, vom Benutzer generierte Informationen:

- Benutzerspezifische Daten und Desktopeinstellungen, die eine immer identische Anzeige des Desktops ermöglichen, egal von welchem Desktop aus sich der Benutzer anmeldet.
- Anwendungsdaten und -einstellungen. Diese Einstellungen ermöglichen z. B. ein Speichern der Symbolleistenpositionen und Voreinstellungen in den Anwendungen.
- Von Benutzeranwendungen konfigurierte Windows-Registrierungseinträge.

Um den Umgang mit diesen Funktionen zu erleichtern, erfordert View Persona Management Speicherplatz auf einer CIFS-Freigabe, die der Größe des lokalen Benutzerprofils entspricht oder sogar größer ist.

Minimierung der Anmelde- und Abmeldezeiten

View Persona Management minimiert die Zeit, die zum An- und Abmelden von Desktops aufgebracht werden muss.

- View erfasst aktuelle Änderungen am Profil auf dem Remote-Desktop und kopiert diese in regelmäßigen Abständen in das Remote-Repository. Der Standardwert lautet alle 10 Minuten. Im Gegensatz dazu warten die servergespeicherten Windows-Profile bis zur Abmeldungszeit und kopieren dann erst alle Änderungen auf den Server.
- Während der Anmeldung lädt View nur die für Windows erforderlichen Dateien herunter, beispielsweise die Benutzerregistrierungsdateien. Andere Dateien werden auf den Remote-Desktop kopiert, wenn der Benutzer oder eine Anwendung sie vom Profilordner auf dem Remote-Desktop aus öffnet.

Sie können View so konfigurieren, dass angegebene Dateien heruntergeladen werden, wenn der Benutzer sich anmeldet, während andere Dateien im Hintergrund heruntergeladen werden.

- Mit View Persona Management werden beim Abmelden nur solche Dateien, die seit der letzten Replikation aktualisiert wurden, in das Remote-Repository kopiert.

Mit View Persona Management können Sie verhindern, dass am Active Directory zur Erstellung eines verwalteten Profils Änderungen vorgenommen werden müssen. Zur Konfiguration der Persona-Verwaltung legen Sie ein zentrales Repository fest, ohne dabei die Eigenschaften des Benutzers im Active Directory zu ändern. Mit diesem zentralen Repository können Sie das Profil des Benutzers in einer Umgebung verwalten, ohne dass sich dies auf die physischen Maschinen auswirkt, an denen sich eventuell Benutzer anmelden.

Mit View Persona Management können die ThinApp-Sandbox-Daten auch im Benutzerprofil gespeichert werden, wenn Sie den Desktops die VMware ThinApp-Anwendungen zur Verfügung stellen. Diese Daten können mit dem Benutzer servergespeichert werden, haben aber keine wesentlichen Auswirkungen auf die Anmeldezeiten. Durch diese Strategie besteht ein besserer Schutz gegen Datenverlust oder Datenbeschädigung.

Konfigurationsoptionen

Sie können View-Personas auf verschiedenen Ebenen konfigurieren: auf einem einzelnen Remote-Desktop, einem Desktop-Pool, einer OU oder auf allen Remote-Desktops in Ihrer Bereitstellung. Sie können auch eine eigenständige Version von View Persona Management auf physischen Computern und virtuellen Maschinen, die nicht von View verwaltet werden, verwenden.

Durch Festlegung der Gruppenrichtlinien (GPOs) ist eine genauere Steuerung der Dateien und Ordner möglich, die eine Persona enthalten soll:

- Legen Sie fest, ob der Ordner mit den lokalen Einstellungen mit eingeschlossen werden soll. Für Windows 7, Windows 8 und Windows Vista betrifft diese Richtlinie den Ordner `AppData\Local`. Bei Windows XP betrifft diese Richtlinie den Ordner `Local Settings`.

- Legen Sie fest, welche Dateien und Ordner bei der Anmeldezeit geladen werden sollen. Beispiel: Anwendungsdaten\Microsoft\Certificates. Innerhalb eines Ordners können Sie außerdem die auszuschließenden Dateien angeben.
- Legen Sie fest, welche Dateien und Ordner nach der Anmeldung des Benutzers am Desktop im Hintergrund heruntergeladen werden sollen. Innerhalb eines Ordners können Sie außerdem die auszuschließenden Dateien angeben.
- Legen Sie fest, welche Dateien und Ordner innerhalb der Persona des Benutzers mit den servergespeicherten Windows-Profilen und nicht mit View Persona Management verwaltet werden sollen. Innerhalb eines Ordners können Sie außerdem die auszuschließenden Dateien angeben.

Wie bei den servergespeicherten Windows-Profilen können Sie auch hier die Ordnerumleitung konfigurieren. Sie können die folgenden Ordner auf eine Netzwerkfreigabe umleiten.

| | | |
|-----------|-------------------|---------------------------|
| Kontakte | Eigene Dokumente | Gespeicherte Spiele |
| Cookies | Eigene Musik | Suchvorgänge |
| Desktop | Eigene Bilder | Startmenü |
| Downloads | Eigene Videos | Startobjekte |
| Favoriten | Netzwerkumgebung | Vorlagen |
| Verlauf | Druckerumgebung | Temporäre Internetdateien |
| Links | Zuletzt verwendet | |

Zur Konfiguration eines Remote-Repositorys zur Speicherung von Personas können Sie entweder eine Netzwerkfreigabe oder einen vorhandenen Active Directory-Benutzerprofilpfad verwenden, den Sie für servergespeicherte Windows-Profilen konfiguriert haben. Die Netzwerkfreigabe kann ein Ordner auf einem Server, ein NAS-Gerät (Network-Attached Storage) oder ein Netzwerk-Server sein. Zum Unterstützen einer großen View-Bereitstellung können Sie separate Repositories für verschiedene Desktop-Pools konfigurieren.

Sie können eine eigenständige Version von View Persona Management auf physischen Computern und virtuellen Maschinen, die nicht von View verwaltet werden, installieren und damit folgende Ziele erreichen:

- Profile auf eigenständigen Systemen und Remote-Desktops freigeben und verwalten.
- Benutzerprofile von physischen Systemen auf Remote-Desktops migrieren.
- Eine phasenweise Migration von physischen Systemen auf Remote-Desktops ausführen.
- Unterstützung aktueller Profile, wenn Benutzer offline gehen.

Einschränkungen

Für View Persona Management bestehen die folgenden Einschränkungen und Beschränkungen:

- Sie müssen über eine View-Lizenz verfügen, welche die View Persona Management-Komponente umfasst.
- View Persona Management erfordert eine CIFS-Freigabe (Common Internet File System).

- Ein Benutzer kann nicht auf dasselbe Profil zugreifen, wenn der Benutzer zwischen Desktops wechselt, die die Benutzerprofile „v1“ und „v2“ haben. Umgeleitete Ordner können jedoch gemeinsam von v1- und v2-Profilen verwendet werden. Windows XP verwendet v1-Profile. Windows Vista, Windows 7 und Windows 8 verwenden v2-Profile.

Verwenden von USB-Geräten mit Remote-Desktops

Administratoren können Remote-Desktops so konfigurieren, dass USB-Geräte wie Flash-Laufwerke, Kameras, VoIP-Geräte und Drucker genutzt werden können. Diese Funktion wird USB-Umleitung genannt und unterstützt die Verwendung des RDP- oder des PCoIP-Anzeigeprotokolls. Ein Remote-Desktop unterstützt maximal 32 USB-Geräte.

Bei Verwendung dieser Funktion stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, auf dem Remote-Desktop zur Verfügung. Es ist sogar möglich, von einem Remote-Desktop aus eine Verbindung mit einem iPad herzustellen und diesen zu verwalten. Sie können zum Beispiel Ihr iPad mit dem auf Ihrem Remote-Desktop installierten iTunes-Programm synchronisieren. Auf einigen Clientgeräten, beispielsweise auf Windows- und Mac OS X-Computern, werden die USB-Geräte in einem Menü in Horizon Client aufgelistet. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

In den meisten Fällen ist es nicht möglich, ein USB-Gerät gleichzeitig auf einem Clientsystem und auf einem Remote-Desktop zu verwenden. Nur wenige Arten von USB-Geräten können vom Remote-Desktop und dem lokalen Computer gemeinsam verwendet werden. Zu diesen Geräten zählen Smartcard-Leser und Eingabegeräte, wie beispielsweise Tastaturen und Zeigegeräte.

Administratoren können angeben, mit welchen Arten von USB-Geräten die Endbenutzer eine Verbindung herstellen dürfen. Für aus mehreren Gerätetypen zusammengesetzte Gerätegruppen, die etwa aus einem Videoeingabegerät und einem Speichergerät bestehen, können Administratoren auf einigen Clientsystemen die Gerätegruppe so aufgliedern, dass ein Gerät (wie etwa das Videoeingabegerät) zulässig ist, das andere Gerät (etwa das Speichergerät) jedoch nicht.

Die USB-Umleitungsfunktion ist in Desktop-Pools verfügbar, die auf einzelnen Benutzer-Computern bereitgestellt werden. Diese Funktion ist nicht in RDS-Desktop-Pools verfügbar.

Hinweis Die USB-Umleitung ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungsmatrix im Dokument „Verwenden von VMware Horizon Client“ für den spezifischen Typ von Desktop- oder mobilem Clientgerät. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon Ihres lokalen Computers auf Ihrem Remote-Desktop verwenden. Echtzeit-Audio/Video ist mit Standard-

Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel und unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Endbenutzer können Skype, Webex, Google Hangouts und andere Online-Konferenzanwendungen auf ihren virtuellen Desktops ausführen. Diese Funktion leitet Video- und Audiodaten mit deutlich weniger Bandbreite an den Remote-Desktop um, als mit der USB-Umleitung erreicht werden kann. Mit Echtzeit-Audio/Video werden Webcam-Bilder und Audioeingaben auf dem Client verschlüsselt und dann an den Remote-Desktop gesendet. Auf Remote-Desktops wird der Stream entschlüsselt und von virtuellen Webcams und virtuellen Mikrofonen wiedergegeben, die von der Drittanbieteranwendung verwendet werden können.

Es ist zwar keine besondere Konfiguration erforderlich, doch Administratoren können Gruppenrichtlinienobjekte und Registrierungsschlüssel für den Remote-Desktop festlegen, um die Framerate und die Bildauflösung zu konfigurieren oder die Funktion ganz auszuschalten. Standardmäßig beträgt die Auflösung 320 x 240 Pixel bei 15 Frames pro Sekunde. Weiterhin können Administratoren bei Bedarf mithilfe von clientseitigen Konfigurationseinstellungen eine bevorzugte Webcam oder ein bevorzugtes Audiogerät festlegen.

Hinweis Diese Funktion ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungs-Matrix im Dokument „Verwenden von VMware Horizon Client“ für den spezifischen Typ von Desktop- oder mobilem Clientgerät. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Verwenden von 3D-Grafikanwendungen

Mithilfe der software- und hardwarebeschleunigten Grafikfunktionen des PCoIP-Anzeigeprotokolls können Remote-Desktop-Benutzer verschiedene 3D-Anwendungen ausführen, wie beispielsweise Google Earth, CAD-Anwendungen und andere grafikintensive Anwendungen.

Virtual Dedicated Graphics Acceleration (vDGA)

Diese Funktion, die in vSphere 5.5 und höher verfügbar ist, weist eine einzige physische GPU (Graphical Processing Unit, Grafikverarbeitungseinheit) auf einem ESXi-Host einer einzelnen virtuellen Maschine zu. Verwenden Sie diese Funktion, wenn Sie hochwertige, hardwarebeschleunigte Workstation-Grafiken benötigen.

Virtual Shared Graphics Acceleration (vSGA)

Bei Verwendung dieser Funktion, die in vSphere 5.1 und höher verfügbar ist, können mehrere virtuelle Maschinen die physischen GPUs auf ESXi-Hosts gemeinsam nutzen. Sie können 3D-Anwendungen für Design, Modellierung und Multimedia verwenden.

Soft 3D

Bei Verwendung von softwarebeschleunigten Grafiken, die in vSphere 5.0 und höher verfügbar sind, können Sie DirectX 9- und OpenGL 2.1-Anwendungen ausführen, ohne dass dazu eine physische GPU erforderlich ist. Diese Funktion eignet sich für weniger grafikintensive 3D-Anwendungen, wie Windows Aero-Themen, Microsoft Office 2010 und Google Earth.

Für diese Funktionen werden bis zu zwei Monitore unterstützt, und die maximale Bildschirmauflösung beträgt 1920 x 1200. Auf den Desktops der virtuellen Maschine muss das Gastbetriebssystem Windows 7 oder höher installiert sein.

Wichtig Weitere Informationen zu den verschiedenen Optionen und Anforderungen in Bezug auf das 3D-Rendern finden Sie im [VMware-Whitepaper](#) zur Grafikbeschleunigung.

Streaming von Multimediadaten auf einen Remote-Desktop

Die Funktion MMR (Multimedia-Umleitung) ermöglicht eine originalgetreue Wiedergabe auf Windows XP-, Windows Vista-, Windows 7- und Windows 8-Clientcomputern, wenn Multimediadateien zu einem Remote-Desktop gestreamt werden.

Mit MMR wird der Multimediadatenstrom auf dem Windows-Clientsystem verarbeitet, d. h. er wird entschlüsselt. Das Clientsystem gibt die Medieninhalte wieder und lagert so die Anforderung vom ESXi-Host aus.

- Für Windows XP- und Windows Vista-Remote-Desktops unterstützt die MMR-Funktion die Mediendateiformate, die das Windows XP- oder Windows Vista-Clientsystem unterstützt, da auf dem Client lokale Decoder vorhanden sein müssen. Diese Dateiformate sind unter anderen MPEG2, WMV, AVI und WAV.
- Für Windows 7-Remote-Desktops und Windows 7- und 8-Clientsysteme unterstützt die MMR-Funktion Medienformate, die den H.264-Video-komprimierungsstandard einhalten. Die Dateiformate M4V, MP4 und MOV werden unterstützt.

Wichtig Windows 8-Remote-Desktops unterstützen MMR nicht. Verwenden Sie für diese View-Agenten die Windows-Medienumleitung, die im Lieferumfang von RDP 7 und später enthalten ist.

Da MMR auf den verschiedenen Betriebssystemen unterschiedlich implementiert wird, unterscheiden sich die Systemanforderungen für Windows 7 von denen für Windows Vista und früheren Betriebssystemen. Weitere Informationen über die Systemanforderungen für diese Funktion finden Sie unter „Verwenden von VMware Horizon Client für Windows“ auf https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Hinweis Sie müssen den MMR-Port in Ihrer Firewall-Software als Ausnahme hinzufügen. Der standardmäßige Port für MMR lautet 9427.

Drucken von einem Remote-Desktop aus

Die virtuelle Druckfunktion ermöglicht Endbenutzern auf einigen Clientsystemen die Verwendung von lokalen oder Netzwerkdruckern über einen Remote-Desktop, ohne dass in dessen Betriebssystem zusätzliche Druckertreiber installiert werden müssen. Das standortbasierte Drucken ermöglicht es Ihnen, Remote-Desktops dem Drucker zuzuordnen, der sich am nächsten am Endpunkt-Clientgerät befindet.

Beim virtuellen Drucken wird ein Drucker, nachdem er zu einem lokalen Clientcomputer hinzugefügt wurde, automatisch zur Liste der verfügbaren Drucker auf dem Remote-Desktop hinzugefügt. Keine weitere Konfiguration ist erforderlich. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe usw. festlegen. Benutzer mit Administratorrechten können weiterhin Druckertreiber auf dem Remote-Desktop installieren, ohne einen Konflikt mit der virtuellen Druckkomponente zu verursachen.

Zum Senden von Druckaufträgen an einen USB-Drucker können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion verwenden.

Das standortbasierte Drucken ermöglicht es IT-Organisationen, Remote-Desktops dem Drucker zuzuordnen, der sich am nächsten am Endpunkt-Clientgerät befindet. 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. Bei Verwendung dieser Funktion müssen die korrekten Druckertreiber nicht auf dem Remote-Desktop installiert sein.

Hinweis Diese Druckfunktionen sind nur auf einigen Clienttypen verfügbar. Informationen dazu, ob eine Druckfunktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungsmatrix im Dokument „Verwenden von VMware Horizon Client“ für den spezifischen Typ von Desktop- oder mobilem Clientgerät. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Verwenden der Single Sign-On-Funktion zur Anmeldung bei einem Remote-Desktop

Dank der Single Sign-On-Funktion (SSO) müssen Endbenutzer ihre Anmeldeinformationen nur einmal eingeben.

Wenn Sie die Single Sign-On-Funktion nicht verwenden, werden Benutzer zweimal zur Anmeldung aufgefordert: Sie werden zuerst aufgefordert, sich am View-Verbindungsserver anzumelden, und danach an ihrem Remote-Desktop. Beim Verwenden von Smartcards müssen sich Benutzer dreimal anmelden, d. h. noch einmal, wenn der Smartcard-Leser zur Eingabe einer PIN auffordert.

Bei Remote-Desktops enthält diese Funktion die GINA-DLL (Graphical Identification and Authentication Dynamic-Link Library) für Windows XP und eine Anmeldeinformationenanbieter-DLL für Windows Vista, Windows 7 und Windows 8.

Verwendung mehrerer Monitore

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

Wenn Sie PCoIP verwenden, das Anzeigeprotokoll von VMware, können Sie die Anzeigeauflösung und die Drehung für jeden Monitor separat anpassen. PCoIP ermöglicht eine echte Sitzung mit mehreren Monitoren, anstelle von einer Erweiterungsmodussitzung.

Eine Erweiterungsmodus-Remote-Sitzung ist im Grunde eine Sitzung mit einem Monitor. Die Monitore müssen die gleiche Größe und Auflösung haben und das Monitorlayout muss in einen Begrenzungsrahmen passen. Wenn Sie ein Anwendungsfenster maximieren, füllt das Fenster alle Monitore aus. Microsoft RDP 6 verwendet den Erweiterungsmodus.

In einer echten Sitzung mit mehreren Monitoren, können die Monitore unterschiedliche Auflösungen und Größen haben, und ein Monitor kann geschwenkt sein. Wenn Sie ein Anwendungsfenster maximieren, wird das Fenster auf das Vollbild des Monitors erweitert, in dem es angezeigt wird.

Für diese Funktion gelten die folgenden Einschränkungen:

- Wenn Sie PCoIP verwenden, können Sie maximal vier Monitore verwenden, um einen Remote-Desktop anzuzeigen, und zwar mit einer Auflösung von bis zu 2560 x 1600, sofern Sie über ausreichend Video-RAM verfügen. Maximal zwei Monitore können übereinander angeordnet werden. Wenn Sie mehr als zwei Monitore verwenden, müssen sich alle Monitore im gleichen Modus befinden und die gleiche Bildschirmauflösung aufweisen. Wenn Sie also drei Monitore verwenden, müssen sich alle drei entweder im Querformat oder im Hochformat befinden und die gleiche Bildschirmauflösung verwenden.
- Um die 3D-Renderfunktion zu verwenden, können Sie bis zu zwei Monitore mit einer Auflösung von bis zu 1920 x 1200 verwenden. Sie müssen das PCoIP-Anzeigeprotokoll verwenden.
- Wenn Sie Microsoft RDP 7 verwenden, können Sie maximal 16 Monitore verwenden, um einen Remote-Desktop anzuzeigen.
- Wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden, muss Microsoft Remotedesktopverbindung (RDV) 6.0 oder höher auf dem Remote-Desktop installiert sein.

Zentrales Verwalten von Desktop- und Anwendungspools

3

Sie können Pools erstellen, die einen, Hunderte oder sogar Tausende von Remote-Desktops enthalten. Als Desktopquelle können Sie virtuelle Maschinen, physische Computer und Windows-Remotedesktopdienste-Hosts (RDS) verwenden. Wenn Sie eine virtuelle Maschine als Basisimage erstellen, kann View anhand dieses Images einen Pool von Remote-Desktops generieren. Außerdem können Sie Anwendungspools erstellen, die Benutzern Fernzugriff auf Anwendungen verschaffen.

Dieses Kapitel enthält die folgenden Themen:

- [Vorteile von Desktop-Pools](#)
- [Vorteile von Anwendungspools](#)
- [Reduzieren und Verwalten von Speicheranforderungen](#)
- [Anwendungsbereitstellung](#)
- [Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten](#)

Vorteile von Desktop-Pools

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

Sie können einen Remote-Desktop-Pool aus folgenden Quellen erstellen:

- Ein physisches System, wie beispielsweise ein physischer Desktop-PC oder ein RDS-Host
- Eine virtuelle Maschine, die auf einem ESXi-Host gehostet und von vCenter Server verwaltet wird
- Eine virtuelle Maschine, die auf einer anderen Virtualisierungsplattform als vCenter Server 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. Durch Festlegen dieser Parameter wird sichergestellt, dass Sie stets über eine ausreichende Anzahl von Remote-Desktops zur unmittelbaren Verwendung 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 Remote-Desktops in einem Pool ermöglicht. Die folgenden Beispiele zeigen einige der verfügbaren Einstellungen:

- Geben Sie an, welches Remote-Anzeigeprotokoll als Standard für den Remote-Desktop verwendet werden soll und ob Benutzer die Standardeinstellung außer Kraft setzen dürfen.
- 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.
- 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.

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

Pools mit fester Zuweisung Jedem Benutzer wird ein bestimmter Remote-Desktop zugewiesen, zu dem er bei jeder Anmeldung zurückkehrt. Benutzer können ihre Desktops individuell anpassen, Anwendungen installieren und Daten speichern.

Pools mit dynamischer Zuweisung Der Remote-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.

Vorteile von Anwendungspools

Mithilfe von Anwendungspools gewähren Sie Benutzern Zugriff auf Anwendungen, die auf Servern in einem Rechenzentrum ausgeführt werden, d. h. nicht auf ihren eigenen PCs oder Geräten.

Anwendungspools bieten mehrere wichtige Vorteile:

- **Barrierefreiheit**
Benutzer können von jedem Gerät im Netzwerk aus auf Anwendungen zugreifen. Außerdem können Sie den sicheren Netzwerkzugriff konfigurieren.
- **Unabhängigkeit der Geräte**
Anwendungspools unterstützen zahlreiche Clientgeräte, wie zum Beispiel Smartphones, Tablets, Laptops, Thin Clients und PCs. Auf den Clientgeräten können verschiedene Betriebssysteme ausgeführt werden, wie zum Beispiel Windows, iOS, Mac OS oder Android.

- **Zugriffssteuerung**

Sie können einem Benutzer oder einer Benutzergruppe schnell und einfach den Zugriff auf Anwendungen gewähren oder verweigern.

- **Schnellere Bereitstellung**

Mithilfe von Anwendungspools lässt sich die Bereitstellung von Anwendungen beschleunigen, da Sie Anwendungen nur auf Servern in einem Rechenzentrum bereitstellen und jeder Server mehrere Benutzer unterstützen kann.

- **Verwaltbarkeit**

Die Verwaltung von Software, die auf Clientcomputern und Clientgeräten bereitgestellt wurde, ist in der Regel sehr ressourcenintensiv. Zu den Verwaltungsaufgaben zählen Bereitstellung, Konfiguration, Wartung, Support sowie Upgrades. Mithilfe von Anwendungspools können Sie die Softwareverwaltung in einem Unternehmen vereinfachen, da die Software auf Servern in einem Rechenzentrum ausgeführt wird, wodurch weniger installierte Kopien erforderlich sind.

- **Sicherheit und Einhaltung gesetzlicher Bestimmungen**

Mithilfe von Anwendungspools können Sie die Sicherheit verbessern, da Anwendungen und die zugehörigen Daten sich zentral in einem Rechenzentrum befinden. Zentralisierte Daten bieten bessere Möglichkeiten, um Sicherheitsprobleme zu vermeiden und die Einhaltung gesetzlicher Bestimmungen zu gewährleisten.

- **Niedrigere Kosten**

Je nach den Bestimmungen von Software-Lizenzverträgen kann das Hosting von Anwendungen in einem Rechenzentrum kostengünstiger sein. Auch andere Faktoren wie eine schnellere Bereitstellung und eine bessere Verwaltbarkeit tragen dazu bei, dass die Softwarekosten im Unternehmen gesenkt werden können.

Reduzieren und Verwalten von Speichieranforderungen

Das Bereitstellen von Desktops auf virtuellen Maschinen, 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 virtuelle Maschinen in einem Pool eine virtuelle Festplatte mit einem Basis-Image gemeinsam nutzen.

- **Verwalten des Speichers mit vSphere**

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.

- **Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung**

VMware Virtual SAN ist eine softwaredefinierte Speicherebene im Lieferumfang von vSphere 5.5 Update 1 oder einer neueren Version, die die in einem Cluster von vSphere-Hosts verfügbaren lokalen physischen Speicherfestplatten virtualisiert. Sie geben bei der Erstellung eines Desktop-Pools nur einen Datenspeicher an. Die unterschiedlichen Komponenten wie Dateien virtueller Maschinen, Replike, Benutzerdaten und Betriebssystemdateien werden auf den geeigneten Solid-State-Drive-Festplatten (SSD) oder direkt angeschlossene Festplatten (HDD) platziert.

- **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.

Verwalten des Speichers mit vSphere

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 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.

Kompatible Funktionen von vSphere 4.1 oder höher

Mit vSphere 4.1 oder höher können Sie nun auch folgende 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 ESXi-Server für die Auslagerungsdateien der virtuellen Maschine auf dem Gastbetriebssystem

Kompatible Funktionen von vSphere 5.0 oder 5.1 oder höher

Mit vSphere 5.0 oder einer neueren Version können Sie nun folgende Funktionen verwenden:

- Mit der View-Speicherbeschleunigungsfunktion können Sie ESXi-Hosts so konfigurieren, dass dort Festplattendaten von virtuellen Maschinen in einem Cache-Speicher zwischengespeichert werden.

Mithilfe dieses inhaltsbasierten Lese-Cache-Speichers (CBRC) kann der IOPS-Wert reduziert und die Systemleistung bei sogenannten Boot Storms verbessert werden, wenn viele Maschinen gestartet werden und gleichzeitig Antivirus-Scans durchführen. Statt das gesamte Betriebssystem wieder und wieder aus dem Speichersystem zu lesen, kann ein Host gemeinsame Datenblöcke aus dem Cache lesen.

- Wenn Remote-Desktops das mit vSphere 5.1 und höher verfügbare platzsparende Diskformat nutzen, wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen.
- Sie können einen Desktop-Pool auf einem Cluster bereitstellen, der bis zu 32 ESXi-Hosts umfasst, müssen dabei jedoch einige Einschränkungen beachten.

Replikatfestplatten müssen in VMFS5-Datenspeichern (oder einer höheren VMFS-Version) bzw. in NFS-Datenspeichern gespeichert werden. Wenn Sie Replikate in einem Datenspeicher einer früheren VMFS-Version als VMFS5 speichern, kann ein Cluster über maximal acht Hosts verfügen.

Betriebssystemfestplatten und persistente Festplatten können in NFS- oder VMFS-Datenspeichern gespeichert werden.

Kompatible Funktionen von vSphere 5.5 Update 1 oder höher

Mit vSphere 5.5 Update 1 oder einer neueren Version können Sie Virtual SAN verwenden, um die lokalen physischen Solid-State-Disks und Festplattenlaufwerke, die auf ESXi-Hosts vorhanden sind, in einen von allen Hosts in einem Cluster gemeinsam genutzten Datenspeicher zu virtualisieren. Virtual SAN bietet Hochleistungsspeicher mit richtlinienbasierter Verwaltung, sodass Sie bei der Erstellung eines Desktop-Pools nur einen Datenspeicher angeben. Die unterschiedlichen Komponenten wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Betriebssystemdateien werden auf den geeigneten Solid-State-Drive-Festplatten (SSD) oder direkt angeschlossene Festplatten (HDD) platziert.

Mithilfe von Virtual SAN können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Profile mit Speicherrichtlinien verwenden. Wenn die Richtlinie wegen eines Host-, Festplatten- oder Netzwerkfehlers oder wegen Änderungen der Arbeitslast nicht mehr eingehalten wird, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen neu und optimiert die Nutzung der Ressourcen im ganzen Cluster. Sie können einen Desktop-Pool auf einem Cluster bereitstellen, der bis zu 32 ESXi-Hosts enthält.

Virtual SAN unterstützt VMware-Funktionen wie HA, vMotion und DRS, die gemeinsamen Speicher voraussetzen, macht jedoch externen gemeinsamen Speicher überflüssig und vereinfacht die Speicherkonfiguration und die Bereitstellung virtueller Maschinen.

Hinweis Virtual SAN ist mit der View-Speicherbeschleunigungsfunktion, aber nicht mit der Funktion platzsparendes Diskformat kompatibel, das Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.

Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung

VMware Virtual SAN ist eine softwaredefinierte Speicherebene im Lieferumfang von vSphere 5.5 Update 1 oder einer neueren Version, die die in einem Cluster von vSphere-Hosts verfügbaren lokalen physischen Speicherfestplatten virtualisiert. Sie geben bei der Erstellung eines Desktop-Pools nur einen Datenspeicher an. Die unterschiedlichen Komponenten wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Betriebssystemdateien werden auf den geeigneten Solid-State-Drive-Festplatten (SSD) oder direkt angeschlossene Festplatten (HDD) platziert.

Virtual SAN implementiert einen richtlinienbasierten Ansatz zur Speicherverwaltung. Wenn Sie Virtual SAN verwenden, definiert View die Speicheranforderungen für virtuelle Maschinen (wie Kapazität, Leistung und Verfügbarkeit) in Form von Standardprofilen mit Speicherrichtlinien, die Sie ändern können. Der Speicher wird gemäß den zugewiesenen Richtlinien bereitgestellt und automatisch konfiguriert. Sie können Virtual SAN für Linked-Clone-Desktop-Tools oder Full-Clone-Desktop-Pools verwenden.

Jede virtuelle Maschine pflegt ihre Richtlinie unabhängig von ihrer physischen Position im Cluster. Wenn die Richtlinie aufgrund eines Host-, Festplatten- oder Netzwerkfehlers oder von Arbeitsauslastungsänderungen nicht mehr konform ist, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen und Lastausgleiche neu, um die Richtlinien der einzelnen virtuellen Maschinen zu erfüllen.

Virtual SAN unterstützt VMware-Funktionen wie HA, vMotion und DRS, die gemeinsamen Speicher voraussetzen, macht jedoch eine externe gemeinsame Speicherinfrastruktur überflüssig und vereinfacht die Speicherkonfiguration und die Bereitstellung virtueller Maschinen.

Anforderungen und Einschränkungen

Die Virtual SAN-Funktion hat bei Verwendung in einer View-Bereitstellung folgende Einschränkungen:

- Diese Version unterstützt die Verwendung der platzsparenden Diskformatfunktion von View nicht, die Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.
- Virtual SAN unterstützt die VAAI-Funktion (View Composer Array Integration) nicht, da Virtual SAN keine NAS-Geräte verwendet.

Hinweis Virtual SAN ist mit der Funktion „View-Speicherbeschleunigung“ kompatibel. Virtual SAN bietet eine Cachingschicht auf SSD-Festplatten, und die Funktion „View-Speicherbeschleunigung“ bietet einen inhaltsbasierten Cache, der E/A-Vorgänge pro Sekunde reduziert und die Leistung bei Startüberlastungen erhöht.

Die Virtual SAN-Funktion hat folgende Anforderungen:

- vSphere 5.5 Update 1 oder eine neuere Version.
- Geeignete Hardware. Beispiel: VMware empfiehlt eine 10-GB-Netzwerkkarte und mindestens eine SSD-Festplatte und eine direkt angeschlossene Festplatte für jeden kapazitätsbeitragenden Knoten. Siehe im [VMware-Kompatibilitätshandbuch](#).
- Ein aus mindestens drei ESXi-Hosts bestehender Cluster. Sie benötigen eine ausreichende Anzahl von ESXi-Hosts für Ihr Setup. Weitere Informationen finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere* unter <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>.
- SSD-Kapazität, die mindestens 10 % der Festplattenkapazität beträgt.
- Eine ausreichende Anzahl von Festplatten für Ihr Setup. Überschreiten Sie eine 75-prozentige Auslastung auf einer Magnetfestplatte nicht.

Weitere Informationen zu Virtual SAN-Anforderungen finden Sie unter „Arbeiten mit Virtual SAN“ im Dokument *vSphere Storage*. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware Virtual SAN finden Sie im White Paper unter <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Reduzieren von Speichieranforderungen 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 2,000 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.

Replizierte und verknüpfte Klone auf dem gleichen Datenspeicher

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 LUN oder verknüpfte Klone in einen Virtual SAN-Datenspeicher bzw. von einem Virtual SAN-Datenspeicher in eine LUN verschieben.

Replizierte und verknüpfte Klone auf verschiedenen Datenspeichern

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 drehenden 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 Antivirenskans.

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

Bei Verwendung von Virtual SAN-Datenspeichern ist es nicht möglich, manuell andere Datenspeicher für Replikate und verknüpfte Klone auszuwählen. Da Virtual SAN Objekte automatisch auf dem passenden Festplattentyp ablegt und alle E/A-Vorgänge zwischenspeichert, ist die Verwendung der mehrstufigen Replikatspeicherung für Virtual SAN-Datenspeicher nicht erforderlich.

Löschbare Festplatten für Auslagerungsdateien und temporäre Dateien

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. Wenn die virtuelle Maschine ausgeschaltet wird, wird die temporäre Festplatte gelöscht. 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.

Persistente Festplatten für dedizierte Desktops

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.

Virtual SAN-Datenspeicher, die lokale Speicherfestplatten eines vSphere-Clusters zusammenfassen

Virtual SAN virtualisiert die lokalen physischen Speicherfestplatten, die auf den ESXi-Hosts verfügbar sind, in einem einzelnen Datenspeicher, der von allen Hosts in einem vSphere-Cluster gemeinsam verwendet wird. Ein Virtual SAN-Datenspeicher besteht aus Solid-State-Laufwerken (SSDs) und Festplattenlaufwerken (HDDs), die auch als Datenfestplatten bezeichnet werden. SSDs werden zum Zwischenspeichern von Lesevorgängen und für die Pufferung von Schreibvorgängen verwendet. Datenfestplatten dienen als dauerhafter Speicher. Diese Strategie bietet einen Hochleistungsspeicher mit automatischer Zwischenspeicherung, sodass Sie beim Erstellen eines Desktop-Pools nur einen Datenspeicher angeben. Die verschiedenen Komponenten, wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Dateien des Betriebssystems, werden auf den passenden SSDs oder Datenfestplatten abgelegt.

Hinweis Virtual SAN erfordert vSphere 5.5 Update 1 oder eine neuere Version sowie die entsprechende Hardware. Siehe im [VMware-Kompatibilitätshandbuch](#).

Wenn Sie Virtual SAN verwenden, definiert View die Speicheranforderungen für virtuelle Maschinen (wie Kapazität, Leistung und Verfügbarkeit) in Form von Standardprofilen mit Speicherrichtlinien, die Sie ändern können. Virtual SAN organisiert die virtuelle Festplatte im logischen Datenspeicher, um die angegebenen Anforderungen zu erfüllen. Weiterhin überwacht Virtual SAN die Richtlinieneinhaltung

während des Lebenszyklus der virtuellen Maschine und erstellt entsprechende Berichte. Wenn die Richtlinie wegen eines Host-, Festplatten- oder Netzwerkfehlers oder wegen Änderungen der Arbeitslast nicht mehr eingehalten wird, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen neu und optimiert die Nutzung der Ressourcen im ganzen Cluster.

Hinweis Wenn Sie einen Linked-Clone-Desktop-Pool erstellen, wird von der übergeordneten virtuellen Maschine ein erster vollständiger Klon erstellt. Ausgehend von diesem vollständigen Klon oder diesem Replikat werden verknüpfte Klone erstellt. Bei Verwendung eines Virtual SAN-Datenspeichers werden standardmäßig gemäß der Verfügbarkeitsrichtlinie zusätzliche Kopien des Replikats und der verknüpften Klone erstellt.

Lokale Datenspeicher für dynamische zustandsfreie Desktops

Linked-Clone-Desktops können auf lokalen Datenspeichern gespeichert werden, die interne Ersatzfestplatten auf ESXi-Hosts sind. Dies kann verschiedene Vorteile bieten, so z.B. eine kostengünstige Hardware, eine schnelle Bereitstellung von virtuellen Maschinen, mehrere hochleistungsfähige Vorgänge zum Ändern des Betriebsstatus und eine vereinfachte Verwaltung. Bei Verwendung von lokalen Speichern werden jedoch die Ihnen zur Verfügung stehenden Optionen für die Konfiguration der vSphere-Infrastruktur beschränkt. Die Verwendung von lokalen Speichern bietet in bestimmten Umgebungen Vorteile, ist jedoch für andere Umgebungen nicht geeignet.

Hinweis Die in diesem Abschnitt beschriebenen Beschränkungen gelten nicht für Virtual SAN-Datenspeicher, die auch lokale Speicherfestplatten verwenden, aber bestimmte Hardware erfordern, wie im vorherigen Abschnitt über Virtual SAN beschrieben.

Die Verwendung von lokalen Speichern funktioniert wahrscheinlich am besten, wenn die Remote-Desktops in Ihrer Umgebung zustandsfrei sind. So könnten Sie etwa lokale Datenspeicher verwenden, wenn Sie zustandsfreie Kiosks oder Unterrichts- und Schulungsstationen bereitstellen.

Falls Sie beabsichtigen, sich die Vorteile von lokalen Datenspeichern zunutze zu machen, müssen Sie die folgenden Einschränkungen sorgfältig bedenken:

- Sie können VMotion, VMware High Availability (HA) und vSphere Distributed Resource Scheduler (DRS) nicht verwenden.
- Sie können nicht die Lastausgleichsfunktion in View Composer für den Lastausgleich bei virtuellen Maschinen innerhalb eines Ressourcenpools einsetzen.
- Sie können weder View Composer-Replikate noch verknüpfte Klone auf getrennten Datenspeichern speichern; VMware empfiehlt hier sogar ausdrücklich, diese auf dem gleichen Datenträger zu speichern.

Falls Sie die Nutzung der lokalen Festplatten durch Steuerung der Zahl der virtuellen Maschinen und deren Festplattenwachstum verwalten, dynamische Zuweisungen verwenden und regelmäßig Aktualisierungs- und Löschvorgänge ausführen, können Sie verknüpfte Klone erfolgreich auf lokalen Datenspeichern bereitstellen.

Weitere Informationen finden Sie im Kapitel zur Erstellung von Desktop-Pools im Dokument *Verwaltung von View*.

Anwendungsbereitstellung

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

- **Bereitstellen von individuellen Anwendungen mithilfe eines RDS-Hosts**

Sie können für Endbenutzer Remoteanwendungen anstelle von Remote-Desktops bereitstellen. Auf kleinen mobilen Endgeräten ist die Navigation in einzelnen Remoteanwendungen möglicherweise einfacher.

- **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.

- **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.

- **Verwenden von bestehenden Prozessen oder VMware Mirage für die Anwendungsbereitstellung**

View bietet Ihnen die Möglichkeit, die derzeit in Ihrem Unternehmen verwendeten Methoden für die Anwendungsbereitstellung weiter zu nutzen. Sie können aber auch Mirage verwenden. 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 individuellen Anwendungen mithilfe eines RDS-Hosts

Sie können für Endbenutzer Remoteanwendungen anstelle von Remote-Desktops bereitstellen. Auf kleinen mobilen Endgeräten ist die Navigation in einzelnen Remoteanwendungen möglicherweise einfacher.

Endbenutzer können für den Zugriff auf Windows-basierte Remoteanwendungen denselben Horizon Client verwenden wie zuvor für den Zugriff auf Remote-Desktops. Außerdem verwenden sie dasselbe PCoIP-Anzeigeprotokoll.

Zur Bereitstellung einer Remoteanwendung installieren Sie die Anwendung auf einem Microsoft RDS-Host (Remote Desktop Session). Ein oder mehrere RDS-Hosts bilden eine RDS-Farm. Auf Basis dieser Farm können Administratoren Anwendungspools ähnlich wie Desktop-Pools erstellen. Eine Farm kann bis zu 200 RDS-Hosts enthalten. Ein View-Pod kann bis zu 200 Farmen unterstützen.

Diese Strategie vereinfacht das Hinzufügen, Entfernen und Aktualisieren von Anwendungen sowie das Hinzufügen und Entfernen von Benutzerberechtigungen für Anwendungen. Außerdem ermöglicht diese Strategie den einfachen Zugriff von jedem Gerät oder Netzwerk auf zentrale oder verteilte Anwendungsfarmen.

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.

VMware 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. Sie können View Administrator verwenden, um VMware ThinApp-Anwendungen für Desktops und Pools zu verteilen.

Wichtig Wenn Sie ThinApp-Anwendungen nicht verteilen, indem Sie sie Desktops und Pools, sondern stattdessen Active Directory-Benutzern und -Gruppen zuweisen, können Sie VMware Workspace verwenden.

Nachdem Sie mithilfe von VMware 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 Architektur Aspekte 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 Architektur Aspekte 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 Remote-Desktops installierte ThinApp-Pakete berücksichtigt werden.

Verwenden von bestehenden Prozessen oder VMware Mirage für die Anwendungsbereitstellung

View bietet Ihnen die Möglichkeit, die derzeit in Ihrem Unternehmen verwendeten Methoden für die Anwendungsbereitstellung weiter zu nutzen. Sie können aber auch Mirage verwenden. 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 exakt zur gleichen Zeit an viele Remote-Desktops verteilen, kann es zu signifikanten Spitzen bei der CPU-Nutzung und Speicher-E/A-Last kommen. 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 Remote-Desktops nutzen möchten, empfiehlt VMware, dass Sie nicht View Composer für die Anwendungsbereitstellung verwenden, sondern stattdessen dedizierte Full-Clone-Desktops erstellen, den Benutzern die Installation von Anwendungen erlauben und dann Mirage verwenden, um die Desktops zu verwalten und zu aktualisieren, ohne die von den Benutzern installierten Anwendungen zu überschreiben.

Wichtig Verwenden Sie Mirage auch zur Verwaltung lokal installierter Offline-Desktops und ihrer Anwendungen. Weitere Informationen finden Sie auf der [Webseite mit der Mirage-Dokumentation](#).

Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten

View bietet zahlreiche Gruppenrichtlinien-Verwaltungsvorlagen (ADM) für eine zentrale Verwaltung und Konfiguration der View-Komponenten und Remote-Desktops.

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-Verbindungsserver-Konfiguration
- Horizon 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 eine Beschreibung der über ADM-Vorlagen verfügbaren Einstellungen finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Architekturentwurfselemente und Planungsanleitungen für Remote-Desktop-Bereitstellungen

4

Ein typischer View-Architekturentwurf verwendet eine Pod-Strategie mit Komponenten, die unter Verwendung einer vSphere 5.1-Infrastruktur oder höher bis zu 10.000 Remote-Desktops unterstützen. Die Pod-Definitionen können je nach Hardwarekonfiguration, den verwendeten View- und vSphere-Softwareversionen und anderen umgebungsspezifischen Entwurfsfaktoren variieren.

Die Beispiele in diesem Dokument veranschaulichen einen skalierbaren Entwurf, 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. IT-Architekten und -Planer können sich so einen Überblick darüber verschaffen, was bei der Bereitstellung einer View-Lösung zu berücksichtigen ist.

Wichtig Die folgenden Themen werden nicht in diesem Kapitel behandelt:

| | |
|--|---|
| Architekturentwurf für gehostete Anwendungen | Ein View-Pod kann bis zu 200 Microsoft-RDS-Hostfarmen unterstützen, wobei jede Farm bis zu 200 RDS-Hosts enthalten kann. Zu den unterstützten Betriebssystemen für RDS-Hosts gehören Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2. Weitere Informationen finden Sie unter <i>Einrichten von Desktop- und Anwendungspools für View</i> . Wenn Sie beabsichtigen, virtuelle Maschinen für RDS-Hosts zu verwenden, lesen Sie auch Konfiguration von virtuellen Maschinen als RDS-Hosts . |
| Architekturentwurf für das View Agent Direct Connect-Plug-In | Wenn dieses Plug-In auf der virtuellen Maschine eines Remote-Desktops ausgeführt wird, kann der Client eine direkte Verbindung mit der virtuellen Maschine herstellen. Alle Remote-Desktop-Funktionen, wie PCoIP, HTML Access, RDP, USB-Umleitung und die Sitzungsverwaltung, funktionieren genau wie bei einer Verbindung über View-Verbindungsserver. Weitere Informationen finden Sie unter <i>Verwaltung des View Agent Direct-Connection-Plug-Ins</i> . |

Dieses Kapitel enthält die folgenden Themen:

- [Anforderungen virtueller Maschinen für Remote-Desktops](#)
- [View ESXi-Knoten](#)
- [Desktop-Pools für bestimmte Nutzertypen](#)
- [Konfigurieren virtueller Maschinen für View-Desktops](#)
- [Konfiguration von virtuellen Maschinen als RDS-Hosts](#)

- [vCenter Server- und View Composer-Konfiguration für virtuelle Maschinen](#)
- [View-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen](#)
- [vSphere-Cluster](#)
- [Speicher- und Bandbreitenanforderungen](#)
- [View-Bausteine](#)
- [View-Pods](#)
- [Vorteile bei Verwendung mehrerer vCenter Server-Instanzen in einer Struktur](#)

Anforderungen virtueller Maschinen für Remote-Desktops

Beim Planen der Spezifikationen für Remote-Desktops hat 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](#)

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 Desktops auf virtuellen Maschinen](#)

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 Desktops auf virtuellen Maschinen](#)

Beim Einschätzen der CPU-Anforderungen müssen Sie Informationen zur durchschnittlichen CPU-Nutzung der verschiedenen Nutzertypen in Ihrem Unternehmen sammeln.

- [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.

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 Anwendungen 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. |
| Kioskbenutzer | Diese Benutzer müssen sich einen Desktop teilen, der sich in einem öffentlichen Bereich befindet. 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 Desktops auf virtuellen Maschinen

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 in zu großem Umfang Windows-Auslagerungsdateien verwendet werden. Wenn die Arbeitsspeicherzuweisung zu hoch ist, kann die Speicherkapazität beeinträchtigt werden, da die Auslagerungsdatei im Gastbetriebssystem sowie die Auslagerungs- und Anhaltedatei für die einzelnen virtuellen Maschinen zu groß werden.

Auswirkungen der Arbeitsspeichergröße auf die Systemleistung

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

- Eine unzureichende Arbeitsspeicherzuweisung kann übermäßig viele Windows-Auslagerungsvorgänge verursachen, wodurch E/A-Vorgänge generiert werden, die zu signifikanten Leistungseinbußen und einer Steigerung der Speicher-E/A-Last führen.

- VMware ESXi unterstützt hoch entwickelte Algorithmen für das Management von Arbeitsspeicherressourcen, z. B. die transparente gemeinsame Seitennutzung 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.

Hinweis Durch die transparente gemeinsame Seitennutzung steigen die Konsolidierungsverhältnisse insgesamt, indem die Gesamtmenge an Hostarbeitsspeicher, der von allen Desktops genutzt wird, reduziert wird. Im Lauf der Zeit konsolidiert die Funktion für die transparente gemeinsame Seitennutzung gemeinsame Arbeitsspeicherblöcke für Desktop-Images, die auf demselben Host ausgeführt werden. Die Vorteile der transparenten gemeinsamen Seitennutzung machen sich im Lauf der Zeit immer mehr bezahlt und hängen von der Anzahl gemeinsamer Arbeitsspeicherblöcke ab. Bei Windows 7 liegt das erwartete Verhältnis der transparenten gemeinsamen Speichernutzung zwischen 20 und 40 Prozent.

- Da für die Leistung virtueller Desktops schnelle Antwortzeiten sehr wichtig sind, legen Sie auf dem ESXi-Host 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 ESXi-Auslagerungsdateien beanspruchte Speicherplatz verringert werden. Höhere Reservierungseinstellungen wirken sich jedoch auf die Fähigkeit aus, Arbeitsspeicher auf einem ESXi-Host 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 ESXi-Hosts für die Suche nach den ESXi-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 dieser Datei kann 100 % des Gastarbeitsspeichers entsprechen. Sie können diese Datei bedenkenlos löschen, da sie in View-Bereitstellungen nicht benötigt wird.

ESXi- 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 ESXi-Auslagerungsdatei 1 GB groß. Diese Datei kann im lokalen Datenspeicher auf dem ESXi-Host oder -Cluster gespeichert werden.

ESXi-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 ESXi-Host benötigte zusätzliche Arbeitsspeicher teilweise von der Anzahl der Monitore, die für Endbenutzer konfiguriert sind, und von der Anzeigeauflösung ab. [Tabelle 4-1. Overhead für PCoIP-Clientanzeige](#) 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

| Standardanzeigeauf lösung | Breite (in Pixel) | Höhe (in Pixel) | Overhead bei einem Monitor | Overhead bei zwei Monitoren | Overhead bei vier Monitoren |
|--------------------------------------|--------------------------|------------------------|---------------------------------------|--|--|
| VGA | 640 | 480 | 2,34MB | 4,69MB | 9,38MB |
| SVGA | 800 | 600 | 3,66MB | 7,32MB | 14,65MB |
| 720p | 1280 | 720 | 7,03MB | 14,65MB | 28,13MB |
| UXGA | 1600 | 1200 | 14,65MB | 29,30MB | 58,59MB |
| 1080p | 1920 | 1080 | 15,82MB | 31,64MB | 63,28MB |
| WUXGA | 1920 | 1200 | 17,58MB | 35,16MB | 70,31MB |
| QXGA | 2048 | 1536 | 24,00MB | 48,00MB | 96,00MB |
| WQXGA | 2560 | 1600 | 31,25MB | 62,50MB | 125,00MB |

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 ESXi-Hosts erforderlich ist. Addieren Sie den Arbeitsspeicher des Gastbetriebssystems zum Overhead-Arbeitsspeicher hinzu und multiplizieren Sie ihn mit der Anzahl virtueller Maschinen.

Wichtig Um die 3D-Renderfunktion zu verwenden, müssen Sie ausreichend VRAM für jeden Remote-Desktop mit Windows 7 oder höher zuweisen.

- Die softwarebeschleunigte Grafikfunktion, die ab vSphere 5.0 zur Verfügung steht, ermöglicht es Ihnen, 3D-Anwendungen wie Windows Aero-Themen oder Google Earth zu verwenden. Diese Funktion erfordert 11,8 MB bis 512 MB (für virtuelle Maschinen mit vSphere 5.1 U1 und höher) bzw. 64 MB (für virtuelle Maschinen mit vSphere 5.0). Der Standardwert ist 64MB.
- Die vSGA-Funktion (Virtual Shared Graphics Acceleration), die ab vSphere 5.1 zur Verfügung steht, ermöglicht mehreren virtuellen Maschinen die gemeinsame Nutzung der physischen GPUs auf den ESXi-Hosts. Sie können 3D-Anwendungen für Design, Modellierung und Multimedia verwenden. Für diese Funktion sind zwischen 64 MB und 512 MB VRAM erforderlich. Der Standardwert ist 96 MB.
- Die vDGA-Funktion (Virtual Dedicated Graphics Acceleration), die ab vSphere 5.5 verfügbar ist, weist eine einzige physische GPU (Graphical Processing Unit, Grafikverarbeitungseinheit) auf einem ESXi-Host einer einzelnen virtuellen Maschine zu. Diese Funktion bietet hochwertige, hardwarebeschleunigte Workstation-Grafiken.

Wenn das 3D-Rendern aktiviert ist, beträgt die Höchstzahl der Monitore 2 und die maximale Auflösung beträgt 1920 x 1200.

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 oder höher sowie 2 GB für 64 Bit-Desktops unter Windows 7 oder höher zuzuweisen. Wenn Sie eine der hardwarebeschleunigten Grafikfunktionen für 3D-Anwendungen nutzen möchten, empfiehlt VMware zwei virtuelle CPUs und 4 GB RAM. 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 Desktops auf virtuellen Maschinen

Beim Einschätzen der CPU-Anforderungen müssen Sie Informationen zur durchschnittlichen CPU-Nutzung der verschiedenen Nutzertypen in Ihrem Unternehmen sammeln.

Die CPU-Anforderungen variieren je nach Nutzertyp. Überprüfen Sie in der Pilotphase mit einem Systemüberwachungsprogramm, z. B. Perfmon in der virtuellen Maschine, esxtop in ESXi oder vCenter Server-Leistungsüberwachungstools, die durchschnittliche und maximale Auslastung 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. Für Desktops mit Windows 7 (64 Bit) und höher sowie für rechenintensive Aufgaben werden zwei virtuelle CPUs empfohlen, wenn Sie 720p-Video über das PCoIP-Anzeigeprotokoll wiedergeben müssen.
- 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.
- Verwenden Sie ein Antivirenprodukt, das mit der VMware vShield-API kompatibel ist. Diese API wurde z. B. in VMware vCloud[®] Networking und Security 5.1 und höher integriert.

Als Faustregel zum Festlegen der Anfangsgröße nehmen Sie an, dass jede virtuelle Maschine 1/10 bis 1/8 eines CPU-Kerns als garantierte Mindestrechenleistung benötigt. Planen Sie daher eine Pilotumgebung mit 8 bis 10 virtuellen Maschinen pro Kern. Wenn Sie beispielsweise von 8 virtuellen Maschinen pro Kern ausgehen und einen 8-Kern-ESXi-Host 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.

- Deaktivieren Sie Windows-Dienste wie den Indexdienst, die Defragmentierung und Wiederherstellungspunkte. Einzelheiten finden Sie in den Themen „Optimieren der Leistung des Windows-Gastbetriebssystems“, „Optimieren der Leistung des Windows 7-Gastbetriebssystems“ und „Überblick über Windows 7-Dienste und -Tasks, die zu einem Wachstum von verknüpften Klonen führen“ in *Einrichten von Desktop- und Anwendungspools für View*.
- 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.
- Aktivieren Sie bei Verwendung von vSphere 5.1 oder höher die Rückgewinnung von Datenträgerplatz für vCenter Server und für die Linked-Clone-Desktop-Pools.

Wenn Desktops mit virtuellen Maschinen das mit vSphere 5.1 oder höheren Versionen verfügbare platzsparende Diskformat nutzen, wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen. Beachten Sie, dass diese Funktion nicht verfügbar ist, wenn Sie einen Virtual SAN-Datenspeicher verwenden.

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

- Die Größe der ESXi-Anhaltedatei entspricht der Größe des Arbeitsspeichers, der der virtuellen Maschine zugewiesen ist.
- Die Größe der Windows-Auslagerungsdatei entspricht standardmäßig 150 % der Arbeitsspeichergröße.
- Die Größe der Protokolldateien kann pro virtuelle Maschine bis zu 100 MB betragen.
- 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.

Wenn Sie View Composer verwenden, wachsen die .vmdk-Dateien mit der Zeit an. Sie können dieses Anwachsen jedoch kontrollieren, indem Sie View Composer-Aktualisierungsvorgänge planen, für VM-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.

View ESXi-Knoten

Bei einem Knoten handelt es sich um einen einzelnen VMware ESXi-Host, auf dem virtuelle Desktop-Maschinen in einer View-Bereitstellung gehostet werden.

View arbeitet am wirtschaftlichsten, wenn Sie das Konsolidierungsverhältnis maximieren, d. h. die Anzahl der Desktops, die von einem ESXi-Host 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, für die Rechenkapazität von 8 bis 10 virtuellen Desktops pro CPU-Kern auszugehen. Informationen zum Berechnen der CPU-Anforderungen der einzelnen virtuellen Maschinen finden Sie unter [Einschätzen der CPU-Anforderungen für Desktops auf virtuellen Maschinen](#).
- Betrachten Sie die Arbeitsspeicherkapazität im Hinblick auf den Arbeitsspeicher für den virtuellen Desktop, den Hostarbeitsspeicher und die Speichermehrfachvergabe. Auch wenn Sie zwischen 8 und 10 virtuelle Maschinen pro CPU-Kern einsetzen können, müssen Sie 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 Desktops auf virtuellen Maschinen](#).

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, Speichieranbindung, Verwaltbarkeit und andere Aspekte dafür ausschlaggebend sein, die Anzahl der Server in einer Bereitstellung zu minimieren.

- Beachten Sie, dass in View 5.2 und höher die View-Speicherbeschleunigung standardmäßig aktiviert ist, sodass Hosts mit ESXi 5.0 und später gemeinsame Festplattendaten von virtuellen Maschinen zwischenspeichern können. Die View-Speicherbeschleunigung kann die Leistung verbessern und die Notwendigkeit von extra Speicher-E/A-Bandbreite verringern, um Startüberlastungen und Antiviren-E/A-Überlastungen zu verwalten. Für diese Funktion wird pro ESXi-Host 1 GB RAM benötigt.
- Berücksichtigen Sie außerdem die Cluster-Anforderungen und eventuelle Failover-Anforderungen. Weitere Informationen finden Sie unter [Bestimmen der Hochverfügbarkeitsanforderungen](#).

Informationen zu den technischen Daten von ESXi-Hosts in vSphere finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere*.

Desktop-Pools für bestimmte Nutzertypen

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 bieten viele Vorteile: Sie lassen sich z. B. leichter unterstützen 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 eventuell 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 virtuellen Linked-Clone-Maschinen oder vollständigen virtuellen Maschinen erstellen. Wenn Sie virtuelle Linked-Clone-Maschinen verwenden, können Sie die persistenten Festplatten sowie die Ordnerumleitung in View Composer konfigurieren. 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**

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**

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 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 nicht mit Benutzern, sondern mit Clientgeräten verknüpft sind, können diese Desktop-Pools verwenden, da Benutzer sich nicht anmelden müssen, um das Clientgerät oder den Remote-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.
- Verwenden Sie gegebenenfalls Virtual SAN-Datenspeicher. Virtual SAN virtualisiert die lokalen physischen Speicherfestplatten, die auf den ESXi-Hosts verfügbar sind, in einem einzelnen Datenspeicher, der von allen Hosts in einem vSphere-Cluster gemeinsam verwendet wird. Mithilfe von Virtual SAN können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Profile mit Speicherrichtlinien verwenden. Weitere Informationen finden Sie unter [Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung](#).
- Bei Bedarf sollten Sie erwägen, Desktops auf lokalen ESXi-Datenspeichern zu speichern. Diese Strategie kann verschiedene Vorteile bieten, so z.B. eine kostengünstige Hardware, eine schnelle Bereitstellung von virtuellen Maschinen, mehrere hochleistungsfähige Vorgänge zum Ändern des Betriebsstatus und eine vereinfachte Verwaltung. Eine Aufstellung der Beschränkungen finden Sie unter [Lokale Datenspeicher für dynamische zustandsfreie Desktops](#).

- Verwenden Sie die Persona-Verwaltungsfunktion, damit die Benutzer wie bei den Windows-Benutzerprofilen immer auf ihre bevorzugten Desktop-Anzeigeeinstellungen und Anwendungseinstellungen zugreifen können. Wenn Ihre Desktops bei der Abmeldung nicht aktualisiert oder gelöscht werden, können Sie die Persona so konfigurieren, dass sie bei der Abmeldung entfernt wird.

Wichtig View Persona Management erleichtert die Implementierung eines Pools mit dynamischer Zuweisung für die Benutzer, die die Einstellungen zwischen den Sitzungen beibehalten möchten. Bisher bestand eine der Einschränkungen von Desktops mit dynamischer Zuweisung darin, dass alle Konfigurationseinstellungen und alle auf dem Remote-Desktop gespeicherten Daten des Endbenutzers verloren gingen, wenn sich dieser abmeldete.

Bei jeder Anmeldung des Benutzers wurde der Desktophintergrund auf das Standard-Hintergrundbild zurückgesetzt, und alle Voreinstellungen für die einzelnen Anwendungen mussten erneut konfiguriert werden. Mit View Persona Management kann der Endbenutzer eines Desktops mit dynamischer Zuweisung nicht zwischen der eigenen Sitzung und der Sitzung auf einem Desktop mit fester Zuweisung unterscheiden.

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 können müssen, erstellen Sie für diese Benutzer Desktops mit fester Zuweisung. Für Büroanwender, die 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 Pools mit dedizierter Zuweisung, damit jeder Büroanwender oder Hauptbenutzer sich jedes Mal an demselben Desktop anmeldet.
- Verwenden Sie die Persona-Verwaltungsfunktion, damit die Benutzer wie bei den Windows-Benutzerprofilen immer auf ihre bevorzugten Desktop-Anzeigeeinstellungen und Anwendungseinstellungen zugreifen können.
- Verwenden Sie vStorage Thin Provisioning, damit jeder Desktop zunächst nur so viel Speicherplatz beansprucht wie die Festplatte für den anfänglichen Betrieb benötigt.
- 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. Verwenden Sie Mirage, um Anwendungen bereitzustellen und zu aktualisieren, ohne die von den Benutzern installierten Anwendungen zu überschreiben.

- Wenn Büroanwender benutzerinstallierte Anwendungen höchstens vorübergehend benötigen, können Sie View Composer-Linked-Clone-Desktops erstellen. Die Desktop-Images nutzen dasselbe Basis-Image und benötigen weniger Speicherplatz als vollständige virtuelle Maschinen.
- Wenn Sie View Composer mit virtuellen Desktops der Version vSphere 5.1 oder höher verwenden, aktivieren Sie die Funktion zur Rückgewinnung von Speicherplatz für vCenter Server und für den Desktop-Pool. Bei Verwendung der Funktion zur Rückgewinnung von Datenträgerplatz wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen.
- Wenn Sie Linked-Clone-Desktops aus View Composer verwenden, implementieren Sie View Persona Management, servergespeicherte Profile oder andere Profilverwaltungslösungen.

Konfigurieren Sie persistente Festplatten, sodass Sie die Linked-Clone-Betriebssystemfestplatten aktualisieren und neu zusammenstellen und eine Kopie des Benutzerprofils auf den persistenten Festplatten speichern können.

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 nicht mit Benutzern, sondern mit Clientgeräten verknüpft sind, können diese Desktop-Pools verwenden, da Benutzer sich nicht anmelden müssen, um das Clientgerät oder den Remote-Desktop zu nutzen. Dennoch müssen Benutzer für manche Anwendungen Anmeldeinformationen zur Authentifizierung bereitstellen.

Desktops auf virtuellen Maschinen, 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-Verbindungsserver-Instanzen für die Verwaltung von Clients im Kioskmodus einzusetzen und dedizierte Organisationseinheiten und Gruppen in Active Directory für die Konten dieser Clients zu erstellen. Bei dieser Vorgehensweise werden die Systeme nicht nur partitioniert und gegen unberechtigten Zugriff geschützt, sondern gleichzeitig wird die Konfiguration und Verwaltung der Clients vereinfacht.

Zum Einrichten des Kioskmodus müssen Sie die Befehlszeilenschnittstelle vdmadmin verwenden und mehrere Verfahren durchführen, die im Dokument *Verwaltung von View* 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 gegebenenfalls Virtual SAN-Datenspeicher. Virtual SAN virtualisiert die lokalen physischen Speicherfestplatten, die auf den ESXi-Hosts verfügbar sind, in einem einzelnen Datenspeicher, der von allen Hosts in einem vSphere-Cluster gemeinsam verwendet wird. Mithilfe von Virtual SAN können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Profile mit Speicherrichtlinien verwenden. Weitere Informationen finden Sie unter [Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung](#).
- Bei Bedarf sollten Sie erwägen, Desktops auf lokalen ESXi-Datenspeichern zu speichern. Diese Strategie kann verschiedene Vorteile bieten, so z.B. eine kostengünstige Hardware, eine schnelle Bereitstellung von virtuellen Maschinen, mehrere hochleistungsfähige Vorgänge zum Ändern des Betriebsstatus und eine vereinfachte Verwaltung. Eine Aufstellung der Beschränkungen finden Sie unter [Lokale Datenspeicher für dynamische zustandsfreie Desktops](#).
- Verwenden Sie ein Active Directory-Gruppenrichtlinienobjekt zum Konfigurieren der standortbasierten Druckfunktion, damit der Desktop den nächstgelegenen Drucker verwendet. Eine vollständige Liste und eine Beschreibung der über Gruppenrichtlinien-Verwaltungsvorlagen (ADM) verfügbaren Einstellungen finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.
- 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 Desktops mit virtuellen Maschinen benötigt werden, vom Gastbetriebssystem abhängen, werden für Windows XP, Windows Vista und Windows 7 und höher gesonderte Konfigurationsbeispiele für virtuelle Desktops angegeben.

Die Beispielseinstellungen für Elemente wie Arbeitsspeicher, Anzahl virtueller Prozessoren und Festplattenspeicher sind View-spezifisch.

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 der folgenden Tabelle aufgeführten Richtlinien gelten für Standard-Desktops mit virtuellen Maschinen unter Windows XP.

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

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

Die in der folgenden Tabelle aufgeführten Richtlinien gelten für Standard-Desktops mit virtuellen Maschinen unter Windows Vista.

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

| Element | Beispiel |
|---|--|
| Betriebssystem | 32 Bit-Windows Vista (mit neuestem Service Pack) |
| Arbeitsspeicher (RAM) | 1GB |
| Virtuelle CPU | 1 |
| Kapazität der Systemfestplatte | 20 GB (Standardeinstellung) |
| Benutzerdatenkapazität (als persistente Festplatte) | 5 GB (Ausgangswert) |
| Virtueller SCSI-Adaptertyp | LSI Logic Parallel (Standardeinstellung) |
| Virtueller Netzwerkadapter | VMXNET 3 |

Die in der folgenden Tabelle aufgeführten Richtlinien gelten für Standard-Desktops mit virtuellen Maschinen unter Windows 7 oder höher.

Tabelle 4-4. Beispiel für einen virtuellen Desktop für Windows 7 oder Windows 8

| Element | Beispiel |
|---|--|
| Betriebssystem | 32 Bit- oder 64 Bit-Windows 7 oder höher (mit dem neuesten Service Pack) |
| Arbeitsspeicher (RAM) | 1 GB (4 GB, wenn Benutzer hardwarebeschleunigte Grafik für das 3D-Rendern benötigen) |
| Virtuelle CPU | 1 (2 für 64 Bit-Systeme, oder wenn Benutzer hochauflösende Videos oder Videos im Vollbildmodus wiedergeben müssen) |
| Kapazität der Systemfestplatte | 24GB (etwas weniger als Standard) |
| Benutzerdatenkapazität (als persistente Festplatte) | 5 GB (Ausgangswert) |

| Element | Beispiel |
|----------------------------|-------------------------------------|
| Virtueller SCSI-Adaptertyp | LSI Logic SAS (Standardeinstellung) |
| Virtueller Netzwerkadapter | VMXNET 3 |

Konfiguration von virtuellen Maschinen als RDS-Hosts

Verwenden Sie RDS-Hosts (Remotedesktopdienste), um gehostete Anwendungen und sitzungsbasierte Remote-Desktops für Endbenutzer bereitzustellen.

Ein RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein. Dieses Beispiel verwendet eine virtuelle Maschine mit den in der folgenden Tabelle aufgelisteten Spezifikationen. Der ESXi-Host für diese virtuelle Maschine kann Teil eines VMware HA-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Tabelle 4-5. Beispiel einer virtuellen Maschine eines RDS-Hosts

| Element | Beispiel |
|---|--|
| Betriebssystem | 64 Bit-Windows Server 2008 R2, Windows Server 2012 oder Windows Server 2012 R2 |
| Arbeitsspeicher (RAM) | 24 GB |
| Virtuelle CPU | 4 |
| Kapazität der Systemfestplatte | 40 GB |
| Virtueller SCSI-Adaptertyp | LSI Logic SAS (Standardeinstellung für Windows Server 2008) |
| Virtueller Netzwerkadapter | VMXNET 3 |
| 1 Netzwerkadapter | 1 Gigabit |
| Maximale Anzahl von Clientverbindungen (einschließlich clientbasierte Remote-Desktopverbindungen und -Anwendungsverbindungen) | 50 |

Weitere Informationen zur RDS-Host-Konfiguration und zu getesteten Arbeitslasten finden Sie im White Paper *VMware Horizon 6 Reference Architecture* unter <http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf>.

vCenter Server- und View Composer-Konfiguration für virtuelle Maschinen

Sie können vCenter Server und View Composer auf derselben virtuellen Maschine oder auf separaten Servern installieren. Für diese Server ist viel mehr Arbeitsspeicher und Prozessorleistung erforderlich als für eine virtuelle Desktop-Maschine.

VMware hat ein Szenario getestet, in dem View Composer unter Verwendung von vSphere 5.1 oder höher 2.000 Desktops pro Pool erstellt und bereitgestellt hat. VMware hat außerdem die Ausführung eines Neuzusammenstellungsvorgangs durch View Composer auf 2.000 Desktops gleichzeitig getestet. Für diese Tests wurden vCenter Server und View Composer auf separaten virtuellen Maschinen installiert.

Die Größe des Desktop-Pools wird durch die folgenden Faktoren beschränkt:

- Jeder Desktop-Pool kann maximal einen vSphere-Cluster enthalten.
- vSphere 5.1-Cluster und später können bis zu 32 Hosts einhalten.

Wenn Sie bei Clustern, die mehr als acht Hosts enthalten, Linked-Clone-Pools verwenden, müssen Replikatfestplatten auf VMFS5-Datenspeichern oder höher, auf NFS-Datenspeichern oder, sofern Sie vSphere 5.5 Update 1 oder höher installiert haben, auf Virtual SAN-Datenspeichern gespeichert werden. Wenn Sie Replikate in einem Datenspeicher einer früheren VMFS-Version als VMFS5 speichern, kann ein Cluster über maximal acht Hosts verfügen. Betriebssystemfestplatten und persistente Festplatten können in NFS- oder VMFS-Datenspeichern gespeichert werden.

- Jeder CPU-Kern verfügt über Rechenkapazität für 8 bis 10 virtuelle Desktops.
- Die Anzahl der für das Subnetz verfügbaren IP-Adressen beschränkt die Anzahl der Desktops im Pool. Wenn Ihr Netzwerk beispielsweise so eingerichtet ist, dass das Subnetz für den Pool nur 256 verwendbare IP-Adressen enthält, wird die Poolgröße auf 256 Desktops beschränkt. Sie können jedoch mehrere Netzwerkbezeichnungen konfigurieren, um die Anzahl von IP-Adressen, die den virtuellen Maschinen in einem Pool zugewiesen werden, zu erweitern.

Obwohl Sie vCenter Server und View Composer auf einem physischen Computer installieren können, werden in diesem Beispiel virtuelle Maschinen mit den in den folgenden Tabellen angegebenen technischen Daten verwendet. Der ESXi-Host für diese virtuellen Maschinen kann Teil eines VMware HA-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Für dieses Beispiel wird davon ausgegangen, dass Sie View mit vSphere 5.1 oder höher und vCenter Server 5.1 oder höher verwenden.

Wichtig Darüber hinaus wird davon ausgegangen, dass View Composer und vCenter Server auf separaten virtuellen Maschinen installiert sind.

Tabelle 4-6. Beispiel für eine virtuelle vCenter Server-Maschine

| Element | Beispiel für eine vCenter Server-Instanz, die 10.000 Desktops verwaltet | Beispiel für eine vCenter Server-Instanz, die 2.000 Desktops verwaltet |
|--------------------------------|---|--|
| Betriebssystem | Windows Server 2008 R2 Enterprise, 64 Bit | Windows Server 2008 R2 Enterprise, 64 Bit |
| Arbeitsspeicher (RAM) | 48GB | 4GB |
| Virtuelle CPU | 16 | 2 |
| Kapazität der Systemfestplatte | 180GB | 40GB |

| Element | Beispiel für eine vCenter Server-Instanz, die 10.000 Desktops verwaltet | Beispiel für eine vCenter Server-Instanz, die 2.000 Desktops verwaltet |
|--|---|--|
| Virtueller SCSI-Adaptertyp | LSI Logic SAS (Standardeinstellung für Windows Server 2008) | LSI Logic SAS (Standardeinstellung für Windows Server 2008) |
| Virtueller Netzwerkadapter | E1000 (Standard) | E1000 (Standard) |
| Maximale Anzahl gleichzeitiger vCenter-Bereitstellungsvorgänge | 20 | 20 |
| Maximale Anzahl gleichzeitiger Betriebsvorgänge | 50 | 50 |

Tabelle 4-7. Beispiel für eine virtuelle View Composer-Maschine

| Element | Beispiel für eine View Composer-Instanz, die 10.000 Desktops verwaltet | Beispiel für eine View Composer-Instanz, die 2.000 Desktops verwaltet |
|--|--|---|
| Betriebssystem | Windows Server 2008 R2 Enterprise, 64 Bit | Windows Server 2008 R2 Enterprise, 64 Bit |
| Arbeitsspeicher (RAM) | 10 GB | 4GB |
| Virtuelle CPU | 4 | 2 |
| Kapazität der Systemfestplatte | 50GB | 40GB |
| Virtueller SCSI-Adaptertyp | LSI Logic SAS (Standardeinstellung für Windows Server 2008) | LSI Logic SAS (Standardeinstellung für Windows Server 2008) |
| Virtueller Netzwerkadapter | VMXNET 3 | VMXNET 3 |
| Maximale View Composer-Poolgröße | 2.000 Desktops | 1,000 Desktops |
| Maximale Anzahl gleichzeitiger View Composer-Wartungsvorgänge | 12 | 12 |
| Maximale Anzahl gleichzeitiger View Composer-Bereitstellungsvorgänge | 8 | 8 |

Wichtig VMware empfiehlt, die Datenbank, mit der vCenter Server und View Composer eine Verbindung herstellen, auf einer separaten virtuellen Maschine zu platzieren.

View-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen

Bei der Installation von View-Verbindungsserver wird die View Administrator-Benutzeroberfläche ebenfalls installiert.

View-Verbindungsserver-Konfiguration

Wenngleich Sie den View-Verbindungsserver auf einem physischen Computer installieren können, wird in diesem Beispiel eine virtuelle Maschine mit den in [Tabelle 4-8. Beispiel einer virtuellen Maschine für View-Verbindungsserver](#) aufgelisteten technischen Daten verwendet. Der ESXi-Host für diese virtuelle Maschine kann Teil eines VMware HA-Clusters sein, damit ein Schutz gegen Ausfälle des physischen Servers besteht.

Tabelle 4-8. Beispiel einer virtuellen Maschine für View-Verbindungsserver

| Element | Beispiel |
|--------------------------------|---|
| Betriebssystem | 64 Bit Windows Server 2008 R2 oder Windows Server 2012 R2 |
| Arbeitsspeicher (RAM) | 10GB |
| Virtuelle CPU | 4 |
| Kapazität der Systemfestplatte | 70 GB |
| Virtueller SCSI-Adaptertyp | LSI Logic SAS (Standardeinstellung für Windows Server 2008) |
| Virtueller Netzwerkadapter | VMXNET 3 |
| Netzwerkkarte | Netzwerkkarte mit 1 Gbit/s |

Aspekte des Cluster-Aufbaus bei View-Verbindungsserver

Sie können mehrere replizierte View-Verbindungsserver-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.

Wichtig Zur Verwendung einer Gruppe replizierter View-Verbindungsserver-Instanzen in einem WAN, MAN (Metropolitan Area Network) oder einem anderen Netzwerk, das kein LAN ist, in einer Situation, in der die View-Bereitstellung sich über mehrere Rechenzentren erstrecken muss, müssen Sie die Cloud Pod Architecture-Funktion verwenden. Sie können vier View-Pods verbinden, sodass eine große Umgebung für das Brokering und die Verwaltung von Desktops in zwei Sites entsteht, die sich an unterschiedlichen geografischen Standorten befinden. Auf diese Weise lassen sich 20.000 Remote-Desktops verwalten. Weitere Informationen finden Sie unter *Verwalten der View-Cloud Pod Architecture*.

Maximale Verbindungsanzahl für View-Verbindungsserver

[Tabelle 4-9. Remote-Desktop-Verbindungen](#) bietet Informationen zu den getesteten Einschränkungen in Bezug auf die Anzahl gleichzeitiger Verbindungen, die eine View-Bereitstellung unterstützen kann.

Dieses Beispiel geht davon aus, dass Sie View mit vSphere 4.1 oder höher und vCenter Server 4.1 oder höher einsetzen. Zudem wird davon ausgegangen, dass der View-Verbindungsserver auf einem Windows Server 2008 R2 Enterprise-Betriebssystem mit 64 Bit ausgeführt wird.

Tabelle 4-9. Remote-Desktop-Verbindungen

| Anzahl der Verbindungsserver-Instanzen pro Bereitstellung | Verbindungstyp | Maximale Anzahl gleichzeitiger Verbindungen |
|---|---|---|
| 1 Verbindungsserver | Direktverbindung, RDP oder PCoIP: | 2.000 (getestete Einschränkung) |
| | Tunnelverbindung, RDP: | 2.000 (feste Einschränkung) |
| | PCoIP Secure Gateway-Verbindung: | 2.000 (feste Einschränkung) |
| 7 Verbindungsserver | Direkte Verbindung, RDP oder PCoIP | 10.000 (getesteter und daher unterstützter Grenzwert) |
| 1 Verbindungsserver | Unified Access auf physische PCs | 2,000 |
| 1 Verbindungsserver | Unified Access auf RDS-Hosts | 2,000 |
| 1 Verbindungsserver | Blast Secure Gateway-Verbindungen zu Remote-Desktops unter Verwendung von HTML Access | 800 |

Verbindungen über das PCoIP Secure Gateway sind erforderlich, wenn Sie für PCoIP-Verbindungen, deren Ausgangspunkt sich außerhalb des Firmennetzwerks befindet, Sicherheitsserver verwenden. Tunnelverbindungen sind bei Verwendung von Sicherheitsservern für RDP-Verbindungen, deren Ausgangspunkt sich außerhalb des Firmennetzwerks befindet, sowie für die USB-Umleitung und MMR-Beschleunigung (Multimedia Redirection) mit einer Verbindung über das PCoIP Secure Gateway erforderlich. Sie können mehrere Sicherheitsserver zu einer einzelnen View-Verbindungsserver-Instanz kombinieren.

Hinweis In diesem Beispiel könnten 5 View-Verbindungsserver-Instanzen zwar 10.000 Verbindungen bewältigen, doch in der Tabelle wird zum Zweck der Verfügbarkeitsplanung der Wert 7 angezeigt, um Verbindungen von innerhalb und außerhalb des Firmennetzwerks zu berücksichtigen.

Wenn beispielsweise 10.000 Benutzer vorhanden sind, von denen sich 8.000 innerhalb des Firmennetzwerks befinden, benötigen Sie 5 View-Verbindungsserver-Instanzen innerhalb des Firmennetzwerks. Wenn eine Instanz ausfällt, ist so gewährleistet, dass die Last von den vier verbleibenden Instanzen bewältigt werden kann. Gleichmaßen benötigen Sie für die 2.000 Verbindungen, die von außerhalb des Firmennetzwerks stammen, 2 View-Verbindungsserver-Instanzen, damit die Last beim Ausfall einer Instanz von der jeweils anderen Instanz bewältigt werden kann.

vSphere-Cluster

View-Bereitstellungen können VMware HA-Cluster (High Availability) als Schutz gegen Ausfälle physischer Server nutzen. Mit vSphere 5.1 und höher kann der Cluster bei Verwendung von View Composer und Speicherung der Replikatfestplatten in NFS- oder VMFS5-Datenspeichern bis zu 32 Server oder Knoten enthalten. Mit vSphere 5.5 Update 1 und höher können Sie Virtual SAN-Datenspeicher verwenden, und der Cluster kann bis zu 32 Server enthalten.

vSphere und vCenter Server bieten zahlreiche Funktionen zum Verwalten von Clustern mit Servern, die Desktops auf virtuellen Maschinen hosten. Die Cluster-Konfiguration ist auch von Bedeutung, da jeder Desktop-Pool auf virtuellen Maschinen einem vCenter Server-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 View-Bereitstellungen kann die Leistung und Reaktionsschnelligkeit von vCenter Server durch das Beschränken auf ein einziges Cluster-Objekt pro Rechenzentrumsobjekt verbessert werden, was nicht die Standardeinstellung ist. Standardmäßig erzeugt vCenter Server neue Cluster innerhalb desselben Rechenzentrumsobjekts.

Bestimmen der Hochverfügbarkeitsanforderungen

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 $128 \times (8-1) = 896$ 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: Beispiele für die Cluster-Konfiguration

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

Das folgende Infrastruktur-Beispiel wurde mit View 5.2 und vSphere 5.1 getestet.

Tabelle 4-10. Beispiel für einen View-Infrastruktur-Cluster

| Element | Beispiel |
|---------------------|---|
| Virtuelle Maschinen | vCenter Server-Instanzen, Active Directory, SQL-Datenbankserver, View Composer, View-Verbindungsserver-Instanzen, Sicherheitsserver, übergeordnete virtuelle Maschinen zur Verwendung als Quellen für Desktop-Pools |
| Knoten (ESXi-Hosts) | 6 Dell PowerEdge R720-Server (16 Kerne x 2 GHz sowie 192 GB RAM auf jedem Host) |
| SSD-Speicher | Virtuelle Maschinen für vCenter Server, View Composer, SQL-Datenbankserver und übergeordnete virtuelle Maschinen |
| Nicht-SSD-Speicher | Virtuelle Maschinen für Active Directory, View-Verbindungsserver und Sicherheitsserver |
| Cluster-Typ | DRS (Distributed Resource Scheduler)/HA |

Tabelle 4-11. Beispiel eines Desktop-Clusters auf einer virtuellen Maschine

| Element | Beispiel |
|---|--|
| Anzahl der Cluster | 5 |
| Anzahl der Desktops und Pools pro Cluster | 1 Pool mit 2.000 Desktops (virtuellen Maschinen) pro Cluster |
| Knoten (ESXi-Hosts) | Im Folgenden sind Beispiele für Server aufgeführt, die für die jeweiligen Cluster verwendet werden könnten: <ul style="list-style-type: none"> ■ 12 Dell PowerEdge R720 (16 Kerne x 2 GHz sowie 192 GB RAM auf jedem Host) ■ 16 Dell PowerEdge R710 (12 Kerne x 2,526 GHz sowie 144GB RAM auf jedem Host) ■ 8 Dell PowerEdge R810 (24 Kerne x 2 GHz sowie 256GB RAM auf jedem Host) ■ 6 Dell PowerEdge R810 + 3 PowerEdge R720 |
| SSD-Speicher | Virtuelle Replikatmaschinen |
| Nicht-SSD-Speicher | 32 Nicht-SSD-Datenspeicher für Klone (450 GB pro Datenspeicher) |
| Cluster-Typ | DRS (Distributed Resource Scheduler)/HA |

Hinweis Mit vSphere 5.1 und höher kann der Cluster bei Verwendung von View Composer und Speicherung der Replikatfestplatten in NFS- oder VMFS5-Datenspeichern bis zu 32 ESXi-Hosts enthalten. Mit vSphere 5.5 Update 1 und höher kann der Cluster bei Verwendung von Virtual SAN-Datenspeichern ebenfalls bis zu 32 Server enthalten. Weitere Informationen finden Sie im Kapitel zur Erstellung von Desktop-Pools im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

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

Speicher- und Bandbreitenanforderungen

Bei der Planung des gemeinsamen Speichers für Desktops auf virtuellen Maschinen, bei der Planung der Bandbreitenanforderungen für den Speicher im Hinblick auf E/A-Überlastungen und bei der Planung der Bandbreitenanforderungen für das Netzwerk müssen verschiedene Aspekte berücksichtigt werden.

Einzelheiten zu den in der Testeinrichtung von VMware verwendeten Speicher- und Netzwerkkomponenten finden Sie in diesen verwandten Themen.

- **Beispiel für gemeinsamen Speicher**

In einer View 5.2-Testumgebung wurden virtuelle View Composer-Replikatmaschinen auf Solid-State-Laufwerken (SSDs) mit hoher Leseleistung platziert, die Zehntausende E/A-Vorgänge pro Sekunde (IOPS) unterstützen. Verknüpfte Klone wurden in herkömmlichen, auf drehenden Medien basierenden Datenspeichern mit geringerer Leistung platziert, die kostengünstiger sind und eine höhere Speicherkapazität bieten.

- **Aspekte der Speicherbandbreite**

In einer View-Umgebung müssen beim Ermitteln der Bandbreitenanforderungen in erster Linie Anmeldungsüberlastungen berücksichtigt werden.

- **Aspekte der Netzwerkbandbreite**

Zur Verarbeitung einer typischen Arbeitslast sind bestimmte virtuelle und physische Netzwerkkomponenten erforderlich.

- **Ergebnisse von View Composer-Leistungstests**

Diese Testergebnisse beschreiben eine View 5.2-Einrichtung mit 10.000 Desktops, in der eine vCenter Server 5.1-Instanz fünf Pools von je 2.000 Desktops mit virtuellen Maschinen verwaltet hat. Für die Bereitstellung eines neuen Pools oder zur Neuzusammenstellung, Aktualisierung oder Neuverteilung eines vorhandenen Pools mit 2.000 virtuellen Maschinen war lediglich ein Wartungsfenster erforderlich. Außerdem wurde ein Anmeldungsüberlastungsszenario mit 10.000 Benutzern getestet.

- **WAN-Unterstützung und PCoIP**

Bei WANs (Wide Area Networks) müssen Sie Bandbreiteneinschränkungen und Wartezeiten berücksichtigen. Das von VMware bereitgestellte PCoIP-Anzeigeprotokoll passt sich an wechselnde Wartezeit- und Bandbreitenbedingungen an.

Beispiel für gemeinsamen Speicher

In einer View 5.2-Testumgebung wurden virtuelle View Composer-Replikatmaschinen auf Solid-State-Laufwerken (SSDs) mit hoher Leseleistung platziert, die Zehntausende E/A-Vorgänge pro Sekunde (IOPS) unterstützen. Verknüpfte Klone wurden in herkömmlichen, auf drehenden Medien basierenden Datenspeichern mit geringerer Leistung platziert, die kostengünstiger sind und eine höhere Speicherkapazität bieten.

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. Die ESXi-Binärdateien, die Auslagerungsdateien virtueller Maschinen und View Composer-Replikate übergeordneter virtueller Maschinen werden im gemeinsamen Speichersystem gespeichert.

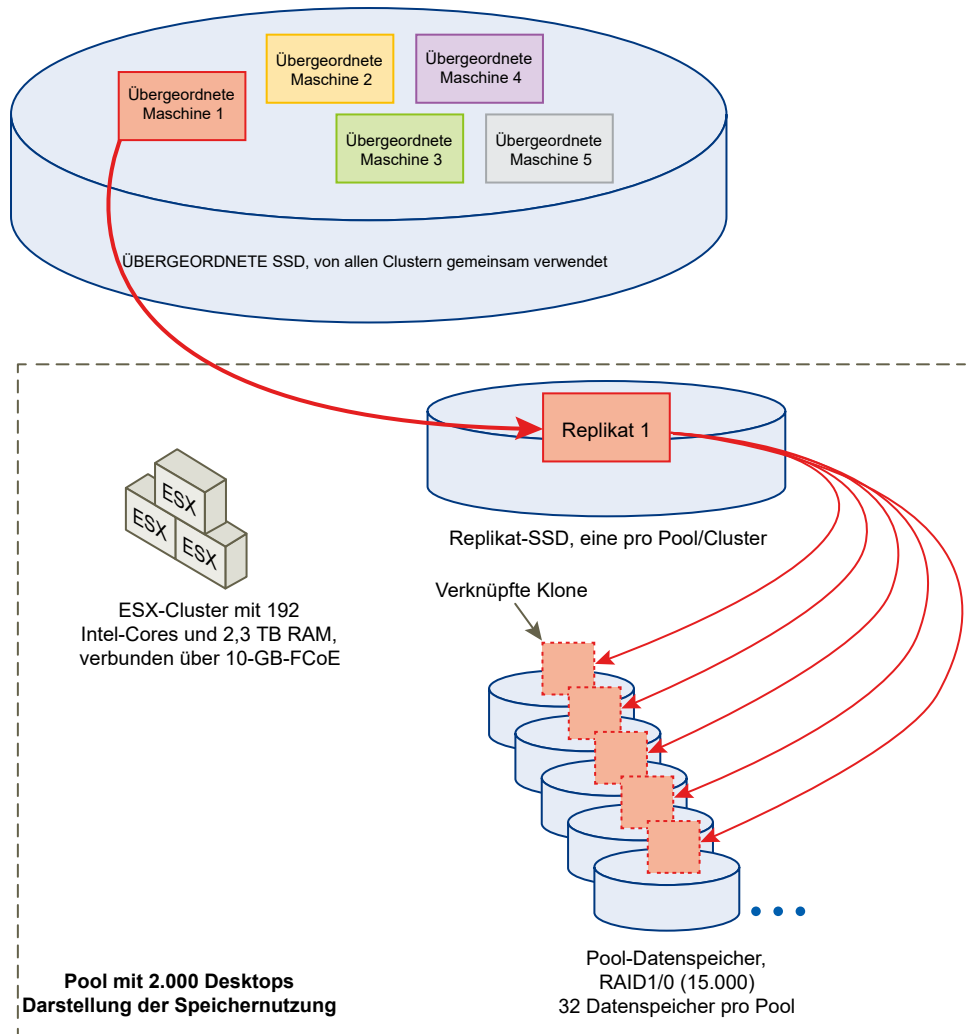
Das externe Speichersystem, das von vSphere verwendet wird, kann ein Fibre-Channel- oder iSCSI-SAN (Storage Area Network) oder ein NFS-NAS (Network File System, Network-Attached Storage) sein. Bei der Virtual SAN-Funktion, die mit vSphere 5.5 Update 1 oder höher zur Verfügung steht, kann auch ein aggregiertes, lokales Server Attached Storage-Speichersystem verwendet werden.

Das folgende Beispiel beschreibt die Strategie des mehrstufigen Speichers, die in einer View 5.2-Testeinrichtung umgesetzt wurde, in der eine vCenter Server-Instanz für die Verwaltung von 10.000 Desktops eingesetzt wurde.

Hinweis Für dieses Beispiel wurde ein View 5.2-Setup verwendet, das vor der Veröffentlichung von VMware Virtual SAN durchgeführt wurde. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware Virtual SAN finden Sie im White Paper unter <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

| | |
|---|--|
| Physischer Speicher | <ul style="list-style-type: none"> ■ Nur EMC VNX7500-Block ■ 1,8 TB Fast Cache (SSD) ■ Acht 10-Gbit-FCoE-Front-End-Verbindungen (4 pro Controller). |
| SSD-Speicherebene | <p>Ein einziger RAID5-Speicherpool:</p> <ul style="list-style-type: none"> ■ 12 * 200-GB-EFD ■ 250-GB-LUN für übergeordnete Images ■ 500-GB-LUN für die Infrastruktur ■ 75-GB-LUNs für Replikatspeicher (1 pro Desktop-Pool-Cluster) |
| Desktop-Speicherebene für die virtuelle Maschine | <p>Zwei RAID 1/0-Speicherpools:</p> <p>Für Pool 1:</p> <ul style="list-style-type: none"> ■ 360 300-GB-HDDs, 15.000 (47 TB verwendbar) ■ 97 450-GB-LUNs für Desktops <p>Für Pool 2:</p> <ul style="list-style-type: none"> ■ 296 300-GB-HDDs, 15.000 (39 TB verwendbar) ■ 7 450-GB-LUNs für die Infrastruktur ■ 85 450-GB-LUNs für Desktops |

Diese Speicherstrategie wird in der folgenden Abbildung veranschaulicht.

Abbildung 4-1. Beispiel eines mehrstufigen Speichers für einen großen Desktop-Pool

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.

Wenn Sie View Composer mit Desktops auf virtuellen Maschinen der Version vSphere 5.1 oder höher verwenden, können Sie die Funktion zur Rückgewinnung von Speicherplatz nutzen. Bei Verwendung dieser Funktion wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen. Bei Verwendung eines Virtual SAN-Datenspeichers wird die Funktion zur Speicherplatzrückgewinnung nicht unterstützt.

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](#).

Hinweis Entscheidungen bezüglich fester Speicherkomponenten sollten am besten während der Pilotphase getroffen werden. Das Hauptkriterium sind die E/A-Vorgänge pro Sekunde (IOPS). Sie können mit einer Strategie des mehrstufigen Speichers oder mit Virtual SAN-Speicher 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

In einer View-Umgebung müssen beim Ermitteln der Bandbreitenanforderungen in erster Linie Anmeldungsüberlastungen berücksichtigt werden.

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

In 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. VMware hat ein Anmeldungsüberlastungsszenario für 10.000 Desktops getestet. Weitere Informationen finden Sie unter [Ergebnisse von View Composer-Leistungstests](#).

Sie können diese Überlastungen durch Befolgen empfohlener Vorgehensweisen minimieren, z. B. durch Staffeln 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 Hochleistungsdatenspeichern oder Verwenden von Virtual SAN im Lieferumfang von vSphere 5.5 Update 1 oder höher 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

Zur Verarbeitung einer typischen Arbeitslast sind bestimmte virtuelle und physische Netzwerkkomponenten erforderlich.

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 (1920 x 1080)
- 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
- Netzwerkbasierendes Drucken

Weitere Informationen finden Sie im Informationsleitfaden *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide* (PCoIP-Anzeigeprotokoll: Größenbestimmungsleitfaden für informations- und szenariobasierte Netzwerke).

Für PCoIP verfügbare Optimierungssteuerungen

Bei Verwendung des PCoIP-Anzeigeprotokolls von VMware können Sie mehrere Elemente anpassen, die sich auf die Bandbreitenverwendung auswirken.

- Sie können die in Zeiten der Netzwerküberlastung verwendete Bildqualitätsstufe und die Frame-Rate konfigurieren. Die Einstellung der Qualitätsstufe ermöglicht Ihnen die Beschränkung der anfänglichen Qualität der geänderten Bereiche für die Bildanzeige. Die nicht geänderten Bildbereiche erreichen stufenweise eine verlustfreie (perfekte) Qualität. Sie können die Frame-Rate von 1 auf 120 Frames pro Sekunde erhöhen.

Diese Steuerung ist besonders für statische Bildschirminhalte geeignet, die nicht aktualisiert werden müssen, oder für Situationen, in denen nur bestimmte Ausschnitte aktualisiert werden müssen.

- Sie können die Build-to-Lossless-Funktion auch komplett deaktivieren, wenn Sie anstelle des stufenweisen Aufbaus einer perfekten Qualität (verlustfrei) die wahrnehmbare verlustfreie Anzeige bevorzugen.

- Sie können steuern, welche Verschlüsselungsalgorithmen vom PCoIP-Endpunkt während der Sitzungs-aushandlung angeboten werden. Standardmäßig sind die Algorithmen Salsa20-256round12 und AES-128-GCM verfügbar.
- Hinsichtlich der Sitzungsbandbreite können Sie die maximale Bandbreite in KBit/s konfigurieren, damit diese der Art der Netzwerkverbindung entspricht, so z. B. einer Internetverbindung mit 4 MBit/s. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle, USB und PCoIP-Steuerung eingeschlossen.

Sie können auch für die für die Sitzung reservierte Bandbreite eine niedrigere Grenze in KBit/s festlegen, sodass der Benutzer nicht warten muss, bis Bandbreite verfügbar ist. Sie können die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für UDP-Pakete bei einer PCoIP-Sitzung von 500 auf 1500 Byte erhöhen.

- Sie können die maximale Bandbreite festlegen, die in einer PCoIP-Sitzung für Audiodaten (Soundwiedergabe) verwendet werden kann.

Außerdem speichert die PCoIP-Client-Bildzwischenspeicherung auf den meisten Clientsystemen den Bildinhalt auf dem Client, um erneute Übertragungen zu vermeiden. Bei der Clientversion 2.0 oder höher hat der Cache eine Standardgröße von 90 MB.

Beispiel für die Netzwerkkonfiguration

In einem Test-Pod unter View 5.2, in dem eine vCenter Server 5.1-Instanz für die Verwaltung von 5 Pools mit je 2.000 virtuellen Maschinen eingesetzt wurde, wurden die Netzwerkanforderungen eines jeden ESXi-Hosts mit der folgenden Hardware und Software erfüllt.

Hinweis Für dieses Beispiel wurde ein View 5.2-Setup verwendet, das vor der Veröffentlichung von VMware Virtual SAN durchgeführt wurde. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware Virtual SAN finden Sie im White Paper unter <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Physische Komponenten für jeden Host

- Brocade 1860 Fabric Adapter mit 10-Gig-Ethernet- und FCoE-Konnektivität für Netzwerk- bzw. Speicherdatenverkehr.
- Verbindung mit einem Brocade VCS Ethernet-Fabric aus 6 VDX6720-60-Switches. Die Switches waren mit einem Juniper J6350-Router und über Uplinks (zwei 1-GB-Verbindungen) mit den übrigen Netzwerkkomponenten verbunden.

vLAN-Übersicht

- Ein 10-GB-vLAN pro Desktop-Pool (5 Pools)
- Ein 1-GB-vLAN für das Verwaltungsnetzwerk
- Ein 1-GB-vLAN für das vMotion-Netzwerk
- Ein 10-GB-vLAN für das Infrastrukturnetzwerk

Virtueller VMotion-dvswitch (1 Uplink pro Host)

Dieser Switch wurde von den ESXi-Hosts der virtuellen Maschinen der Infrastruktur, der übergeordneten Maschinen sowie der virtuellen Desktop-Maschinen verwendet.

- Jumbo-Frame (9000 MTU)
- 1 kurzlebige verteilte Portgruppe
- Privates VLAN und 192.168.x.x-Adressierung

Infra-dvswitch (2 Uplinks pro Host)

Dieser Switch wurde von den ESXi-Hosts der virtuellen Maschinen der Infrastruktur verwendet.

- Jumbo-Frame (9000 MTU)
- 1 kurzlebige verteilte Portgruppe
- Infrastruktur-VLAN /24 (256 Adressen)

Desktop-dvswitch (2 Uplinks pro Host)

Dieser Switch wurde von den ESXi-Hosts der übergeordneten Maschinen sowie der virtuellen Desktop-Maschinen verwendet.

- Jumbo-Frame (9000 MTU)
- 6 kurzlebige verteilte Portgruppen
- 5 Desktop-Portgruppen (1 pro Pool)
- Bei jedem Netzwerk handelte es sich um ein /21-Netzwerk, 2048 Adressen

Ergebnisse von View Composer-Leistungstests

Diese Testergebnisse beschreiben eine View 5.2-Einrichtung mit 10.000 Desktops, in der eine vCenter Server 5.1-Instanz fünf Pools von je 2.000 Desktops mit virtuellen Maschinen verwaltet hat. Für die Bereitstellung eines neuen Pools oder zur Neuzusammenstellung, Aktualisierung oder Neuverteilung eines vorhandenen Pools mit 2.000 virtuellen Maschinen war lediglich ein Wartungsfenster erforderlich. Außerdem wurde ein Anmeldungsüberlastungsszenario mit 10.000 Benutzern getestet.

Die hier aufgeführten Testergebnisse wurden mit den in den folgenden Themen beschriebenen Software-, Hardware- und Konfigurationseinstellungen erzielt:

- Die in [View-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen](#) beschriebenen Desktop- und Poolkonfigurationen
- Die in [Beispiel für gemeinsamen Speicher](#) beschriebenen Komponenten eines mehrstufigen Speichers
- Die in [Aspekte der Netzwerkbandbreite](#) beschriebenen Netzwerkkomponenten

Kapazität für eine einstündige Anmeldungsüberlastung mit 10.000 Benutzern

Hinweis Für dieses Beispiel wurde ein View 5.2-Setup verwendet, das vor der Veröffentlichung von VMware Virtual SAN durchgeführt wurde. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware Virtual SAN finden Sie im White Paper unter <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>. Testergebnisse mit verschiedenen Arbeitslasten und View-Vorgängen bei Verwendung von Virtual SAN finden Sie im White Paper zur Referenzarchitektur unter <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf>.

In einer Testeinrichtung wurden die folgenden Desktop- und Poolkonfigurationen für ein Anmeldungsüberlastungsszenario für 10.000 Desktops verwendet. Die Betriebsrichtlinie für Desktops wurde auf „Immer eingeschaltet“ festgelegt.

Die Anmeldungsüberlastung dauerte für 10.000 Desktops 60 Minuten und es wurde eine normale Verteilung von Anmeldezeiten verwendet. Die virtuellen Maschinen waren vor Beginn der Anmeldungsüberlastung eingeschaltet und verfügbar. Nach der Anmeldung wurde eine Arbeitslast gestartet, die die folgenden Anwendungen umfasste: Adobe Reader, Microsoft Outlook, Internet Explorer, Microsoft Word und Editor.

Im Folgenden sind weitere Einzelheiten zur Anmeldungsüberlastung aus diesem Test aufgeführt:

- 95% der Anmeldungen erfolgten innerhalb eines Fensters mit einer Standardabweichung von +/- 2 (40 Minuten).
- 68 % der Anmeldungen erfolgten innerhalb eines Fensters mit einer Standardabweichung von +/- 1 (20 Minuten).
- Die Spitzenanmelderate betrug 400/Minute oder 6,67/Sekunde.

Erforderliche Zeit für die Bereitstellung eines Pools

Pools werden entweder vorab beim Erstellen des Pools oder nach Bedarf zu einem späteren Zeitpunkt bereitgestellt, wenn den Pools Benutzer zugewiesen werden. Der Bereitstellungsvorgang umfasst das Erstellen der virtuellen Maschine und deren Konfiguration für die Verwendung des richtigen Betriebssystem-Image und der richtigen Netzwerkeinstellungen.

In einer Testeinrichtung, die bereits aus 4 Pools mit je 2.000 virtuellen Maschinen bestand, dauerte die Bereitstellung eines fünften Pools mit 2.000 virtuellen Maschinen 4 Stunden. Alle virtuellen Maschinen wurden vorab bereitgestellt.

Erforderliche Zeit für die Neuzusammenstellung eines Pools

Bei einer Neuzusammenstellung können Sie Betriebssystem-Patches bereitstellen, Anwendungen installieren und aktualisieren oder die Desktop-Hardwareeinstellungen der virtuellen Maschinen in einem Pool ändern. Bevor Sie einen Pool neu zusammenstellen, erstellen Sie einen Snapshot einer virtuellen Maschine, die über eine neue Konfiguration verfügt. Bei der Neuzusammenstellung werden alle virtuellen Maschinen innerhalb des Pools anhand dieses Snapshots aktualisiert.

In einer Testeinrichtung mit 5 Pools mit je 2.000 virtuellen Maschinen dauerte die Neuzusammenstellung eines Pools mit 2.000 virtuellen Maschinen 6 Stunden und 40 Minuten. Vor dem Start der Neuzusammenstellung waren alle virtuellen Maschinen eingeschaltet und verfügbar.

Erforderliche Zeit für die Aktualisierung eines Pools

Da die Größe einer Festplatte im Lauf der Zeit steigt, können Sie Speicherplatz sparen, indem Sie Desktops bei der Abmeldung der Benutzer aktualisieren und den ursprünglichen Zustand wiederherstellen. Alternativ können Sie einen Zeitplan für regelmäßige Aktualisierungen der Desktops festlegen. Zum Beispiel können Sie einstellen, dass Desktops täglich, wöchentlich oder monatlich aktualisiert werden.

In einer Testeinrichtung mit 5 Pools mit je 2.000 virtuellen Maschinen dauerte die Aktualisierung eines Pools mit 2.000 virtuellen Maschinen 2 Stunden und 40 Minuten. Vor dem Start der Aktualisierung waren alle virtuellen Maschinen eingeschaltet und verfügbar.

Erforderliche Zeit für die Neuverteilung eines Pools

Bei einem Vorgang zur Neuverteilung für einen Desktop werden Linked-Clone-Desktops erneut auf die verfügbaren logischen Laufwerke verteilt. Durch eine Neuverteilung wird Speicherplatz auf überlasteten Laufwerken gespart und sichergestellt, dass Laufwerke optimal ausgelastet sind. Sie können auch mithilfe eines Neuverteilungsvorgangs alle virtuellen Maschinen in einem Desktop-Pool auf einen oder von einem Virtual SAN-Datenspeicher migrieren.

In einer Teststruktur mit 5 Pools mit je 2.000 virtuellen Maschinen wurden für einen Test 2 Datenspeicher zur Struktur hinzugefügt. Für einen weiteren Test wurden 2 Datenspeicher aus der Struktur entfernt. Nach dem Hinzufügen oder Entfernen der Datenspeicher wurde für einen der Pools eine Neuverteilung durchgeführt. Die Neuverteilung eines Pools mit 2.000 virtuellen Maschinen dauerte 9 Stunden. Vor dem Start der Neuverteilung waren alle virtuellen Maschinen eingeschaltet und verfügbar.

WAN-Unterstützung und PCoIP

Bei WANs (Wide Area Networks) 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.

Informationen über die Steuerungen, die mit View 5 eingeführt wurden und zur Regulierung des Bandbreitenverbrauchs durch PCoIP verwendet werden können, finden Sie unter [Für PCoIP verfügbare Optimierungssteuerungen](#).

Bandbreitenanforderungen für verschiedene Typen von Nutzern

Bei der Festlegung der Mindestbandbreitenanforderungen für PCoIP sollten Sie mit den folgenden Schätzwerten planen:

- 100 bis 150 KBit/s mittlere Bandbreite für einen Desktop mit einfacher Büroproduktivität: typische Büroanwendungen ohne Video- und 3D-Grafikanwendungen mit den Windows- und View-Standard Einstellungen.
- 50 bis 100 KBit/s mittlere Bandbreite für einen Desktop mit optimierter Büroproduktivität: typische Büroanwendungen ohne Video- und 3D-Grafikanwendungen mit optimierten Windows Desktop-Einstellungen und optimierter View-Anwendung.
- 400 bis 600 KBit/s mittlere Bandbreite für virtuelle Desktops mit Verwendung von mehreren Monitoren, 3D, Aero und Office 2010.
- 500 KBit/s bis 1 MBit/s minimale Spitzenbandbreite für die Gewährleistung von Zusatzkapazität für Bursts von Anzeigeänderungen. Im Allgemeinen sollten Sie Ihr Netzwerk mit einer mittleren Bandbreite dimensionieren; eventuell wäre jedoch auch die Spitzenbandbreite denkbar, um Bursts von Imaging-Datenverkehr, die bei Änderungen großer Bildschirmanzeigen entstehen, Rechnung zu tragen.
- 2 MBit/s pro gleichzeitigem Benutzer, der 480p Video ausführt, je nach konfigurierter Frameraten-Begrenzung und Typ des Videos.

Hinweis Der Schätzwert von 50 bis 150 KBit/s pro typischem Benutzer beruht auf der Vorannahme, dass alle Benutzer kontinuierlich arbeiten und ähnliche Aufgaben über einen 8 bis 10 Stunden dauernden Arbeitstag ausführen. Der Wert der 50 KBit/s-Bandbreitennutzung leitet sich aus View Planner-Tests auf einem LAN ab, bei dem die Build-to-Lossless-Funktion deaktiviert ist. Die einzelnen Situationen können sich darin unterscheiden, dass einige Benutzer eventuell öfter inaktiv sind und fast keine Bandbreite nutzen, wodurch mehrere Benutzer pro Verknüpfung möglich sind. Deshalb gelten diese Richtlinien nur als Startpunkt für detailliertere Bandbreiten-Planungen und -Tests.

Im folgenden Beispiel wird gezeigt, wie Sie die Anzahl der gleichzeitigen Benutzer einer Zweigstelle oder einer Außenstelle errechnen können, die über eine T1-Leitung mit 1,5 MBit/s verfügt.

Szenario einer Zweigstelle oder einer Außenstelle

- Die Benutzer verfügen über grundlegende Microsoft Office-Produktivitätsanwendungen, keine Video-Anwendungen, keine 3D-Grafikanwendungen sowie USB-Tastatur- und Mausgeräte.
- Die für jeden typischen Büronutzer erforderliche Bandbreite auf View liegt zwischen 50 und 150 KBit/s.
- Die T1-Netzwerk-Kapazität liegt bei 1,5 MBit/s.
- Die Bandbreitennutzung beträgt 80 Prozent (Nutzungsfaktor von 0,8).

Formel zur Bestimmung der Anzahl unterstützter Benutzer

- Im schlechtesten Fall benötigen die Benutzer 150 KBit/s: $(1,5 \text{ MBit/s} \times 0,8) / 150 \text{ KBit/s} = (1.500 \times 0,8) / 150 = 8$ Benutzer
- Im besten Fall benötigen die Benutzer 50 KBit/s: $(1,5 \text{ MBit/s} \times 0,8) / 50 \text{ KBit/s} = (1.500 \times 0,8) / 50 = 24$ Benutzer

Ergebnis

Diese Außenstelle kann zwischen 8 und 24 gleichzeitige Benutzer pro T1-Leitung mit einer Kapazität von 1,5 MBit/s unterstützen.

Wichtig Eventuell müssen Sie die Desktop-Einstellungen für View und Windows optimieren, um diese Nutzerdichte zu erreichen.

Diese Informationen sind ein Auszug aus dem Informationsleitfaden mit dem Namen *VMware View 5 with PCoIP: Network Optimization Guide (VMware View 5 with PCoIP: Leitfaden zur Netzwerkoptimierung)*.

View-Bausteine

Ein Baustein besteht aus physischen Servern, einer vSphere-Infrastruktur, View-Servern, gemeinsam genutztem Speicher und Desktops auf virtuellen Maschinen für Endbenutzer. Ein View-Pod kann bis zu fünf Bausteine umfassen.

Tabelle 4-12. Beispiel eines LAN-basierten View-Bausteins für 2.000 Desktops auf virtuellen Maschinen

| Element | Beispiel |
|---|--|
| vSphere-Cluster | 1 oder mehr |
| Netzwerk-Switch mit 80 Ports | 1 |
| Gemeinsames Speichersystem | 1 |
| vCenter Server mit View Composer auf demselben Host | 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) |

Mit vSphere 4.1 und höher kann jede vCenter Server-Instanz bis zu 10.000 virtuelle Maschinen unterstützen. So können Sie mit Bausteinen arbeiten, die mehr als 2.000 Desktops auf virtuellen Maschinen enthalten. Die tatsächliche Größe der Bausteine hängt jedoch noch von anderen Beschränkungen ab, die für View spezifisch sind.

Wenn die View-Struktur nur einen Baustein enthält, können Sie zu Redundanz Zwecken zwei View-Verbindungsserver-Instanzen einsetzen.

View-Pods

Ein Pod ist eine Organisationseinheit, die durch Einschränkungen der Skalierbarkeit von View bestimmt wird.

Beispiel einer Struktur mit fünf Bausteinen

Ein herkömmlicher View-Pod integriert fünf Bausteine mit je 2.000 Benutzern, die Sie als eine Einheit verwalten können.

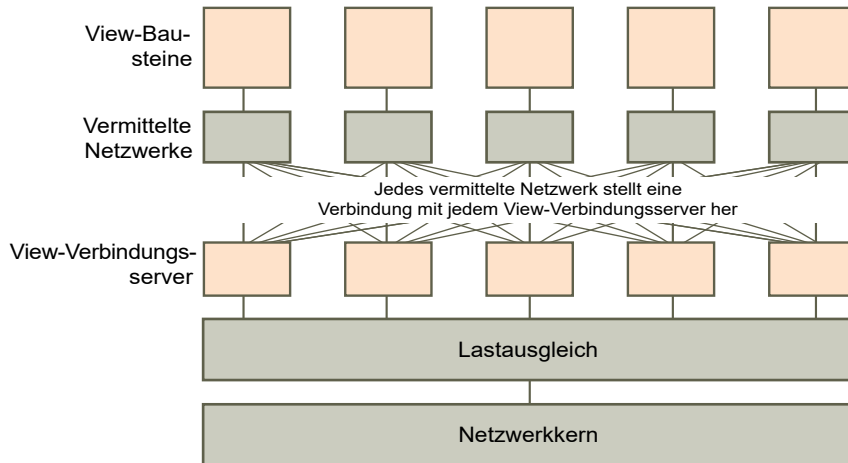
Tabelle 4-13. Beispiel eines LAN-basierten View-Pods aus fünf Bausteinen

| Element | Anzahl bzw. Größe |
|----------------------------------|--|
| Bausteine für einen View-Pod | 5 |
| vCenter Server und View Composer | 5 (1 virtuelle Maschine zum Hosten beider Komponenten in jedem Baustein) |
| Datenbankserver | 5 MS SQL Server- oder Oracle-Datenbankserver (1 eigenständiger Datenbankserver in jedem Baustein) |
| View-Verbindungsserver | 7 (5 für Verbindungen von innerhalb des Unternehmensnetzwerks und 2 für Verbindungen von außerhalb) |
| vLANs | Siehe Tabelle 4-12. Beispiel eines LAN-basierten View-Bausteins für 2.000 Desktops auf virtuellen Maschinen. |
| 10-Gbit-Ethernet-Modul | 1 |
| Modularer Netzwerk-Switch | 1 |

Mit vSphere 4.1 und höher kann jede vCenter Server-Instanz bis zu 10.000 virtuelle Maschinen unterstützen. So können Sie mit Bausteinen arbeiten, die mehr als 2.000 Desktops auf virtuellen Maschinen enthalten. Die tatsächliche Größe der Bausteine hängt jedoch noch von anderen Beschränkungen ab, die für View spezifisch sind.

Bei beiden hier beschriebenen Beispielen kann ein Netzwerkern für eingehende Anforderungen einen Lastausgleich auf den View-Verbindungsserver-Instanzen ausführen. Durch Unterstützung eines Redundanz- und Failover-Mechanismus, zumeist auf Netzwerkebene, kann verhindert werden, dass der Lastausgleichsdienst selbst zu einer Fehlerquelle wird. Das Virtual Router Redundancy Protocol (VRRP) kann beispielsweise mit dem Lastausgleichsdienst kommunizieren, um Redundanz- und Failover-Funktionen hinzuzufügen.

Wenn eine View-Verbindungsserver-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-Verbindungsserver-Instanz verbinden und ihre Desktop-Sitzung an der Stelle fortsetzen können, an der es zum Ausfall gekommen war.

Abbildung 4-2. Pod-Diagramm für 10.000 Desktops mit virtuellen Maschinen

Beispiel-Pod mit einer vCenter Server-Instanz

Der View-Pod im vorherigen Abschnitt bestand aus mehreren Bausteinen. Jeder Baustein unterstützte 2.000 virtuelle Maschinen mit einer einzelnen vCenter Server-Instanz. VMware hat eine Vielzahl von Anfragen von Kunden und Partnern erhalten, die eine einzelne vCenter Server-Instanz für die Verwaltung eines View-Pods verwenden möchten. Der Grund für diese Anforderung ist, dass eine einzelne Instanz von vCenter Server 10.000 virtuelle Maschinen unterstützen kann. Bei Verwendung von View 5.2 und höher können Kunden mit einer einzelnen vCenter Server-Instanz eine Umgebung mit 10.000 Desktops verwalten. In diesem Thema wird eine Architektur beschrieben, die auf einer vCenter Server-Instanz für die Verwaltung von 10.000 Desktops basiert.

Obwohl es möglich ist, eine vCenter Server-Instanz und eine View Composer-Instanz für 10.000 Desktops zu verwenden, entsteht dabei eine einzelne Fehlerquelle. Beim Ausfall dieser vCenter Server-Instanz können für die gesamte Desktop-Bereitstellung keine Betriebs-, Bereitstellungs- und Neuanpassungsvorgänge mehr ausgeführt werden. Aus diesem Grund sollten Sie sich für eine Bereitstellungsarchitektur entscheiden, mit der Ihre Anforderungen im Hinblick auf die Ausfallsicherheit der Komponenten erfüllt werden.

In diesem Beispiel besteht ein Pod mit 10.000 Benutzern aus physischen Servern, einer vSphere-Infrastruktur, View-Servern, gemeinsamem Speicher und 5 Clustern mit je 2.000 virtuellen Desktops.

Tabelle 4-14. Beispiel eines LAN-basierten View-Pods mit einer vCenter Server-Instanz

| Element | Beispiel |
|---|---|
| vSphere-Cluster | 6 (5 Cluster mit einem Linked-Clone-Pool pro Cluster und 1 Infrastruktur-Cluster) |
| vCenter Server | 1 |
| View Composer | 1 (eigenständiger) |
| Datenbankserver | 1 (eigenständiger) MS SQL Server- oder Oracle-Datenbankserver |
| Active Directory Server (Active Directory-Server) | 1 oder 2 |
| View-Verbindungsserver-Instanzen | 5 |

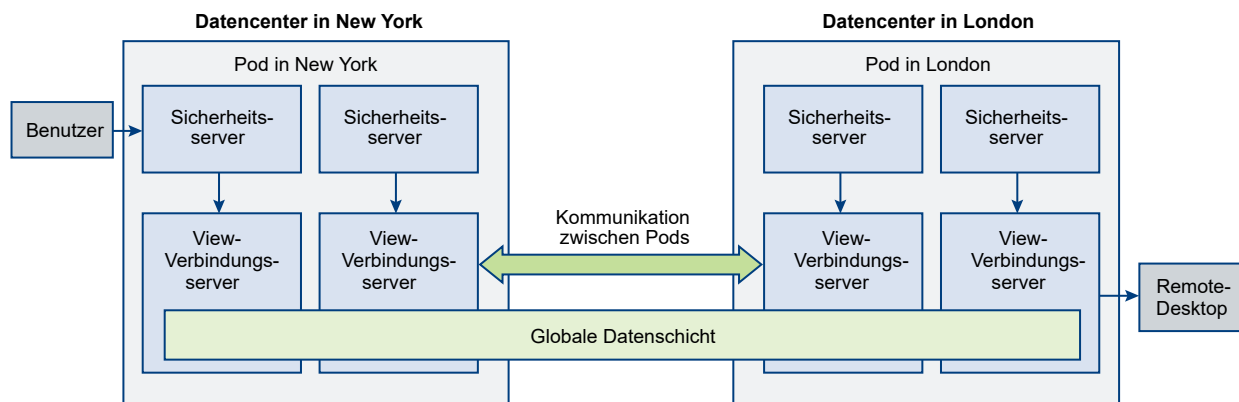
| Element | Beispiel |
|-------------------|---|
| Sicherheitsserver | 5 |
| vLANs | 8 (5 für die Desktop-Pool-Cluster und je 1 für Verwaltung, vMotion und den Infrastruktur-Cluster) |

Cloud Pod Architecture - Übersicht

Zur Verwendung einer Gruppe replizierter View-Verbindungsserver-Instanzen in einem WAN, MAN (Metropolitan Area Network) oder einem anderen Netzwerk, das kein LAN ist, in einer Situation, in der die View-Bereitstellung sich über mehrere Rechenzentren erstrecken muss, müssen Sie die Cloud Pod Architecture-Funktion verwenden.

Diese Funktion verwendet standardmäßige View-Komponenten für die Verwaltung mehrerer Rechenzentren, die globale und flexible Zuordnung zwischen Benutzern und Desktops, die Bereitstellung von Desktops mit hoher Verfügbarkeit sowie die Wiederherstellung nach einem Ausfall (Disaster Recovery). Sie können vier View-Pods verbinden, sodass eine große Umgebung für das Brokering und die Verwaltung von Desktops in zwei Sites entsteht, die sich an unterschiedlichen geografischen Standorten befinden. Auf diese Weise lassen sich 20.000 Remote-Desktops verwalten.

Das folgende Diagramm ist ein Beispiel einer einfachen Cloud Pod Architecture-Topologie.



In der Beispieltopologie werden zwei zuvor eigenständige View-Pods in verschiedenen Rechenzentren zu einem Pod-Verbund kombiniert. Ein Endbenutzer kann in dieser Umgebung eine Verbindung mit einer View-Verbindungsserver-Instanz im Rechenzentrum in New York herstellen und eine Sitzung auf einem Desktop im Rechenzentrum in London erhalten.

Für diese Funktion gelten die folgenden Einschränkungen:

- In dieser Version wird die Verwendung der Funktion HTML Access nicht unterstützt. Bei HTML Access können Endbenutzer mithilfe eines Webbrowsers eine Verbindung mit Remote-Desktops herstellen und müssen keine Clientsoftware auf ihren lokalen Systemen installieren.
- In dieser Version wird die Verwendung von Windows-basierten Remoteanwendungen, die auf einem Microsoft RDS-Host gehostet werden, nicht unterstützt.

Weitere Informationen finden Sie unter *Verwalten der ViewCloud Pod Architecture*.

Vorteile bei Verwendung mehrerer vCenter Server-Instanzen in einer Struktur

Beim Erstellen eines Entwurfs für eine View-Produktionsumgebung mit über 500 Desktops müssen verschiedene Aspekte berücksichtigt werden, um zwischen einer und mehreren vCenter Server-Instanzen abzuwägen.

Ab View 5.2 unterstützt VMware die Verwaltung von bis zu 10.000 virtuellen Desktop-Maschinen innerhalb eines einzelnen View-Pods mit einem einzigen Server, auf dem vCenter 5.1 oder höher installiert ist. Bevor Sie versuchen, 10.000 virtuelle Maschinen mit einer einzigen vCenter Server-Instanz zu verwalten, sollten Sie die folgenden Aspekte berücksichtigen:

- Dauer der Wartungsfenster in Ihrem Unternehmen
- Toleranz von View-Komponentenausfällen
- Häufigkeit von Betriebs-, Bereitstellungs- und Neuanpassungsvorgängen
- Einfachheit der Infrastruktur

Dauer von Wartungsfenstern

Die Einstellungen für parallele Betriebs-, Bereitstellungs- und Neuanpassungsvorgänge für virtuelle Maschinen werden pro vCenter Server-Instanz festgelegt.

| | |
|--|--|
| Pod-Entwürfe mit einer vCenter Server-Instanz | <p>Die Einstellungen für parallele Vorgänge bestimmen, wie viele Vorgänge zu einem bestimmten Zeitpunkt für einen ganzen View-Pod in einer Warteschlange platziert werden können.</p> <p>Wenn Sie z. B. eine maximale Anzahl von 20 parallelen Bereitstellungsvorgängen festlegen und in einem Pod über nur eine vCenter Server-Instanz verfügen, werden die Bereitstellungsvorgänge bei einem Desktop-Pool mit mehr als 20 virtuellen Maschinen serialisiert. Nachdem 20 gleichzeitige Vorgänge in der Warteschlange platziert wurden, muss je ein Vorgang abgeschlossen werden, bevor mit dem nächsten Vorgang begonnen wird. In großen View-Bereitstellungen kann dieser Bereitstellungsvorgang viel Zeit in Anspruch nehmen.</p> |
| Pod-Entwürfe mit mehreren vCenter Server-Instanzen | Jede Instanz kann gleichzeitig 20 virtuelle Maschinen bereitstellen. |

Um sicherzustellen, dass innerhalb eines Wartungsfensters mehr Vorgänge gleichzeitig ausgeführt werden können, können Sie Ihrem Pod mehrere vCenter Server-Instanzen (bis zu fünf) hinzufügen und mehrere Desktop-Pools in vSphere-Clustern bereitstellen, die von verschiedenen vCenter Server-Instanzen verwaltet werden. Ein vSphere-Cluster kann jeweils nur von einer vCenter Server-Instanz verwaltet werden. Um Parallelität über mehrere vCenter Server-Instanzen hinweg zu erreichen, müssen Sie Ihre Desktop-Pools entsprechend bereitstellen.

Toleranz von Komponentenausfällen

vCenter Server wird in View-Pods für Betriebs-, Bereitstellungs- und Neuanpassungsvorgänge (Aktualisierung, Neuzusammenstellung und Neuverteilung) eingesetzt. Nachdem ein Desktop auf einer virtuellen Maschine bereitgestellt und eingeschaltet wurde, hängt View bei der Ausführung normaler Vorgänge nicht von vCenter Server ab.

Da jeder vSphere-Cluster von einer einzelnen vCenter Server-Instanz verwaltet werden muss, stellt dieser Server in jedem View-Entwurf eine einzelne Fehlerstelle dar. Das gleiche Risiko gilt für jede View Composer-Instanz. (Zwischen jeder View Composer- und vCenter Server-Instanz besteht eine 1:1-Zuordnung.) Durch Verwendung eines der folgenden Produkte können die Auswirkungen eines vCenter Server- oder View Composer-Ausfalls reduziert werden:

- VMware vSphere High Availability (HA)
- VMware vCenter Server Heartbeat™
- Kompatible Failover-Produkte anderer Anbieter

Wichtig Um eine dieser Failover-Strategien umzusetzen, darf die vCenter Server-Instanz nicht in einer virtuellen Maschine installiert werden, die Teil des Clusters ist, den die vCenter Server-Instanz verwaltet.

Zusätzlich zu diesen automatisierten Optionen für das vCenter Server-Failover können Sie den ausgefallenen Server auch auf einer neuen virtuellen Maschine oder auf einem neuen physischen Server neu erstellen. Die meisten wichtigen Informationen werden in der vCenter Server-Datenbank gespeichert.

Die Risikotoleranz ist ein wichtiger Faktor bei der Entscheidung, ob in Ihrem Pod-Entwurf eine oder mehrere vCenter Server-Instanzen eingesetzt werden sollen. Wenn es erforderlich ist, Desktop-Verwaltungsaufgaben wie Betriebs- und Neuanpassungsvorgänge für alle Desktops gleichzeitig auszuführen, sollten Sie die Auswirkungen eines Ausfalls jeweils auf eine geringere Anzahl von Desktops beschränken, indem Sie mehrere vCenter Server-Instanzen bereitstellen. Wenn es tolerierbar ist, dass Ihre Desktop-Umgebung für eine längere Zeit nicht verfügbar ist, um Verwaltungs- oder Bereitstellungsvorgänge auszuführen, oder wenn Sie sich für einen manuellen Vorgang für die Wiederherstellung entscheiden, können Sie eine einzelne vCenter Server-Instanz für Ihren Pod bereitstellen.

Häufigkeit von Betriebs-, Bereitstellungs- und Neuanpassungsvorgängen

Bestimmte Betriebs-, Bereitstellungs- und Neuanpassungsvorgänge für Desktops auf virtuellen Maschinen können ausschließlich durch Administratoraktionen initiiert werden, sind üblicherweise vorhersehbar und steuerbar und können auf festgelegte Wartungsfenster beschränkt werden. Andere Betriebs- und Neuanpassungsvorgänge für Desktops auf virtuellen Maschinen werden durch Benutzerverhalten ausgelöst. Dazu zählen u. a. die Verwendung der Einstellungen „Bei Abmeldung aktualisieren“ oder „Bei Abmeldung anhalten“ sowie Skriptaktionen wie die Verwendung von Distributed Power Management (DPM) bei einer längeren Zeit der Benutzerinaktivität, um nicht genutzte ESXi-Hosts auszuschalten.

Wenn für Ihren View-Entwurf keine von Benutzern ausgelösten Betriebs- und Neuanpassungsvorgänge erforderlich sind, ist eine einzelne vCenter Server-Instanz wahrscheinlich ausreichend, um Ihre Anforderungen zu erfüllen. Wenn von Benutzern ausgelöste Betriebs- und Neuanpassungsvorgänge nur selten auftreten, entstehen keine langen Warteschlangen mit diesen Vorgängen. Folglich kommt es für den View-Verbindungsserver auch nicht zu Zeitüberschreitungen, weil er darauf warten muss, dass vCenter Server die angeforderten Vorgänge innerhalb der definierten Grenzwerte für parallele Vorgänge ausführt.

Viele Kunden entscheiden sich für die Bereitstellung von dynamischen Pools und die Verwendung der Einstellung „Bei Abmeldung aktualisieren“ für eine einheitliche Bereitstellung von Desktops ohne veraltete Daten aus früheren Sitzungen. Zu veralteten Daten zählen z. B. nicht zurückgeforderte Seiten in `pagefile.sys` oder in Windows-temp-Dateien. Mit dynamischen Pools lassen sich außerdem die Auswirkungen von schädlicher Software reduzieren, indem Desktops häufig auf einen bekannten „sauberen“ Zustand zurückgesetzt werden.

Einige Kunden senken den Energieverbrauch, indem View so konfiguriert wird, dass nicht verwendete Desktops ausgeschaltet werden. Dadurch kann vSphere DRS (Distributed Resources Scheduler) die ausgeführten virtuellen Maschinen auf einer möglichst geringen Anzahl von ESXi-Hosts konsolidieren. Die nicht genutzten Hosts werden anschließend von VMware Distributed Power Management ausgeschaltet. In solchen Szenarien kann der größeren Anzahl von Betriebs- und Neuanpassungsvorgängen besser Rechnung getragen werden, indem mehrere vCenter Server-Instanzen eingesetzt werden. Denn mit einer solchen Konfiguration werden Zeitüberschreitungen bei der Ausführung der Vorgänge verhindert.

Einfachheit der Infrastruktur

Der Einsatz einer einzelnen vCenter Server-Instanz in einem großen View-Entwurf bietet entscheidende Vorteile, wie z. B. eine zentrale Verwaltung von „optimierten“ Master-Images und übergeordneten virtuellen Maschinen, eine einzige vCenter Server-Ansicht, die auf die View Administrator-Konsolenansicht abgestimmt ist, sowie eine geringere Anzahl von Back-End-Produktionsdatenbanken und -Datenbankservern. Auch die Disaster Recovery-Planung ist bei einer vCenter Server-Instanz einfacher als bei mehreren Instanzen. Sie sollten die Vorteile beim Einsatz mehrerer vCenter Server-Instanzen (z. B. die Dauer von Wartungsfenstern und die Häufigkeit von Betriebs- und Neuanpassungsvorgängen) sorgfältig gegen die Nachteile (z. B. der zusätzliche Aufwand für die Verwaltung der Images übergeordneter virtueller Maschinen und die höhere Anzahl von erforderlichen Infrastrukturkomponenten) abwägen.

Möglicherweise ist ein kombinierter Ansatz für Ihren Entwurf die beste Lösung. Sie können sich für sehr große und relativ statische Pools entscheiden, die von einer vCenter Server-Instanz verwaltet werden, und gleichzeitig mehrere kleinere, dynamischere Desktop-Pools bereitstellen, die von mehreren vCenter Server-Instanzen verwaltet werden. Die beste Strategie für die Aktualisierung vorhandener großer Strukturen besteht darin, zunächst die VMware-Softwarekomponenten Ihrer vorhandenen Struktur zu aktualisieren. Bevor Sie Ihren Pod-Entwurf ändern, sollten Sie die Auswirkungen der Verbesserungen bei den Betriebs-, Bereitstellungs- und Neuanpassungsvorgängen in der neuesten Version auswerten und anschließend mit einer Erweiterung Ihrer Desktop-Pools experimentieren, um das ideale Verhältnis einer höheren Anzahl von großen Desktop-Pools zu ermitteln, die über eine geringere Anzahl von vCenter Server-Instanzen verwaltet werden.

Planen von Sicherheitsfunktionen

5

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

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu Clientverbindungen](#)
- [Auswählen einer Benutzerauthentifizierungsmethode](#)
- [Einschränken des Zugriffs auf Remote-Desktops](#)
- [Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von Remote-Desktops und -Anwendungen](#)
- [Implementieren empfohlener Vorgehensweisen zum Sichern von Clientsystemen](#)
- [Zuweisen von Administratorrollen](#)
- [Vorbereiten des Einsatzes eines Sicherheitsservers](#)
- [Grundlegendes zu View-Kommunikationsprotokollen](#)

Grundlegendes zu Clientverbindungen

Horizon Client und View Administrator kommunizieren mit einem View-Verbindungsserver-Host über sichere HTTPS-Verbindungen. Informationen zum Serverzertifikat auf dem View-Verbindungsserver werden beim SSL-Handshake zwischen Client und Server an den Client übergeben.

Die einleitende Horizon Client-Verbindung zur Benutzerauthentifizierung und zur Auswahl von Remote-Desktops und -Anwendungen wird eingerichtet, wenn ein Benutzer Horizon Client öffnet und einen vollqualifizierten Domännennamen für den View-Verbindungsserver- oder Sicherheitsserver-Host angibt. Die View Administrator-Verbindung wird hergestellt, wenn ein Administrator die View Administrator-URL in einen Web-Browser eingibt.

Während der Installation des View-Verbindungservers wird ein standardmäßiges SSL-Serverzertifikat generiert. Dieses Zertifikat wird SSL-Clients standardmäßig 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 ist 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.

■ Clientverbindungen unter Verwendung des PCoIP Secure Gateway

Wenn Clients über das PCoIP-Anzeigeprotokoll von VMware eine Verbindung mit einem Remote-Desktop oder einer Remote-Anwendung herstellen, kann Horizon Client eine zweite Verbindung mit der PCoIP Secure Gateway-Komponente auf einer View-Verbindungsserver-Instanz oder auf einem Sicherheitsserver herstellen. Diese Verbindung bietet die erforderliche Sicherheit und Konnektivität beim Zugriff auf Remote-Desktops und -Anwendungen über das Internet.

■ Getunnelte Clientverbindungen mit Microsoft RDP

Wenn Benutzer eine Verbindung mit einem Remote-Desktop mithilfe des Microsoft RDP-Anzeigeprotokolls herstellen, kann Horizon Client eine zweite HTTPS-Verbindung mit dem View-Verbindungsserver-Host herstellen. Diese Verbindung wird als Tunnelverbindung bezeichnet, da sie einen Tunnel für den RDP-Datenverkehr darstellt.

■ Direkte Clientverbindungen

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

Clientverbindungen unter Verwendung des PCoIP Secure Gateway

Wenn Clients über das PCoIP-Anzeigeprotokoll von VMware eine Verbindung mit einem Remote-Desktop oder einer Remote-Anwendung herstellen, kann Horizon Client eine zweite Verbindung mit der PCoIP Secure Gateway-Komponente auf einer View-Verbindungsserver-Instanz oder auf einem Sicherheitsserver herstellen. Diese Verbindung bietet die erforderliche Sicherheit und Konnektivität beim Zugriff auf Remote-Desktops und -Anwendungen über das Internet.

Sicherheitsserver umfassen eine PCoIP Secure Gateway-Komponente, die die folgenden Vorteile bietet:

- Im Unternehmensrechenzentrum wird nur Datenverkehr von Remote-Desktops und -Anwendungen der Benutzer verarbeitet, die authentifiziert wurden.
- Benutzer können nur auf Ressourcen zugreifen, für deren Zugriff sie berechtigt sind.
- Diese Verbindung unterstützt PCoIP, ein erweitertes Remote-Anzeige-Protokoll für eine effizientere Netzwerknutzung, indem Videoanzeigepakete nicht in TCP, sondern in UDP gekapselt werden.
- PCoIP wird standardmäßig mithilfe der AES-128-Verschlüsselung geschützt. Sie können die Verschlüsselungsmethode jedoch in AES-256 ändern.

- Sofern PCoIP nicht durch eine Netzwerkkomponente blockiert wird, ist kein VPN erforderlich.
Beispiel: Beim Versuch, von einem Hotelzimmer aus auf einen Remote-Desktop oder eine Remote-Anwendung zuzugreifen, stellt der Benutzer möglicherweise fest, dass der vom Hotel verwendete Proxy nicht für die Übertragung über PCoIP konfiguriert ist.

Weitere Informationen finden Sie unter [Firewall-Regeln für Sicherheitsserver im Umkreisnetzwerk](#).

Sicherheitsserver mit PCoIP-Unterstützung werden unter den Betriebssystemen Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2 ausgeführt und nutzen die 64 Bit-Architektur umfassend. Diese Sicherheitsserver können zudem Intel-Prozessoren mit Unterstützung für AESNI (AES New Instructions) für eine optimierte Leistung bei der PCoIP-Verschlüsselung/-Entschlüsselung nutzen.

Getunnelte Clientverbindungen mit Microsoft RDP

Wenn Benutzer eine Verbindung mit einem Remote-Desktop mithilfe des Microsoft RDP-Anzeigeprotokolls herstellen, kann Horizon Client eine zweite HTTPS-Verbindung mit dem View-Verbindungsserver-Host herstellen. 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 HTTPS-Verbindung auf mehrere Desktops zugreifen, wodurch der gesamte Protokoll-Overhead reduziert wird.
- Da 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-Verbindungsserver-Instanzen endet die sichere HTTPS-Verbindung beim View-Verbindungsserver. In einer Bereitstellung mit Umkreisnetzwerk (DMZ) endet die sichere HTTPS-Verbindung beim Sicherheitsserver. Informationen zu DMZ-Bereitstellungen und Sicherheitsservern finden Sie unter [Vorbereiten des Einsatzes eines Sicherheitsservers](#).

Clients, die das PCoIP-Anzeigeprotokoll verwenden, können die Tunnelverbindung zur USB-Umleitung und MMR-Beschleunigung (Multimedia Redirection) nutzen. Für alle anderen Daten verwendet PCoIP jedoch das PCoIP Secure Gateway auf einem Sicherheitsserver. Weitere Informationen finden Sie unter [Clientverbindungen unter Verwendung des PCoIP Secure Gateway](#).

Direkte Clientverbindungen

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

Bei direkten Clientverbindungen wird zwar zur Authentifizierung von Benutzern und zur Auswahl von Remote-Desktops und -anwendungen eine HTTPS-Verbindung zwischen dem Client und dem View-Verbindungsserver-Host aufgebaut, aber die zweite HTTPS-Verbindung (die Tunnelverbindung) wird nicht verwendet.

Für direkte PCoIP-Verbindungen sind die folgenden integrierten Sicherheitsfunktionen verfügbar:

- PCoIP unterstützt die AES-Verschlüsselung (Advanced Encryption Standard), die standardmäßig eingeschaltet ist, und verwendet IP Security (IPsec).
- PCoIP arbeitet mit VPN-Clients anderer Anbieter zusammen.

Bei Clients, die mit dem Microsoft-Anzeigeprotokoll RDP arbeiten, dürfen direkte Clientverbindungen mit Remote-Desktops nur verwendet werden, wenn sich Ihre Bereitstellung innerhalb eines Firmennetzwerks befindet. Bei direkten Clientverbindungen wird RDP-Datenverkehr unverschlüsselt über die Verbindung zwischen dem Client und der virtuellen Desktop-Maschine gesendet.

Auswählen einer Benutzerauthentifizierungsmethode

View nutzt die vorhandene Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Um eine zusätzliche Sicherheitsebene zu schaffen, können Sie View in Zwei-Faktor-Authentifizierungslösungen wie RSA SecurID und RADIUS und Smart Card-Authentifizierungslösungen integrieren.

- **Active Directory-Authentifizierung**

Jede View-Verbindungsserver-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.

- **Verwenden der zweistufigen Authentifizierung**

Sie können eine View-Verbindungsserver-Instanz konfigurieren, sodass Benutzer eine RSA SecurID-Authentifizierung oder RADIUS (Remote Authentication Dial-In User Service)-Authentifizierung verwenden müssen.

- **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. Ein vom US-Verteidigungsministerium verwendeter Smartcard-Typ wird als Common Access Card (CAC) bezeichnet.

- **Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist**

Wenn Benutzer mit Horizon Client für Windows das Kontrollkästchen **Anmelden als aktueller Benutzer** aktivieren, werden die Anmeldeinformationen, die sie bei der Anmeldung am Clientsystem angegeben haben, für die Authentifizierung an der View-Verbindungsserver-Instanz und am Remote-Desktop verwendet. Es ist keine weitere Benutzerauthentifizierung erforderlich.

Active Directory-Authentifizierung

Jede View-Verbindungsserver-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.

Wenn eine View-Verbindungsserver-Instanz beispielsweise 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 Horizon Client mit der View-Verbindungsserver-Instanz verbinden. Bei diesem Treuhandvertrag muss es sich um eine externe, nicht transitive bidirektionale Vertrauensbeziehung handeln.

Ähnlich verhält es sich auch, wenn eine Vertrauensstellung zwischen Domäne A und einem MIT Kerberos-Bereich in einer gemischten Domänenumgebung besteht: Die Benutzer aus dem Kerberos-Bereich können den Kerberos-Bereichsnamen auswählen, wenn sie sich über Horizon Client mit der View-Verbindungsserver-Instanz verbinden.

View-Verbindungsserver 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-Verbindungsserver 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 bei ihren Remote-Desktops und -Anwendungen anmelden.

Über die Befehlszeilenschnittstelle `vdmadmin` können Administratoren eine Domänenfilterung konfigurieren, mit deren Hilfe die Domänen eingeschränkt werden, die eine View-Verbindungsserver-Instanz durchsucht und die den Benutzer angezeigt werden. Weitere Informationen finden Sie im Dokument *Verwaltung von View*.

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.

Verwenden der zweistufigen Authentifizierung

Sie können eine View-Verbindungsserver-Instanz konfigurieren, sodass Benutzer eine RSA SecurID-Authentifizierung oder RADIUS (Remote Authentication Dial-In User Service)-Authentifizierung verwenden müssen.

- RADIUS unterstützt ein breites Spektrum an alternativen tokenbasierten Zwei-Faktor-Authentifizierungsmöglichkeiten.
- View bietet auch eine offene Standarderweiterungsschnittstelle, die es Drittanbietern ermöglicht, fortschrittliche Authentifizierungserweiterungen in View zu integrieren.

Da Zwei-Faktor-Authentifizierungslösungen wie RSA SecurID und RADIUS mit Authentifizierungsmanagern arbeiten, die auf separaten Servern installiert sind, müssen Sie diese Server für den View-Verbindungsserver-Host konfigurieren und zugänglich machen. Wenn Sie beispielsweise RSA SecurID verwenden, wäre RSA Authentication Manager der Authentifizierungsmanager. Wenn Sie RADIUS verwenden, wäre der Authentifizierungsmanager ein RADIUS-Server.

Für die Verwendung der Zwei-Faktor-Authentifizierung muss jeder Benutzer über einen Token wie einen RSA SecurID-Token verfügen, der bei seinem Authentifizierungsmanager registriert ist. Bei einem Zwei-Faktor-Authentifizierungstoken handelt es sich um Hardware oder Software, über die in festgelegten Intervallen ein Authentifizierungscode generiert wird. Oft erfordert die Authentifizierung Kenntnis einer PIN und eines Authentifizierungscodes.

Wenn es mehrere View-Verbindungsserver-Instanzen gibt, können Sie die Zwei-Faktor-Authentifizierung für einige Instanzen konfigurieren und für andere eine andere Benutzerauthentifizierungsmethode einrichten. Sie können beispielsweise die Zwei-Faktor-Authentifizierung nur für Benutzer konfigurieren, die von außerhalb des Firmennetzwerks über das Internet auf Remote-Desktops und -Anwendungen zugreifen.

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. Ein vom US-Verteidigungsministerium verwendeter Smartcard-Typ wird als Common Access Card (CAC) bezeichnet.

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

Alle Clientverbindungen, einschließlich Clientverbindungen, die die Smartcard-Authentifizierung verwenden, sind für SSL aktiviert.

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. Informationen dazu, ob ein bestimmter Horizon Client-Typ Smartcards unterstützt, finden Sie in der Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist

Wenn Benutzer mit Horizon Client für Windows das Kontrollkästchen **Anmelden als aktueller Benutzer** aktivieren, werden die Anmeldeinformationen, die sie bei der Anmeldung am Clientsystem angegeben haben, für die Authentifizierung an der View-Verbindungsserver-Instanz und am Remote-Desktop verwendet. Es ist keine weitere Benutzerauthentifizierung erforderlich.

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

- Auf der View-Verbindungsserver-Instanz werden Anmeldedaten verschlüsselt und in der Benutzersitzung zusammen mit dem Benutzernamen, der Domäne und dem optionalen UPN gespeichert. Die Anmeldeinformationen werden hinzugefügt, wenn eine Authentifizierung erfolgt, und gelöscht, wenn das Sitzungsobjekt zerstört wird. Das Sitzungsobjekt wird zerstört, 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 in View LDAP oder in einer Datei auf der Festplatte gespeichert.
- Auf dem Clientsystem werden die Anmeldedaten der Benutzer verschlüsselt in einer Tabelle im Authentication Package, einer Komponente von Horizon Client, gespeichert. Die Anmeldeinformationen 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 mit Gruppenrichtlinieneinstellungen von Horizon Client die Verfügbarkeit des Kontrollkästchens **Als aktueller Benutzer anmelden** steuern und seine Standardeinstellung festlegen. Außerdem können Administratoren mithilfe einer Gruppenrichtlinie festlegen, welche View-Verbindungsserver-Instanzen die Benutzeridentitäts- und Anmeldedaten akzeptieren, die übergeben werden, wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** in Horizon Client aktiviert ist.

Für die Funktion „Anmelden als aktueller Benutzer“ gelten folgende Einschränkungen und Anforderungen:

- Wenn die Smartcard-Authentifizierung auf einer View-Verbindungsserver-Instanz erforderlich ist, schlägt die Authentifizierung bei Benutzern fehl, die das Kontrollkästchen **Anmelden als aktueller Benutzer** aktiviert haben, wenn sie eine Verbindung zur View-Verbindungsserver-Instanz herstellen. Diese Benutzer müssen sich bei der Anmeldung an View-Verbindungsserver erneut mit ihrer Smartcard und ihrer PIN authentifizieren.
- Die Uhrzeit auf dem System, an dem sich der Client anmeldet, und die Uhrzeit auf dem View-Verbindungsserver-Host müssen synchronisiert werden.
- Wenn die standardmäßige Zuweisung des Benutzerrechts **Auf diesen Computer vom Netzwerk aus zugreifen** auf dem Clientsystem geändert wird, muss die Änderung gemäß Beschreibung in VMware Knowledge Base-Artikel 1025691 erfolgen.
- Die Client-Maschine muss in der Lage sein, mit dem Active Directory-Unternehmensserver zu kommunizieren, und darf keine zwischengespeicherten Anmeldedaten für die Authentifizierung verwenden. Wenn sich Benutzer beispielsweise von außerhalb des Unternehmensnetzwerks bei ihren Client-Maschinen anmelden, werden zwischengespeicherte Anmeldedaten für die Authentifizierung verwendet. Wenn der Benutzer dann versucht, eine Verbindung mit einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz herzustellen, ohne zunächst eine VPN-Verbindung herzustellen, wird der Benutzer aufgefordert, Anmeldedaten anzugeben, und die Funktion „Als aktueller Benutzer anmelden“ funktioniert nicht.

Einschränken des Zugriffs auf Remote-Desktops

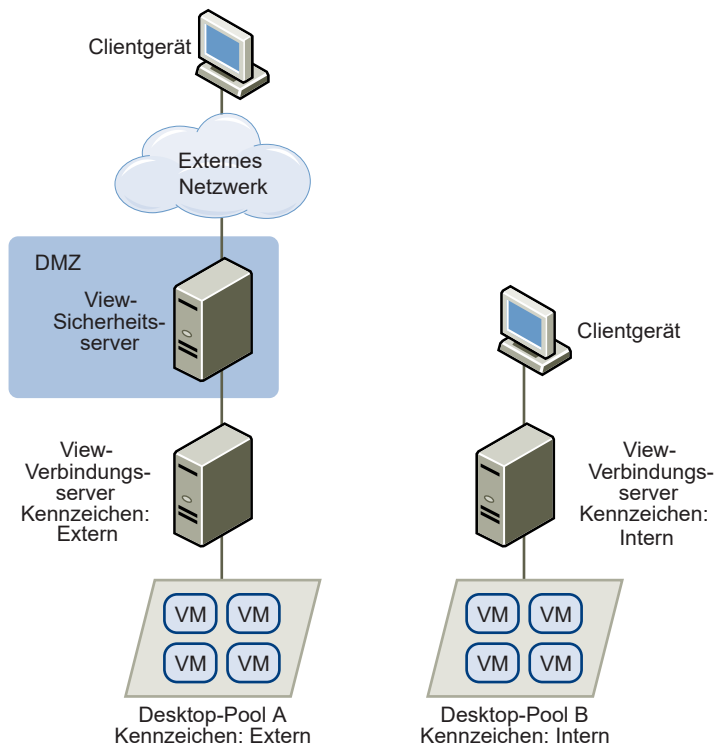
Mithilfe der Einschränkungsfunktion für Berechtigungen können Sie den Zugriff auf Remote-Desktops basierend auf der View-Verbindungsserver-Instanz einschränken, mit der sich ein Benutzer verbindet.

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

Angenommen, Ihre View-Bereitstellung umfasst zwei View-Verbindungsserver-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-Verbindungsserver-Instanz zu, die die internen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Extern“ der View-Verbindungsserver-Instanz zu, die mit dem Sicherheitsserver kombiniert wird 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 bei der als „Extern“ gekennzeichneten View-Verbindungsserver-Instanz anmelden. Ebenso können interne Benutzer keine als „Extern“ gekennzeichneten Desktop-Pools sehen, da sie sich bei der als „Intern“ gekennzeichneten View-Verbindungsserver-Instanz anmelden. [Abbildung 5-1. Beispiel für eingeschränkte Berechtigungen](#) 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-Verbindungsserver-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-Verbindungsserver-Instanz anzumelden.

Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von Remote-Desktops und -Anwendungen

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

Beispielsweise können Sie Gruppenrichtlinieneinstellungen zum Durchführen der folgenden Aufgaben verwenden.

- Angeben der View-Verbindungsserver-Instanzen, die Benutzeridentitäts- und Anmeldeinformationen akzeptieren können, die übergeben werden, wenn ein Benutzer das Kontrollkästchen **Als aktueller Benutzer anmelden** in Horizon Client für Windows aktiviert.
- Aktivieren von Single Sign-On für die Smartcard-Authentifizierung in Horizon Client.

- Konfigurieren der Server-SSL-Zertifikatprüfung in Horizon Client.
- Verhindern, dass Benutzer Anmeldeinformationen über die Horizon Client-Befehlszeilenoptionen bereitstellen.
- Verhindern, dass Systeme, die Horizon Client nicht verwenden, über RDP eine Verbindung mit Remote-Desktops herstellen. Sie können über diese Richtlinie festlegen, dass Verbindungen über Horizon Client verwaltet werden müssen. Folglich müssen Benutzer View verwenden, um Verbindungen mit Remote-Desktops herzustellen.

Im Dokument *Einrichten von Desktop- und Anwendungspools in View* finden Sie Informationen zur Verwendung von Gruppenrichtlinieneinstellungen für Remote-Desktops und Horizon Client.

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.

Eine umfassende Referenz zu allen Sicherheitsfunktionen, die View bietet, finden Sie im Dokument *Sicherheit von View*.

Zuweisen von Administratorrollen

Eine wichtige Verwaltungsaufgabe in einer View-Umgebung besteht darin festzustellen, wer View Administrator verwenden kann und zur Ausführung welcher Aufgaben diese Benutzer autorisiert sind.

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-Verbindungsserver-Instanz, in der eine Teilmenge der View-Verbindungsserver-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-Verbindungsserver ein Paar und leitet den gesamten Datenverkehr an diese Instanz weiter. Sie können mehrere Sicherheitsserver zu einem einzelnen Verbindungsserver kombinieren. Dieses Konzept bietet eine weitere Sicherheitsebene, indem die View-Verbindungsserver-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-Verbindungsserver-Instanzen im internen Netzwerk konfigurieren. Informationen zu bestimmten Ports finden Sie unter [Firewall-Regeln für Sicherheitsserver im Umkreisnetzwerk](#).

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

Hinweis Sicherheitsserver umfassen ein PCoIP Secure Gateway, sodass Clients, die das PCoIP-Anzeigeprotokoll verwenden, anstelle eines VPNs einen Sicherheitsserver verwenden können.

Informationen über das Einrichten von VPNs für die Nutzung von PCoIP finden Sie in den VPN-Lösungsdokumenten, die im Abschnitt „Technology Partner Resources“ des Technical Resource Centers unter <http://www.vmware.com/products/view/resources.html> zur Verfügung stehen.

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.

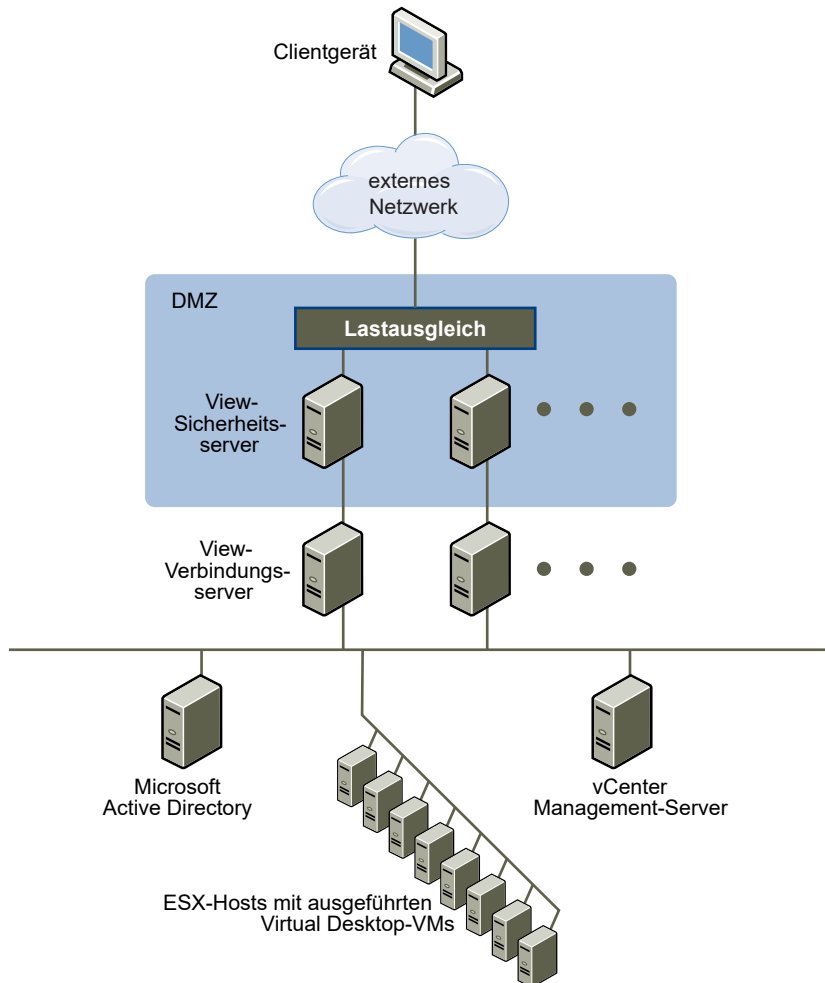
Um den Geltungsbereich von Frame-Broadcasts einzuschränken, sollten View-Verbindungsserver-Instanzen, die mit Sicherheitsservern ein Paar bilden, in einem isolierten Netzwerk bereitgestellt werden. Mit dieser Topologie kann ein böswilliger Benutzer im internen Netzwerk daran gehindert werden, die Kommunikation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

Alternativ dazu können Sie möglicherweise erweiterte Sicherheitsfunktionen in Ihrem Netzwerk-Switch einsetzen, um die böswillige Überwachung der Sicherheitsserver- und View-Verbindungsserver-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.

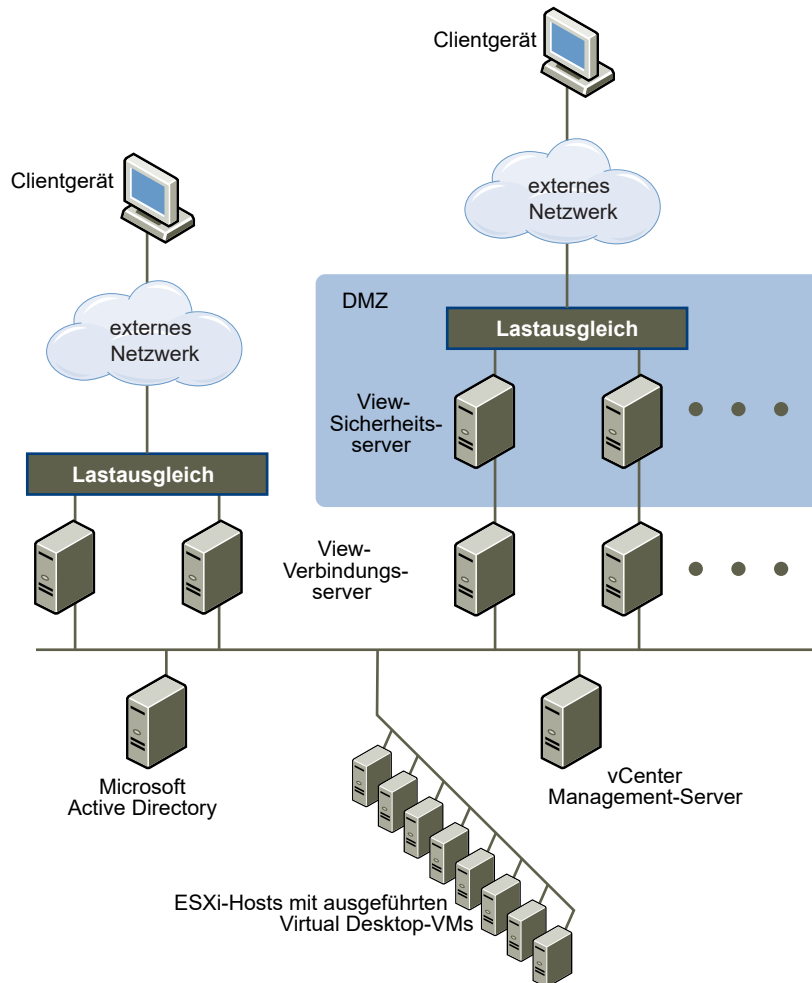
Die Topologie in [Abbildung 5-2. Sicherheitsserver mit Lastausgleich in einem Umkreisnetzwerk](#) zeigt eine hochverfügbare Umgebung mit zwei mit Lastausgleich arbeitenden Sicherheitsservern in einem DMZ. Die Sicherheitsserver im Umkreisnetzwerk kommunizieren mit zwei View-Verbindungsserver-Instanzen innerhalb des internen Netzwerks.

Abbildung 5-2. Sicherheitsserver mit Lastausgleich in einem Umkreisnetzwerk

Wenn Benutzer sich von außerhalb des Firmennetzwerks mit einem Sicherheitsserver verbinden, müssen sie sich erfolgreich authentifizieren, bevor sie auf Remote-Desktops und -Anwendungen zugreifen können. Bei entsprechenden Firewall-Regeln auf beiden Seiten des DMZ eignet sich diese Topologie für den Zugriff auf Remote-Desktops und -Anwendungen von Clientgeräten aus, die mit dem Internet verbunden sind.

Sie können mit jeder Instanz von View-Verbindungsserver 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. Mehrere Sicherheitsserver](#) zeigt eine Umgebung, in der vier View-Verbindungsserver-Instanzen 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-Verbindungsserver-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-Verbindungsserver arbeitet mit standardmäßigen Lastausgleichslösungen von Drittanbietern zusammen,

Firewalls für Sicherheitsserver im Umkreisnetzwerk

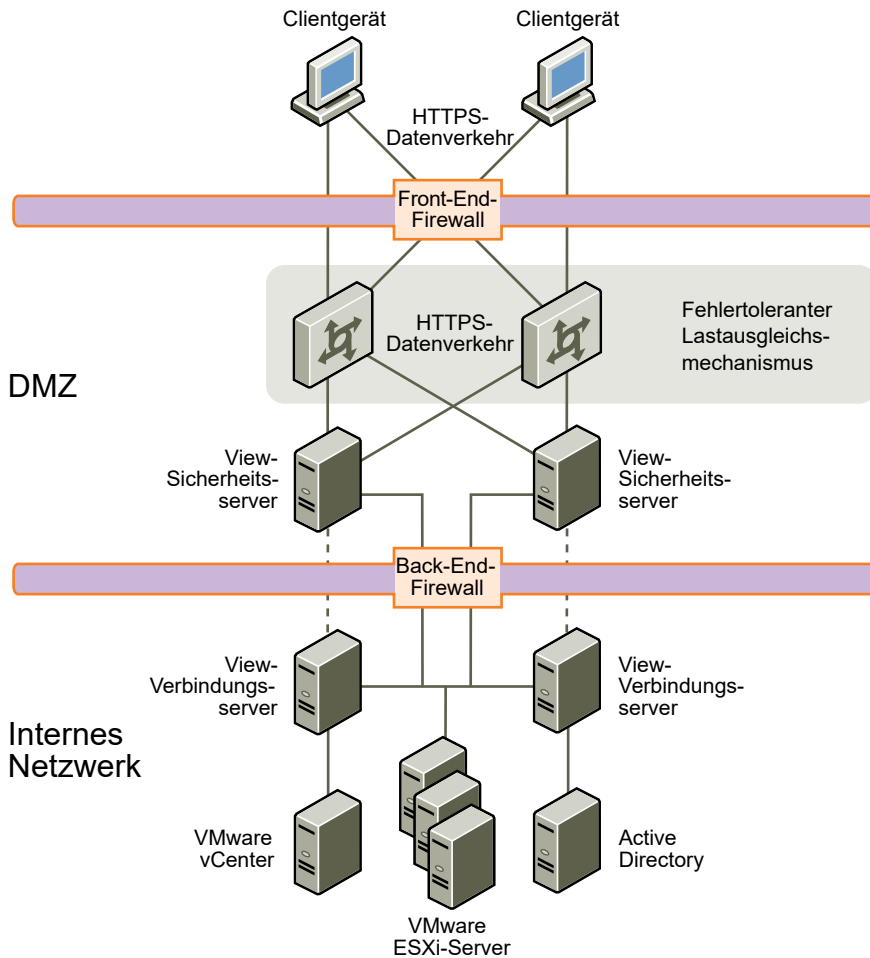
Eine Bereitstellung von Sicherheitsservern in einem Umkreisnetzwerk muss zwei Firewalls aufweisen.

- 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. Zwei-Firewall-Topologie 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. Während der Installation werden View-Dienste standardmäßig für die Überwachung an bestimmten Netzwerkports eingerichtet. Um Organisationsrichtlinien einzuhalten oder Konflikte zu verhindern, können die verwendeten Portnummern bei Bedarf geändert werden.

Wichtig Weitere Einzelheiten und Sicherheitsempfehlungen finden Sie im Dokument *Sicherheit von View*.

Regeln für die Front-End-Firewall

Damit externe Clientgeräte eine Verbindung mit einem Sicherheitsserver in einer DMZ herstellen können, muss die Front-End-Firewall an bestimmten TCP- und UDP-Ports Datenverkehr zulassen. Die Regeln der Front-End-Firewall sind unter [Tabelle 5-1. Regeln für die Front-End-Firewall](#) zusammengefasst.

Tabelle 5-1. Regeln für die Front-End-Firewall

| Quelle | Standardports | Protokoll | Ziel | Standardports | Hinweise |
|-------------------|------------------------------|-----------|-------------------|----------------------|--|
| Horizon Client | TCP beliebig | HTTP | Sicherheitsserver | TCP 80 | (Optional) Externe Clientgeräte verbinden sich mit einem Sicherheitsserver innerhalb des Umkreisnetzwerks an TCP-Port 80 und werden automatisch an HTTPS umgeleitet. Informationen über Sicherheitsüberlegungen im Zusammenhang mit dem Zulassen von Benutzerverbindungen über HTTP anstelle von HTTPS finden Sie im Handbuch <i>Sicherheit von View</i> . |
| Horizon Client | TCP beliebig | HTTPS | Sicherheitsserver | TCP 443 | Externe Clientgeräte stellen die Verbindung mit einem Sicherheitsserver innerhalb der DMZ an TCP-Port 443 her, um mit einer Verbindungsserver-Instanz und Remote-Desktops und -anwendungen zu kommunizieren. |
| Horizon Client | TCP beliebig UDP beliebig | PCoIP | Sicherheitsserver | TCP 4172 UDP 4172 | Externe Clientgeräte stellen die Verbindung mit einem Sicherheitsserver innerhalb der DMZ an TCP-Port 4172 und UDP-Port 4172 her, um mit einem Remote-Desktop oder -anwendung über PCoIP zu kommunizieren. |
| Sicherheitsserver | UDP 4172 | PCoIP | Horizon Client | UDP beliebig | Sicherheitsserver senden PCoIP-Daten zurück an ein externes Clientgerät von UDP-Port 4172. Der UDP-Zielpart ist der Quellport der empfangenen UDP-Pakete. Da diese Pakete Antwortdaten enthalten, ist es normalerweise nicht erforderlich, für diesen Datenverkehr eine explizite Firewallregel hinzuzufügen. |
| Client-Webbrowser | TCP beliebig | HTTPS | Sicherheitsserver | TCP 8443 | Bei Verwendung von HTML Access stellt der externe Web Client an HTTPS-Port 8443 eine Verbindung mit einem Sicherheitsserver innerhalb der DMZ her, um mit Remote-Desktops zu kommunizieren. |

Regeln für die Back-End-Firewall

Um einem Sicherheitsserver die Kommunikation mit den einzelnen View-Verbindungsserver-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 Remote-Desktopanwendungen und View-Verbindungsserver-Instanzen miteinander kommunizieren können. Die Regeln der Back-End-Firewall sind unter [Tabelle 5-2. Regeln für die Back-End-Firewall](#) zusammengefasst.

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

| Quelle | Standardports | Protokoll | Ziel | Standardports | Hinweise |
|-------------------|---------------|-----------|-------------------|---------------|--|
| Sicherheitsserver | UDP 500 | IPSec | Verbindungsserver | UDP 500 | Sicherheitsserver verhandeln IPSec mit den einzelnen View-Verbindungsserver-Instanzen an UDP-Port 500. |
| Verbindungsserver | UDP 500 | IPSec | Sicherheitsserver | UDP 500 | View-Verbindungsserver-Instanzen antworten auf Sicherheitsserver an UDP-Port 500. |

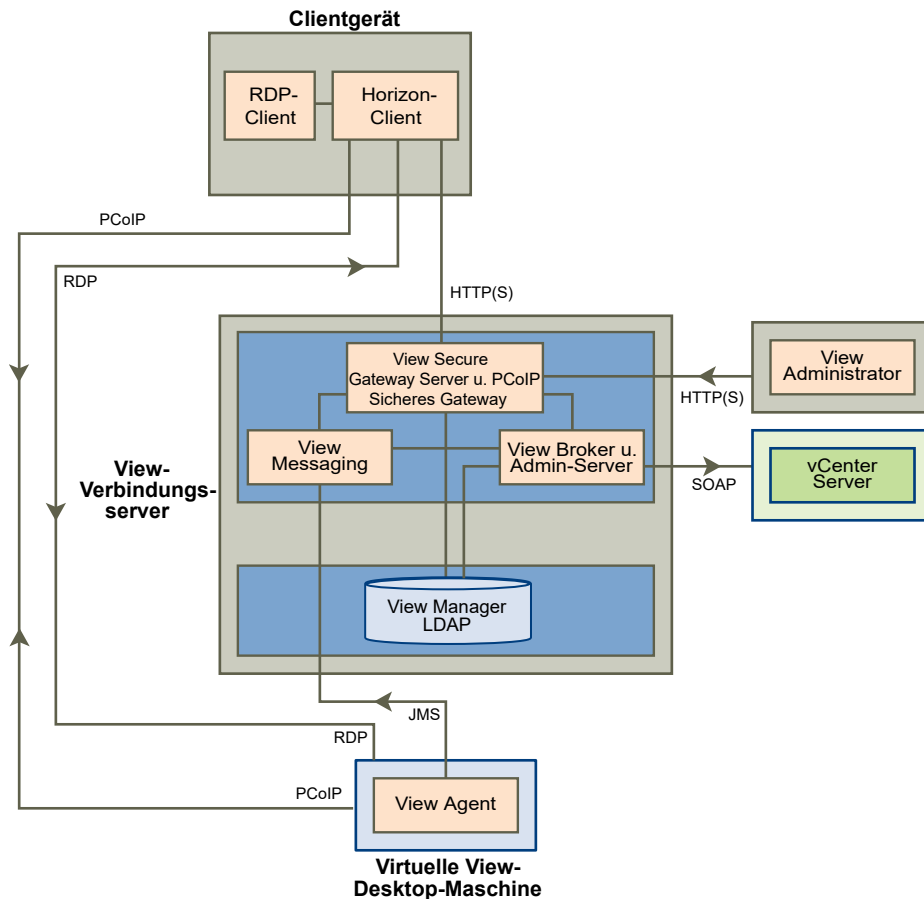
| Quelle | Standard ports | Protokoll | Ziel | Standard ports | Hinweise |
|--------------------------------|---------------------------|-----------------|--------------------------------|----------------------|---|
| Sicherheitsserver | UDP 4500 | NAT-T ISAKMP | Verbindungsserver | UDP 4500 | Erforderlich, wenn zwischen dem Sicherheitsserver und der View-Verbindungsserver-Instanz, mit der der Sicherheitsserver kombiniert ist, NAT verwendet wird. Sicherheitsserver verwenden UDP-Port 4500 für NAT-Traversal und zum Aushandeln der IPsec-Sicherheit. |
| Verbindungsserver | UDP 4500 | NAT-T ISAKMP | Sicherheitsserver | UDP 4500 | Wenn NAT verwendet wird, reagieren View-Verbindungsserver-Instanzen auf Anfragen von Sicherheitsservern an UDP-Port 4500. |
| Sicherheitsserver | TCP beliebig | AJP13 | Verbindungsserver | TCP 8009 | Sicherheitsserver verbinden sich mit View-Verbindungsserver-Instanzen an TCP-Port 8009, um Web-Datenverkehr von externen Clientgeräten weiterzuleiten. Wenn Sie IPSec aktivieren, verwendet AJP13-Datenverkehr den TCP-Port 8009 nach der Kombination nicht. Stattdessen wird entweder NAT-T (UDP-Port 4500) oder ESP verwendet. |
| Sicherheitsserver | TCP beliebig | JMS | Verbindungsserver | TCP 4001 | Sicherheitsserver verbinden sich mit View-Verbindungsserver-Instanzen an TCP-Port 4001, um Java Message Service (JMS)-Datenverkehr auszutauschen. |
| Sicherheitsserver | TCP beliebig | RDP | Remote-Desktop | TCP 3389 | Sicherheitsserver stellen an TCP-Port 3389 eine Verbindung mit Remote-Desktops her, um RDP-Datenverkehr auszutauschen. |
| Sicherheitsserver | TCP beliebig | MMR | Remote-Desktop | TCP 9427 | Sicherheitsserver stellen an TCP-Port 9427 eine Verbindung mit Remote-Desktops her, um MMR-Datenverkehr zu empfangen. |
| Sicherheitsserver | TCP beliebig UDP 55000 | PCoIP | Remote-Desktop oder -anwendung | TCP 4172 UDP 4172 | Sicherheitsserver stellen an TCP-Port 4172 und UDP-Port 4172 eine Verbindung mit Remote-Desktops und -anwendungen her, um PCoIP-Datenverkehr auszutauschen. |
| Remote-Desktop oder -anwendung | UDP 4172 | PCoIP | Sicherheitsserver | UDP 55000 | Remote-Desktops und -anwendungen senden PCoIP-Daten von UDP-Port 4172 an einen Sicherheitsserver zurück. Der Ziel-UDP-Port ist der Quell-Port der empfangenen UDP-Datenpakete; da es sich dabei um Antwort-Daten handelt, ist es gewöhnlich nicht nötig, dafür eine explizite Firewallregel hinzuzufügen. |
| Sicherheitsserver | TCP beliebig | USB-R | Remote-Desktop | TCP 32111 | Sicherheitsserver stellen an TCP-Port 32111 eine Verbindung mit Remote-Desktops her, um umgeleiteten USB-Datenverkehr zwischen einem externen Clientgerät und dem Remote-Desktop auszutauschen. |
| Sicherheitsserver | TCP beliebig | HTTPS | Remote-Desktop | TCP 22443 | Wenn Sie HTML Access verwenden, stellen Sicherheitsserver eine Verbindung mit Remote-Desktops an HTTPS-Port 22443 her, um mit dem Blast-Agent zu kommunizieren. |

| Quelle | Standard ports | Protokoll | Ziel | Standard ports | Hinweise |
|-------------------|----------------|-----------|-------------------|----------------|--|
| Sicherheitsserver | | ESP | Verbindungssever | | Gekapselter AJP13-Datenverkehr, wenn keine NAT-Ausnahme erforderlich ist. ESP ist IP-Protokoll 50. Portnummern werden nicht angegeben. |
| Verbindungssever | | ESP | Sicherheitsserver | | Gekapselter AJP13-Datenverkehr, wenn keine NAT-Ausnahme erforderlich ist. ESP ist IP-Protokoll 50. Portnummern werden nicht angegeben. |

Grundlegendes zu View-Kommunikationsprotokollen

View-Komponenten tauschen Nachrichten mithilfe mehrerer Protokolle aus.

[Abbildung 5-5. View-Komponenten und -Protokolle ohne Sicherheitsserver](#) veranschaulicht die Protokolle, die die einzelnen Komponenten für die Kommunikation verwenden, wenn kein Sicherheitsserver konfiguriert ist. Das bedeutet, dass der sichere Tunnel für RDP und das PCoIP Secure Gateway nicht aktiviert sind. Diese Konfiguration kann in einer typischen LAN-Umgebung verwendet werden.

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

Hinweis Diese Abbildung zeigt direkte Verbindungen für Clients, die PCoIP oder RDP verwenden. In der Standardeinstellung werden jedoch direkte Verbindungen für PCoIP und Tunnelverbindungen für RDP verwendet.

In [Tabelle 5-3. Standardports](#) finden Sie die Standardports, die von den einzelnen Protokollen verwendet werden.

[Abbildung 5-6. View-Komponenten und -Protokolle mit Sicherheitsserver](#) veranschaulicht die Protokolle, die die einzelnen Komponenten für die Kommunikation verwenden, wenn ein Sicherheitsserver konfiguriert ist. Diese Konfiguration kann in einer typischen WAN-Umgebung verwendet werden.

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

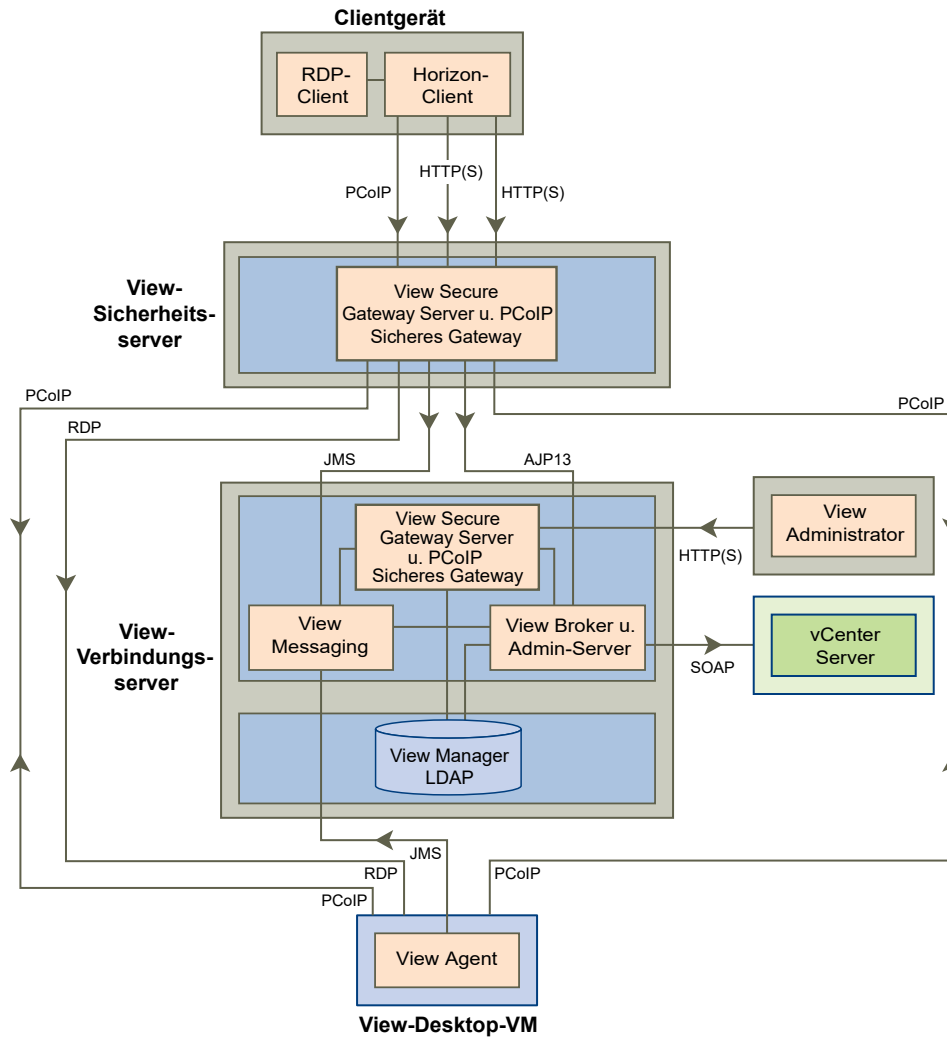


Tabelle 5-3. Standardports zeigt die Standardports, die von den einzelnen Protokollen verwendet werden. Um Organisationsrichtlinien einzuhalten oder Konflikte zu verhindern, können die verwendeten Portnummern bei Bedarf geändert werden.

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 |

| Protokoll | Port |
|----------------|---|
| RDP | TCP-Port 3389 Für MMR wird neben RDP der TCP-Port 9427 verwendet. Hinweis Wenn die View-Verbindungsserver-Instanz für direkte Clientverbindungen konfiguriert ist, können sich diese Protokolle direkt vom Client aus mit dem Remote-Desktop verbinden, ohne getunnelt durch die View Secure Gateway Server-Komponente übertragen zu werden. |
| SOAP | TCP-Port 80 oder 443 |
| PCoIP | Jeder TCP-Port von Horizon Client zum Port 4172 des Remote-Desktops oder der Remote-Anwendung. PCoIP verwendet auch den UDP-Port 50002 von Horizon Client (oder den UDP-Port 55000 vom PCoIP Secure Gateway) zum Port 4172 des Remote-Desktops oder der Remote-Anwendung. |
| PCoIP oder RDP | Für die USB-Umleitung vom Client zum Remote-Desktop wird neben PCoIP oder RDP der TCP-Port 32111 genutzt. |

TCP-Ports für die Kommunikation zwischen View-Verbindungsserver-Instanzen

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

View Broker und Administration Server

Die View Broker-Komponente, die Hauptkomponente eines View-Verbindungservers, ist für die gesamte Benutzerinteraktion zwischen Clients und dem View-Verbindungsserver zuständig. Zu View Broker gehört auch die Komponente Administration Server, die von der View Administrator-Web-Oberfläche verwendet wird.

View Broker arbeitet eng mit vCenter Server zusammen, um eine erweiterte Verwaltung von Remote-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 Clientsystemen und einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz.

Wenn Sie die Tunnelverbindung für View-Verbindungsserver 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 Remote-Desktop verbinden, ohne getunnelt durch die View Secure Gateway Server-Komponente übertragen zu werden.

Hinweis Clients, die das PCoIP-Anzeigeprotokoll verwenden, können die Tunnelverbindung zur USB-Umleitung und MMR-Beschleunigung (Multimedia Redirection) nutzen. Für alle anderen Daten verwendet PCoIP jedoch das PCoIP Secure Gateway auf einem Sicherheitsserver.

View Secure Gateway Server ist auch dafür zuständig, anderen Web-Datenverkehr von Clients an die View Broker-Komponente weiterzuleiten, auch den Datenverkehr, der bei der Benutzerauthentifizierung und bei der Auswahl von Desktops und Anwendungen entsteht. View Secure Gateway Server leitet darüber hinaus Web-Datenverkehr vom View Administrator-Client zur Komponente Administration Server weiter.

PCoIP Secure Gateway

Sicherheitsserver umfassen das PCoIP Secure Gateway. Bei aktiviertem PCoIP Secure Gateway können Clients, die PCoIP verwenden, nach der Authentifizierung eine weitere sichere Verbindung zu einem Sicherheitsserver herstellen. Über diese Verbindung können Clients über das Internet auf Remote-Desktops und -anwendungen zugreifen.

Wenn Sie das PCoIP Secure Gateway aktivieren, wird PCoIP-Datenverkehr von einem Sicherheitsserver an Remote-Desktops und -anwendungen weitergeleitet. Wenn Clients, die PCoIP nutzen, auch die USB-Umleitungsfunktion oder MMR-Beschleunigung (Multimedia Redirection) verwenden, können Sie das sichere View-Gateway zum Weiterleiten dieser Daten aktivieren.

Wenn Sie direkte Clientverbindungen konfigurieren, wird PCoIP-Datenverkehr und anderer Datenverkehr direkt von einem Client an einen Remote-Desktop oder eine Remoteanwendung geleitet.

Wenn Benutzer wie Heim- oder mobile Benutzer über das Internet auf Desktops zugreifen, bieten Sicherheitsserver die erforderliche Sicherheit und Konnektivität, sodass keine VPN-Verbindung benötigt wird. Das PCoIP Secure Gateway gewährleistet, dass im Unternehmensrechenzentrum nur Remote-Datenverkehr der Benutzer verarbeitet wird, die authentifiziert wurden. Endbenutzer können nur auf Ressourcen zugreifen, für deren Zugriff sie berechtigt sind.

View LDAP

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

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

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

View Messaging

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

Diese Komponente unterstützt die JMS-API (Java Message Service), die für die Nachrichtenvermittlung in 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-Verbindungsserver-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-Verbindungsserver

Bestimmte Ports müssen an der Firewall für View-Verbindungsserver-Instanzen und Sicherheitsserver geöffnet werden.

Wenn Sie View-Verbindungsserver installieren, kann das Installationsprogramm optional die erforderlichen Regeln für die Windows-Firewall für Sie konfigurieren. Mit diesen Regeln werden die standardmäßig verwendeten Ports geöffnet. Wenn Sie nach der Installation die Standardports ändern, müssen Sie die Windows-Firewall manuell konfigurieren, damit Horizon Client-Geräte über die aktualisierten Ports eine Verbindung mit View herstellen können.

Wenn Sie HTML Access mit View-Verbindungsserver installieren, konfiguriert das Installationsprogramm die **VMware Horizon View-Verbindungsserver (Blast-In)**-Regel in der Windows-Firewall so, dass der von HTML Access verwendete TCP-Port 8443 geöffnet wird.

Die folgende Tabelle enthält eine Aufstellung der Standardports, die automatisch während der Installation geöffnet werden können. Wenn nicht anders angegeben, handelt es sich hierbei um eingehende Ports.

Tabelle 5-4. Ports, die während der View-Verbindungsserver-Installation geöffnet werden

| Protokoll | Ports | Typ der View-Verbindungsserver-Instanz |
|-----------|--|--|
| JMS | TCP 4001 | Standard- und Replikatserver |
| JMSIR | TCP 4100 | Standard- und Replikatserver |
| AJP13 | TCP 8009 | Standard- und Replikatserver |
| HTTP | TCP 80 | Standard-, Replikat- und Sicherheitsserver |
| HTTPS | TCP 443 | Standard-, Replikat- und Sicherheitsserver |
| PCoIP | TCP 4172 eingehend; UDP 4172 beide Richtungen | Standard-, Replikat- und Sicherheitsserver |
| HTTPS | TCP 8443 | Standard-, Replikat- und Sicherheitsserver. Nachdem die erste Verbindung mit View hergestellt ist, stellt der Webbrowser auf einem Clientgerät an TCP-Port 8443 eine Verbindung mit dem Blast Secure Gateway her. Das Blast Secure Gateway muss auf einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz aktiviert sein, damit diese zweite Verbindung stattfinden kann. |
| HTTPS | TCP 8472 | Standard- und Replikatserver Für die Cloud Pod Architecture-Funktion: für die Interpod-Kommunikation verwendet. |

| Protokoll | Ports | Typ der View-Verbindungsserver-Instanz |
|-----------|-----------|--|
| HTTP | TCP 22389 | Standard- und Replikatserver Für die Cloud Pod Architecture-Funktion: für die globale LDAP-Replikation verwendet. |
| HTTPS | TCP 22636 | Standard- und Replikatserver Für die Cloud Pod Architecture-Funktion: für die sichere globale LDAP-Replikation verwendet. |

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) |

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.

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

Firewall-Regeln für Active Directory

Wenn zwischen der View-Umgebung und dem Active Directory-Server eine Firewall vorhanden ist, müssen Sie sicherstellen, dass alle erforderlichen Ports geöffnet sind.

Zum Beispiel muss View-Verbindungsserver 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.

Überblick über die Schritte zum Einrichten einer View-Umgebung

6

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

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

| Schritt | Aufgabe |
|---------|--|
| 1 | Richten Sie die benötigten Administratoren und Benutzergruppen in Active Directory ein. Anweisungen: <i>Installation von View</i> und vSphere-Dokumentation. |
| 2 | Sofern Sie diese Aufgaben noch nicht ausgeführt haben, müssen Sie zunächst ESXi-Hosts und vCenter Server installieren und einrichten. Anweisungen: VMware vSphere-Dokumentation. |
| 3 | Wenn Sie Linked-Clone-Desktops bereitstellen möchten, installieren Sie View Composer entweder auf dem vCenter Server-System oder auf einem separaten Server. Installieren Sie ebenso die View Composer-Datenbank. Anweisungen: Dokument <i>Installation von View</i> . |
| 4 | Installieren und konfigurieren Sie View-Verbindungsserver. Installieren Sie ebenso die Ereignisdatenbank. Anweisungen: Dokument <i>Installation von View</i> . |
| 5 | Erstellen Sie mindestens eine virtuelle Maschine, die als Vorlage für Desktop-Pools auf Basis vollständiger Klone oder als übergeordnete virtuelle Maschine von Linked-Clone-Desktop-Pools verwendet werden kann. Anweisungen: <i>Einrichten von Desktop- und Anwendungspools in View</i> . |
| 6 | Richten Sie einen RDS-Host ein und installieren Sie Anwendungen, die für Endbenutzer remote ausgeführt werden sollen. |
| 7 | Erstellen Sie Desktop-Pools, Anwendungspools oder beides. Anweisungen: <i>Einrichten von Desktop- und Anwendungspools in View</i> . |
| 8 | Steuern Sie den Benutzerzugriff auf Desktops. Anweisungen: <i>Einrichten von Desktop- und Anwendungspools in View</i> . |
| 9 | Installieren Sie Horizon Client auf den Computern der Endbenutzer und lassen Sie die Endbenutzer auf ihre Remote-Desktops und -anwendungen zugreifen. Anweisungen: Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html . |
| 10 | (Optional) Erstellen und konfigurieren Sie zusätzliche Administratoren, um verschiedene Zugriffsebenen auf bestimmte Bestandsobjekte und -einstellungen zu ermöglichen. Anweisungen: Dokument <i>Verwaltung von View</i> . |

| Schritt | Aufgabe |
|---------|--|
| 11 | <p>(Optional) Konfigurieren Sie Richtlinien, um das Verhalten von View-Komponenten, Desktop- und Anwendungspools und Endbenutzern zu steuern.</p> <p>Anweisungen: <i>Einrichten von Desktop- und Anwendungspools in View.</i></p> |
| 12 | <p>(Optional) Konfigurieren Sie View Persona Management. Die Benutzer erhalten dann bei jeder Anmeldung bei einem Desktop Zugriff auf personalisierte Daten und Einstellungen.</p> <p>Anweisungen: <i>Einrichten von Desktop- und Anwendungspools in View.</i></p> |
| 13 | <p>(Optional) Um eine zusätzliche Sicherheitsebene zu schaffen, können Sie eine Smart Card-Authentifizierungslösung oder eine RADIUS-Zwei-Faktor-Authentifizierungslösung integrieren.</p> <p>Anweisungen: Dokument <i>Verwaltung von View.</i></p> |