

# Planung der Horizon 7-Architektur

13. Dezember 2018

VMware Horizon 7 7.7



vmware®

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

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

Die VMware-Website enthält auch die neuesten Produkt-Updates.

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/de)

# Inhalt

## Planung der Horizon 7 -Architektur 5

### 1 Einführung in Horizon 7 6

Vorteile der Verwendung von Horizon 7 6

Funktionen von Horizon 7 9

Zusammenspiel der Komponenten 12

Integrieren und Anpassen von Horizon 7 17

### 2 Planen einer umfassenden Benutzerumgebung 24

Funktionsunterstützungs-Matrix für Horizon Agent 24

Auswählen eines Anzeigeprotokolls 25

Verwenden veröffentlichter Anwendungen 32

Verwenden von Horizon Persona Management zur Speicherung von Benutzerdaten und -einstellungen 33

Verwenden von USB-Geräten mit Remote-Desktops und -anwendungen 35

Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone 36

Verwenden von 3D-Grafikanwendungen 36

Streaming von Multimediadaten auf einen Remote-Desktop 37

Drucken von einem Remote-Desktop aus 38

Verwenden des Single Sign-On für die Anmeldung 39

Monitore und Bildschirmauflösung 39

### 3 Zentrales Verwalten von Desktop- und Anwendungspools 42

Vorteile von Desktop-Pools 42

Vorteile von Anwendungspools 43

Reduzieren und Verwalten von Speicheranforderungen 44

Anwendungsbereitstellung 55

Verwalten von Benutzern und Desktops mithilfe von Active Directory-Gruppenrichtlinienobjekten 59

### 4 Architekturentwurfselemente und Planungsanleitungen für Remote-Desktop-Bereitstellungen 61

Anforderungen virtueller Maschinen für Remote-Desktops 62

Horizon 7 ESXi -Knoten 68

Desktop-Pools für bestimmte Nutzertypen 69

Konfigurieren virtueller Maschinen für View-Desktops 75

Konfiguration von virtuellen Maschinen als RDS-Hosts 76

vCenter Server - und View Composer-Konfiguration für virtuelle Maschinen 77

Horizon-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen 78

[vSphere -Cluster 82](#)

[Speicher- und Bandbreitenanforderungen 84](#)

[Horizon 7 -Bausteine 96](#)

[Horizon 7 -Pods 96](#)

[Vorteile bei Verwendung mehrerer vCenter Server-Instanzen in einer Struktur 99](#)

## **5 Planen von Sicherheitsfunktionen 103**

[Grundlegendes zu Clientverbindungen 103](#)

[Auswählen einer Benutzerauthentifizierungsmethode 106](#)

[Einschränken des Zugriffs auf Remote-Desktops 110](#)

[Verwenden von Gruppenrichtlinieneinstellungen zum Sichern von Remote-Desktops und -Anwendungen 112](#)

[Verwenden von Intelligente Richtlinien 112](#)

[Implementieren von Best Practices zum Sichern von Clientsystemen 113](#)

[Zuweisen von Administratorrollen 113](#)

[Vorbereiten des Einsatzes eines Sicherheitsservers 114](#)

[Grundlegendes zu Kommunikationsprotokollen 120](#)

## **6 Überblick über die Schritte zum Einrichten einer Horizon 7 -Umgebung 130**

# Planung der Horizon 7 -Architektur

*Planung der Horizon 7-Architektur* enthält eine Einführung zu VMware Horizon™ 7, einschließlich einer Beschreibung der Hauptfunktionen und Bereitstellungsoptionen, sowie einen Überblick darüber, wie die Komponenten üblicherweise in einer Produktionsumgebung eingerichtet werden.

Diese Anleitung liefert Antworten auf die folgenden Fragen:

- Behebt das Produkt die zu lösenden Probleme?
- Wäre es möglich und kostengünstig, diese Lösung in Ihrem Unternehmen zu implementieren?

Nicht alle Funktionen von VMware Horizon 7 sind in allen Editionen verfügbar. 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 sind für Entscheidungsträger im IT-Bereich, Architekten, Administratoren und andere bestimmt, die sich mit den Komponenten und den Möglichkeiten dieses Produkts vertraut machen möchten. Anhand dieser Informationen können Architekten und Planer bestimmen, ob Horizon 7 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 Horizon 7

Mit Horizon 7 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 Horizon 7](#)
- [Funktionen von Horizon 7](#)
- [Zusammenspiel der Komponenten](#)
- [Integrieren und Anpassen von Horizon 7](#)

## Vorteile der Verwendung von Horizon 7

Das Verwalten von Unternehmensdesktops mit Horizon 7 bietet zahlreiche Vorteile: höhere Zuverlässigkeit, Sicherheit, Hardware-Unabhängigkeit und mehr Komfort.

### Zuverlässigkeit und Sicherheit

Desktops und Anwendungen können durch Integration in VMware vSphere<sup>®</sup> und Virtualisierung von Server-, Speicher- und Netzwerkressourcen zentralisiert werden. Das Platzieren von Desktop-Betriebssystemen und Anwendungen auf einem Server im Rechenzentrum bietet folgende 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 VMware Identity Manager 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 mithilfe dieses benutzerdefinierten App-Speichers auf Anwendungen zugreifen.

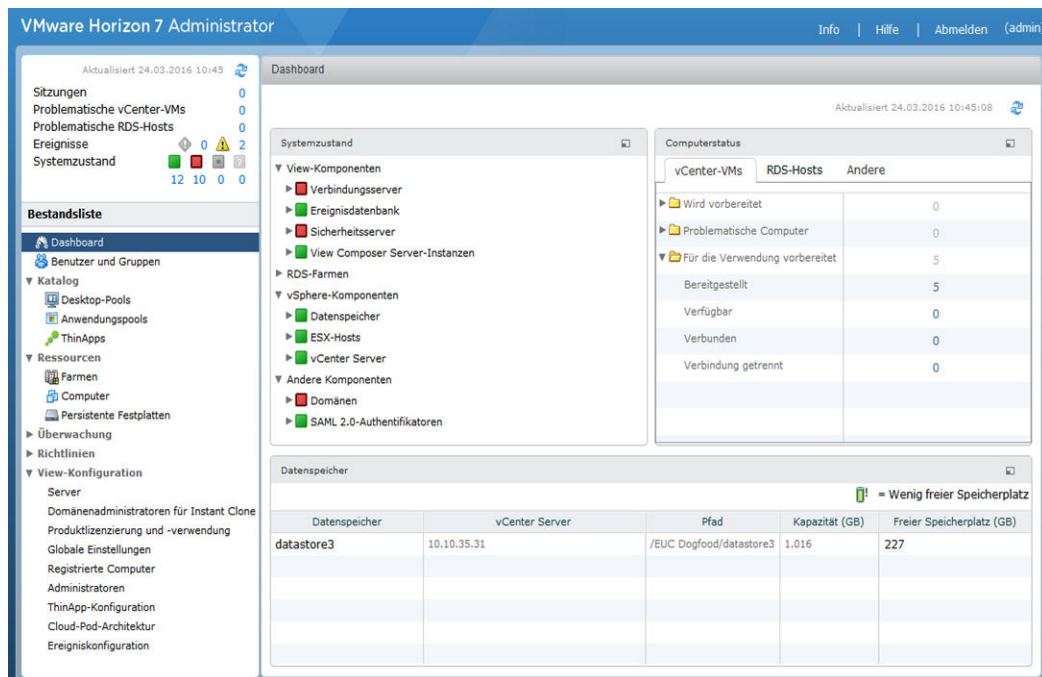
- Durch die Fähigkeit zur Bereitstellung von Remote-Desktops mit vorerstellten Active Directory-Konten können die Anforderungen von gesperrten Active Directory-Umgebungen, in denen nur der Lesezugriff gestattet ist, erfüllt werden.
- Datensicherungen können geplant werden, ohne berücksichtigen zu müssen, 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 Horizon 7-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 zum Ändern von Einstellungen. [Abbildung 1-1](#) bietet ein Beispiel für die browserbasierte Benutzeroberfläche von Horizon Administrator.

**Abbildung 1-1. Verwaltungskonsole mit Dashboard-Anzeige**



Andere Funktionen, die mehr Komfort bieten, sind die VMware-Remote-Anzeigeprotokolle PCoIP (PC-over-IP) und Blast Extreme. Diese Anzeigeprotokolle bieten 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 veröffentlichten Anwendung 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 VMware Identity Manager können IT-Manager die Web-basierte VMware Identity Manager-Verwaltungsoberfläche verwenden, um Benutzer- und Gruppenberechtigungen für Remote-Desktops zu überwachen.
- Die Integration in VMware App Volumes, einem System zur Anwendungsbereitstellung in Echtzeit, ermöglicht Unternehmen eine maßgeschneiderte Bereitstellung und Verwaltung von Anwendungen. Mit App Volumes können Sie Anwendungen selbst dann Benutzern, Gruppen oder Zielcomputern zuordnen, wenn die Benutzer bei ihrem Desktop angemeldet sind. Anwendungen können auch in Echtzeit bereitgestellt, zugestellt, aktualisiert und zurückgezogen werden.
- Mit Horizon Persona Management können physische und virtuelle Desktops zentral verwaltet werden, unter anderem die Einstellungen für Benutzerprofile, Zugriffsberechtigungen für Anwendungen, Richtlinien und die Systemleistung. Persona Management kann für Benutzer von physischen Desktops vor der Umwandlung in virtuelle Desktops bereitgestellt werden.
- Mit VMware User Environment Manager erhalten Endbenutzer einen personalisierten Windows-Desktop, der auf ihre jeweilige Arbeitssituation abgestimmt ist, d. h. der Zugriff auf erforderliche IT-Ressourcen basiert auf Kriterien wie Rolle, Gerät und Standort.
- 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 6.0 oder einer neueren Version können Sie VVOL (virtuelle Volumes) verwenden. Diese Funktion ordnet virtuelle Festplatten und deren Derivate, Klone, Snapshots und Replikate direkt Objekten, die als virtuelle Volumes bezeichnet werden, auf einem Speichersystem zu. Durch diese Zuordnung kann vSphere speicherintensive Vorgänge wie etwa Snapshot-Erstellung, Klonen und Replikation an das Speichersystem auslagern. Beispielsweise dauert ein Klonvorgang, der vorher eine Stunde benötigte, mit VVOL nun möglicherweise nur ein paar Minuten.



- Mit vSphere 5.5 Update 1 oder einer neueren Version können Sie vSAN 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 Horizon 7-Speicherbeschleuniger wird die IOPS-Speicherbelastung erheblich verringert. Damit werden Anmeldungen von Endbenutzern 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 veröffentlichte Anwendungen 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.

Remote-Desktops können auf PCs, Macs, Thin Clients sowie auf PCs ausgeführt werden, die als Thin Clients, Tablets und Smartphones betrieben werden. Die veröffentlichten Anwendungen werden auf einer Teilmenge dieser Geräte ausgeführt. Unterstützung für neue Geräte wird vierteljährlich hinzugefügt.

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

## Funktionen von Horizon 7

Die benutzerfreundlichen Funktionen von Horizon 7 bieten Sicherheit und ermöglichen eine zentrale Steuerung und Skalierbarkeit.

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

- Auf bestimmten Clientgeräten kann von einem virtuellen Desktop auf allen lokalen oder über das Netzwerk verbundenen Druckern gedruckt werden, die auf dem 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.
- Die Umleitung des lokalen Druckers wurde für folgende Drucker entwickelt:
  - Drucker, die direkt mit der USB-Schnittstelle oder mit seriellen Ports auf dem Client verbunden sind.
  - Spezielle Drucker wie z. B. Barcodedrucker und Etikettendrucker, die mit dem Client verbunden sind.
  - Netzwerkdrucker in einem Remotenetzwerk, die nicht von der virtuellen Sitzung angesteuert werden können.
- Mehrere Monitore können eingesetzt werden. Wenn Sie die PCoIP- und Blast Extreme-Anzeigeprotokolle verwenden, können Sie durch die Mehrfachmonitorunterstützung die Anzeigeauflösung und -drehung für jeden Monitor gesondert anpassen.
- 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 Horizon Persona Management, um die Benutzereinstellungen und -daten zwischen den Sitzungen beizubehalten, auch wenn der Desktop aktualisiert oder neu zusammengestellt wurde. Persona Management kann die Benutzerprofile in einem Remoteprofilspeicher (CIFS-Freigabe) in konfigurierbaren Intervallen replizieren.

Sie können auch eine eigenständige Version von Persona Management auf physischen Computern und virtuellen Maschinen, die nicht von Horizon 7 verwaltet werden, verwenden.

Horizon 7 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/TLS-Tunnels zur Gewährleistung, 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 Horizon 7 können Endbenutzeranmeldungen in größerem Umfang mit den gleichen Speicherressourcen abgewickelt werden. Diese Speicherbeschleunigungsfunktion nutzt Funktionen der vSphere 5-Plattform zur Erstellung eines Host-Speicher-caches für gewöhnliche Blockleseroutinen.
- Konfiguration von Horizon-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 von Linked Clones dergestalt, dass Festplattenspeicher eingespart und die Update- und Patch-Verwaltung des Betriebssystems vereinfacht wird
- Mit der in Horizon 7 eingeführten Instant Clone-Funktion können Sie schnell Desktop-Images erstellen, die virtuelle Festplatten und Arbeitsspeicher gemeinsam mit einem übergeordneten Image nutzen. Instant Clones bieten nicht nur die Speicherplatzeffizienz von View Composer-Linked-Clones. Damit wird auch die Verwaltung von Patches und Aktualisierungen des Betriebssystems vereinfacht, da keine Aktualisierung, Neuzusammenstellung und Neuverteilung mehr durchgeführt werden muss. Für Instant Clones ist das Desktop-Wartungsfenster insgesamt nicht mehr erforderlich.

Die folgenden Funktionen ermöglichen eine zentrale Verwaltung:

- Microsoft Active Directory zum Verwalten des Zugriffs auf Remote-Desktops und -anwendungen und zum Verwalten von Richtlinien.
- Persona-Verwaltung zur Vereinfachung und Vereinheitlichung der Migration von physischen auf virtuelle Desktops.
- Die webbasierte Verwaltungskonsole zum ortsunabhängigen Verwalten von Remote-Desktops und -anwendungen.
- Verwendung von Horizon 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 VMware Identity Manager, sodass Endbenutzer über das Webportal für Benutzer auf Remote-Desktops zugreifen und VMware Identity Manager über einen Browser innerhalb eines Remote-Desktops verwenden können.

- Integration in Mirage™ und Horizon FLEX™ 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.

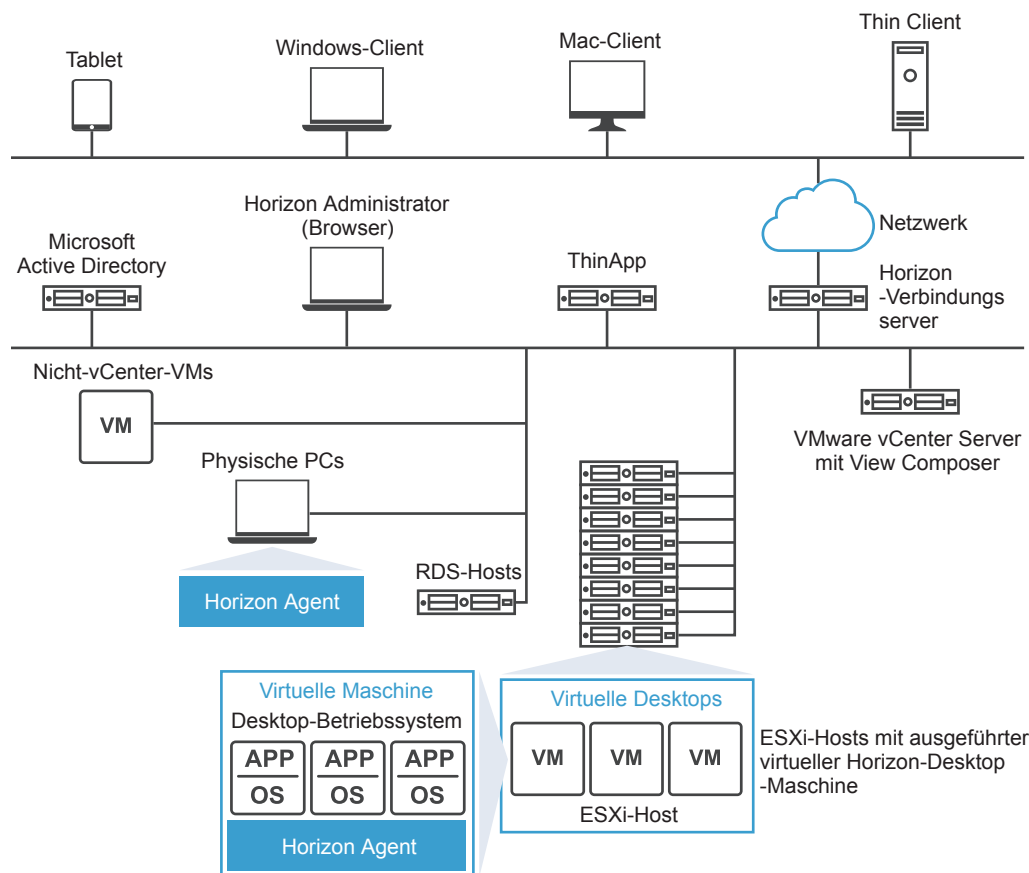
## Zusammenspiel der Komponenten

Endbenutzer starten Horizon Client, um sich beim Horizon-Verbindungsserver anzumelden. Dieser Server, der in Windows Active Directory integriert ist, bietet Zugriff auf Remotedesktops, die auf einem VMware vSphere-Server, einem physischen PC oder einem Microsoft RDS-Host gehostet werden. Horizon Client bietet außerdem Zugriff auf veröffentlichte Anwendungen auf einem Microsoft RDS-Host.

**Hinweis** Horizon 7 unterstützt Domänenfunktionsebenen von Active Directory-Domänendiensten (AD DS). Weitere Informationen zu unterstützten AD DS-Domänenfunktionsebenen finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150351>.

Abbildung 1-2 zeigt die Beziehung zwischen den Hauptkomponenten einer Bereitstellung von Horizon 7.

Abbildung 1-2. Allgemeines Beispiel einer Horizon 7 -Umgebung



## Clientgeräte

Ein Hauptvorteil von Horizon 7 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 Horizon 7 Thin Client-Software und können so konfiguriert werden, dass Benutzer Horizon 7 Thin Client als einzige Anwendung direkt auf dem Gerät starten können. 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 Horizon 7 auf einem Thin Client-Desktop können Sie beispielsweise ein neueres Betriebssystem wie Windows 8.x 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.

## Horizon-Verbindungsserver

Diese Software dient als Vermittler für Clientverbindungen. Der Horizon-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.

Der 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 des Verbindungservers. Deren Konfigurationsdaten werden in einem eingebetteten LDAP-Verzeichnis gespeichert und an die Mitglieder der Gruppe repliziert.

Außerhalb der unternehmenseigenen Firewall können Sie im Umkreisnetzwerk den Verbindungsserver als Sicherheitsserver installieren und konfigurieren oder eine Unified Access Gateway-Appliance installieren. Sicherheitsserver und Unified Access Gateway-Appliances im Umkreisnetzwerk kommunizieren mit Verbindungsserver-Instanzen innerhalb der Firewall des Unternehmens. Mithilfe von Sicherheitsservern und Unified Access Gateway-Appliances wird gewährleistet, dass im Unternehmensrechenzentrum nur der Datenverkehr von Remote-Desktops und -anwendungen der Benutzer verarbeitet wird, die sicher 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 Verbindungsserver wird auf einem Server unter Windows Server 2008 R2 oder Windows Server 2012 R2 installiert, und zwar vorzugsweise auf einer virtuellen VMware-Maschine. Weitere Informationen zu Unified Access Gateway-Appliances finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

---

**Wichtig** Es ist möglich, eine Horizon 7-Konfiguration ohne einen Verbindungsserver zu erstellen. Wenn Sie das Horizon 7 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 genauso wie bei einer Verbindung über den Verbindungsserver. Weitere Informationen finden Sie unter *Verwaltung des Horizon 7 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, Blast Extreme und Microsoft RDP für Remote-Desktops. Geschwindigkeit und Anzeigequalität von PCoIP und Blast Extreme 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. Weitere Informationen finden Sie in der Horizon Client-Dokumentation unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.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. Weitere Informationen finden Sie in der Horizon Client-Dokumentation unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.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 Horizon Connection Server-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 Verbindungsserver zur Verfügung stehen.

Wenn Sie die HTML Access-Funktion verwenden, enthält die Webseite auch einen Link zum Zugriff auf Remote-Desktops und -anwendungen 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://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

## Horizon Agent

Sie installieren den Horizon 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, Horizon Persona Management und Zugriff auf lokal angeschlossene USB-Geräte bereitzustellen.

Wenn die Desktop-Quelle eine virtuelle Maschine ist, installieren Sie den Horizon Agent-Dienst zuerst auf dieser virtuellen Maschine und nutzen Sie anschließend die virtuelle Maschine als Vorlage bzw. als übergeordnetes Element von Linked Clones oder Instant Clones. 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 Horizon-Verbindungsserver herstellen. Sie werden nicht erneut aufgefordert, um eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herzustellen.

## Horizon Administrator

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

Bei der Installation einer Verbindungsserver-Instanz wird die Anwendung Horizon Administrator ebenfalls installiert. Diese Anwendung ermöglicht Administratoren die ortsunabhängige Verwaltung von 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 von Linked Clones anhand einer angegebenen übergeordneten virtuellen Maschine erstellen, wodurch die Speicherkosten um bis zu 90 % reduziert werden.

Jeder Linked Clone fungiert als unabhängiger Desktop (mit eindeutigem/r Hostnamen/IP-Adresse), aber dennoch benötigt der Linked Clone 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.

Sie können auch View Composer zum Erstellen automatischer Farmen von Linked-Clone-Microsoft-RDS-Hosts verwenden und so veröffentlichte Anwendungen für Endbenutzer bereitstellen.

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.

---

**Wichtig** View Composer ist eine optionale Komponente. Für die Bereitstellung von Instant Clones ist die Installation von View Composer nicht erforderlich.

---

## 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 Horizon 7, darunter Horizon Connection Server-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 oder einem Windows Server 2012 R2-Server installieren, und zwar vorzugsweise auf einer virtuellen VMware-Maschine.



## Integrieren und Anpassen von Horizon 7

Zum Verbessern der Effektivität von Horizon 7 in Ihrer Organisation können Sie mehrere Schnittstellen einsetzen, um Horizon 7 in externe Anwendungen zu integrieren oder Verwaltungsskripts zu erstellen, die über die Befehlszeile oder im Batchmodus ausgeführt werden können.

### Integrieren in andere Komponenten

Horizon 7 kann in folgende VMware-Produkte integriert werden.

#### **VMware Cloud on AWS**

VMware Cloud on AWS ermöglicht Ihnen außerdem das Erstellen von vSphere-Rechenzentren auf Amazon Web Services. Diese vSphere-Rechenzentren enthalten vCenter Server für die Verwaltung Ihres Rechenzentrums, vSAN für die Speicherung und VMware NSX für das Netzwerk. Sie können ein lokales Rechenzentrum mit Ihrem Cloud-Software-Defined Data Center verbinden und beide über eine einzelne vSphere Client-Schnittstelle verwalten. Mit einem verbundenen AWS-Konto können Sie von virtuellen Maschinen in Ihrem SDDC auf AWS-Dienste wie EC2 und S3 zugreifen. Weitere Informationen finden Sie in der Dokumentation zu VMware Cloud on AWS unter <https://docs.vmware.com/de/VMware-Cloud-on-AWS/index.html>.

Ab Horizon 7 Version 7.5 können Sie vollständige Horizon 7-Klone in VMware Cloud on AWS bereitstellen. Sie können z. B. eine Horizon 7-Umgebung bereitstellen, die in lokalen Rechenzentren und VMware Cloud on AWS-Instanzen eine Cloud-Pod-Architektur verwendet. So kann Horizon 7 auf einfache Weise in einer Hybrid Cloud-Umgebung ausgeführt und die Verwaltung der SDDC-Infrastruktur an VMware ausgelagert werden.

#### **VMware Identity Manager**

Sie können VMware Identity Manager in Horizon 7 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.

Mit der True SSO-Funktion können Benutzer, die sich mit Smartcards oder der Zwei-Faktor-Authentifizierung authentifizieren, auf ihre Remote-Desktops oder -anwendungen zugreifen, ohne Active Directory-Anmeldeinformationen eingeben zu müssen.

- Endbenutzer können von einem Remote-Desktop aus auf VMware Identity Manager 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 Client-system oder -gerät eine Clientanwendung installieren zu müssen.
- IT-Manager können die browserbasierte Verwaltungskonsole von VMware Identity Manager verwenden, um Benutzer- und Gruppenberechtigungen für Remote-Desktops zu überwachen.

## **VMware Mirage und Horizon FLEX**

Sie können mithilfe von Mirage und Horizon FLEX Anwendungen auf dedizierten Full-Clone-Remote-Desktops bereitstellen und aktualisieren, ohne benutzerinstallierte Anwendungen oder Daten zu überschreiben.

Mirage bietet eine bessere virtuelle Offline-Desktoplösung als die Funktion „Lokaler Modus“, die früher Bestandteil von Horizon 7 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.

## **VMware App Volumes**

VMware App Volumes ist ein integriertes und vereinheitlichtes Anwendungsbereitstellungs- und Benutzerverwaltungssystem für Horizon 7 und andere virtuelle Umgebungen. Von App Volumes verwaltete Daten werden in speziellen VMDKs oder VHDs, den so genannten AppStacks, gespeichert, die beim Anmelden oder Neustarten mit jeder Windows-Benutzersitzung verknüpft werden. Dadurch wird sichergestellt, dass Benutzer die aktuellsten Anwendungen und Daten erhalten. App Volumes stellt auch einen weiteren Container für dauerhafte vom Benutzer installierte Anwendungen und Einstellungen bereit. Dieser wird als beschreibbares Volume bezeichnet und ebenfalls beim Anmelden und Neustarten geladen. Benutzerprofil- und Richtlinieneinstellungen können auch mithilfe der App Volumes-Plattform verwaltet werden.

## **VMware User Environment Manager**

Sie können mit der Funktion „Intelligente Richtlinien“ Richtlinien zur Steuerung des Verhaltens der USB-Umleitung, des virtuellen Druckens, der Zwischenablagenumleitung, der Clientlaufwerksumleitung und der Funktionen für das PCoIP-Anzeigeprotokoll auf bestimmten Remote-Desktops erstellen.

len. Mithilfe von User Environment Manager können IT-Verantwortliche steuern, welche Einstellungen die Benutzer personalisieren dürfen. Außerdem lassen sich damit Umgebungseinstellungen wie Netzwerke und standortspezifische Drucker zuordnen. Mit der Funktion „Intelligente Richtlinien“ besteht die Möglichkeit, Richtlinien zu erstellen, die nur beim Eintreten bestimmter Bedingungen wirksam werden. Sie können beispielsweise eine Richtlinie konfigurieren, mit der die Clientlaufwerksumleitung dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit einem Remote-Desktop herstellt.

### **VMware Unified Access Gateway**

Unified Access Gateway-Funktionen sind ein sicheres Gateway für Benutzer, die auf Remote-Desktops und -anwendungen von außerhalb der Unternehmens-Firewall zugreifen möchten. Unified Access Gateway ist eine Appliance, die in einer demilitarisierten Netzwerkzone (DMZ) installiert wird. Verwenden Sie Unified Access Gateway, um sicherzustellen, dass nur Datenverkehr in das Rechenzentrum des Unternehmens gelangt, der zu einem sicher authentifizierten Remotebenutzer gehört. Sie können anstelle von Horizon 7-Sicherheitsservern Unified Access Gateway-Appliances verwenden. Weitere Informationen finden Sie in der Dokumentation Unified Access Gateway.

## **Integrieren in gängige Videokonferenzsoftware**

Sie können Audio- und Videokonferenzsoftware mit Horizon 7 verwenden.

### **Flash URL-Umleitung**

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf Clientendpunkte wird die Last auf dem ESXi-Host im Rechenzentrum reduziert, 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://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

## Microsoft Lync 2013

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, lagert das Lync-VDI-Plug-In die gesamte Medienverarbeitung vom Rechenzentrumsserver auf den Clientendpunkt aus 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 Whitepaper zu VMware Horizon 6 und Microsoft Lync 2013 unter <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf>.

---

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

---

## Skype for Business

Benutzer können optimierte Audio- und Videoanrufe mit Skype for Business innerhalb eines virtuellen Desktops vornehmen, ohne die virtuelle Infrastruktur negativ zu beeinflussen oder das Netzwerk zu überladen. Alle Medienverarbeitungsabläufe während eines Audio- und Videoanrufs mit Skype erfolgen auf dem Clientcomputer und nicht auf dem virtuellen Desktop.

Die Software „Virtualization Pack für Skype for Business“ wird standardmäßig im Rahmen der Installationsprogramme von Horizon Client für Windows (4.6 und höher), Horizon Client für Linux (4.6 und höher) und Horizon Client für Mac (4.7 oder höher) installiert. Ein Horizon-Administrator muss das VMware Virtualization Pack für Skype for Business bei der Installation von Horizon Agent auch auf dem virtuellen Desktop installieren. Weitere Informationen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*. Informationen zur Konfiguration von Skype for Business finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

## Integrieren von Horizon 7 in Business Intelligence-Software

Sie können den Horizon-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 *Horizon 7-Integration*.

Alternativ können Sie Horizon 7-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 *Horizon 7-Installation*.

## Verwenden von Horizon PowerCLI-Cmdlets zum Erstellen von Verwaltungsskripts

Sie können Horizon PowerCLI-Cmdlets mit VMware PowerCLI verwenden. Verwenden Sie Horizon-PowerCLI-Cmdlets zum Ausführen verschiedener Verwaltungsaufgaben für Horizon-Komponenten.

Weitere Informationen zu Horizon PowerCLI-Cmdlets erhalten Sie im Handbuch *VMware PowerCLI Cmdlets Reference*.

Informationen zu den API-Spezifikationen für das Erstellen erweiterter Funktionen und Skripts zur Verwendung mit Horizon PowerCLI finden Sie in der View API-Referenz im [VMware Developer Center](#).

Weitere Informationen zu Beispielskripts, mit denen Sie Ihre eigenen Horizon PowerCLI-Skripts erstellen können, erhalten Sie in der [Horizon PowerCLI-Community auf GitHub](#).

Mithilfe der Horizon PowerCLI-Cmdlets können Sie verschiedene Verwaltungsaufgaben für Horizon 7-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

## Ändern von LDAP-Konfigurationsdaten in Horizon 7

Wenn Sie die Konfiguration von Horizon 7 mithilfe von Horizon Administrator ändern, werden die entsprechenden LDAP-Daten im Repository aktualisiert. Der Horizon-Verbindungsserver speichert Konfigurationsdaten in einem mit LDAP kompatiblen Repository. Wenn Sie beispielsweise einen Desktop-Pool hinzufügen, speichert der 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 Horizon 7 exportieren. Diese Befehle sind für fortgeschrittene Administratoren bestimmt, die Konfigurationsdaten anhand von Skripts und nicht über Horizon Administrator oder Horizon PowerCLI aktualisieren möchten.

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

- Übertragen von Konfigurationsdaten zwischen Verbindungsserver-Instanzen
- Definieren einer großen Anzahl von Horizon 7-Objekten, z. B. Desktop-Pools, und Hinzufügen dieser Objekte zu Ihren Verbindungsserver-Instanzen ohne Horizon Administrator oder Horizon PowerCLI
- Sichern einer Konfiguration, damit der Zustand einer Verbindungsserver-Instanz wiederhergestellt werden kann

Weitere Informationen finden Sie im Dokument *Horizon 7-Integration*.

## Verwenden des Befehls „vdmadmin“

Über die Befehlszeilenschnittstelle `vdmadmin` kann eine Vielzahl von Verwaltungsaufgaben für eine Verbindungsserver-Instanz ausgeführt werden. Sie können `vdmadmin` zur Durchführung von Verwaltungsaufgaben einsetzen, die innerhalb der Horizon Administrator-Benutzeroberfläche nicht möglich sind oder die automatisch über Skripts ausgeführt werden sollen.

Weitere Informationen finden Sie im Dokument *Horizon 7-Verwaltung*.

# Planen einer umfassenden Benutzerumgebung

## 2

Horizon 7 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.

Horizon 7 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 Horizon Agent](#)
- [Auswählen eines Anzeigeprotokolls](#)
- [Verwenden veröffentlichter Anwendungen](#)
- [Verwenden von Horizon Persona Management zur Speicherung von Benutzerdaten und -einstellungen](#)
- [Verwenden von USB-Geräten mit Remote-Desktops und -anwendungen](#)
- [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 des Single Sign-On für die Anmeldung](#)
- [Monitore und Bildschirmauflösung](#)

## Funktionsunterstützungs-Matrix für Horizon 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. Eine aktualisierte Liste unterstützter Windows 10-Betriebssysteme finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2149393>. Zu anderen Windows-Betriebssystemen als Windows 10 finden Sie Informationen im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150295>.

Eine Liste der speziellen Funktionen für die Remoteerfahrung, die auf Windows-Betriebssystemen unterstützt werden, auf denen Horizon Agent installiert ist, erhalten Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150305>.

---

**Hinweis** Informationen darüber, welche Funktionen auf den verschiedenen Typen von Clientgeräten unterstützt werden, finden Sie in der Horizon Client-Dokumentation unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>

---

Darüber hinaus bieten verschiedene VMware-Partner Thin Client- und Zero Client-Geräte für Horizon 7-Bereitstellungen an. Welche Funktionen für die einzelnen Thin Client- oder Zero Client-Geräte verfügbar sind, richtet sich jeweils nach dem Hersteller und Modell sowie nach der vom jeweiligen Unternehmen gewählten Konfiguration. Informationen zu Herstellern und Modellen für Thin Client- und Zero Client-Geräte finden Sie im [VMware-Kompatibilitätshandbuch](#), das 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 den von VMware bereitgestellten Protokollen Blast Extreme und PCoIP (PC-over-IP) und RDP (Remote Desktop Protocol) von Microsoft 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 Extreme-Protokoll benutzt. Ebenso wird Blast Extreme für einen Linux-Remote-Desktop verwendet.

---

## VMware Blast Extreme

VMware Blast Extreme ist für die mobile Cloud optimiert und unterstützt das breiteste Spektrum an H.264-fähigen Clientgeräten. Unter den Anzeigeprotokollen bietet VMware Blast den niedrigsten CPU-Verbrauch und die längste Akkunutzungsdauer für mobile Geräte. VMware Blast Extreme kann eine Zunahme der Latenz oder eine Verringerung der Bandbreite kompensieren und sowohl TCP als auch UDP als Netzwerktransportprotokoll verwenden.

Das VMware Blast-Anzeigeprotokoll kann für veröffentlichte Anwendungen und Remote-Desktops, die virtuelle Maschinen oder gemeinsame Sitzungen über RDS-Hosts verwenden, genutzt werden. Der RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein. Das VMware Blast-Anzeigeprotokoll funktioniert nicht auf physischen Computern mit Einzelbenutzern mit Ausnahme der Enterprise Edition von Windows 10 RS4 und späteren Versionen.

---

**Hinweis** Filme und TV-Anwendungen werden für physische Computer mit Windows 10 RS4 nicht unterstützt.

---

## Funktionen von VMware Blast Extreme

Zu den wichtigsten Funktionen von VMware Blast Extreme zählen:

- Benutzer außerhalb der Unternehmensfirewall können dieses Protokoll mit dem Virtual Private Network (VPN) des Unternehmens verwenden, oder Benutzer können sichere, verschlüsselte Verbindungen mit einem Sicherheitsserver oder mit einer Access Point-Appliance in der Unternehmens-DMZ herstellen.
- AES (Advanced Encryption Standard) 128 Bit-Verschlüsselung wird unterstützt und ist standardmäßig aktiviert. Sie können die Verschlüsselungsmethode jedoch auf AES-256 ändern.
- Verbindungen von allen Arten von Clientgeräten.
- Optimierungssteuerungen zur Reduzierung der Bandbreitennutzung im LAN und WAN.
- Die mithilfe von PerfMon auf Windows-Agenten angezeigten Leistungsindikatoren bieten eine präzise Darstellung des aktuellen Systemstatus, der regelmäßig für die folgenden Elemente aktualisiert wird:
  - Blast-Sitzung
  - Bildverarbeitung
  - Audio
  - CDR
  - USB: USB-Indikatoren, die mithilfe von PerfMon auf Windows-Agenten angezeigt werden, sind gültig, wenn der USB-Datenverkehr für die Verwendung von VMware Virtual Channel VVC konfiguriert ist.
  - Skype for Business: Leistungsindikatoren dienen nur der Steuerung des Datenverkehrs.
  - Zwischenablage
  - RTAV
  - Funktionen für seriellen Port und Scannerumleitung
  - Virtuelles Drucken
  - HTML5 MMR
  - Windows Media MMR: Leistungsindikatoren werden nur dann angezeigt, wenn Sie diese Funktion zur Verwendung von VMware Virtual Channel (VVC) konfiguriert haben.

- Netzwerkkontinuität während des kurzzeitigen Verlustes der Netzwerkverbindung auf Windows-Clients.
- 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 einem Remote-Desktop oder einer veröffentlichten Anwendung. 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 einigen Clients können Sie bis zu vier Monitore mit einer Auflösung bis zu 2560 x 1600 pro Anzeige oder bis zu drei Monitore mit einer Auflösung von 4K (3840 x 2160) für Windows 7-Remote-Desktops mit deaktiviertem Aero verwenden. 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 bis zu 1920 x 1200 oder ein Monitor mit einer Auflösung von 4K (3840 x 2160) unterstützt.

- USB-Umleitung wird für einige Client-Typen unterstützt.
- MMR-Umleitung wird für einige Windows-Clientbetriebssysteme und einige Remote-Desktop-Betriebssysteme (mit installiertem Horizon Agent) unterstützt.
- Es werden Verbindungen mit physischen Maschinen, an die kein Monitor angeschlossen ist, mit NVIDIA-Grafikkarten unterstützt. Für eine optimale Leistung verwenden Sie eine Grafikkarte, die die H. 264-Codierung unterstützt.

Wenn Sie über eine diskrete Add-In-GPU und eine eingebettete GPU verfügen, verwendet das Betriebssystem eventuell standardmäßig die eingebettete GPU. Zur Behebung dieses Problems können Sie das Gerät im Gerätemanager deaktivieren oder entfernen. Wenn das Problem weiterhin auftritt, haben Sie die Möglichkeit, den WDDM-Grafiktreiber für die eingebettete GPU zu installieren oder die eingebettete GPU im System-BIOS zu deaktivieren. Informationen zur Deaktivierung der eingebetteten GPU finden Sie in Ihrer Systemdokumentation.



**Vorsicht** Durch die Deaktivierung der eingebetteten GPU kann auch eine bestimmte Funktionalität wie der Konsolenzugriff auf das BIOS-Setup oder der NT Boot Loader beeinträchtigt sein.

---

Informationen darüber, welche Clientgeräte spezifische VMware Blast Extreme-Funktionen unterstützen, finden Sie unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

## Wake on LAN

Wake on LAN wird für physische Maschinen mit der Enterprise Edition von Windows 10 RS4 und spätere Versionen unterstützt. Mit dieser Funktion können Benutzer physische Maschinen beim Herstellen der Verbindung mit Horizon Connection Server aktivieren. Für die Wake-on-LAN-Funktion gelten folgende Voraussetzungen:

- Wake on LAN (WoL) wird nur in IPv4-Umgebungen unterstützt.
- Die physische Maschine muss so konfiguriert werden, dass sie beim Empfang von Wake-on-LAN-Paketen aktiviert wird, wenn Wake on LAN sowohl in den BIOS-Einstellungen als auch den Einstellungen für die Netzwerkkarte aktiviert ist.
- Zielport 9 wird für WoL-Pakete vom Verbindungsserver verwendet.
- WoL-Pakete sind IP-gesteuerte Broadcast-Pakete, die Horizon Agent beim Senden von Horizon Connection Server erreichen müssen. Wake-on-LAN-Funktionen in diesen Szenarios:
  - Verbindungsserver und Horizon Agent auf der physischen Maschine befinden sich im selben Subnetz in einer LAN-Umgebung.
  - Alle Router zwischen Verbindungsserver und Horizon Agent werden so konfiguriert, dass das IP-gesteuerte Broadcast-Paket für das Zielsubnetz der physischen Maschine zugelassen ist, die Sie aktivieren möchten.

---

**Hinweis** Die Wake-on-LAN-Funktion unterstützt keine dynamischen Zuweisungspools von einem physischen Windows 10-Agenten. Das WoL-Paket wird nur an dedizierte Zuweisungspools gesendet, die für einen bestimmten Benutzer zugelassen sind.

---

## Empfohlene Einstellungen für das Gastbetriebssystem

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 Grafikkbeschleunigung) für grafikintensive Anwendungen wie CAD-Anwendungen sind 4 GB RAM erforderlich.

## Videoqualitätsanforderungen

<b>480p-formatiertes Video</b>	Die Videowiedergabe mit 480p oder niedriger bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über eine virtuelle CPU verfügt. Wenn Sie eine Videowiedergabe in hochauflösendem Flash- oder im Vollbildmodus wünschen, erfordert 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.
<b>720p-formatiertes Video</b>	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.
<b>1080p-formatiertes Video</b>	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.
<b>3D-Rendering</b>	<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 ermöglichen es virtuellen Maschinen, die physischen GPUs (Grafikverarbeitungseinheiten) auf einem vSphere-Host freizugeben oder eine physische GPU für einen einzelnen virtuellen Desktop zu reservieren.</p> <p>Bei 3D-Anwendungen werden bis zu zwei Monitore unterstützt, 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 <a href="#">Verwenden von 3D-Grafikanwendungen</a>.</p>

## Hardwareanforderungen für Clientsysteme

Informationen zu den Prozessor- und Speicheranforderungen für den spezifischen Typ des Desktop- oder des mobilen Clientgeräts finden Sie unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

## PCoIP

PCoIP (PC over IP) ermöglicht ein optimiertes Desktoperlebnis bei der Bereitstellung einer veröffentlichten Anwendung 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.

Das PCoIP-Anzeigeprotokoll kann für veröffentlichte Anwendungen und für Remote-Desktops, die virtuelle Maschinen verwenden, physische Computer, die Teradici-Hostkarten enthalten, oder Desktops mit freigegebenen Sitzungen auf einem RDS-Host verwendet werden.

## 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 oder mit einer Access Point-Appliance in der Unternehmens-DMZ herstellen.
- AES (Advanced Encryption Standard) 128 Bit-Verschlüsselung wird unterstützt und ist standardmäßig aktiviert. Sie können die Verschlüsselungsmethode jedoch auf 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 einem Remote-Desktop oder einer veröffentlichten Anwendung. 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 einigen Clients können Sie bis zu vier Monitore mit einer Auflösung bis zu 2560 x 1600 pro Anzeige oder bis zu drei Monitore mit einer Auflösung von 4K (3840 x 2160) für Windows 7-Remote-Desktops mit deaktiviertem Aero verwenden. 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 bis zu 1920 x 1200 oder ein Monitor mit einer Auflösung von 4K (3840 x 2160) unterstützt.

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

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

Informationen darüber, welche Client-Geräte spezifische PCoIP-Funktionen unterstützen, finden Sie unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

## Empfohlene Einstellungen für das Gastbetriebssystem

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

- |                                 |   |
|---------------------------------|---|
| <b>480p-formatiertes Video</b>  | Die Videowiedergabe mit 480p oder niedriger bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über eine virtuelle CPU verfügt. Wenn Sie eine Videowiedergabe in hochauflösendem Flash- oder im Vollbildmodus wünschen, erfordert 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.  |
| <b>720p-formatiertes Video</b>  | Die Videowiedergabe mit 720p bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über zwei virtuelle CPUs verfügt. Bei der 720p-Video-wiedergabe in hoch auflösendem oder Vollbildmodus könnte die Leistung beeinträchtigt sein.   |
| <b>1080p-formatiertes Video</b> | 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.   |
| <b>3D-Rendering</b>             | <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 <a href="#">Verwenden von 3D-Grafikanwendungen</a>.</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://docs.vmware.com/de/VMware-Horizon-Client/index.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. (Für veröffentlichte Anwendungen werden nur das PCoIP-Anzeigeprotokoll und das VMware Blast-Anzeigeprotokoll unterstützt.) Microsoft RDP ermöglicht Folgendes:

- RDP 7 lässt eine echte Mehrfachmonitorsitzung 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.

Sie müssen den Hotfix KB3080079 von Microsoft anwenden, damit TLSv1.1- und TLSv1.2-Verbindungen mit Windows 7 und Windows Server 2008 R2 unterstützt werden.

## 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://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

---

**Hinweis** Mobile 3.x-Clientgeräte verwenden ausschließlich das PCoIP-Anzeigeprotokoll. Mobile 4.x-Clients verwenden nur das PCoIP-Anzeigeprotokoll oder das VMware Blast-Anzeigeprotokoll.

---

## Verwenden veröffentlichter Anwendungen

Sie können mit Horizon Client nicht nur auf veröffentlichte Desktops, sondern auch auf Windows-basierte Remoteanwendungen sicher zugreifen.

Dank dieser Funktion sehen Benutzer nach dem Start von Horizon Client und der Anmeldung bei einem Horizon 7 Server zusätzlich zu den Remote-Desktops alle veröffentlichten Anwendungen, 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 Client-Desktop angezeigt wird.

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

- Wenn eine Anwendung mit einer Multi-Tier-Architektur eingerichtet ist, in der die Komponenten besser funktionieren, wenn sie geografisch nicht zu weit voneinander entfernt sind, ist die Verwendung von veröffentlichten Anwendungen 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 veröffentlichten 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 ist die Funktionsweise von veröffentlichten Horizon 7-Anwendungen vergleichbar anderer Remotelösungen für Anwendungen. Veröffentlichte Horizon 7-Anwendungen werden entweder mit dem Blast Extreme- oder mit dem PCoIP-Anzeigeprotokoll für eine optimierte Benutzerumgebung bereitgestellt.

## **Verwenden von Horizon Persona Management zur Speicherung von Benutzerdaten und -einstellungen**

Sie können Horizon Persona Management mit Remote-Desktops und mit physischen Computern und virtuellen Maschinen, die nicht von Horizon 7 verwaltet werden, verwenden. 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 die Handhabung dieser Funktionen zu erleichtern, erfordert Persona Management Speicherplatz auf einer CIFS-Freigabe, die der Größe des lokalen Benutzerprofils entspricht oder sogar größer ist.

## Minimierung der Anmelde- und Abmeldezeiten

Persona Management minimiert die Zeit, die zum An- und Abmelden von Desktops notwendig ist. Während der Anmeldung lädt Horizon 7 nur die für Windows erforderlichen Dateien herunter, beispielsweise die Benutzerregistrierungsdateien. Horizon 7 erfasst aktuelle Änderungen am Profil auf dem Remote-Desktop und kopiert diese in regelmäßigen Abständen in das Remote-Repository.

Mit Persona Management können Sie vermeiden, dass an Active Directory Änderungen für die Verwendung eines verwalteten Profils 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 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 Horizon 7 Personas auf mehreren 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 Persona Management auf physischen Computern und virtuellen Maschinen, die nicht von Horizon 7 verwaltet werden, verwenden.

Durch Festlegung von Gruppenrichtlinien (GPOs) ist eine genauere Steuerung der Dateien und Ordner möglich, die eine Persona enthalten soll. Sie können angeben, ob der Ordner mit persönlichen Einstellungen enthalten sein soll, welche Dateien bei der Anmeldung geladen werden, welche Dateien nach der Benutzeranmeldung im Hintergrund heruntergeladen werden sollen und welche Dateien in der Persona eines Benutzers mit der Windows-Funktionalität für servergespeicherte Profile statt mit Persona Management verwaltet werden sollen.

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	

## Einschränkungen

Für Persona Management bestehen die folgenden Einschränkungen und Beschränkungen:

- Diese Funktion wird für Instant-Clone-Desktop-Pools nicht unterstützt.
- Sie müssen über eine Horizon 7-Lizenz verfügen, die die Persona Management-Komponente umfasst.
- Persona Management erfordert eine CIFS-Freigabe (Common Internet File System).
- Diese Funktion wird nicht für die Verwendung mit einer persistenten Festplatte in Windows 10-Linked-Clone-Desktop-Pools unterstützt.

## Verwenden von USB-Geräten mit Remote-Desktops und -anwendungen

Administratoren können virtuelle Desktops so konfigurieren, dass USB-Geräte wie Flash-Laufwerke, Kameras, VoIP-Geräte und Drucker genutzt werden können. Diese Funktion wird als USB-Umleitung bezeichnet. Ein virtueller Desktop unterstützt maximal 128 USB-Geräte.

Sie können auch bestimmte lokal verbundene USB-Geräte umleiten, um sie an veröffentlichten Desktops und Anwendungen zu verwenden. Informationen zu den spezifischen unterstützten Gerätetypen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Bei Verwendung dieser Funktion in Desktop-Pools, die auf Maschinen für Einzelbenutzer bereitgestellt werden, stehen die meisten USB-Geräte, die an das lokale Client-System 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-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 von einem Remote-Desktop und dem lokalen Computer gemeinsam verwendet werden. Zu diesen Geräten zählen Smart-card-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-Umleitung ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungs-Matrix im Horizon Client-Dokument zur Installation und Einrichtung für den spezifischen Typ von Clientgerät.

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

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon des lokalen Client-Systems auf einem Remote-Desktop oder in einer veröffentlichten Anwendung verwenden. Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel. Die Funktion unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Endbenutzer können Skype, Webex, Google Hangouts und andere Online-Konferenzanwendungen auf ihren Remote-Desktops ausführen. Diese Funktion leitet Video- und Audiodaten mit weniger Bandbreite an den Agent-Computer um, als mit der USB-Umleitung erreicht werden kann. Mit Echtzeit-Audio/Video werden Webcam-Bilder und Audioeingaben auf dem Client-System codiert und dann an den Agent-Computer gesendet. Auf dem Agent-Computer können eine virtuelle Webcam und ein virtuelles Mikrofon den Stream decodieren und wiedergeben, sodass er von der Drittanbieteranwendung verwendet werden kann.

Dazu ist keine besondere Konfiguration erforderlich. Administratoren können jedoch Gruppenrichtlinien und Registrierungsschlüssel auf Agent-Seite festlegen, um die Frame-Rate und Bildauflösung zu konfigurieren oder die Funktion zu deaktivieren. Standardmäßig beträgt die Auflösung 320 x 240 Pixel bei 15 Frames pro Sekunde. Bei Bedarf können Administratoren 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 zur Installation und Einrichtung für den spezifischen Typ von Desktop- oder mobilem Clientgerät.

---

## Verwenden von 3D-Grafikanwendungen

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

### **NVIDIA GRID vGPU (Hardwarebeschleunigung durch gemeinsam genutzte GPU)**

Mithilfe dieser Funktion in vSphere 6.0 und höher kann eine physische GPU (Graphical Processing Unit, Grafikverarbeitungseinheit) auf einem ESXi-Host von virtuellen Maschinen gemeinsam genutzt werden. Verwenden Sie diese Funktion, wenn Sie hochwertige, hardwarebeschleunigte Workstation-Grafiken benötigen.

### **AMD Multiuser GPU mit vDGA**

Diese Funktion ist in vSphere 6.0 und höher verfügbar und erlaubt es mehreren virtuellen Maschinen, eine AMD GPU gemeinsam zu nutzen, indem die GPU wie mehrere PCI-Passthrough-Geräte dargestellt wird. Diese Funktion bietet flexible hardwarebeschleunigte 3D-Profile, die von einfachen Benutzern von 3D-Aufgaben bis hin zu Hauptbenutzern von anspruchsvollen Workstation-Grafiken reichen.

### **Virtual Dedicated Graphics Acceleration (vDGA)**

Diese Funktion, die in vSphere 5.5 Update 2 und höher verfügbar ist, weist eine einzige physische GPU auf einem ESXi-Host einer einzelnen virtuellen Maschine zu. Verwenden Sie diese Funktion, wenn Sie hochwertige, hardwarebeschleunigte Workstation-Grafiken benötigen.

---

**Hinweis** Für einige Intel vDGA-Karten wird eine bestimmte vSphere 6-Version benötigt. Nähere Informationen finden Sie in der „VMware Hardware-Kompatibilitätsliste“ unter <http://www.vmware.com/resources/compatibility/search.php>. Zudem muss für Intel vDGA die integrierte Intel GPU statt diskreter GPUs wie bei anderen Herstellern verwendet werden.

---

### **Virtual Shared Graphics Acceleration (vSGA)**

Bei Verwendung dieser Funktion, die in vSphere 5.5 Update 2 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 5.5 Update 2 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.

NVIDIA GRID vGPU und vDGA werden in veröffentlichten Anwendungen unterstützt, die auf Microsoft RDS-Hosts ausgeführt werden.

---

**Wichtig** Weitere Informationen zu den verschiedenen Auswahlmöglichkeiten und Anforderungen der 3D-Wiedergabe finden Sie im [VMware Whitepaper](#) zur Grafikbeschleunigung, im [NVIDIA GRID vGPU Handbuch zur Bereitstellung für VMware Horizon 6.1](#) und im [NVIDIA GRID Virtual GPU Benutzerhandbuch](#).

---

## **Streaming von Multimediadaten auf einen Remote-Desktop**

Die Windows Media MMR-Funktion (Multimedia Redirection, Multimedia-Umleitung) für Windows 7- und Windows 8/8.1-Desktops und -Clients ermöglicht eine originalgetreue Wiedergabe auf Windows-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. In Windows Media Player unterstützte Medienformate werden unterstützt, beispielsweise: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3; WAV.

---

**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.

Die Umleitung des lokalen Druckers wurde für folgende Drucker entwickelt:

- Drucker, die direkt mit der USB-Schnittstelle oder mit seriellen Ports auf dem Clientgerät verbunden sind.
- Spezielle Drucker wie z. B. Barcodedrucker und Etikettendrucker, die mit dem Client verbunden sind.
- Netzwerkdrucker in einem Remotenetzwerk, die nicht von der virtuellen Sitzung angesteuert werden können.

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 Handbuch zur Installation und Einrichtung für den spezifischen Typ von Desktop- oder mobilem Clientgerät. Besuchen Sie <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

---

## Verwenden des Single Sign-On für die Anmeldung

Dank der Single Sign-On-Funktion (SSO, einmalige Anmeldung) müssen Endbenutzer ihre Active Directory-Anmeldeinformationen nur einmal eingeben.

Wenn Sie die Single Sign-On-Funktion nicht verwenden, werden Benutzer zweimal zur Anmeldung aufgefordert: Sie werden aufgefordert, sich zuerst mit ihren Active Directory-Anmeldedaten beim Horizon-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.

Für Remote-Desktops enthält diese Funktion eine Anmeldedatenanbieter-DLL.

## True SSO

Mit der True SSO-Funktion müssen Benutzer keine Active Directory-Anmeldedaten mehr eingeben. Nachdem sich Benutzer bei VMware Identity Manager mit einer Nicht-AD-Methode (z. B. RSA SecurID- oder RADIUS-Authentifizierung) angemeldet haben, werden Benutzer nicht aufgefordert, zusätzlich Active Directory-Anmeldeinformationen einzugeben, um einen Remote-Desktop oder eine Anwendung zu verwenden.

Für eine Benutzerauthentifizierung mithilfe von Smartcards oder Active Directory-Anmeldeinformationen ist die True SSO-Funktion nicht erforderlich, kann aber auch für diese Fälle konfiguriert werden. Vom Benutzer eingegebene AD-Anmeldeinformationen werden dann ignoriert und es wird die True SSO-Funktion verwendet.

Mit der True SSO-Funktion wird ein eindeutiges kurzlebiges Zertifikat für die Windows-Anmeldung generiert. Damit solche kurzlebigen Zertifikate für den Benutzer generiert werden können, müssen Sie eine Zertifizierungsstelle, wenn noch keine vorhanden ist, und einen Registrierungsserver für Zertifikate einrichten. Zur Installation des Registrierungservers führen Sie das Installationsprogramm für den Verbindungsserver aus und wählen die Option „Registrierungsserver“ aus.

Die True SSO-Funktion trennt die Authentifizierung (Überprüfung der Benutzeridentität) vom Zugriff (z. B. auf einen Windows-Desktop oder eine Windows-Anwendung). Die Anmeldeinformationen des Benutzers sind durch ein digitales Zertifikat geschützt. Es werden keine Kennwörter aufbewahrt oder im Rechenzentrum übertragen. Weitere Informationen finden Sie im Dokument *Horizon 7-Verwaltung*.

## Monitore und Bildschirmauflösung

Sie können einen Remote-Desktop auf mehrere Monitore erweitern. Wenn Sie einen hochauflösenden Monitor besitzen, können Sie den Remote-Desktop oder die Remoteanwendung in voller Auflösung sehen.

Sie haben die Möglichkeit, den Anzeigemodus „Alle Monitore“ auszuwählen, um einen Remote-Desktop auf mehreren Monitoren anzuzeigen. Wenn Sie im Modus „Alle Monitore“ das Fenster minimiert haben, wechselt es nach der Maximierung zurück in den Modus „Alle Monitore“. Dies gilt ebenso für ein minimiertes Vollbildfenster: Nach der Maximierung wird wieder der Vollbildmodus auf einem Monitor angezeigt.

## Verwenden aller Monitore in einer Mehrfachmonitorumgebung

Unabhängig vom Anzeigeprotokoll können Sie mit einem Remote-Desktop mehrere Monitore verwenden. Wenn Horizon Client alle Monitore verwendet und Sie ein Anwendungsfenster maximieren, wird das Fenster nur in dem Monitor auf die Vollbildansicht erweitert, der das Fenster enthält.

Horizon Client unterstützt die folgenden Monitorkonfigurationen:

- Wenn Sie zwei Monitore verwenden, müssen sich die Monitore nicht im gleichen Modus befinden. Wenn Sie zum Beispiel einen Laptop verwenden, der mit einem externen Monitor verbunden ist, kann sich der externe Monitor sowohl im Quer- als auch im Hochformat befinden.
- Monitore können nur dann nebeneinander, in Zweiergruppen oder vertikal übereinander platziert werden, wenn Sie zwei Monitore verwenden und die maximale Gesamtlänge weniger als 4096 Pixel beträgt.
- Um die 3D-Rendering-Funktion nutzen zu können, muss das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwendet werden. Sie können bis zu zwei Monitore mit einer Auflösung von bis zu 1920x1200 verwenden. Für eine Auflösung von 4K (3840 X 2160) wird nur ein Monitor unterstützt.
- Mit dem VMware Blast- oder dem PCoIP-Anzeigeprotokoll wird eine Bildschirmauflösung von 4K (3840 x 2160) für den Remote-Desktop unterstützt. Die Anzahl der unterstützten 4K-Bildschirme hängt von der Hardwareversion der virtuellen Maschine des Desktops und der Windows-Version ab.

Hardwareversion	Windows-Version	Anzahl der unterstützten 4K-Bildschirme
10 (ESXi 5.5.x-kompatibel)	7, 8, 8.x, 10	1
11 (ESXi 6.0-kompatibel)	7 (3D-Rendern-Funktion deaktiviert und Windows Aero deaktiviert)	3
11	7 (3D-Rendern-Funktion aktiviert)	1
11	8, 8.x, 10	1
13	8, 8.x, 10	4

- 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.



## Verwenden eines Monitors in einer Mehrfachmonitorumgebung

Wenn Sie über mehrere Monitore verfügen, aber mit Horizon Client nur einen Monitor verwenden möchten, können Sie festlegen, dass ein Remote-Desktop-Fenster nicht im Modus „Alle Monitore“ geöffnet wird. Standardmäßig wird das Fenster auf dem primären Monitor geöffnet. Weitere Informationen finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

## Verwenden des hochauflösenden Modus

Wenn Sie das VMware Blast- oder das PCoIP-Anzeigeprotokoll verwenden, unterstützt Horizon Client bei einigen Clienttypen auch sehr hohe Auflösungen für Clientsysteme mit hochauflösenden Anzeigegeräten. Die Option zur Aktivierung des hochauflösenden Modus wird nur angezeigt, wenn das Clientsystem hochauflösende Anzeigegeräte unterstützt.

Die Hardwarecodierung ist standardmäßig aktiviert, nachdem Sie vGPU in der virtuellen Maschine konfiguriert haben. Die Hardwarecodierung ist für alle unterstützten Konfigurationen mit mehreren Monitoren aktiviert, ausgenommen sind vGPU-Profile, die weniger als 1 GB Videospeicher verwenden. Aufgrund von NVENC-Speicherrestriktionen verwenden diese den Softwaredecoder. Sehen Sie hierzu *NVENC requires at least 1 Gbyte of frame buffer* in <https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vsphere/index.html>

# 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 Horizon 7 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

Horizon 7 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 ein physischer Desktop-PC.
- 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 Horizon Agent unterstützt.
- Ein sitzungsbasierter Desktop auf einem RDS-Host. Weitere Informationen zum Erstellen von Desktop-Pools von einem RDS-Host finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

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 für View Composer-Linked-Clone-VMs oder Full-Clone-VMs an, ob die virtuelle Maschine ausgeschaltet werden soll, wenn sie nicht verwendet wird, oder ob sie gelöscht werden soll. Instant-Clone-VMs sind immer eingeschaltet.
- Für View Composer-Linked-Clone-VMs können Sie angeben, 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. Instant Clones benötigen eine andere Anpassungsspezifikation namens ClonePrep von VMware.

Sie können auch angeben, wie Desktops in einem Pool Benutzern zugewiesen werden.

#### **Pools mit fester Zuweisung**

Jedem Benutzer wird ein bestimmter Remote-Desktop zugewiesen, zu dem er bei jeder Anmeldung zurückkehrt. Dedizierte Zuweisungspools erfordern ein Verhältnis von 1:1 zwischen Desktops und Benutzern. Beispielsweise wird für eine Gruppe von 100 Benutzern ein Pool von 100 Desktops benötigt.

#### **Pools mit dynamischer Zuweisung**

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. Der Remote-Desktop wird nach jeder Verwendung optional gelöscht und erneut erstellt, wodurch eine hohe Kontrolle der Umgebung möglich ist.

## **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, MacOS 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 Speicheranforderungen**

Das Bereitstellen von Desktops auf virtuellen Maschinen, die von vCenter Server verwaltet werden, bietet sämtliche Speichervorteile, die zuvor nur für virtuelle Server möglich waren. Die Verwendung von Instant Clones oder von View Composer-Linked-Clones als Desktop-Computer erhöht die Verfügbarkeit von Speicherplatz, da alle virtuelle Maschinen in einem Pool gemeinsam eine virtuelle Festplatte mit einem Basis-Image 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 VMware vSAN für Hochleistungsspeicher und die richtlinienbasierte Verwaltung**

VMware vSAN ist eine softwaredefinierte Speicherebene im Lieferumfang von vSphere 5.5 Update 2 oder einer neueren Version, die die in einem Cluster von vSphere-Hosts verfügbaren lokalen physischen Speicherfestplatten virtualisiert. Sie geben bei der Erstellung eines automatisierten Desktop-Pools oder einer automatisierten Farm 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 angeschlossenen Festplatten (HDD) platziert.

- **Verwenden von VVOL (virtuelle Volumes) für VM-basierte Speicherung und richtlinienbasierte Verwaltung**

Mit VVOL (virtuelle Volumes) (verfügbar in vSphere 6.0 oder höher) wird eine einzelne virtuelle Maschine, und nicht der Datenspeicher, zu einer Speicherverwaltungskomponente. Die Speicherhardware erlangt die Kontrolle über den Inhalt der virtuellen Festplatte, das Layout und die Verwaltung.

- **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.

- **Reduzieren der Speicheranforderungen mit Instant Clones**

Die Instant-Clones-Funktion nutzt die vSphere vmFork-Technologie (verfügbar mit vSphere 6.0U1 und höher) zur Stilllegung eines ausgeführten Basis-Image oder einer übergeordneten virtuellen Maschine und erstellt auf schnelle Weise einen Pool von virtuellen Desktops bzw. passt diesen an.

## 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 Datencentern 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 5.5 Update 2 oder höher

Mit vSphere 5.5 Update 2 oder einer neueren Version können Sie vSAN 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. vSAN 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 angeschlossenen Festplatten (HDD) platziert.

Mithilfe von vSAN 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 vSAN die Daten der betroffenen virtuellen Maschinen neu und optimiert die Nutzung der Ressourcen im ganzen Cluster. Sie können einen Desktop-Pool in einem Cluster bereitstellen, der bis zu 20 ESXi-Hosts enthält.

vSAN 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.

---

**Wichtig** Die in vSphere 6.0 und höheren Versionen verfügbare vSAN-Funktion enthält viele Leistungsverbesserungen. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf. Weitere Informationen zu vSAN in vSphere 6 oder höher finden Sie im Dokument *Verwalten von VMware vSAN*.

---

**Hinweis** vSAN ist mit der View-Speicherbeschleunigungsfunktion, aber nicht mit der Funktion platzsparendes Datenträgerformat kompatibel, die Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.

---

Mit vSphere 5.5 Update 2 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.
- 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 6.0 oder höher

Mit vSphere 6.0 oder einer neueren Version können Sie VVOL (virtuelle Volumes) verwenden. Diese Funktion ordnet virtuelle Festplatten und deren Derivate, Klone, Snapshots und Replikate direkt Objekten, die als virtuelle Volumes bezeichnet werden, auf einem Speichersystem zu. Durch diese Zuordnung kann vSphere speicherintensive Vorgänge wie etwa Snapshot-Erstellung, Klonen und Replikation an das Speichersystem auslagern.

Mithilfe von VVOL können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Speicherrichtlinienprofile in vSphere verwenden. Diese Speicherrichtlinienprofile legen Speicherdienste für jede einzelne virtuelle Maschine fest. Durch diese detaillierte Bereitstellung wird die Kapazitätsauslastung erhöht. Sie können einen Desktop-Pool auf einem Cluster bereitstellen, der bis zu 32 ESXi-Hosts enthält.

---

**Hinweis** VVOL ist zur View-Speicherbeschleunigungsfunktion, aber nicht zur Funktion platzsparendes Datenträgerformat kompatibel, die Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.

---

**Hinweis** VVOL wird von Instant Clones nicht unterstützt.

---

## Verwenden von VMware vSAN für Hochleistungsspeicher und die richtlinienbasierte Verwaltung

VMware VMware vSAN ist eine softwaredefinierte Speicherebene im Lieferumfang von vSphere 5.5 Update 2 oder einer neueren Version, die die in einem Cluster von vSphere-Hosts verfügbaren lokalen physischen Speicherfestplatten virtualisiert. Sie geben bei der Erstellung eines automatisierten Desktop-Pools oder einer automatisierten Farm 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 angeschlossenen Festplatten (HDD) platziert.

vSAN implementiert einen richtlinienbasierten Ansatz zur Speicherverwaltung. Wenn Sie vSAN verwenden, definiert Horizon 7 die Speicheranforderungen für virtuelle Maschinen wie Kapazität, Leistung und Verfügbarkeit in Form von standardmäßigen Speicherrichtlinienprofilen und stellt diese automatisch für virtuelle Desktops auf vCenter Server bereit. Die Richtlinien werden automatisch und einzeln pro Festplatte (vSAN-Objekte) angewendet und sind während des gesamten Lebenszyklus des virtuellen Desktops gültig. Der Speicher wird gemäß den zugewiesenen Richtlinien bereitgestellt und automatisch konfiguriert. Sie können diese Richtlinien in vCenter ändern. Horizon erstellt vSAN-Richtlinien für Linked-Clone-Desktop-Pools, Instant-Clone-Desktop-Pools, Full-Clone-Desktop-Pools oder für eine automatisierte Farm pro Horizon-Cluster.

Sie können die Verschlüsselung für einen vSAN-Cluster aktivieren, um alle ruhenden Daten im vSAN-Datenspeicher zu verschlüsseln. Die vSAN-Verschlüsselung ist mit vSAN Version 6.6 oder höher verfügbar. Weitere Informationen zur Verschlüsselung eines vSAN-Clusters finden Sie in der Dokumentation zu *VMware vSAN*.

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 vSAN die Daten der betroffenen virtuellen Maschinen und Lastausgleiche neu, um die Richtlinien der einzelnen virtuellen Maschinen zu erfüllen.

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

---

**Wichtig** Die in vSphere 6.0 und höher verfügbare vSAN-Funktion enthält im Vergleich zur Funktion aus vSphere 5.5 Update 2 viele Leistungsverbesserungen. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf. VMware vSAN 6.0 unterstützt auch eine vollständige Flash-Architektur, die Flash-basierte Geräte für das Zwischenspeichern und das permanente Speichern verwendet.

---

## Anforderungen und Einschränkungen

Für die vSAN-Funktion gelten bei Verwendung in einer Horizon 7-Bereitstellung folgende Einschränkungen:

- Diese Version unterstützt die Verwendung der platzsparenden Diskformatfunktion von Horizon 7 nicht, die Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.
- vSAN unterstützt die VCAI-Funktion (View Composer Array Integration) nicht, da vSAN keine NAS-Geräte verwendet.

---

**Hinweis** vSAN ist mit der Funktion „View-Speicherbeschleunigung“ kompatibel. vSAN bietet eine Cachingsschicht 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.

---

Für die vSAN-Funktion gelten die folgenden Anforderungen.

- vSphere 5.5 Update 2 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 ausreichend ESXi-Hosts, um Ihr Setup unterzubringen, selbst wenn Sie zwei ESXi-Hosts mit einem gestreckten vSAN-Cluster verwenden. Weitere Informationen finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere*.
- 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 vSAN-Anforderungen finden Sie unter „Arbeiten mit vSAN“ im Dokument *vSphere 5.5 Update 2 Storage*. Für vSphere 6 oder höher finden Sie Informationen im Dokument *Verwalten von VMware vSAN*. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen Horizon 7-Desktop-Infrastrukturen für VMware vSAN finden Sie im Whitepaper unter <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.



## Verwenden von VVOL (virtuelle Volumes) für VM-basierte Speicherung und richtlinienbasierte Verwaltung

Mit VVOL (virtuelle Volumes) (verfügbar in vSphere 6.0 oder höher) wird eine einzelne virtuelle Maschine, und nicht der Datenspeicher, zu einer Speicherverwaltungskomponente. Die Speicherhardware erlangt die Kontrolle über den Inhalt der virtuellen Festplatte, das Layout und die Verwaltung.

Bei VVOL ersetzen abstrakte Speichercontainer die traditionellen Speichervolumes, die auf LUNs oder NFS-Freigaben basieren. Diese Funktion ordnet virtuelle Festplatten und deren Derivate, Klone, Snapshots und Replikate direkt Objekten, die als virtuelle Volumes bezeichnet werden, auf einem Speichersystem zu. Durch diese Zuordnung kann vSphere speicherintensive Vorgänge wie etwa Snapshot-Erstellung, Klonen und Replikation an das Speichersystem auslagern. Dies bedeutet beispielsweise, dass ein Klonvorgang, der vorher eine Stunde dauerte, nun mit VVOL möglicherweise nur ein paar Minuten dauert.

---

**Wichtig** Einer der Hauptvorteile von virtuellen Volumes besteht in der Möglichkeit, die Softwarerichtlinien-basierte Verwaltung (SPBM) zu verwenden. Für diese Version erstellt Horizon 7 jedoch keine standardmäßigen granularen Speicherrichtlinien, die von vSAN angelegt werden. Stattdessen können Sie eine globale Standardspeicherrichtlinie in vCenter Server festlegen, die für alle VVOL-Datenspeicher gilt.

---

VVOL bietet die folgenden Vorteile:

- VVOL unterstützt das Auslagern einer Reihe von Vorgängen auf Speicherhardware. Hierzu zählen die Snapshot-Erstellung, das Klonen und Storage DRS
- Mit VVOL können Sie erweiterte Speicherdienste wie etwa Replikation, Verschlüsselung, Deduplizierung und Komprimierung für einzelne virtuelle Festplatten verwenden.
- VVOL unterstützt vSphere-Funktionen wie vMotion, Storage vMotion, Snapshots, Linked-Clones, Flash Read Cache und DRS.
- Sie können VVOL mit Speicher-Arrays verwenden, die vSphere APIs for Array Integration (VAAI) unterstützen.

## Anforderungen und Einschränkungen

Für die VVOL-Funktion gelten bei Verwendung in einer Horizon 7-Bereitstellung folgende Einschränkungen:

- Diese Version unterstützt die Verwendung der platzsparenden Diskformatfunktion von Horizon 7 nicht, die Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.
- Die Verwendung von View Composer Array Integration (VCAI) wird von VVOL nicht unterstützt.
- VVOL-Datenspeicher werden für Instant Clone-Desktop-Pools nicht unterstützt.

---

**Hinweis** VVOL ist mit der Funktion „View-Speicherbeschleunigung“ kompatibel. vSAN bietet eine Cachingsschicht 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.

---

Für die VVOL-Funktion gelten folgende Anforderungen:

- vSphere 6.0 oder höher.
- Geeignete Hardware. Bestimmte Speicherhersteller sind für die Bereitstellung von Speicheranbietern verantwortlich, die in vSphere integriert werden können und VVOL unterstützen. Jeder Speicheranbieter muss durch VMware zertifiziert und ordnungsgemäß bereitgestellt sein.
- Alle virtuellen Festplatten, die Sie in einem virtuellen Datenspeicher bereitstellen, müssen ein gerades Vielfaches von 1 MB sein.

VVOL ist eine Funktion von vSphere 6.0. Weitere Informationen zu Anforderungen, Funktionalität, Hintergrund und Setup-Anforderungen finden Sie in den Themen zu VVOL im Dokument *vSphere Storage*.

## Reduzieren von Speicheranforderungen mit View Composer

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

View Composer arbeitet mit einem Basis-Image (bzw. einer übergeordneten virtuellen Maschine) und erstellt einen Pool mit bis zu 2.000 virtuellen Linked-Clone-Maschinen. Jeder Linked Clone fungiert als unabhängiger Desktop (mit eindeutigem/r Hostnamen/IP-Adresse), aber dennoch benötigt der Linked Clone wesentlich weniger Speicherplatz.

## Replizierte Klone und Linked Clones auf dem gleichen Datenspeicher

Wenn Sie einen Linked-Clone-Desktop-Pool oder eine Farm von Microsoft RDS-Hosts erstellen, wird zunächst ein vollständiger Clone von der übergeordneten virtuellen Maschine angelegt. 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 Linked-Clone Desktop-Pools aus einer LUN in eine andere LUN oder Linked-Clone Desktop-Pools in einen vSAN-Datenspeicher bzw. von einem vSAN-Datenspeicher in eine LUN verschieben.

## Replizierte Klone und Linked Clones auf verschiedenen Datenspeichern

Alternativ dazu können Sie View Composer-Replikate und Linked Clones 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 Linked Clones 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 Linked Clones 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 Antivirenschans.

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

Bei Verwendung von vSAN-Datenspeichern oder VVOL-Datenspeichern (virtuelle Volumes) ist es nicht möglich, manuell andere Datenspeicher für Replikate und Linked Clones auszuwählen. Da vSAN und VVOL (virtuelle Volumes) automatisch Objekte auf dem passenden Festplattentyp ablegen und alle E/A-Vorgänge zwischenspeichern, ist die Verwendung der mehrstufigen Replikatspeicherung für vSAN- und VVOL-Datenspeicher nicht erforderlich.

## Löschbare Festplatten für Auslagerungsdateien und temporäre Dateien

Bei der Erstellung eines Linked-Clone-Pools oder einer Farm 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 von Linked Clones 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 Linked Clone 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.

## 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 vSAN-Datenspeicher, die auch lokale Speicherfestplatten verwenden, aber bestimmte Hardware erfordern, wie im vorherigen Abschnitt über vSAN 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 Linked Clones 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 Linked Clones erfolgreich auf lokalen Datenspeichern bereitstellen.

Weitere Informationen finden Sie im Kapitel zur Erstellung von Desktop-Pools im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

## Reduzieren der Speicheranforderungen mit Instant Clones

Die Instant-Clones-Funktion nutzt die vSphere vmFork-Technologie (verfügbar mit vSphere 6.0U1 und höher) zur Stilllegung eines ausgeführten Basis-Image oder einer übergeordneten virtuellen Maschine und erstellt auf schnelle Weise einen Pool von virtuellen Desktops bzw. passt diesen an.

Instant Clones nutzen mit der übergeordneten virtuellen Maschine zum Zeitpunkt der Erstellung nicht nur die virtuellen Festplatten gemeinsam, sondern auch deren Arbeitsspeicher. Jeder Instant Clone fungiert als unabhängiger Desktop (mit eindeutigem/r Hostnamen/IP-Adresse), allerdings benötigt der Instant Clone wesentlich weniger Speicherplatz. Instant Clones verringern die erforderliche Speicherkapazität um 50% bis 90%. Ebenso werden die gesamten Arbeitsspeicheranforderungen zum Zeitpunkt der Klonerstellung reduziert. Weitere Informationen zu Speicheranforderungen und Größenbeschränkungen finden Sie im VMware-Knowledgebase-Artikel <https://kb.vmware.com/kb/2150348>.

## Replikate und Instant Clones auf dem gleichen Datenspeicher

Wenn Sie einen Instant-Clone-Desktop-Pool erstellen, wird von der virtuellen Master-Maschine ein erster vollständiger Klon angelegt. 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.

## Replikate und Instant Clones auf verschiedenen Datenspeichern

Alternativ dazu können Sie Instant-Clone-Replikate und Instant Clones 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 Instant Clones 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 Instant Clones in einem großen Pool geeignet sind. Konfigurationen des mehrstufigen Speichers können zur kostengünstigen Verarbeitung intensiver E/A-Szenarios verwendet werden. Hierzu gehört die gleichzeitige Ausführung geplanter Antivirenschans.

Bei Verwendung von vSAN-Datenspeichern ist es nicht möglich, manuell andere Datenspeicher für Replikate und Instant Clones auszuwählen. Da vSAN Objekte automatisch auf dem passenden Festplattentyp ablegt und alle E/A-Vorgänge zwischenspeichert, ist die Verwendung der mehrstufigen Replikatspeicherung für vSAN-Datenspeicher nicht erforderlich. Instant-Clone-Pools werden in Verbindung mit vSAN-Datenspeichern unterstützt.

## Speichern von Instant Clones auf lokalen Datenspeichern

Virtuelle Instant-Clone-Maschinen können auf lokalen Datenspeichern gespeichert werden, die interne Ersatzfestplatten auf ESXi-Hosts darstellen. 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 Horizon 7-Umgebungen Vorteile, ist jedoch nicht für alle Umgebungen geeignet.

---

**Hinweis** Die in diesem Thema beschriebenen Einschränkungen gelten nicht für vSAN-Datenspeicher, die auch lokale Speicherfestplatten verwenden, jedoch spezifische Hardware benötigen.

---

Die Verwendung von lokalen Speichern funktioniert wahrscheinlich am besten, wenn die Horizon 7-Desktops in Ihrer Umgebung zustandsfrei sind. So könnten Sie etwa lokale Datenspeicher verwenden, wenn Sie zustandsfreie Kiosks oder Unterrichts- und Schulungsstationen bereitstellen.

Ziehen Sie die Verwendung von lokalen Datenspeichern in Betracht, wenn Ihre virtuellen Maschinen über dynamische Zuweisungen verfügen, nicht für einzelne Endbenutzer vorgesehen sind und in regelmäßigen Abständen, wie beispielsweise bei der Abmeldung von Benutzern, gelöscht oder aktualisiert werden. Mit diesem Ansatz können Sie die Festplattennutzung auf jedem lokalen Datenspeicher steuern, ohne die virtuellen Maschinen über Datenspeicher hinweg zu verschieben oder deren Last auszugleichen.

Sie müssen jedoch die Einschränkungen berücksichtigen, die die Verwendung von lokalen Datenspeichern in Ihrer Horizon 7-Desktop- oder Farmbereitstellung mit sich bringen:

- Sie können vMotion nicht zur Verwaltung von virtuellen Volumes verwenden.
- Sie können VMware High Availability nicht verwenden.
- Sie können den vSphere Distributed Resource Scheduler (DRS) nicht verwenden.

Wenn Sie Instant Clones auf einem einzelnen ESXi-Host mit einem lokalen Datenspeicher bereitstellen, müssen Sie einen Cluster mit diesem ESXi-Host konfigurieren. Wenn Sie über einen Cluster mit zwei oder mehr ESXi-Hosts mit lokalen Datenspeichern verfügen, müssen Sie den lokalen Datenspeicher jedes einzelnen Hosts im Cluster auswählen. Andernfalls kann der Instant Clone nicht erstellt werden. Dieses Verhalten unterscheidet sich vom Verhalten lokaler Datenspeicher mit View Composer-Linked-Clones.

- Sie können ein Replikat und Instant Clones nicht in verschiedenen Datenspeichern speichern.

- Wenn Sie lokale herkömmliche Festplatten auswählen, kommt die Performance möglicherweise nicht an kommerziell erhältliche Speicher-Arrays heran. Lokale herkömmliche Laufwerke und ein Speicher-Array mögen vielleicht ähnliche Kapazitäten aufweisen, jedoch haben lokale herkömmliche Laufwerke nicht dieselben Durchsatzraten wie ein Speicher-Array. Der Durchsatz erhöht sich mit steigender Spindelzahl. Wenn Sie direkt angeschlossene SSDs (Solid-State-Drives) auswählen, übersteigt die Performance wahrscheinlich diejenige vieler Speicher-Arrays.
- Wenn Sie die Vorteile des lokalen Speichers nutzen möchten, müssen Sie sorgfältig die Auswirkungen bedenken, wenn Ihnen vMotion, Hochverfügbarkeit, DRS und andere Funktionen nicht zur Verfügung stehen. Wenn Sie für die Nutzung lokaler Festplatten die Zahl der virtuellen Maschinen und deren Festplattenwachstum steuern, können Sie, wenn Sie dynamische Zuweisungen verwenden und regelmäßig Aktualisierungs- und Löschvorgänge ausführen, Instant Clones erfolgreich auf lokalen Datenspeichern bereitstellen.
- Lokale Datenspeicher werden für Instant Clones sowohl für virtuelle Desktops wie für veröffentlichte Desktops unterstützt.

## Unterschiede zwischen Instant Clones und View Composer-Linked-Clones

Da Instant Clones erheblich schneller erstellt werden können als Linked Clones, sind die nachfolgenden Linked-Clone-Funktionen bei der Bereitstellung eines Instant-Clone-Pools nicht mehr erforderlich:

- Instant Clone-Pools unterstützen keine Konfiguration einer separaten, temporären virtuellen Festplatte zum Speichern der Auslagerungs- und temporären Dateien des Gastbetriebssystems. Jedes Mal, wenn sich ein Benutzer von einem Instant Clone abmeldet, löscht View automatisch den Clone, stellt dann auf der Grundlage des neuesten für den Pool verfügbaren Betriebssystem-Image einen anderen Instant Clone bereit und schaltet diesen ein. Alle Auslagerungs- und temporären Dateien des Gastbetriebssystems werden bei der Abmeldung automatisch gelöscht.
- Instant-Clone-Pools unterstützen nicht das Erstellen einer separaten persistenten virtuellen Festplatte für jeden virtuellen Desktop. Stattdessen können Sie die Windows-Profil- und -Anwendungsdaten des Endbenutzers auf benutzerbeschreibbaren Festplatten von App Volumes speichern. Wenn sich der Endbenutzer anmeldet, wird für ihn eine benutzerbeschreibbare Festplatte mit einem Instant-Clone-Desktop verknüpft. Darüber hinaus können benutzerbeschreibbare Festplatten zum Speichern benutzerinstallierter Anwendungen verwendet werden.
- Aufgrund des kurzlebigen Charakters von Instant Clone-Desktops wird das speichereffiziente Festplattenformat SE-Sparse mit seinem Bereinigungs- oder Verkleinerungsprozess von Instant Clones nicht unterstützt.
- Instant-Clone-Desktop-Pools sind mit Storage vMotion kompatibel. Linked-Clone-Desktop-Pools von View Composer sind nicht mit Storage vMotion kompatibel.

## Anwendungsbereitstellung

Mit Horizon 7 stehen mehrere Optionen zur Anwendungsbereitstellung zur Verfügung: Sie können herkömmliche Anwendungsbereitstellungstechniken verwenden, veröffentlichte Anwendungen statt eines Remote-Desktops bereitstellen, mit VMware ThinApp erstellte Anwendungspakete verteilen, Anwendungen als Bestandteil eines View Composer- oder Instant-Clone-Basis-Image bereitstellen oder Anwendungen mit App Volumes anfügen.

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

Sie können für Endbenutzer veröffentlichte Anwendungen anstelle von Remote-Desktops bereitstellen. Auf kleinen mobilen Endgeräten ist die Navigation in einzelnen veröffentlichten Anwendungen 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.

- **Bereitstellen von Anwendungen und System-Updates mit Instant Clones**

Da Instant-Clone-Desktop-Pools ein Basis-Image gemeinsam nutzen, können Sie Updates und Patches schnell durch Aktualisierung der übergeordneten virtuellen Maschine bereitstellen.

- **Verwalten von VMware ThinApp-Anwendungen in Horizon 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.

- **Bereitstellen und Verwalten von Anwendungen mit App Volumes**

VMware App Volumes stellt durch die Virtualisierung der Anwendungen über der Betriebssystemebene eine alternative Möglichkeit der Anwendungsverwaltung bereit. Bei Anwendung dieses Konzepts verhalten sich Anwendungen, Datendateien, Einstellungen, Middleware und Konfigurationen wie getrennte, geschichtete Container.

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

Horizon 7 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 veröffentlichte Anwendungen anstelle von Remote-Desktops bereitstellen. Auf kleinen mobilen Endgeräten ist die Navigation in einzelnen veröffentlichten Anwendungen möglicherweise einfacher.

Endbenutzer können für den Zugriff auf veröffentlichte Windows-basierte Anwendungen denselben Horizon Client verwenden wie zuvor für den Zugriff auf Remote-Desktops. Außerdem verwenden sie dasselbe Blast Extreme- oder PCoIP-Anzeigeprotokoll.

Zur Bereitstellung einer veröffentlichten Anwendung 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. Empfehlungen für die Farmgröße finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150348>.

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)

---

**Hinweis** Da Sie auch View Composer für das Erstellen von Farmen von Linked-Clone-Microsoft-RDS-Hosts verwenden können, ermöglicht die Funktion zur Neuzusammenstellung die Aktualisierung des Gastbetriebssystems und der Anwendungen auf den RDS-Hosts.

---

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.



## Bereitstellen von Anwendungen und System-Updates mit Instant Clones

Da Instant-Clone-Desktop-Pools ein Basis-Image gemeinsam nutzen, können Sie Updates und Patches schnell durch Aktualisierung der übergeordneten virtuellen Maschine bereitstellen.

Mit der Image-Übertragungsfunktion können Sie fortlaufend Änderungen an der übergeordneten virtuellen Maschine vornehmen, einen Snapshot des neuen Status erstellen und die neue Image-Version an alle Benutzer und Desktops übertragen. Mit fortlaufenden Aktualisierungen kann die mit der Poolwartung verbundene Ausfallzeit minimiert werden. Wenn sich ein Benutzer von einem virtuellen Instant-Clone-Desktop abmeldet, löscht Horizon 7 den Instant Clone und erstellt dann aus der aktuellen Image-Version einen neuen Instant Clone, der für den nächsten angemeldeten Benutzer bereit steht.

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)

## Verwalten von VMware ThinApp -Anwendungen in Horizon 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 Horizon 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 Identity Manager 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 Architekturaspekte berücksichtigt werden wie bei der herkömmlichen Softwarebereitstellung mit MSI-Paketen. Die Speicherkonfiguration für das Anwendungs-Repository muss sowohl für per Streaming übertragene Anwendungen als auch für auf Remote-Desktops installierte ThinApp-Pakete berücksichtigt werden.

## Bereitstellen und Verwalten von Anwendungen mit App Volumes

VMware App Volumes stellt durch die Virtualisierung der Anwendungen über der Betriebssystemebene eine alternative Möglichkeit der Anwendungsverwaltung bereit. Bei Anwendung dieses Konzepts verhalten sich Anwendungen, Datendateien, Einstellungen, Middleware und Konfigurationen wie getrennte, geschichtete Container.

Diese Container werden als Anwendungsstapel (oder AppStacks) bezeichnet, wenn der schreibgeschützte Modus aktiv ist, bzw. als beschreibbare Volumes, wenn der Lesen-Schreiben-Modus aktiv ist. Administratoren können mit App Volumes Manager AppStacks erstellen und Anwendungsberechtigungen zuweisen sowie bereitgestellte AppStacks dem System, einem Benutzer oder einer Gruppe zustellen. Über App Volumes zugestellte Anwendungen werden wie vom System installierte Anwendungen angezeigt und bleiben den Benutzern über verschiedene Sitzungen und Geräte hinweg zugeordnet. Administratoren können Anwendungen in Echtzeit aktualisieren oder ersetzen und zugewiesene Anwendungen entweder sofort, wenn der Benutzer noch angemeldet ist, oder bei der nächsten Anmeldung bzw. beim nächsten Neustart entfernen.

Weitere Informationen finden Sie in der Dokumentation zu VMware App Volumes, die unter <https://docs.vmware.com/de/VMware-App-Volumes/index.html> verfügbar ist.

## Verwenden von bestehenden Prozessen oder VMware Mirage für die Anwendungsbereitstellung

Horizon 7 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 über feste Anforderungen für die Installation ihrer eigenen Anwendungen verfügen und wenn diese Anwendungen dauerhaft auf dem Remote-Desktop gültig sind, können Sie für die Anwendungsbereitstellung anstelle von View Composer Instant Clones in Verbindung mit App Volumes verwenden. Alternativ erstellen Sie dedizierte Full-Clone-Desktops, ermöglichen Sie Benutzern die Installation von Anwendungen und verwalten bzw. aktualisieren Sie dann mit Mirage die Desktops, ohne benutzerinstallierte 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

Horizon 7 bietet zahlreiche administrative Gruppenrichtlinien-ADMX-Vorlagen für eine zentrale Verwaltung und Konfiguration der Horizon 7-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
- Konfiguration des Verbindungsservers
- Horizon Client-Konfiguration
- Horizon 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 Horizon Administrator zur Verfügung stehen. Sie können Gruppenrichtlinienobjekte auch nutzen, um Richtlinien festzulegen, die nicht auf der Benutzeroberfläche verfügbar sind. Eine vollständige Liste und Beschreibung der über ADMX-Vorlagen verfügbaren Einstellungen finden Sie unter *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

## Verwenden von intelligenten Richtlinien

Sie können mit Intelligente Richtlinien auch Richtlinien zur Steuerung des Verhaltens der USB-Umleitung, des virtuellen Drucks, der Zwischenablagenumleitung, der Clientlaufwerksumleitung und der Funktionen für das PCoIP-Anzeigeprotokoll auf bestimmten Remote-Desktops erstellen. Diese Funktion erfordert User Environment Manager.

Mit Intelligente Richtlinien besteht die Möglichkeit, Richtlinien zu erstellen, die nur beim Eintreten bestimmter Bedingungen wirksam werden. Sie können beispielsweise eine Richtlinie konfigurieren, mit der die Clientlaufwerksumleitung dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit einem Remote-Desktop herstellt.

Im Allgemeinen überschreiben Horizon-Richtlinieneinstellungen, die Sie für Remote-Desktop-Funktionen in User Environment Manager konfiguriert haben, die entsprechenden Registrierungsschlüssel und Gruppenrichtlinieneinstellungen.

# Architekturentwurfselemente und Planungsanleitungen für Remote-Desktop-Bereitstellungen

## 4

Ein typischer Horizon 7-Architekturentwurf verwendet eine Pod-Strategie. Die Pod-Definitionen können je nach Hardwarekonfiguration, den verwendeten Horizon 7- 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 Horizon 7-Lösung zu berücksichtigen ist.

**Wichtig** Die folgenden Themen werden nicht in diesem Kapitel behandelt:

Architekturentwurf für gehostete Anwendungen	Ein Horizon 7-Pod kann Farmen von Microsoft RDS-Hosts unterstützen, wobei jede Farm RDS-Hosts enthält. Weitere Informationen finden Sie unter <i>Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7</i> . Wenn Sie beabsichtigen, virtuelle Maschinen für RDS-Hosts zu verwenden, lesen Sie auch <a href="#">Konfiguration von virtuellen Maschinen als RDS-Hosts</a> .
Architekturentwurf für das Horizon 7 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 Horizon 7 Agent Direct-Connection-Plug-Ins</i> .

Dieses Kapitel enthält die folgenden Themen:

- [Anforderungen virtueller Maschinen für Remote-Desktops](#)
- [Horizon 7 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](#)
- [Horizon-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen](#)
- [vSphere-Cluster](#)
- [Speicher- und Bandbreitenanforderungen](#)

- [Horizon 7-Bausteine](#)
- [Horizon 7-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 Festplattenspeichergroße, 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 Festplattenspeichergroße, 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.

<b>Sachbearbeiter</b>	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.
<b>Büroanwender</b>	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.
<b>Hauptbenutzer</b>	Hauptbenutzer sind Anwendungsentwickler und Nutzer grafikintensiver Anwendungen.
<b>Kioskbenutzer</b>	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.
- 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 View Composer-Linked-Clone-VMs 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 von Linked Clones und kann außerdem die Leistung verbessern. Wenngleich Sie die Größe unter Windows anpassen können, kann sich dies negativ auf die Anwendungsleistung auswirken.

Bei Instant Clones werden alle Auslagerungsdateien und temporären Dateien von Gastbetriebssystemen beim Abmeldevorgang automatisch gelöscht, sodass sie nicht sehr groß werden können. Jedes Mal, wenn sich ein Benutzer von einem Instant Clone-Desktop abmeldet, löscht Horizon den Clone, stellt dann auf der Grundlage des neuesten für den Pool verfügbaren Betriebssystem-Image einen anderen Instant Clone bereit und schaltet diesen ein.

### Windows-Ruhezustandsdatei für Laptops

Die Größe dieser Datei kann 100 % des Gastarbeitsspeichers entsprechen. Sie können diese Datei bedenkenlos löschen, da sie in Horizon-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 Verwendung von PCoIP oder Blast Extreme

Neben dem Systemarbeitsspeicher benötigt eine virtuelle Maschine auch einen gewissen kleineren Umfang an Arbeitsspeicher auf dem ESXi-Host für Video-Overheads. Diese Anforderung an VRAM-Größe hängt von der jeweiligen Bildschirmauflösung und der Anzahl der für den Endbenutzer konfigurierten Bildschirme ab. [Tabelle 4-1](#) zeigt die Menge des Arbeitsspeicher-Overheads an, der für verschiedene Konfigurationen benötigt wird. Die in den Spalten angegebenen Arbeitsspeicherwerte sind zusätzlich zum Arbeitsspeicher zu verstehen, der für andere PCoIP- oder Blast Extreme-Funktionen benötigt wird.

**Tabelle 4-1. PCoIP- oder Blast Extreme-Clientanzeige-Overhead**

Standardanzeigeauflösung	Breite (in Pixel)	Höhe (in Pixel)	Overhead bei einem Monitor	Overhead bei zwei Monitoren	Overhead bei drei Monitoren	Overhead bei vier Monitoren
VGA	640	480	1,20 MB	3,20 MB	4,80 MB	5,60 MB
WXGA	1280	800	4,00 MB	12,50 MB	18,75 MB	25,00 MB
1080p	1920	1080	8,00 MB	25,40 MB	38,00 MB	50,60 MB
WQXGA	2560	1600	16,00 MB	60,00 MB	84,80 MB	109,60 MB
UHD (4K)	3840	2160	32,00 MB	78,00 MB	124,00 MB	Nicht unterstützt

Zur Berechnung der Systemanforderungen müssen die VRAM-Werte zu den Werten für den grundlegenden Arbeitsspeicher der virtuellen Maschine hinzu gezählt werden. Der Overhead-Speicher wird automatisch berechnet und konfiguriert, wenn Sie in Horizon Administrator die maximale Anzahl an Monitoren und die Bildschirmauflösung festlegen.

Wenn Sie die 3D-Wiedergabefunktion verwenden und Soft3D oder vSGA auswählen, können Sie unter Verwendung der zusätzlich benötigten VRAM-Werte in einem Horizon Administrator-Steuerelement zur Konfiguration von VRAM für 3D-Gäste eine erneute Berechnung durchführen. Alternativ und für andere Arten der Grafikbeschleunigung als Soft3D und vSGA können Sie die genaue VRAM-Speichergröße angeben, wenn Sie VRAM mithilfe des vSphere Client verwalten.

Standardmäßig entspricht die Konfiguration mit mehreren Monitoren der Hosttopologie. Für mehr als zwei Monitore wird ein zusätzlicher Overhead im Voraus berechnet, damit weitere Topologie-Schemata möglich sind. Wenn beim Start der Remote-Desktop-Sitzung ein schwarzer Bildschirm angezeigt wird, prüfen Sie, ob die Werte für die Anzahl der Monitore und die Bildschirmauflösung, die in Horizon Administrator festgelegt sind, dem Hostsystem entsprechen. Oder passen Sie die Größe des Speichers manuell an, indem Sie in Horizon Administrator **Verwaltung mithilfe des vSphere Client** wählen und dann den Gesamtwert für den Videospeicher auf den Höchstwert 128 MB festlegen.

## 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 32 Bit-Desktops unter Windows 7 oder höher sowie 2 GB für 64 Bit-Desktops unter Windows 7 oder höher zuzuteilen. 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. Virtuelle duple oder vierfache CPUs sind für virtuelle 64-Bit-Windows 7 Maschinen empfohlen, die intensive Aufgaben ausführen, beispielsweise CAD-Anwendungen, Abspielen von HD-Videos oder Bildschirmauflösungen von 4K.
- 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:

- Verwenden Sie Instant Clones oder View Composer-Linked-Clones zum Aktualisieren von Images, anstatt mit Softwareverwaltungs-Agenten auf jeden einzelnen virtuellen Desktop Software-Updates herunterzuladen.
- 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<sup>®</sup> 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. Weitere Einzelheiten dazu finden Sie im *Einrichten von virtuellen Desktops in Horizon 7*-Dokument.
- Wählen Sie eine virtuelle Festplattengröße, die künftiges Wachstum zulässt, aber nicht unrealistisch groß ist.
- Verwenden Sie zentrale Dateifreigaben oder eine persistente View Composer-Festplatte oder App Volumes für benutzergenerierte 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.

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.

Bei Verwendung von Instant Clones werden die .vmdk-Dateien im Verlauf einer Anmeldesitzung größer. Sobald sich ein Benutzer abmeldet, wird der Instant-Clone-Desktop automatisch gelöscht, und es wird ein neuer Instant Clone erstellt, der für den nächsten angemeldeten Benutzer bereit steht. Mit diesem Vorgehen wird der Desktop effektiv aktualisiert und auf seine ursprüngliche Größe zurückgesetzt.

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

## Horizon 7 ESXi -Knoten

Bei einem Knoten handelt es sich um einen einzelnen VMware ESXi-Host, auf dem virtuelle Desktop-Maschinen in einer Horizon 7-Bereitstellung gehostet werden.

Horizon 7 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 Arbeitsspeicher Menge 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, Speicheranbindung, Verwaltbarkeit und andere Aspekte dafür ausschlaggebend sein, die Anzahl der Server in einer Bereitstellung zu minimieren.

- In Horizon 7 ist die View-Speicherbeschleunigung standardmäßig aktiviert, sodass Hosts mit ESXi 5.5 Update 2 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 *VMware vSphereMaximalwerte für die Konfiguration von* .

## Desktop-Pools für bestimmte Nutzertypen

Horizon 7 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, die auch als nicht persistente Desktops bezeichnet werden, bieten viele Vorteile. Sie lassen sich z. B. leichter unterstützen und verursachen geringere Speicherkosten. Außerdem müssen virtuelle Maschinen nur begrenzt gesichert werden und die Disaster Recovery- und Business Continuity-Optionen sind weniger komplex und kostengünstiger.

### **Zustandsbehaftete Desktop-Images**

Diese Images, die auch als persistente Desktops bezeichnet werden, erfordern u. U. herkömmliche Image-Verwaltungstechniken. Zustandsbehaftete Images können in Verbindung mit bestimmten Speichersystemtechnologien geringe Speicherkosten verursachen. Sicherungs- und Wiederherstellungstechnologien wie VMware Site Recovery Manager sind bei der Erwägung von Sicherungs-, Disaster Recovery- und Business Continuity-Strategien von großer Bedeutung.

Zustandslose Desktop-Images können in Horizon 7 auf zweierlei Weise erstellt werden:

- Sie können dynamische Zuweisungspools oder dedizierte Zuweisungspools von Instant-Clone-VMs erstellen. Ordnerumleitung und servergespeicherte Profile lassen sich optional zum Speichern von Benutzerdaten verwenden.
- Sie können View Composer zum Erstellen dynamischer oder dedizierter Zuweisungspools von Linked-Clone-VMs verwenden. Die Profile für die Ordnerumleitung und das Roaming können optional für das Speichern von Benutzerdaten oder das Konfigurieren persistenter Festplatten für persistente Benutzerdaten verwendet werden.

Zustandsbehaftete Desktop-Images können in Horizon 7 auf verschiedene Weise erstellt werden:

- Sie können vollständige Klone und vollständige virtuelle Maschinen erstellen. Einige Hersteller von Speichermedien bieten kostengünstige Speicherlösungen für vollständige Klone 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.
- Sie können Pools mit virtuellen Instant-Clone- oder Linked-Clone-Maschinen erstellen und mithilfe benutzerbeschreibbarer App Volumes-Festplatten Benutzerdaten und vom Benutzer installierte Anwendungen anfügen.

Ob Sie zustandslose oder zustandsbehaftete Desktops erstellen, hängt vom jeweiligen Nutzertyp ab.

- **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 die folgenden Pooleinstellungen für Instant-Clone-Desktop-Pools:

- Die Ressourcennutzung lässt sich für Instant-Clone-Pools durch eine Bereitstellung nach Bedarf optimieren, mit der der Pool je nach Nutzung vergrößert oder verkleinert wird. Stellen Sie sicher, dass ausreichend Ersatz-Desktops zur Abdeckung der Anmeldequote festgelegt sind.
- Für Instant-Clone-Desktop-Pools löscht Horizon 7 automatisch den Instant Clone, sobald sich der Benutzer abmeldet. Da immer ein neuer Instant Clone erstellt wird und für den nächsten Benutzer zum Anmelden zur Verfügung steht, wird der Desktop praktisch bei jeder Abmeldung aktualisiert.

Verwenden Sie die folgenden Pooleinstellungen für Linked-Clone-Desktop-Pools von View Composer:

- Für View Composer-Desktop-Pools legen Sie bei Bedarf die Aktion fest, die beim Abmelden von Benutzern 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.

- Gegebenenfalls speichern Sie bei der Benutzung von View Composer-Linked-Clone-Pools die Desktops auf lokalen ESXi-Datenspeichern. 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](#). Instant-Clone-Pools werden in Verbindung mit lokalen Datenspeichern nicht unterstützt.

---

**Hinweis** Informationen zu anderen Arten von Speicheroptionen finden Sie unter [Reduzieren und Verwalten von Speicheranforderungen](#).

---

- 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** Persona Management erleichtert die Implementierung eines Pools mit dynamischer Zuweisung für diejenigen 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 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.

---

Verwenden Sie die folgenden allgemeinen Pooleinstellungen für alle Desktop-Pools:

- 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 Instant-Clone- oder View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Datacenter beanspruchen als vollständige virtuelle Maschinen.

## 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.



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 die folgenden Pooleinstellungen für Instant-Clone-Desktop-Pools:

- Wenn Sie Instant-Clone-Desktops verwenden, implementieren Sie die Dateifreigabe, servergespeicherte Profile oder eine andere Profilverwaltungslösung.

Verwenden Sie die folgenden Pooleinstellungen für Linked-Clone-Desktop-Pools von View Composer:

- Wenn Sie View Composer mit virtuellen Desktops der Version vSphere 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 Persona Management, servergespeicherte Profile oder andere Profilverwaltungslösungen. Sie können durch Konfiguration persistenter Festplatten auch die Linked-Clone-Betriebssystemfestplatten aktualisieren sowie neu zusammenstellen und eine Kopie des Benutzerprofils auf den persistenten Festplatten speichern.
- 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 die folgenden allgemeinen Pooleinstellungen für alle Desktop-Pools:

- Manche Hauptbenutzer und Büroanwender wie Wirtschaftsprüfer, Vertriebsleiter oder Marktforschungsanalysten müssen sich unter Umständen jedes Mal beim gleichen Desktop anmelden. Erstellen Sie für diese Personen dedizierte Zuweisungspools.
- 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, stehen zwei Optionen zur Verfügung. Eine Möglichkeit besteht darin, Desktops vollständiger virtueller Maschinen zu erstellen.

Die andere Option besteht in der Erstellung eines Linked-Clone- oder Instant Clone-Pools sowie im Speichern benutzerinstallierter Anwendungen und Benutzerdaten zwischen Anmeldesitzungen mit App Volumes.

- Wenn Büroanwender benutzerinstallierte Anwendungen nur vorübergehend benötigen, können Sie View Composer-Linked-Clone-Desktops oder Instant-Clone-Desktops erstellen. Die Desktop-Images nutzen dasselbe Basis-Image und benötigen weniger Speicherplatz als vollständige virtuelle Maschinen.

## 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 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 *Horizon 7-Verwaltung* unter den Themen zum Kioskmodus dokumentiert sind.

Im Zuge dieser Einrichtung können Sie die im Folgenden aufgeführten Instant-Clone-Desktop-Pool-Einstellungen verwenden.

- Werden Instant-Clone-Desktop-Pools verwendet, dann löscht Horizon 7 automatisch den Instant Clone, wenn sich der Benutzer abmeldet. Da immer ein neuer Instant Clone erstellt wird und für den nächsten Benutzer zum Anmelden zur Verfügung steht, wird der Desktop praktisch bei jeder Abmeldung aktualisiert.

Bei dieser Einrichtung können Sie die im Folgenden aufgeführten Einstellungen für Linked-Clone-Desktop-Pools von View Composer verwenden.

- Wenn Sie View Composer-Linked-Clone-Desktops verwenden, sollten Sie eine Aktualisierungsrichtlinie einrichten, damit der Desktop häufig aktualisiert wird, z. B. bei jeder Benutzerabmeldung.

- 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](#). Instant-Clone-Pools werden in Verbindung mit lokalen Datenspeichern nicht unterstützt.

---

**Hinweis** Informationen zu anderen Arten von Speicheroptionen finden Sie unter [Reduzieren und Verwalten von Speicheranforderungen](#).

---

Im Rahmen dieser Einrichtung können Sie die im Folgenden aufgeführten allgemeinen Einstellungen für alle Desktop-Pools 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 Instant-Clone- oder View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Datacenter beanspruchen als vollständige virtuelle Maschinen.
- Verwenden Sie ein Active Directory-Gruppenrichtlinienobjekt zum Konfigurieren der standortbasierten Druckfunktion, damit der Desktop den nächstgelegenen Drucker verwendet. Eine vollständige Liste und Beschreibung der über administrative Gruppenrichtlinien-ADMX-Vorlagen verfügbaren Einstellungen finden Sie unter *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.
- Legen Sie mit einem Gruppenrichtlinienobjekt oder mit intelligenten Richtlinien fest, ob lokale USB-Geräte mit dem Desktop verbunden werden, wenn der Desktop gestartet wird oder wenn das jeweilige USB-Gerät an den Clientcomputer angeschlossen wird.

## Konfigurieren virtueller Maschinen für View-Desktops

Die Beispieleinstellungen für Elemente wie Arbeitsspeicher, Anzahl virtueller Prozessoren und Festplattenspeicher sind Horizon 7-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 7 oder höher.

**Tabelle 4-2. 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)
Virtueller SCSI-Adaptertyp	LSI Logic SAS (Standardeinstellung)
Virtueller Netzwerkadapter	VMXNET 3

## Konfiguration von virtuellen Maschinen als RDS-Hosts

Verwenden Sie RDS-Hosts (Remotedesktopdienste), um veröffentlichte Anwendungen und sitzungs-basierte 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 4-3. Beispiel einer virtuellen Maschine eines RDS-Hosts**

Element	Beispiel
Betriebssystem	64 Bit Windows Server 2008 R2 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 sitzungsbasierte Remote-Desktopverbindungen und veröffentlichte Anwendungsverbindungen)	50

**Hinweis** Wenn Sie am unteren Ende der Ressourcenspezifikationen RDS-Hosts konfigurieren, treten möglicherweise Ressourceneinschränkungen auf, wenn alle Funktionen anstelle der Standardinstallation verwendet werden.

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.
- Bei manchen Konfigurationen können Cluster bis zu 32 Hosts enthalten. Bei anderen Konfigurationen sind Cluster auf acht Hosts beschränkt. Weitere Informationen finden Sie unter [vSphere-Cluster](#).
- 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 Horizon 7 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 4-4. 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	10-24 GB, je nach vSphere-Version

**Tabelle 4-4. Beispiel für eine virtuelle vCenter Server -Maschine (Fortsetzung)**

Element	Beispiel für eine vCenter Server-Instanz, die 10.000 Desktops verwaltet	Beispiel für eine vCenter Server-Instanz, die 2.000 Desktops verwaltet
Virtuelle CPU	16	2-8 GB, je nach vSphere-Version
Kapazität der Systemfestplatte	180GB	40 GB
Virtueller SCSI-Adaptertyp	LSI Logic SAS (Standardeinstellung für Windows Server 2008)	LSI Logic SAS (Standardeinstellung für Windows Server 2008)
Virtueller Netzwerkadapter	E1000 (Standard)	VMXNET 3 (E1000, die Standardeinstellung, ist ausreichend)
Maximale Anzahl gleichzeitiger vCenter-Bereitstellungsvorgänge	20	20
Maximale Anzahl gleichzeitiger Betriebsvorgänge	50	50

**Tabelle 4-5. 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 oder mehr, je nach vSphere-Version	4-10GB, je nach vSphere-Version
Virtuelle CPU	4 GB oder mehr, je nach vSphere-Version	2-4 GB, je nach vSphere-Version
Kapazität der Systemfestplatte	50GB	40 GB
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.

## Horizon-Verbindungsserver: Konfigurieren von Maximalwerten und virtuellen Maschinen

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

## Konfiguration des Verbindungsservers

Auch wenn Sie den Verbindungsserver auf einem physischen Computer installieren können, wird in diesem Beispiel eine virtuelle Maschine mit den im Beispiel einer virtuellen Maschine für 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 4-6. Beispiel einer virtuellen Maschine für View-Verbindungsserver**

Element	Beispiel
Betriebssystem	Eine Auflistung der unterstützten Betriebssysteme finden Sie im Dokument <i>Horizon 7-Installation</i> .
Arbeitsspeicher (RAM)	10 GB
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 beim Verbindungsserver

Sie können mehrere replizierte Verbindungsserver-Instanzen in einer Gruppe bereitstellen, um den Lastausgleich und eine hohe Verfügbarkeit zu unterstützen. Gruppen replizierter Instanzen sind auf die Unterstützung des Clusterings innerhalb einer im LAN verbundenen Umgebung mit einem einzigen Rechenzentrum ausgelegt.

**Wichtig** Zur Verwendung einer Gruppe replizierter Verbindungsserver-Instanzen in einem WAN, MAN (Metropolitan Area Network) oder einem anderen Netzwerk, das kein LAN ist, in einer Situation, in der die Horizon-Bereitstellung sich über mehrere Rechenzentren erstrecken muss, müssen Sie die Cloud-Pod-Architektur-Funktion verwenden. Sie können 25 Pods verbinden, um eine große Umgebung für das Brokering und die Verwaltung von Desktops in fünf Sites bereitzustellen, die sich an unterschiedlichen geografischen Standorten befinden. Auf diese Weise lassen sich Desktops und Anwendungen für bis zu 50.000 Sitzungen zur Verfügung stellen. Weitere Informationen finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

## Maximale Anzahl an Verbindungen für den Verbindungsserver

„Remote-Desktop-Verbindungen“ bietet Informationen zu den getesteten Einschränkungen in Bezug auf die Anzahl gleichzeitiger Verbindungen, die eine Horizon 7-Bereitstellung unterstützen kann.

**Tabelle 4-7. Remote-Desktop-Verbindungen**

Anzahl der Verbindungs- server-Instanzen pro Bereitstel- lung	Verbindungstyp	Maximale Anzahl gleichzeitiger Ver- bindungen
1 Verbindungsserver	Direkte Verbindung, RDP, Blast Extreme oder PCoIP	4.000 (getestete Konfiguration)
1 Verbindungsserver	Tunnelverbindung, RDP	2.000 (Standardkonfiguration) 4.000 (getestete Konfiguration)
1 Verbindungsserver	PCoIP Secure Gateway-Verbindung	2.000 (Standardkonfiguration) 4.000 (getestete Konfiguration)
1 Verbindungsserver	Blast Secure Gateway-Verbindung	2.000 (Standardkonfiguration) 4.000 (getestete Konfiguration)
1 Verbindungsserver	Unified Access auf physische PCs	2.000 (getestete Konfiguration)
1 Verbindungsserver	Unified Access auf RDS-Hosts	2.000 (getestete Konfiguration)
7 Verbindungsserver	Direkte Verbindung, RDP, Blast Extreme oder PCoIP	20.000 (getestete Konfiguration)

**Hinweis** Getestete Konfigurationen werden vollständig unterstützt. Um die getestete Konfiguration von maximal 4.000 gleichzeitigen Verbindungen auf einem einzelnen Verbindungsserver für eine Tunnelverbindung, ein PCoIP Secure Gateway und ein Blast Secure Gateway zu realisieren, erstellen Sie die `locked.properties`-Datei auf der virtuellen Maschine, auf der der Verbindungsserver installiert ist: `C:\Program Files\VMware\VMware View\Server\sslgateway\conf`. Legen Sie anschließend `maxConnections=4000` in der Datei `locked.properties` fest und starten Sie den Verbindungsserver neu. Unified Access Gateway unterstützt derzeit 2.000 Sitzungen, daher werden 14 Unified Access Gateway-Appliances für den Test von 20.000 Sitzungen verwendet.

Verbindungen über das PCoIP Secure Gateway sind erforderlich, wenn Sie für PCoIP-Verbindungen, deren Ausgangspunkt sich außerhalb des Firmennetzwerks befindet, Sicherheitsserver oder Unified Access Gateway-Appliances verwenden. Verbindungen über das Blast Secure Gateway sind erforderlich, wenn Sie für Blast Extreme- oder HTML Access-Verbindungen, deren Ausgangspunkt sich außerhalb des Unternehmensnetzwerks befindet, Sicherheitsserver oder Unified Access Gateway-Appliances verwenden. Tunnelverbindungen sind bei Verwendung von Sicherheitsservern oder Unified Access Gateway-Appliances für RDP-Verbindungen, deren Ausgangspunkt sich außerhalb des Unternehmensnetzwerks befindet, sowie für die Beschleunigung der USB-Umleitung und der Multimedia-Umleitung (MMR) mit einer Verbindung über das PCoIP oder Blast Secure Gateway erforderlich. Sie können mehrere Sicherheitsserver zu einer einzelnen Verbindungsserver-Instanz koppeln.

Obwohl ein einzelner Sicherheitsserver oder eine einzelne Unified Access Gateway-Appliance bis zu 2.000 gleichzeitige Verbindungen unterstützt, können Sie statt nur einem Sicherheitsserver pro Verbindungsserver-Instanz (mit 2.000 Sitzungen) auch 2 oder 4 Sicherheitsserver verwenden. Die Überwachung des Sicherheitsservers kann ergeben, dass die Aktivität für 2.000 Benutzer zu hoch ist. Der erforderliche Arbeitsspeicher und die CPU-Auslastung können es erforderlich machen, dass Sie mehr Sicher-



heitsserver pro Verbindungsserver-Instanz hinzufügen müssen, um die Arbeitslast zu verteilen. Beispielsweise können Sie zwei Sicherheitsserver für jeweils 1.000 Verbindungen oder aber vier Sicherheitsserver für jeweils 500 Verbindungen verwenden. Das Verhältnis zwischen Sicherheitsservern und Verbindungsserver-Instanzen hängt von den Anforderungen der jeweiligen Umgebung ab.

Die Anzahl der Verbindungen pro Unified Access Gateway-Appliance ist mit der Anzahl der Sicherheitsserver vergleichbar. Weitere Informationen zu Unified Access Gateway-Appliances finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

**Hinweis** In diesem Beispiel könnten 5 (entsprechend konfigurierte) Verbindungsserver-Instanzen 20.000 Verbindungen bewältigen. Zum Zweck der Verfügbarkeitsplanung und um Verbindungen von innerhalb und außerhalb des Unternehmensnetzwerks zu berücksichtigen, wird in der Tabelle jedoch der Wert 7 angezeigt.

Wenn beispielsweise 20.000 Benutzer vorhanden sind, von denen sich 16.000 innerhalb des Unternehmensnetzwerks befinden, benötigen Sie 5 Verbindungsserver-Instanzen innerhalb des Unternehmensnetzwerks. Wenn eine Instanz ausfällt, ist so gewährleistet, dass die Last von den vier verbleibenden Instanzen bewältigt werden kann. Ebenso benötigen Sie für die 4.000 Verbindungen, die von außerhalb des Firmennetzwerks stammen, 2 Verbindungsserver-Instanzen, damit die Arbeitslast beim Ausfall einer Instanz von der jeweils anderen Instanz verarbeitet werden kann.

Bei diesen Zahlen wird davon ausgegangen, dass externe Verbindungen über ein Gateway vorhanden sind. In diesem Beispiel würde jede der Verbindungsserver-Instanzen, die externe Verbindungen behandelt, mit 3 Sicherheitsservern gekoppelt, damit beim Ausfall eines Sicherheitsservers die beiden verbleibenden Sicherheitsserver die Last verarbeiten können. Wenn Sie anstelle von Sicherheitsservern Unified Access Gateway-Appliances verwenden, benötigen Sie insgesamt 3, deren Last über beide Verbindungsserver-Instanzen ausgeglichen wird, damit beim Ausfall einer Appliance die beiden verbleibenden Appliances die Last verarbeiten können.

In allen Fällen müssen Benutzer die Verbindung wieder herstellen, wenn sie einen ausgefallenen Verbindungsserver oder ein ausgefallenes Gateway benutzt haben.

## Hardwareanforderungen für Unified Access Gateway mit Horizon 7

VMware empfiehlt die Verwendung von 4 vCPUs und 10 GB RAM für Unified Access Gateway-Appliances zur Unterstützung der maximalen Anzahl an Verbindungen bei der Anwendung mit Horizon 7.

**Tabelle 4-8. Hardwareanforderungen für Unified Access Gateway**

Element	Beispiel
Betriebssystem	OVA (SUSE Linux Enterprise 12 (64 Bit))
Arbeitsspeicher (RAM)	4 GB
Virtuelle CPU	4
Kapazität der Systemfestplatte	20 GB (eine Änderung der Standardprotokollebene erfordert zusätzlichen Speicherplatz)
Virtueller SCSI-Adaptertyp	LSI Logic Parallel (Standard für OVA)

**Tabelle 4-8. Hardwareanforderungen für Unified Access Gateway (Fortsetzung)**

Element	Beispiel
Virtueller Netzwerkadapter	VMXNET 3
Netzwerkkarte	Netzwerkkarte mit 1 GBit/s
Netzwerkzuordnung	Einzelne NIC-Option

## vSphere -Cluster

Horizon 7-Bereitstellungen können VMware HA-Cluster (High Availability) als Schutz gegen Ausfälle physischer Server nutzen. In Abhängigkeit von Ihrer Konfiguration können Cluster bis zu 32 Knoten 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 Horizon 7-Bereitstellungen kann die Leistung und Reaktionsfähigkeit 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.

Unter den folgenden Bedingungen können vSphere-Cluster bis zu 32 ESXi-Hosts oder Knoten enthalten:

- vSphere 5.1 und höher, mit View Composer-Linked-Clone-Pools und Speicherreplikatfestplatten auf NFS-Datenspeichern oder VMFS5 oder neueren Datenspeichern
- vSphere 6.0 und höher und Speicher-Pools auf VVOL-Datenspeichern

Wenn Sie vSphere 5.5 Update 1 und höher verwenden und Pools in vSAN-Datenspeichern speichern, können die vSphere-Cluster bis zu 20 ESXi-Hosts enthalten.

Wenn Sie View Composer-Replikate in 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.

Weitere Informationen finden Sie im Kapitel zur Erstellung von Desktop-Pools im Dokument *Einrichten von virtuellen Desktops in Horizon 7*. Die Netzwerkanforderungen hängen vom Servertyp, von der Anzahl der Netzwerkadapter und von der vMotion-Konfiguration ab.

## 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 Horizon 7-spezifisch. Informationen zu den Grenzwerten von HA-Clustern in vSphere finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere*.

**Hinweis** Das folgende Infrastrukturbeispiel wurde mit View 5.2 und vSphere 5.1 getestet. Im Beispiel werden View Composer-Linked-Clones statt Instant Clones verwendet, da der Test mit View 5.2 durchgeführt wurde. Die Instant-Clone-Funktion wurde mit Horizon 7 eingeführt. Zu den anderen nicht mit View 5.2 verfügbaren Funktionen gehören vSAN und virtuelle Volumes (VVOL).

**Tabelle 4-9. Beispiel für einen Horizon 7 -Infrastruktur-Cluster**

Element	Beispiel
Virtuelle Maschinen	vCenter Server-Instanzen, Active Directory, SQL-Datenbankserver, View Composer, 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

**Tabelle 4-9. Beispiel für einen Horizon 7 -Infrastruktur-Cluster (Fortsetzung)**

Element	Beispiel
Nicht-SSD-Speicher	Virtuelle Maschinen für Active Directory, Verbindungsserver und Sicherheitsserver
Cluster-Typ	DRS (Distributed Resource Scheduler)/HA

**Tabelle 4-10. 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"> <li>■ 12 Dell PowerEdge R720 (16 Kerne x 2 GHz sowie 192 GB RAM auf jedem Host)</li> <li>■ 16 Dell PowerEdge R710 (12 Kerne x 2,526 GHz sowie 144GB RAM auf jedem Host)</li> <li>■ 8 Dell PowerEdge R810 (24 Kerne x 2 GHz sowie 256 GB RAM auf jedem Host)</li> <li>■ 6 Dell PowerEdge R810 + 3 PowerEdge R720</li> </ul>
SSD-Speicher	Virtuelle Replikatmaschinen
Nicht-SSD-Speicher	32 Nicht-SSD-Datenspeicher für Klone (450 GB pro Datenspeicher)
Cluster-Typ	DRS (Distributed Resource Scheduler)/HA

## 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. Linked-Clones wurden in herkömmlichen, auf drehenden Medien basierenden Datenspeichern mit geringerer Leistung platziert, die kostengünstiger sind und eine höhere Speicherkapazität bieten. Im Beispiel werden View-Composer-Linked-Clones statt Instant Clones verwendet, da der Test mit View 5.2 durchgeführt wurde. Die Instant-Clone-Funktion wurde mit Horizon 7 eingeführt.

### ■ [Aspekte der Speicherbandbreite](#)

In einer Horizon 7-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**

Bei WANs (Wide Area Networks) müssen Sie Bandbreiteneinschränkungen und Wartezeiten berücksichtigen. Die von VMware zur Verfügung gestellten PCoIP- und Blast Extreme-Anzeigeprotokolle ermöglichen die Anpassung an eine unterschiedliche Latenz- und Bandbreitenbedingungen.

## **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. Linked-Clones wurden in herkömmlichen, auf drehenden Medien basierenden Datenspeichern mit geringerer Leistung platziert, die kostengünstiger sind und eine höhere Speicherkapazität bieten. Im Beispiel werden View-Composer-Linked-Clones statt Instant Clones verwendet, da der Test mit View 5.2 durchgeführt wurde. Die Instant-Clone-Funktion wurde mit Horizon 7 eingeführt.

Die Planung des Speicherentwurfs ist eine der wichtigsten Voraussetzungen für eine erfolgreiche Horizon 7-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 vSAN-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 der mehrstufigen Speicherung, die in einer View 5.2-Testeinrichtung umgesetzt wurde, in der eine vCenter Server-Instanz für die Verwaltung von 10.000 Desktops eingesetzt wurde.

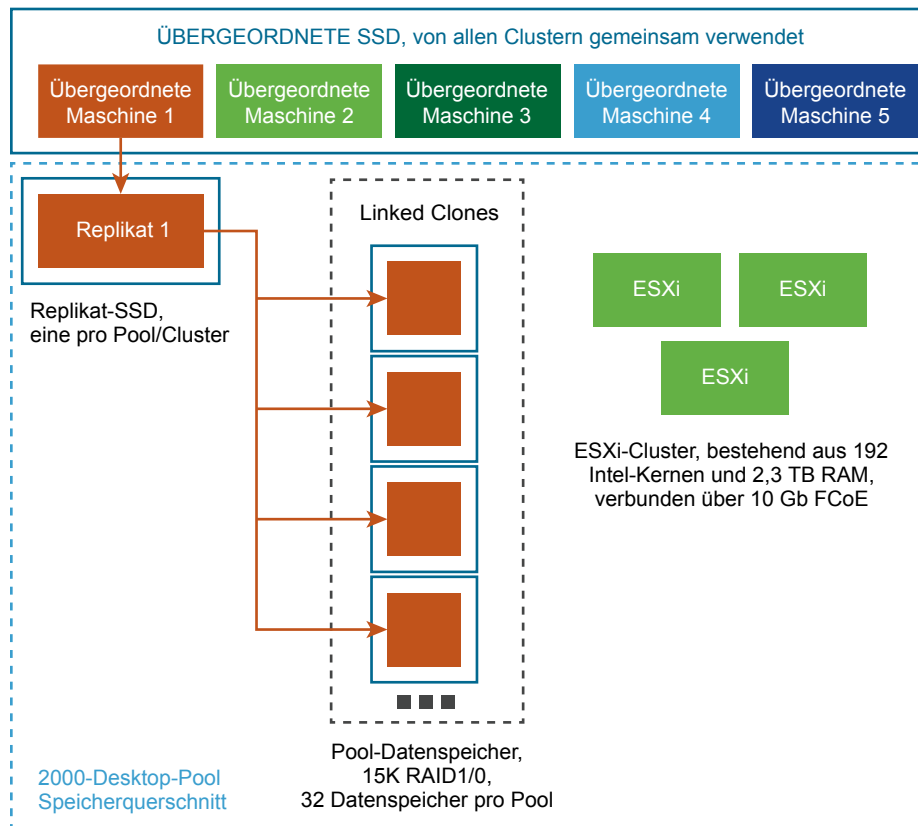
**Hinweis** Für dieses Beispiel wurde ein View 5.2-Setup verwendet, das vor der Veröffentlichung von VMware vSAN durchgeführt wurde. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware vSAN finden Sie im Whitepaper unter

<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Die in vSphere 6.0 und höher verfügbare vSAN-Funktion enthält im Vergleich zur Funktion aus vSphere 5.5 Update 1 viele Leistungsverbesserungen. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf. Weitere Informationen zu vSAN in vSphere 6 oder höher finden Sie im Dokument *Verwalten von VMware vSAN*.

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

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 vSAN-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 vSAN-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 Horizon 7-Umgebung müssen beim Ermitteln der Bandbreitenanforderungen in erster Linie Anmeldungsüberlastungen berücksichtigt werden.

Obwohl viele Elemente beim Entwurf eines Speichersystems zur Unterstützung einer Horizon 7-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 Horizon 7-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 Staffelung von Updates für unterschiedliche virtuellen Maschinen. Sie können im Rahmen einer Pilotphase auch verschiedene Abmeldungsrichtlinien testen, um zu bestimmen, ob virtuelle Maschinen angehalten oder ausgeschaltet werden sollen, wenn Benutzerabmeldungen zu einer E/A-Überlastung führen. Durch Speichern von View Composer-Replikaten in separaten Hochleistungs-Datenspeichern können Sie intensive, gleichzeitige Lesevorgänge beschleunigen, um E/A-Überlastungen zu bewältigen. Beispielsweise können Sie die folgenden Speicherstrategien verwenden:

- Manuelle Konfiguration der Pool-Einstellungen, sodass Replikate auf separaten Hochleistungs-Datenspeichern gespeichert werden.
- Verwenden der vSAN-Funktion (verfügbar für vSphere 5.5 Update 1 oder höher), die mithilfe der Softwarerichtlinien-basierten Verwaltung die für Replikate zu verwendenden Festplattentypen bestimmt.



- Verwenden der VVOL-Funktion (virtuelle Volumes) (verfügbar für vSphere 6.0 oder höher) die mithilfe der Softwarerichtlinien-basierten Verwaltung die für Replikate zu verwendenden Festplattentypen bestimmt.

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- oder Blast Extreme-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).

## Bei PCoIP und Blast Extreme verfügbare Optimierungssteuerungen

Bei Verwendung des PCoIP- oder Blast Extreme-Anzeigeprotokolls von VMware können Sie verschiedene Elemente anpassen, die sich auf die Bandbreitennutzung 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. Sie können zudem die Frame-Rate anpassen.

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

- 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- oder Blast-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 Sitzung von 500 auf 1500 Byte erhöhen.

Weitere Informationen finden Sie in den Abschnitten „PCoIP – Allgemeine Einstellungen“ und „VMware Blast – Richtlinieneinstellungen“ in *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

## 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 vSAN durchgeführt wurde. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware vSAN finden Sie im Whitepaper unter

<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Im Beispiel werden View-Composer-Linked-Clones statt Instant Clones verwendet, weil der Test mit View 5.2 durchgeführt wurde. Die Instant-Clone-Funktion wurde mit Horizon 7 eingeführt.

### 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 [Horizon-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 vSAN durchgeführt wurde. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware vSAN finden Sie im Whitepaper 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 vSAN finden Sie im Whitepaper zur Referenzarchitektur unter

<http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf>.

Die in vSphere 6.0 und höher verfügbare vSAN-Funktion enthält im Vergleich zur Funktion aus vSphere 5.5 Update 1 viele Leistungsverbesserungen. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf. Weitere Informationen zu vSAN in vSphere 6 oder höher finden Sie im Dokument *Verwalten von VMware vSAN*.

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 mit folgenden Anwendungen aufgerufen: 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 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 vSAN-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**

Bei WANs (Wide Area Networks) müssen Sie Bandbreiteneinschränkungen und Wartezeiten berücksichtigen. Die von VMware zur Verfügung gestellten PCoIP- und Blast Extreme-Anzeigeprotokolle ermöglichen die Anpassung an eine unterschiedliche Latenz- und Bandbreitenbedingungen.

Beim Verwenden des Anzeigeprotokolls RDP ist ein WAN-Optimierungsprodukt zum Beschleunigen von Anwendungen für Benutzer in Niederlassungen und kleinen Büroumgebungen erforderlich. Bei PCoIP und Blast Extreme 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 und Blast Extreme UDP-basiert sind, ist diese Art der WAN-Beschleunigung nicht erforderlich.
- 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 und Blast Extreme verfügen über sehr viele höhere Komprimierungsverhältnisse.

Erläuterungen der Steuerelemente zur Anpassung der Art und Weise, wie PCoIP und Blast Extreme die Bandbreite in Anspruch nehmen, finden Sie unter [Bei PCoIP und Blast Extreme 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 Horizon 7- Standardeinstellungen.
- 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 Horizon 7-Anwendung.
- 400 bis 600 KBit/s mittlere Bandbreite für virtuelle Desktops mit Verwendung von mehreren Monitoren, 3D, Aero und Microsoft Office.
- 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 Begrenzung von Frame-Rate und Videotyp.

---

**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 Horizon 7 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:  $(1,5 \text{ MBit/s} \times 0,8) / 150 \text{ KBit/s} = (1.500 \times 0,8) / 150 = 8 \text{ Benutzer}$
- Im besten Fall benötigen die Benutzer 50 KBit/s:  $(1,5 \text{ MBit/s} \times 0,8) / 50 \text{ KBit/s} = (1.500 \times 0,8) / 50 = 24 \text{ Benutzer}$

### 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 Horizon 7 und Windows optimieren, um diese Nutzerdichte zu erreichen.

---

## Horizon 7 -Bausteine

Ein Baustein besteht aus physischen Servern, einer vSphere-Infrastruktur, Horizon 7-Servern, gemeinsam genutztem Speicher und Desktops auf virtuellen Maschinen für Endbenutzer. Ein Baustein ist ein logisches Konstrukt. Seine Größe sollte 2.000 Horizon-Desktops nicht übersteigen. Kunden verwenden meist bis zu fünf Bausteine in einem Horizon 7-Pod, obwohl Sie theoretisch mehr Bausteine verwenden können, solange der Pod nicht 10.000 Sitzungen und 7 Horizon-Verbindungsserver-Instanzen überschreitet.

**Tabelle 4-11. Beispiel eines LAN-basierten Horizon-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)

Jeder vCenter Server kann 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 Horizon 7 spezifisch sind.

Wenn der Pod nur einen Baustein enthält, können Sie zu Redundanz Zwecken zwei Verbindungsserver-Instanzen einsetzen.

## Horizon 7 -Pods

Ein Pod ist eine Organisationseinheit, die durch Einschränkungen der Skalierbarkeit von Horizon 7 bestimmt wird.

### Beispiel einer Struktur mit fünf Bausteinen

Ein herkömmlicher Horizon 7-Pod integriert fünf Bausteine mit je 2.000 Benutzern, die Sie als eine Einheit verwalten können.

**Tabelle 4-12. Beispiel eines LAN-basierten Horizon 7 -Pods aus fünf Bausteinen**

Element	Anzahl bzw. Größe
Bausteine für einen Horizon 7-Pod	5
vCenter Server und View Composer	5 (1 virtuelle Maschine zum Hosten beider Komponenten in jedem Baustein)



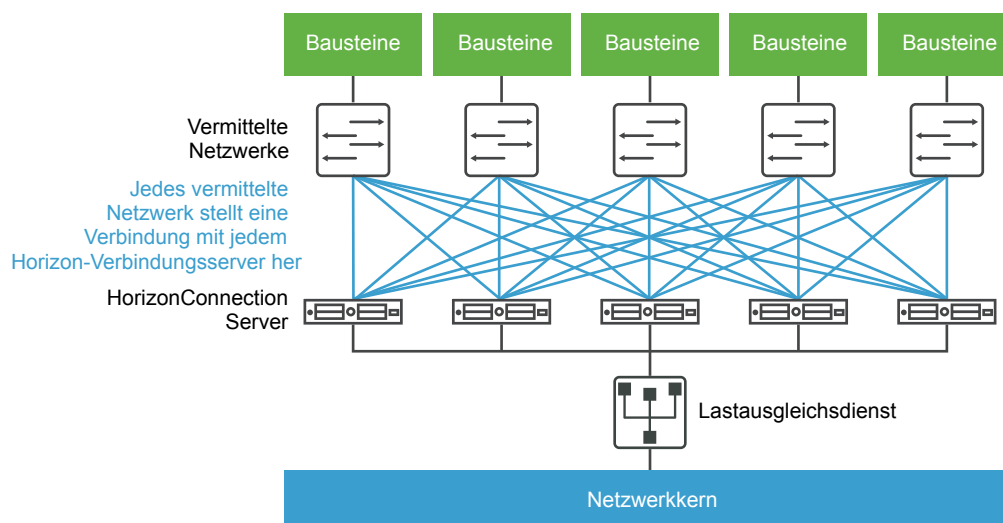
**Tabelle 4-12. Beispiel eines LAN-basierten Horizon 7 -Pods aus fünf Bausteinen (Fortsetzung)**

Element	Anzahl bzw. Größe
Datenbankserver	5 MS SQL Server- oder Oracle-Datenbankserver (1 eigenständiger Datenbankserver in jedem Baustein)
Verbindungsserver	7 (5 für Verbindungen von innerhalb des Unternehmensnetzwerks und 2 für Verbindungen von außerhalb)
vLANs	Siehe <a href="#">Tabelle 4-11</a> .
10-Gbit-Ethernet-Modul	1
Modularer Netzwerk-Switch	1

Jede vCenter Server-Instanz kann bis zu 35.000 registrierte 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 Horizon 7 spezifisch sind.

Bei beiden hier beschriebenen Beispielen kann ein Netzwerkkern für eingehende Anforderungen einen Lastausgleich auf den 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 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, so dass sich Benutzer mit einer anderen Verbindungsserver-Instanz verbinden und ihre Desktop-Sitzung an der Stelle fortsetzen können, an der es zum Ausfall gekommen ist.

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

## Beispiel-Pod mit einer vCenter Server -Instanz

Der Horizon 7-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 Horizon 7-Pods verwenden möchten. Der Grund für diese Anforderung ist, dass eine einzelne Instanz von vCenter Server 10.000 virtuelle Maschinen unterstützen kann. Kunden können eine einzelne vCenter Server-Instanz verwenden, um eine Umgebung mit 10.000 Desktops zu verwalten. In diesem Thema wird eine Architektur beschrieben, die auf einer einzelnen 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, Horizon 7-Servern, gemeinsamem Speicher und 5 Clustern mit je 2.000 virtuellen Desktops.

**Tabelle 4-13. Beispiel eines LAN-basierten Horizon 7 -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-Datenbank-server
Active Directory-Server	1 oder 2
Verbindungsserver-Instanzen	5
Sicherheitsserver	5
vLANs	8 (5 für die Desktop-Pool-Cluster und je 1 für Verwaltung, vMotion und den Infrastruktur-Cluster)

## Cloud-Pod-Architektur – Übersicht

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

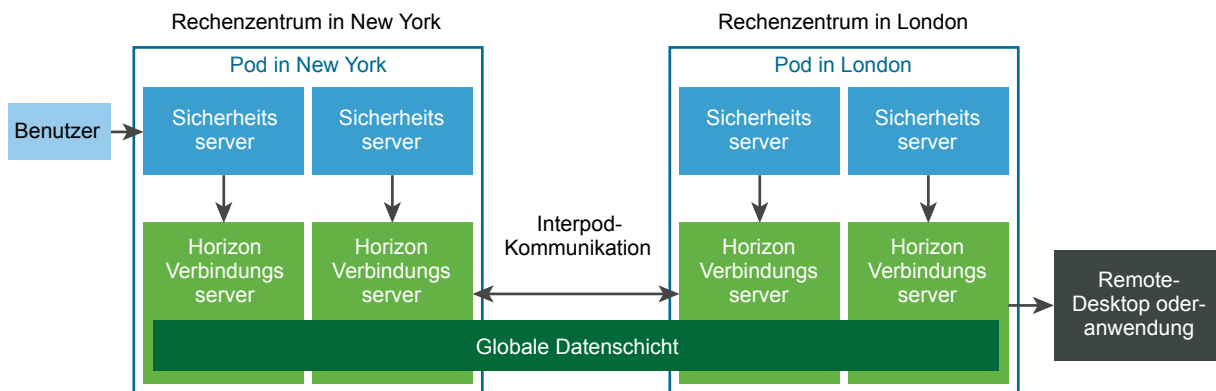
Diese Funktion verwendet standardmäßige Horizon-Komponenten für die Verwaltung mehrerer Rechenzentren, die globale und flexible Zuordnung zwischen Benutzern und Desktops, die Bereitstellung von Desktops mit hoher Verfügbarkeit sowie die Notfallwiederherstellung.

Eine typische Cloud-Pod-Architektur-Topologie besteht aus zwei oder mehr Pods, die in einem Pod-Verbund miteinander verknüpft sind. Für einen Pod-Verbund gelten bestimmte Einschränkungen.

**Tabelle 4-14. Einschränkungen für einen Pod-Verbund**

Objekt	Einschränkung
Sitzungen insgesamt	200.000
Pods	25
Sitzungen pro Pod	10.000
Sites	10
Verbindungsserver-Instanzen	175

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



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

Die Funktion Cloud-Pod-Architektur wird in einer IPv6-Umgebung nicht unterstützt.

Weitere Informationen finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

## Vorteile bei Verwendung mehrerer vCenter Server-Instanzen in einer Struktur

Beim Erstellen eines Entwurfs für eine Horizon 7-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 Horizon 7-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 Horizon 7-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	Die Einstellungen für parallele Vorgänge bestimmen, wie viele Vorgänge zu einem bestimmten Zeitpunkt für einen ganzen Horizon 7-Pod in einer Warteschlange platziert werden können.  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 Horizon 7-Bereitstellungen kann dieser Bereitstellungsvorgang viel Zeit in Anspruch nehmen.
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 Horizon 7-Pods für Betriebs-, Bereitstellungs- und Neuanpassungsvorgänge (Aktualisierung, Neuzusammenstellung und Neuverteilung) eingesetzt. Nachdem ein Desktop auf einer virtuellen Maschine bereitgestellt und eingeschaltet wurde, hängt Horizon 7 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 Horizon 7-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)
- 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 Horizon 7-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 vorkommen, entstehen keine langen Warteschlangen. Folglich kommt es für den Horizon-Verbindungsserver auch nicht zu Zeitüberschreitungen, wenn 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 Horizon 7 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 Horizon 7-Entwurf bietet offenkundige Vorteile, wie z. B. eine zentrale Verwaltung von „optimierten“ Master-Images und übergeordneten virtuellen Maschinen, eine einzige vCenter Server-Ansicht, die auf die Horizon Administrator-Konsolensicht 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

Horizon 7 bietet leistungsstarke Netzwerksicherheitsfunktionen zum Schutz vertraulicher Unternehmensdaten. Zur Optimierung der Sicherheit können Sie Horizon 7 mit verschiedenen Authentifizierungslösungen anderer Anbieter integrieren, einen Sicherheitsserver einsetzen und die Einschränkungsfunktion für Berechtigungen implementieren.

---

**Wichtig** Horizon 6 Version 6.2 und höhere Versionen führen kryptografische Vorgänge mit FIPS-140-2-konformen (Federal Information Processing Standard) Algorithmen aus. Zur Aktivierung dieser Algorithmen installieren Sie Horizon 7 im FIPS-Modus. Allerdings werden im FIPS-Modus nicht alle Funktionen unterstützt. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*.

---

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](#)
- [Verwenden von Intelligente Richtlinien](#)
- [Implementieren von Best Practices zum Sichern von Clientsystemen](#)
- [Zuweisen von Administratorrollen](#)
- [Vorbereiten des Einsatzes eines Sicherheitsservers](#)
- [Grundlegendes zu Kommunikationsprotokollen](#)

## Grundlegendes zu Clientverbindungen

Horizon Client und Horizon Administrator kommunizieren mit einem Horizon-Verbindungsserver-Host über sichere HTTPS-Verbindungen. Informationen zum Serverzertifikat auf dem Verbindungsserver werden beim TLS-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 Verbindungsserver, den Sicherheitsserver oder den Unified Access Gateway-Host angibt. Die Horizon Administrator-Verbindung wird hergestellt, wenn ein Administrator die Horizon Administrator-URL in einen Webbrowser eingibt.

Während der Installation des Verbindungsservers wird ein standardmäßiges TLS-Serverzertifikat generiert. Dieses Zertifikat wird TLS-Clients standardmäßig präsentiert, wenn sie eine sichere Seite wie die Horizon 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. Bei Verwendung nicht zertifizierter Zertifikate besteht die Gefahr, dass nicht vertrauenswürdige Stellen Datenverkehr abfangen können, indem sie sich als Ihr Server ausgeben.

- **Clientverbindungen mit PCoIP und Blast Secure Gateway**

Wenn Clients über das PCoIP-Anzeigeprotokoll oder das Blast Extreme-Anzeigeprotokoll von VMware eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen, kann Horizon Client eine zweite Verbindung mit der betreffenden Secure Gateway-Komponente auf einer Horizon-Verbindungsserver-Instanz, auf einem Sicherheitsserver oder auf einer Unified Access Gateway-Appliance 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 mit dem Horizon-Verbindungsserver-Host eine zweite HTTPS-Verbindung herstellen. Diese Verbindung wird als Tunnelverbindung bezeichnet, da sie einen Tunnel für den RDP-Datenverkehr darstellt.

- **Direkte Clientverbindungen**

Administratoren können Horizon-Verbindungsserver-Einstellungen so konfigurieren, dass Remote-Desktop- und veröffentlichte Anwendungssitzungen direkt zwischen dem Clientsystem und der virtuellen Maschine mit der veröffentlichten Anwendung oder mit dem Remote-Desktop unter Umgehung des Horizon-Verbindungsserver-Hosts eingerichtet werden. Dieser Verbindungstyp wird als „direkte Clientverbindung“ bezeichnet.

## **Clientverbindungen mit PCoIP und Blast Secure Gateway**

Wenn Clients über das PCoIP-Anzeigeprotokoll oder das Blast Extreme-Anzeigeprotokoll von VMware eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen, kann Horizon Client eine zweite Verbindung mit der betreffenden Secure Gateway-Komponente auf einer Horizon-Verbindungsserver-Instanz, auf einem Sicherheitsserver oder auf einer Unified Access Gateway-Appliance herstellen. Diese Verbindung bietet die erforderliche Sicherheit und Konnektivität beim Zugriff auf Remote-Desktops und -anwendungen über das Internet.



Sicherheitsserver und Unified Access Gateway-Appliances enthalten eine PCoIP Secure Gateway-Komponente und eine Blast Secure Gateway-Komponente. Diese bieten die folgenden Vorteile:

- 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.
- Die PCoIP Secure Gateway-Verbindung unterstützt PCoIP, die Blast Secure Gateway-Verbindung unterstützt Blast Extreme. Beides sind fortschrittliche Remote-Anzeigeprotokolle, die das Netzwerk effizienter nutzen, indem Videoanzeigepakete in UDP statt TCP gekapselt werden.
- PCoIP und Blast Extreme werden standardmäßig durch die AES-128-Verschlüsselung geschützt. Sie können die Verschlüsselungsmethode jedoch in AES-256 ändern.
- Sofern das Anzeigeprotokoll nicht durch eine Netzwerkkomponente blockiert wird, ist kein VPN erforderlich. Beispiel: Beim Versuch, von einem Hotelzimmer aus auf einen Remote-Desktop oder eine Remoteanwendung zuzugreifen, stellt der Benutzer möglicherweise fest, dass der vom Hotel verwendete Proxy nicht für die Übertragung von UDP-Paketen konfiguriert ist.

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

Sicherheitsserver werden unter den Betriebssystemen Windows Server 2008 R2 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 Verschlüsselung/Entschlüsselung nutzen.

Weitere Informationen zu virtuellen Unified Access Gateway-Appliances finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

## Getunnelte Clientverbindungen mit Microsoft RDP

Wenn Benutzer eine Verbindung mit einem Remote-Desktop mithilfe des Microsoft RDP-Anzeigeprotokolls herstellen, kann Horizon Client mit dem Horizon-Verbindungsserver-Host eine zweite HTTPS-Verbindung 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 Horizon 7 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 Verbindungsserver-Instanzen endet die sichere HTTPS-Verbindung beim Verbindungsserver. In einer Bereitstellung mit Umkreisnetzwerk (DMZ) endet die sichere HTTPS-Verbindung bei einem Sicherheitsserver oder bei einer Unified Access Gateway-Appliance. Informationen zu DMZ-Bereitstellungen und Sicherheitsservern finden Sie unter [Vorbereiten des Einsatzes eines Sicherheitsservers](#).

Clients, die das PCoIP- oder das Blast Extreme-Anzeigeprotokoll verwenden, können die Tunnelverbindung zur Beschleunigung der USB-Umleitung und der Multimedia-Umleitung (MMR) nutzen. Für alle anderen Daten verwendet PCoIP jedoch das PCoIP Secure Gateway und Blast Extreme das Blast Secure Gateway auf einem Sicherheitsserver oder auf einer Unified Access Gateway-Appliance. Weitere Informationen finden Sie unter [Clientverbindungen mit PCoIP und Blast Secure Gateway](#).

Weitere Informationen zu virtuellen Unified Access Gateway-Appliances finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

## Direkte Clientverbindungen

Administratoren können Horizon-Verbindungsserver-Einstellungen so konfigurieren, dass Remote-Desktop- und veröffentlichte Anwendungssitzungen direkt zwischen dem Clientsystem und der virtuellen Maschine mit der veröffentlichten Anwendung oder mit dem Remote-Desktop unter Umgehung des Horizon-Verbindungsserver-Hosts eingerichtet werden. Dieser Verbindungstyp wird als „direkte Clientverbindung“ bezeichnet.

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

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

- PCoIP und Blast Extreme unterstützen die AES-Verschlüsselung (Advanced Encryption Standard), die standardmäßig aktiviert ist, und verwenden IP Security (IPsec).
- Es werden VPN-Clients von Fremdherstellern unterstützt.

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

Horizon 7 nutzt die vorhandene Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Um eine zusätzliche Sicherheitsebene zu schaffen, können Sie Horizon 7 in Zwei-Faktor-Authentifizierungslösungen wie RSA SecurID und RADIUS und Smart Card-Authentifizierungslösungen integrieren.

- **Active Directory-Authentifizierung**

Jede Horizon-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 Horizon-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 **Als aktueller Benutzer anmelden** aktivieren, werden die Anmeldeinformationen, die sie bei der Anmeldung am Clientsystem angegeben haben, für die Authentifizierung an der Horizon-Verbindungsserver-Instanz und am Remote-Desktop verwendet. Es ist keine weitere Benutzerauthentifizierung erforderlich.

## Active Directory-Authentifizierung

Jede Horizon-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 Verbindungsserver-Instanz beispielsweise zur Domäne A gehört und eine Vertrauensstellung zwischen Domäne A und Domäne B besteht, können sich Benutzer sowohl von Domäne A als auch von Domäne B über Horizon Client mit der Verbindungsserver-Instanz verbinden.

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 Verbindungsserver-Instanz verbinden.

Sie können Benutzer und Gruppen in folgenden Active Directory-Domänen platzieren:

- Die Verbindungsserver-Domäne
- Eine unterschiedliche Domäne mit einer Zwei-Wege-Vertrauensbeziehung mit der Domäne des Verbindungservers

- Eine Domäne in einer anderen Gesamtstruktur als die Domäne des Verbindungsservers, die von der Domäne des Verbindungsservers in einer externen Ein-Weg- oder Bereichs-Vertrauensbeziehung als vertrauenswürdig eingestuft wird.
- Eine Domäne in einer anderen Gesamtstruktur als die Domäne des Verbindungsservers, die von der Domäne des Verbindungsservers in einer transitiven Ein-Weg- oder Zwei-Wege-Gesamtstruktur-Vertrauensbeziehung als vertrauenswürdig eingestuft wird.

Der 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 der Verbindungsserver rasch eine vollständige Liste mit Domänen bestimmen. Die Zeit dafür nimmt jedoch mit der steigenden Zahl von Domänen oder bei Abnahme der Konnektivität 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 Verbindungsserver-Instanz durchsucht und die dem Benutzer angezeigt werden. Weitere Informationen finden Sie im Dokument *Horizon 7 Verwaltung*.

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 Horizon-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.
- Horizon 7 bietet auch eine offene Standarderweiterungsschnittstelle, die es Drittanbietern ermöglicht, fortschrittliche Authentifizierungserweiterungen in Horizon 7 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 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 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.

Horizon 7 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 Verbindungsserver-Instanzen für die Smartcard-Authentifizierung konfigurieren. Die Aktivierung einer Verbindungsserver-Instanz für den Einsatz der Smartcard-Authentifizierung erfordert zumeist das Hinzufügen Ihres Stammzertifikats zu einer Vertrauensspeicherdatei und die anschließende Änderungen der Verbindungsserver-Einstellungen.

Alle Clientverbindungen, einschließlich Clientverbindungen, die die Smartcard-Authentifizierung verwenden, sind für TLS/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 darüber, ob ein bestimmter Typ von Horizon Client Smartcards unterstützt, finden Sie in der Horizon Client-Dokumentation unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.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 **Als aktueller Benutzer anmelden** aktivieren, werden die Anmeldeinformationen, die sie bei der Anmeldung am Clientsystem angegeben haben, für die Authentifizierung an der Horizon-Verbindungsserver-Instanz und am Remote-Desktop verwendet. Es ist keine weitere Benutzerauthentifizierung erforderlich.

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

- Auf der 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 Horizon 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 Verbindungsserver-Instanzen die Benutzeridentitäts- und Anmeldedaten akzeptieren, die übergeben werden, wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** in Horizon Client aktiviert ist.

Die Funktion „Rekursives Entsperren“ wird aktiviert, sobald sich ein Benutzer beim Verbindungsserver mit der Funktion „Als aktueller Benutzer anmelden“ anmeldet. Die Funktion der rekursiven Entsperrung entsperrt alle Remotesitzungen, wenn der Clientcomputer entsperrt wird. Administratoren können die Funktion „Rekursives Entsperren“ mit der globalen Richtlinieneinstellung **Remotesitzungen entsperren, wenn der Clientcomputer entsperrt wird** in Horizon Client steuern. Weitere Informationen zu globalen Richtlinieneinstellungen für Horizon Client finden Sie in der Horizon Client-Dokumentation auf der Webseite [VMware Horizon Clients-Dokumentation](#).

Für die Funktion „Als aktueller Benutzer anmelden“ gelten folgende Einschränkungen und Anforderungen:

- Wenn die Smartcard-Authentifizierung auf einer Verbindungsserver-Instanz erforderlich ist, schlägt die Authentifizierung bei Benutzern fehl, die das Kontrollkästchen **Als aktueller Benutzer anmelden** aktivieren, wenn sie eine Verbindung zur Verbindungsserver-Instanz herstellen. Diese Benutzer müssen sich bei der Anmeldung beim 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 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 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 Horizon-Verbindungsserver-Instanz einschränken, mit der sich ein Benutzer verbindet.

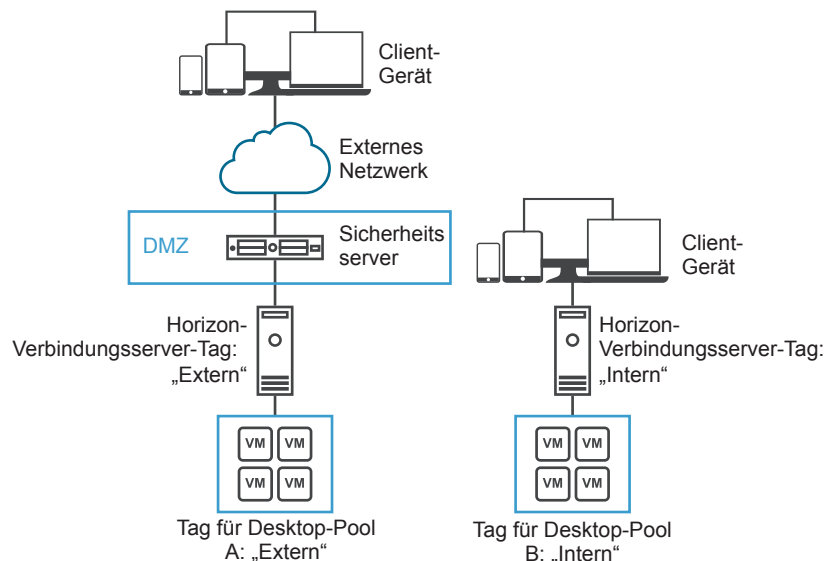
Für die Einschränkung von Berechtigungen weisen Sie einer Verbindungsserver-Instanz ein oder mehrere Kennzeichen zu. Wenn Sie anschließend einen Desktop-Pool konfigurieren, wählen Sie die Kennzeichen der Verbindungsserver-Instanzen aus, die auf den Desktop-Pool zugreifen sollen. Wenn Benutzer sich über eine Verbindungsserver-Instanz mit Kennzeichen anmelden, können sie nur auf die Desktop-Pools zugreifen, die mindestens ein übereinstimmendes Kennzeichen oder keine Kennzeichen aufweisen.

Angenommen, Ihre Horizon 7-Bereitstellung umfasst zwei 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 Verbindungsserver-Instanz zu, die den internen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Extern“ der Verbindungsserver-Instanz zu, die mit dem Sicherheitsserver gekoppelt wird und die Ihre 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 über die als „Extern“ gekennzeichneten Verbindungsserver-Instanz anmelden. Ebenso können interne Benutzer keine als „Extern“ gekennzeichneten Desktop-Pools sehen, da sie sich über die als „Intern“ gekennzeichneten Verbindungsserver-Instanz anmelden. [Abbildung 5-1](#) veranschaulicht diese Konfiguration.

**Abbildung 5-1. Beispiel für eingeschränkte Berechtigungen**



Außerdem können Sie mithilfe eingeschränkter Berechtigungen den Desktop-Zugriff auf der Basis der Benutzerauthentifizierungsmethode steuern, die Sie für eine bestimmte 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 Verbindungsserver-Instanz anzumelden.

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

Horizon 7 umfasst administrative Gruppenrichtlinien-ADMX-Vorlagen mit sicherheitsbezogenen Gruppenrichtlinieneinstellungen, mit deren Hilfe Sie Ihre Remote-Desktops und -Anwendungen sichern können.

Beispielsweise können Sie Gruppenrichtlinieneinstellungen zum Durchführen der folgenden Aufgaben verwenden.

- Legen Sie die Verbindungsserver-Instanzen fest, die 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-TLS-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 Horizon 7 verwenden, um Verbindungen mit Remote-Desktops herzustellen.

Informationen zur Verwendung von Remote-Desktop- und Horizon Client-Gruppenrichtlinieneinstellungen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

## Verwenden von Intelligente Richtlinien

Sie können mit Intelligente Richtlinien Richtlinien zur Steuerung des Verhaltens der USB-Umleitung, des virtuellen Drucks, der Zwischenablagenumleitung, der Clientlaufwerksumleitung und der Funktionen für das PCoIP-Anzeigeprotokoll auf bestimmten Remote-Desktops steuern. Sie können auch mit Intelligente Richtlinien das Verhalten der veröffentlichten Anwendungen steuern.

Mit Intelligente Richtlinien besteht die Möglichkeit, Richtlinien zu erstellen, die nur beim Eintreten bestimmter Bedingungen wirksam werden. Sie können beispielsweise eine Richtlinie konfigurieren, mit der die Clientlaufwerksumleitung dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit einem Remote-Desktop herstellt.

Die Intelligente Richtlinien-Funktion erfordert User Environment Manager. Weitere Informationen finden Sie unter Intelligente Richtlinien in *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.



## Implementieren von Best Practices zum Sichern von Clientsystemen

Implementieren Sie diese Best Practices, 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 Horizon 7 bietet, finden Sie im Dokument *Sicherheit von Horizon 7*.

## Zuweisen von Administratorrollen

Eine wichtige Verwaltungsaufgabe in einer Horizon 7-Umgebung besteht darin, festzulegen, wer Horizon Administrator verwenden kann und zur Ausführung welcher Aufgaben diese Benutzer autorisiert sind.

Die Autorisierung zum Ausführen von Aufgaben in Horizon 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, welche Objekte ein Administrator in Horizon Administrator anzeigen kann.

Ein Administrator kann Ordner erstellen, um Desktop-Pools zu unterteilen, und die Verwaltung bestimmter Desktop-Pools an andere Administratoren in Horizon 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.

Horizon 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 Horizon-Verbindungsserver-Instanz, in der eine Teilmenge der Verbindungsserver-Funktionen ausgeführt wird. Mithilfe eines Sicherheitsservers können Sie eine weitere Sicherheitsebene zwischen dem Internet und Ihrem internen Netzwerk einführen.

---

**Wichtig** Mit Horizon 6 Version 6.2 und höheren Versionen können Sie Unified Access Gateway-Appliances anstelle von Sicherheitsservern verwenden. Unified Access Gateway-Appliances werden als gehärtete virtuelle Appliances bereitgestellt, denen eine Linux-Appliance zugrunde liegt, die für einen sicheren Zugriff angepasst wurde. Weitere Informationen zu virtuellen Unified Access Gateway-Appliances finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

---

Ein Sicherheitsserver befindet sich in einem Umkreisnetzwerk und fungiert als Proxy-Host für Verbindungen innerhalb Ihres vertrauenswürdigen Netzwerks. Jeder Sicherheitsserver bildet mit einer Instanz des Verbindungsservers 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 Verbindungsserver-Instanz vor dem öffentlichen Internet abgeschirmt wird und alle ungeschützten Sitzungsanforderungen automatisch 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 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 Verbindungsserver-Instanz verbinden können, müssen Sie keinen Sicherheitsserver implementieren.

---

**Hinweis** Sicherheitsserver beinhalten eine PCoIP Secure Gateway-Komponente und eine Blast Secure Gateway-Komponente. Dies gibt Clients mit einem PCoIP- oder Blast Extreme-Anzeigeprotokoll die Möglichkeit, einen Sicherheitsserver anstelle eines VPN zu verwenden.

Informationen zum 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 folgen Sie diesen empfohlenen Sicherheitsrichtlinien und Vorgehensweisen.

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 Horizon-Verbindungsserver-Instanzen, die mit Sicherheitsservern gekoppelt sind, in einem isolierten Netzwerk bereitgestellt werden. Mit dieser Topologie können böswillige Benutzer im internen Netzwerk daran gehindert werden, die Kommunikation zwischen den Sicherheitsservern und den Verbindungsserver-Instanzen zu überwachen.

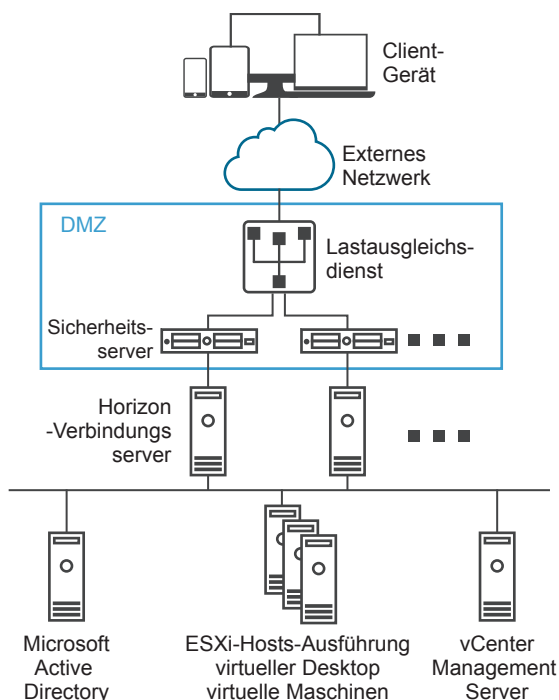
Alternativ dazu können Sie möglicherweise erweiterte Sicherheitsfunktionen in Ihrem Netzwerk-Switch einsetzen, um die böswillige Überwachung der Sicherheitsserver- und Verbindungsserver-Kommunikation zu verhindern und sich vor Überwachungsangriffen wie ARP Cache Poisoning zu schützen. Weitere Informationen 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](#) zeigt eine hochverfügbare Umgebung mit zwei mit Lastausgleich arbeitenden Sicherheitsservern in einer DMZ. Die Sicherheitsserver im Umkreisnetzwerk kommunizieren mit zwei Horizon-Verbindungsserver-Instanzen innerhalb des internen Netzwerks.

**Abbildung 5-2. Sicherheitsserver mit Lastausgleich in einem Umkreisnetzwerk**

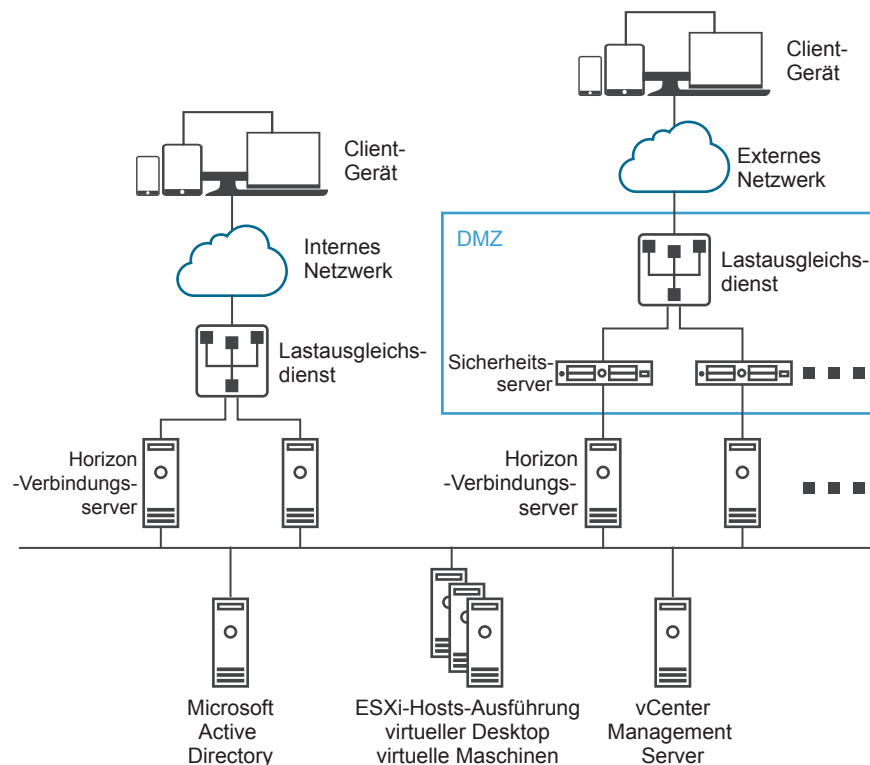


Wenn Benutzer sich von außerhalb des Firmennetzwerks mit einem Sicherheitsserver verbinden, müssen sie sich erfolgreich authentifizieren, bevor sie auf Remote-Desktops und -Anwendungen zugreifen können. Bei entsprechenden Firewall-Regeln auf beiden Seiten des DMZ eignet sich diese Topologie für den Zugriff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

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

Die Topologie in [Abbildung 5-3](#) zeigt eine Umgebung, in der vier 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 Verbindungsserver-Instanzen, die mit den Sicherheitsservern gekoppelt sind, 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. Der Verbindungsserver bietet jedoch keine eigene Lastausgleichsfunktionalität. Der Verbindungsserver kann zusammen mit Standardlastausgleichslösungen von Drittanbietern verwendet werden.

## Firewalls für Sicherheitsserver im Umkreisnetzwerk

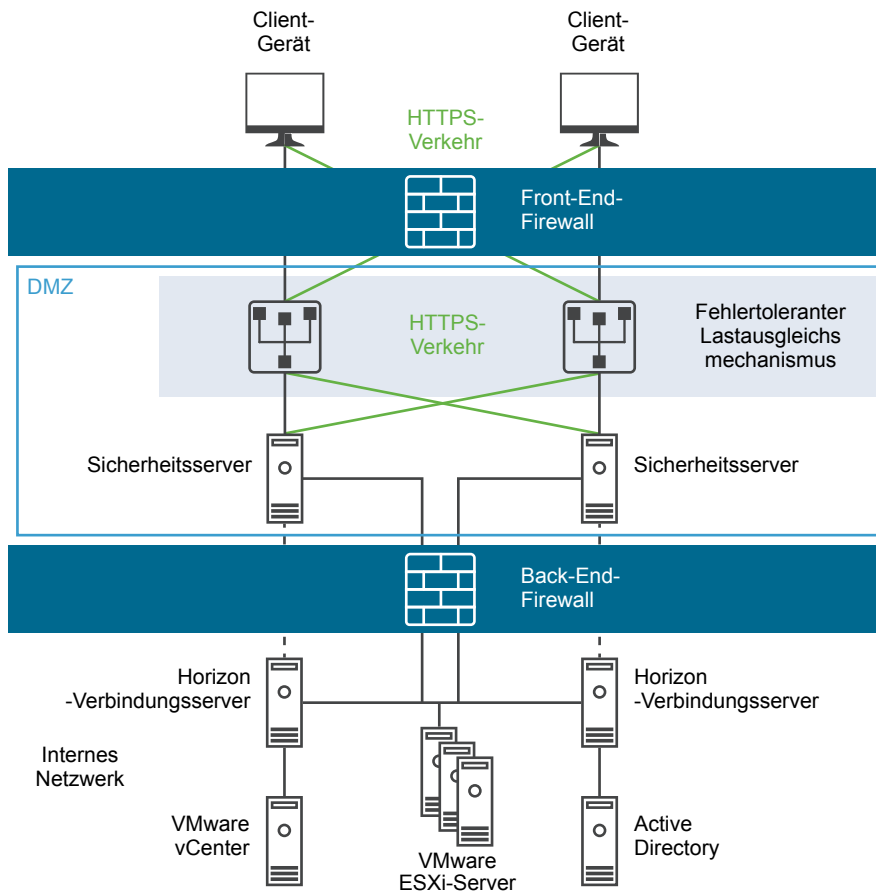
Eine Bereitstellung von Sicherheitsservern in einem Umkreisnetzwerk muss zwei Firewalls aufweisen.

- 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. Weitere Informationen zu den Ports, die Sie für Sicherheitsserver konfigurieren müssen, finden im Dokument *Horizon 7-Sicherheit*.

Die folgende Abbildung 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 Horizon 7-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 Horizon 7*.

### 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](#) 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 zu Sicherheitsüberlegungen im Zusammenhang mit dem Zulassen von Benutzerverbindungen über HTTP anstelle von HTTPS finden Sie im Handbuch <i>Sicherheit von Horizon 7</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-Zielpport ist der Quellport der empfangenen UDP-Pakete. Da diese Pakete Antwortdaten enthalten, ist es normalerweise nicht erforderlich, für diesen Datenverkehr eine explizite Firewallregel hinzuzufügen.
Horizon Client- oder Client-Webbrowser	TCP beliebig	HTTPS	Sicherheitsserver	TCP 8443 UDP 8443	Externe Clientgeräte und externe Webclients (HTML Access) stellen im Umkreisnetzwerk (DMZ) am HTTPS-Port 8443 eine Verbindung mit einem Sicherheitsserver 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-Desktop-Anwendungen und Verbindungsserver-Instanzen miteinander kommunizieren können. [Tabelle 5-2](#) enthält eine Übersicht der Back-End-Firewallregeln.

**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 Verbindungsserver-Instanzen an UDP-Port 500.
Verbindungsserver	UDP 500	IPSec	Sicherheitsserver	UDP 500	Verbindungsserver-Instanzen antworten auf Sicherheitsserver an UDP-Port 500.
Sicherheitsserver	UDP 4500	NAT-T ISAKMP	Verbindungsserver	UDP 4500	Erforderlich, wenn zwischen dem Sicherheitsserver und der Verbindungsserver-Instanz, mit der der Sicherheitsserver gekoppelt 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, antworten Verbindungsserver-Instanzen auf Anfragen von Sicherheitsservern an UDP-Port 4500.
Sicherheitsserver	TCP beliebig	AJP13	Verbindungsserver	TCP 8009	Sicherheitsserver verbinden sich mit 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 Verbindungsserver-Instanzen an TCP-Port 4001, um Java Message Service (JMS)-Datenverkehr auszutauschen.
Sicherheitsserver	TCP beliebig	JMS	Verbindungsserver	TCP 4002	Sicherheitsserver verbinden sich mit Verbindungsserver-Instanzen an TCP-Port 4002, um einen sicheren 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 am TCP-Port 9427 eine Verbindung mit Remote-Desktops her, um den Datenverkehr von Multimedia-Umleitungen (MMR) und Clientlaufwerksumleitungen zu empfangen.

**Tabelle 5-2. Regeln für die Back-End-Firewall (Fortsetzung)**

Quelle	Standardports	Protokoll	Ziel	Standardports	Hinweise
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 oder UDP beliebig	Blast Extreme	Remote-Desktop oder -anwendung	TCP oder UDP 22443	Sicherheitsserver stellen am TCP- und UDP-Port 22443 eine Verbindung mit Remote-Desktops und -anwendungen her, um den Blast-Extreme-Datenverkehr auszutauschen.
Sicherheitsserver	TCP beliebig	HTTPS	Remote-Desktop	TCP 22443	Wenn Sie HTML Access verwenden, stellen Sicherheitsserver eine Verbindung mit Remote-Desktops am HTTPS-Port 22443 her, um mit dem Blast Extreme-Agent zu kommunizieren.
Sicherheitsserver		ESP	Verbindungs-server		Gekapselter AJP13-Datenverkehr, wenn keine NAT-Ausnahme erforderlich ist. ESP ist IP-Protokoll 50. Portnummern werden nicht angegeben.
Verbindungs-server		ESP	Sicherheitsserver		Gekapselter AJP13-Datenverkehr, wenn keine NAT-Ausnahme erforderlich ist. ESP ist IP-Protokoll 50. Portnummern werden nicht angegeben.

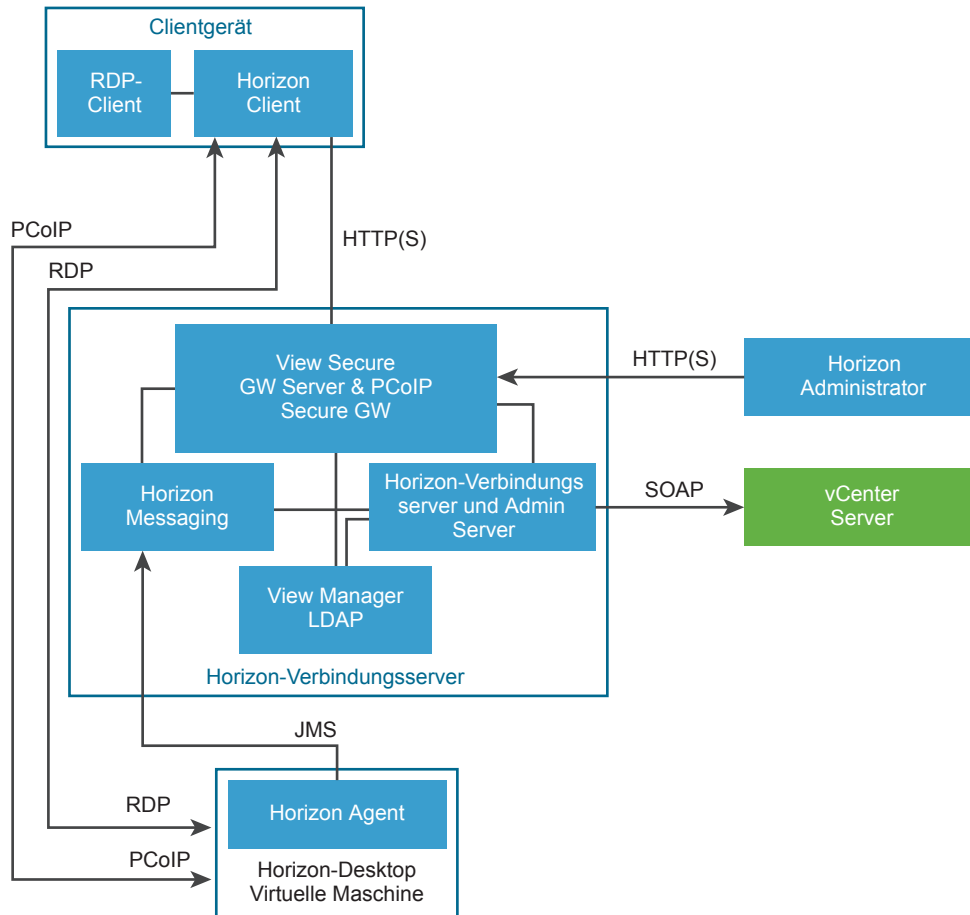
## Grundlegendes zu Kommunikationsprotokollen

Horizon 6- und Horizon 7-Komponenten tauschen Meldungen mithilfe mehrerer unterschiedlicher Protokolle aus.

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



**Abbildung 5-5. Horizon 6- und Horizon 7-Komponenten und -Protokolle ohne Sicherheitsserver**

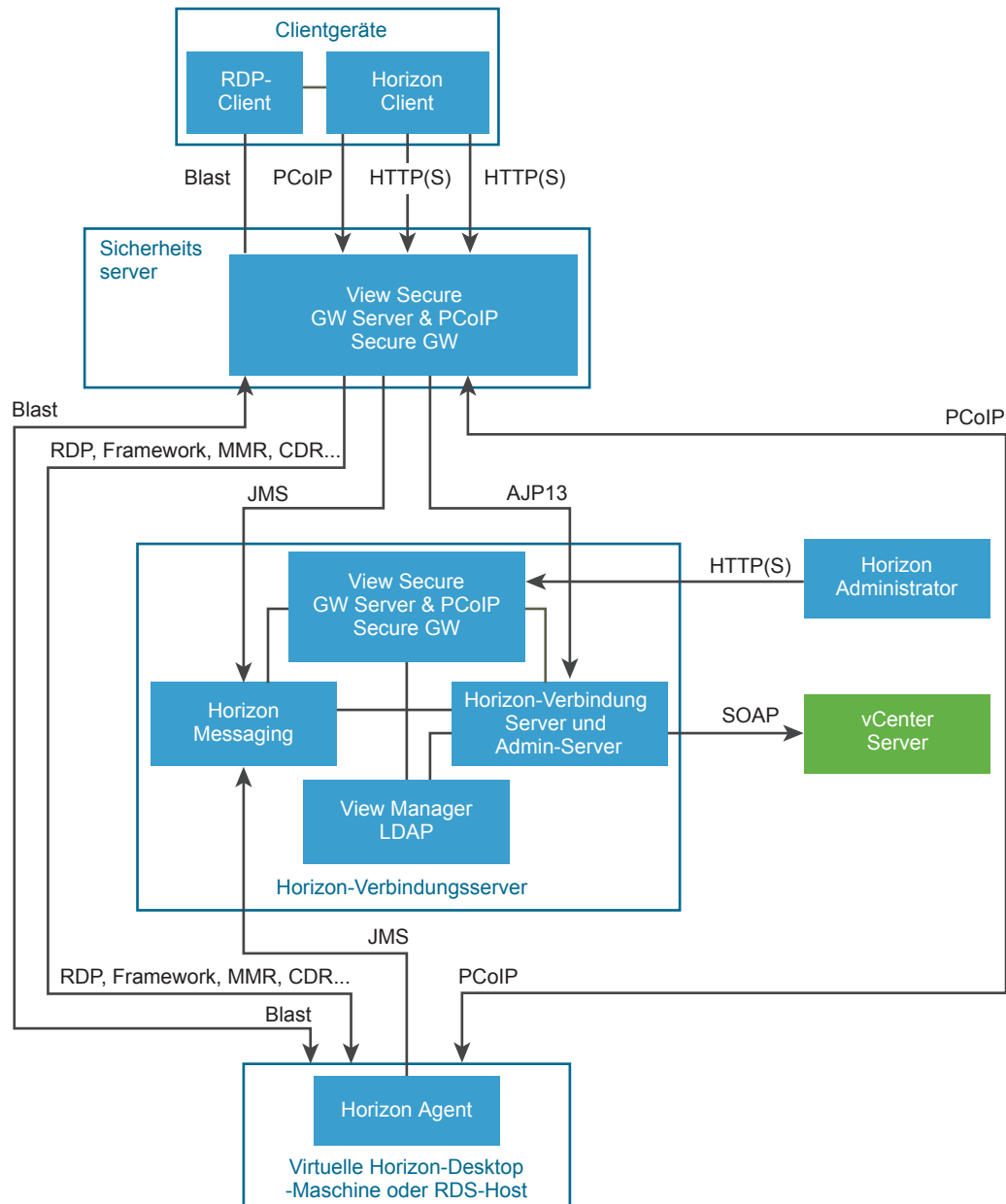


**Hinweis** Diese Abbildung zeigt direkte Verbindungen für Clients, die PCoIP oder RDP verwenden. In der Standardeinstellung werden jedoch direkte Verbindungen für PCoIP und Tunnelverbindungen für RDP verwendet.

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

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

**Abbildung 5-6. Horizon 6- und Horizon 7-Komponenten und -Protokolle mit Sicherheitsserver**



**Tabelle 5-3** 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 TCP-Port 4002
AJP13	TCP-Port 8009  <b>Hinweis</b> AJP13 wird nur in einer Sicherheitsserverkonfiguration verwendet.
HTTP	TCP-Port 80
HTTPS	TCP-Port 443
MMR/CDR	Für Multimedia-Umleitung und Clientlaufwerksumleitung, TCP-Port 9427
RDP-	TCP-Port 3389  <b>Hinweis</b> Wenn die 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	TCP-Port 4172 UDP-Ports 4172, 50002, 55000
USB-Umleitung	TCP-Port 32111. Dieser Port wird auch zur Zeitzonensynchronisierung verwendet.
VMware Blast Extreme	TCP-Ports 8443, 22443 UDP-Ports 443, 8443, 22443
HTML Access	TCP-Ports 8443, 22443

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

Verbindungsserver-Instanzen in einer Gruppe nutzen zusätzliche TCP-Ports für die Kommunikation untereinander. Beispielsweise verwenden Verbindungsserver-Instanzen Port 4100 oder 4101 zum Übertragen von JMS-Datenverkehr (JMSIR) zwischen View-Verbindungsserver-Instanzen. Firewalls werden im Allgemeinen nicht zwischen den Verbindungsserver-Instanzen in einer Gruppe verwendet.

## View Secure Gateway Server

View Secure Gateway Server ist die serverseitige Komponente der sicheren HTTPS-Verbindung zwischen Clientsystemen und einem Sicherheitsserver, einer Unified Access Gateway-Appliance oder einer Verbindungsserver-Instanz.

Wenn Sie die Tunnelverbindung für Verbindungsserver konfigurieren, wird von RDP, USB und der Multimedia-Umleitung (MMR) 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- oder das Blast Extreme-Anzeigeprotokoll verwenden, können die Tunnelverbindung zur Beschleunigung der USB-Umleitung und der Multimedia-Umleitung (MMR) nutzen. Für alle anderen Daten verwendet PCoIP jedoch das PCoIP Secure Gateway und Blast Extreme das Blast Secure Gateway auf einem Sicherheitsserver oder auf einer Unified Access Gateway-Appliance.

---

View Secure Gateway Server ist auch dafür zuständig, anderen Web-Datenverkehr von Clients an den Verbindungsserver 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 Horizon Administrator-Client zur Komponente Administration Server weiter.

## Blast Secure Gateway

Sicherheitsserver und Unified Access Gateway-Appliances enthalten eine Blast Secure Gateway-Komponente. Bei aktiviertem Blast Secure Gateway können Clients, die Blast Extreme oder HTML Access verwenden, nach der Authentifizierung eine weitere sichere Verbindung zu einem Sicherheitsserver oder zu einer Unified Access Gateway-Appliance herstellen. Über diese Verbindung können Clients über das Internet auf Remote-Desktops und -anwendungen zugreifen.

Wenn Sie die Blast Secure Gateway-Komponente aktivieren, wird der Blast Extreme-Datenverkehr von einem Sicherheitsserver oder einer Unified Access Gateway-Appliance zu Remote-Desktops und -anwendungen weitergeleitet. Wenn Clients, die Blast Extreme nutzen, auch die USB-Umleitungsfunktion oder die MMR-Beschleunigung (Multimedia Redirection) verwenden, können Sie die View Secure Gateway-Komponenten zum Weiterleiten dieser Daten aktivieren.

Wenn Sie direkte Clientverbindungen konfigurieren, wird der Blast Extreme-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 oder Unified Access Gateway-Appliances die erforderliche Sicherheit und Konnektivität, so dass keine VPN-Verbindung benötigt wird. Das Blast Secure Gateway gewährleistet, dass im Unternehmensrechenzentrum nur Remote-Datenverkehr von authentifizierten Benutzern verarbeitet wird. Endbenutzer können nur auf Ressourcen zugreifen, für deren Zugriff sie berechtigt sind.

Ein nativer Blast-Client, der über ein Blast Secure Gateway arbeitet, erwartet, dass die TLS-Verbindung seiner Blast-Sitzung durch das TLS-Zertifikat authentifiziert wird, das auf dem Blast Secure Gateway konfiguriert ist. Wenn die Blast-Verbindung des Clients andere TLS-Zertifikate sieht, wird die Verbindung unterbrochen, und der Client meldet eine Nichtübereinstimmung des Zertifikatfingerabdrucks.

Wenn Sie sich dafür entscheiden, dass der Client seine Verbindung zu einem TLS-terminierenden Proxy herstellt, der zwischen dem Client und dem Blast Secure Gateway platziert ist, können Sie die Zertifikatsanforderung des Clients erfüllen und einen Nichtübereinstimmungsfehler des Fingerabdrucks vermeiden, indem Sie dafür sorgen, dass der Proxy eine Kopie des Zertifikats (und des privaten Schlüssels) des Blast Secure Gateway vorlegt, sodass die Blast-Verbindung vom Client erfolgreich hergestellt werden kann.

Eine Alternative zum Kopieren des Zertifikats des Blast Secure Gateway in den Proxy besteht darin, dem Proxy ein eigenes TLS-Zertifikat zur Verfügung zu stellen und dann das Blast Secure Gateway so zu konfigurieren, dass der Client darauf hingewiesen wird, das Proxy-Zertifikat und nicht das Zertifikat des Blast Secure Gateway zu erwarten und zu akzeptieren.

Sie können das Blast Secure Gateway in ein Unified Access Gateway konfigurieren, indem Sie das Proxy-Zertifikat unter **Blast-Proxy-Zertifikat** in den Horizon-Einstellungen des Unified Access Gateway hochladen. Weitere Informationen finden Sie im Dokument *Bereitstellen und Konfigurieren von VMware Unified Access Gateway* unter <https://docs.vmware.com/de/Unified-Access-Gateway/index.html>.

---

**Hinweis** Es wird nur das Proxy-Zertifikat hochgeladen. Der entsprechende private Schlüssel wird nicht an das Unified Access Gateway weitergegeben.

---

## PCoIP Secure Gateway

Sicherheitsserver und Unified Access Gateway-Appliances enthalten eine PCoIP Secure Gateway-Komponente. Bei aktiviertem PCoIP Secure Gateway können Clients, die PCoIP verwenden, nach der Authentifizierung eine weitere sichere Verbindung zu einem Sicherheitsserver oder einer Unified Access Gateway-Appliance herstellen. Über diese Verbindung können Clients über das Internet auf Remote-Desktops und -anwendungen zugreifen.

Wenn Sie die PCoIP Secure Gateway-Komponente aktivieren, wird der PCoIP-Datenverkehr von einem Sicherheitsserver oder einer Unified Access Gateway-Appliance zu 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 oder Unified Access Gateway-Appliances 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 Konfigurationspeicher aller Horizon 7-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 Horizon 7-Komponenten darstellen.

View LDAP bietet ferner eine Gruppe von Plug-In-DLLs für Horizon 7, um anderen Horizon 7-Komponenten Automatisierungs- und Benachrichtigungsdienste bereitzustellen.

## Horizon Messaging

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

Diese Komponente unterstützt die JMS-API (Java Message Service), die für die Nachrichtenvermittlung in Horizon 7 verwendet wird.

Die Validierung der Nachrichten zwischen Komponenten verwendet DSA-Schlüssel. Die Schlüsselgröße beträgt standardmäßig 512 Bits, außer im FIPS-Modus. Hier beträgt die Schlüsselgröße 2048 Bits.

---

**Hinweis** Wenn der Sicherheitsmodus für Nachrichten auf **Erweitert** festgelegt ist, wird anstelle der Verschlüsselung auf Nachrichtenbasis SSL/TLS für sichere JMS-Verbindungen verwendet. Im erweiterten Sicherheitsmodus für Nachrichten wird die Validierung nur für einen Nachrichtentyp durchgeführt. Für den erweiterten Nachrichtenmodus empfiehlt VMware die Erhöhung der Schlüsselgröße auf 2048 Bits. Wenn Sie den erweiterten Sicherheitsmodus für Nachrichten nicht verwenden, empfiehlt VMware, den Standardwert von 512 Bits nicht zu ändern, da eine Erhöhung der Schlüsselgröße Einfluss auf Leistung und Skalierbarkeit hat.

---

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

## Firewallregeln für Horizon-Verbindungsserver

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

Wenn Sie 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 Horizon 7 herstellen können.

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 Horizon-Verbindungsserver-Installation geöffnet werden**

Protokoll	Ports	Typ der Horizon-Verbindungsserver-Instanz
JMS	TCP 4001	Standard- und Replikatserver
JMS	TCP 4002	Standard- und Replikatserver
JMSIR	TCP 4100	Standard- und Replikatserver
JMSIR	TCP 4101	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 UDP 8443	Standard-, Replikat- und Sicherheitsserver. Nachdem die erste Verbindung mit Horizon 7 hergestellt worden ist, stellt der Webbrowser oder das Clientgerät eine Verbindung mit dem Blast Secure Gateway an TCP-Port 8443 her. Die zweite Verbindung kann nur hergestellt werden, wenn das Blast Secure Gateway auf einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz aktiviert ist.
HTTPS	TCP 8472	Standard- und Replikatserver Für die Funktion Cloud-Pod-Architektur: für die podübergreifende Kommunikation verwendet.
HTTP	TCP 22389	Standard- und Replikatserver Für die Funktion Cloud-Pod-Architektur: für die globale LDAP-Replikation verwendet.
HTTPS	TCP 22636	Standard- und Replikatserver Für die Funktion Cloud-Pod-Architektur: für die sichere globale LDAP-Replikation verwendet.

## Firewall-Regeln für View Agent oder Horizon Agent

Mit den Installationsprogrammen für View Agent und Horizon Agent lassen sich optional Windows-Firewallregeln auf Remote-Desktops und RDS-Hosts für das Öffnen der standardmäßigen Netzwerkports konfigurieren. Wenn nicht anders angegeben, handelt es sich hierbei um eingehende Ports.

Die Installationsprogramme für View Agent und Horizon Agent konfigurieren die lokale Firewallregel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389).

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

Wenn Sie die RDP-Portnummer nach der Installation ändern, müssen Sie die dazugehörigen Firewall-Regeln ändern. Wenn Sie den Standard-Port nach der Installation ändern, müssen Sie die Windows-Firewall-Regeln manuell neu konfigurieren, um den Zugriff auf den aktualisierten Port zu erlauben. Weitere Informationen finden Sie unter „Ersetzen von Standardports für View-Dienste“ im Dokument *Horizon 7-Installation*.

Die Windows-Firewallregeln für View Agent oder Horizon Agent auf RDS-Hosts zeigen an, dass ein Block von 256 zusammenhängenden UDP-Ports für den eingehenden Datenverkehr geöffnet ist. Dieser Portblock ist für die interne Verwendung von VMware Blast in View Agent oder Horizon Agent vorgesehen. Ein spezieller Microsoft-signierter Treiber auf RDS-Hosts blockiert den eingehenden Datenverkehr zu diesen Ports von externen Quellen. Aufgrund dieses Treibers behandelt die Windows-Firewall die Ports als geschlossen.

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.

**Tabelle 5-5. Während der View Agent- oder Horizon Agent -Installation geöffnete TCP- und UDP-Ports**

Protokoll	Ports
RDP-	TCP-Port 3389
USB-Umleitung und Zeitzonensynchronisierung	TCP-Port 32111
MMR (Multimedia-Umleitung) und CDR (Clientlaufwerksumleitung)	TCP-Port 9427
PCoIP	<p>Für RDS-Hosts verwendet PCoIP die folgenden Portnummern: TCP-Port 4172 und UDP-Port 4172 (bidirektional).</p> <p>Für Desktops verwendet PCoIP Portnummern aus einem konfigurierbaren Bereich. Standardmäßig verbindet TCP 4172 mit 4173 und UDP verbindet 4172 mit 4182. Die Firewall-Regeln hierfür legen keine Portnummern fest, sondern folgen dynamisch den Ports, die von jedem PCoIP-Server geöffnet werden. Die ausgewählten Portnummern werden über den Verbindungsserver an den Client übertragen.</p>
VMware Blast	<p>TCP-Port 22443</p> <p>UDP-Port 22443 (bidirektional)</p> <p><b>Hinweis</b> UDP wird auf Linux-Desktops nicht verwendet.</p>
HTML Access	TCP-Port 22443

## Firewall-Regeln für Active Directory

Wenn zwischen der Horizon 7-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 Horizon 7 - Umgebung

## 6

Führen Sie diese allgemeinen Aufgaben aus, um Horizon 7 zu installieren und eine erste Bereitstellung zu konfigurieren.

**Tabelle 6-1. Checkliste für die Installation und Einrichtung von Horizon 7**

Schritt	Aufgabe
1	Richten Sie die benötigten Administratoren und Benutzergruppen in Active Directory ein. Anweisungen: <i>Installation von Horizon 7</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	(Optional) 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 Horizon 7</i> .
4	Installieren und konfigurieren Sie den Horizon-Verbindungsserver. Installieren Sie ebenso die Ereignisdatenbank. Anweisungen: Dokument <i>Installation von Horizon 7</i> .
5	Erstellen Sie mindestens eine virtuelle Maschine, die als Vorlage für Full-Clone-Desktop-Pools oder als übergeordnete virtuelle Maschine für Linked-Clone-Desktop-Pools oder für Instant-Clone-Desktop-Pools verwendet werden kann. Anweisungen: <i>Einrichten von virtuellen Desktops in Horizon 7</i> .
6	(Optional) Richten Sie einen RDS-Host ein und installieren Sie Anwendungen, die für Endbenutzer remote ausgeführt werden sollen. Anweisungen: <i>Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7</i> .
7	Erstellen Sie Desktop-Pools, Anwendungspools oder beides. Anweisungen: <i>Einrichten von virtuellen Desktops in Horizon 7</i> und <i>Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7</i> .
8	Steuern Sie den Benutzerzugriff auf Desktops. Anweisungen: <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</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 <a href="https://docs.vmware.com/de/VMware-Horizon-Client/index.html">https://docs.vmware.com/de/VMware-Horizon-Client/index.html</a> .
10	(Optional) Erstellen und konfigurieren Sie zusätzliche Administratoren, um verschiedene Zugriffsebenen auf bestimmte Bestandsobjekte und -einstellungen zu ermöglichen. Anweisungen: Dokument <i>Administration von Horizon 7</i> .

**Tabelle 6-1. Checkliste für die Installation und Einrichtung von Horizon 7 (Fortsetzung)**

Schritt	Aufgabe
11	(Optional) Konfigurieren Sie Richtlinien, um das Verhalten von Horizon 7-Komponenten, Desktop- und Anwendungspools und Endbenutzern zu steuern. Anweisungen: <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7.</i>
12	(Optional) Konfigurieren Sie Horizon Persona Management. Die Benutzer erhalten dann bei jeder Anmeldung bei einem Desktop Zugriff auf personalisierte Daten und Einstellungen. Anweisungen: <i>Einrichten von virtuellen Desktops in Horizon 7.</i>
13	(Optional) Um eine zusätzliche Sicherheitsebene zu schaffen, können Sie eine Smart Card-Authentifizierungslösung oder eine RADIUS-Zwei-Faktor-Authentifizierungslösung integrieren. Anweisungen: Dokument <i>Administration von Horizon 7.</i>