

Verwendung von VMware Horizon View Client für Windows

Horizon View 5.3

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

DE-001158-00

vmware[®]

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

<http://www.vmware.com/de/support/>

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

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

docfeedback@vmware.com

Copyright © 2012, 2013 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

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

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

Inhalt

Verwendung von VMware Horizon View Client für Windows	5
1 Systemanforderungen und Setup von Windows-basierten View Clients	7
Systemanforderungen für Windows-Clients	7
Hardwareanforderungen für Desktops im lokalen Modus	9
Voraussetzungen für die Verwendung der Multimedia-Umleitung (MMR)	10
Unterstützte View-Desktop-Betriebssysteme	11
Voraussetzungen für die Verwendung von Microsoft Lync mit Horizon View Client	11
Clientbrowseranforderungen für View Portal	12
Anforderungen für die Smartcard-Authentifizierung	13
Vorbereitung von View-Verbindungsserver für View Client	13
Durch VMware gesammelte View Client-Daten	14
2 Installation von View Client für Windows	17
Installieren von View Client (Windows-basiert) oder View Client with Local Mode	17
Installieren von View Client unter Verwendung von View Portal	19
Konfigurieren der im View Portal angezeigten View Client-Download-Links	20
Unbeaufsichtigte Installation von View Client	21
3 Konfigurieren von View Client für die Endbenutzer	27
Verwenden von URIs zur Konfiguration von View Client	27
Konfigurieren der Zertifikatsprüfungen für Endbenutzer	32
Ausführen von View Client über die Befehlszeile	34
4 Verwaltung der Serververbindungen und Desktops	39
Anmeldung an einem View-Desktop	39
Wechseln zwischen Desktops	42
Abmelden oder Trennen von Desktops	42
5 Arbeiten auf einem View-Desktop	45
Funktionsunterstützungs-Matrix	45
Internationalisierung	47
Verbinden von USB-Geräten	47
Konfigurieren von Clients zur erneuten Verbindung beim Neustart der USB-Geräte	49
Kopieren und Einfügen von Text und Bildern	50
Drucken auf einem View-Desktop	51
Steuern der Adobe Flash-Anzeige	52
Verwenden der Funktion der relativen Mausbewegung für CAD- und 3D-Anwendungen	53
6 Arbeiten mit Desktops im lokalen Modus	55
Erstmaliges Auschecken eines Desktops im lokalen Modus	55

Herunterfahren oder Anhalten eines lokalen Desktops	56
Backup eines Desktops	56
Einchecken eines Desktops	57
Rollback eines Desktops	58
Konfigurieren der Ressourcennutzung für Endpunkte	58
7 Fehlerbehebung für View Client	65
Vorgehensweise, wenn View Client unerwartet beendet wird	65
Zurücksetzen eines Desktops	65
Deinstallieren von View Client	66
Index	67

Verwendung von VMware Horizon View Client für Windows

Dieses Handbuch, *Verwendung von VMware Horizon View Client für Windows*, bietet Informationen über die Installation und Verwendung der VMware® Horizon View™-Software auf einem Microsoft Windows-Client-System zur Verbindungsherstellung mit einem View-Desktop im Rechenzentrum.

Die Informationen in diesem Dokument umfassen Systemanforderungen und Anweisungen zur Installation und Verwendung von Horizon View Client für Windows.

Diese Informationen sind für Administratoren bestimmt, die eine Bereitstellung von Horizon View mit Microsoft Windows-Client-Systemen ermöglichen müssen, so z. B. Desktops und Laptops. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Vorgängen in Rechenzentren vertraut sind.

Systemanforderungen und Setup von Windows-basierten View Clients

1

Systeme, auf denen View-Clientkomponenten ausgeführt werden, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Auf Windows-Systemen verwendet View Client zum Herstellen einer Verbindung mit View-Verbindungsserver die Interneteinstellungen von Microsoft Internet Explorer (einschließlich Proxy-Einstellungen). Stellen Sie sicher, dass die richtigen Internet Explorer-Einstellungen festgelegt sind und Sie über Internet Explorer auf die View-Verbindungsserver-URL zugreifen können. Sie können Internet Explorer 7, 8 oder 9 verwenden.

Dieses Kapitel behandelt die folgenden Themen:

- [„Systemanforderungen für Windows-Clients“](#), auf Seite 7
- [„Hardwareanforderungen für Desktops im lokalen Modus“](#), auf Seite 9
- [„Voraussetzungen für die Verwendung der Multimedia-Umleitung \(MMR\)“](#), auf Seite 10
- [„Unterstützte View-Desktop-Betriebssysteme“](#), auf Seite 11
- [„Voraussetzungen für die Verwendung von Microsoft Lync mit Horizon View Client“](#), auf Seite 11
- [„Clientbrowseranforderungen für View Portal“](#), auf Seite 12
- [„Anforderungen für die Smartcard-Authentifizierung“](#), auf Seite 13
- [„Vorbereitung von View-Verbindungsserver für View Client“](#), auf Seite 13
- [„Durch VMware gesammelte View Client-Daten“](#), auf Seite 14

Systemanforderungen für Windows-Clients

View Client für Windows kann auf PCs oder Laptops installiert werden, die ein Microsoft Windows 8-, Windows 7-, Vista- oder XP-Betriebssystem verwenden.

Sowohl die PCs oder Laptops, auf denen Sie View Client installieren, als auch die Peripheriegeräte müssen bestimmte Systemanforderungen erfüllen.

Modell Standardmäßiges x86-System oder x86-System mit 64-Bit-Kompatibilität für Desktop- oder Laptopcomputer

Arbeitsspeicher Mindestens 1GB Arbeitsspeicher (RAM)

Betriebssysteme

Betriebssystem	Version	SP
Windows 8-Desktop	32- oder 64-Bit	-
Windows 7	32- oder 64-Bit	Ohne oder SP1

Betriebssystem	Version	SP
Windows XP	32-Bit	SP3
Windows Vista	32-Bit	SP1 oder SP2

Für Windows 7 und Windows Vista werden die folgenden Editionen unterstützt: Home, Enterprise, Professional/Business und Ultimate. Für Windows XP werden die Editionen Home und Professional unterstützt.

Für Windows 8 werden die folgenden Editionen unterstützt: Windows 8 Pro - Desktop und Windows 8 Enterprise - Desktop.

View-Verbindungsserver, Security Server und View Agent

4.6.1 oder höher

Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, empfiehlt VMware die Verwendung eines Sicherheitsservers. Mit einem Sicherheitsserver erfordern die Clientsysteme keine VPN-Verbindung.

Anzeigeprotokoll für Horizon View

PCoIP oder RDP

Hardwareanforderungen für PCoIP

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.
- ARM-Prozessor mit NEON- (bevorzugt) oder WMMX2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 1 GHz oder schneller.
- Verfügbarer RAM über den Systemanforderungen zur Unterstützung verschiedener Monitorkonfigurationen. Im Allgemeinen gilt die folgende Formel:

$$20\text{MB} + (24 * (\# \text{ monitors}) * (\text{monitor width}) * (\text{monitor height}))$$

Als grobes Maß können Sie die folgenden Berechnungen verwenden:

$$1 \text{ monitor: } 1600 \times 1200: 64\text{MB}$$

$$2 \text{ monitors: } 1600 \times 1200: 128\text{MB}$$

$$3 \text{ monitors: } 1600 \times 1200: 256\text{MB}$$

Hardwareanforderungen für RDP

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.
- ARM-Prozessor mit NEON- (bevorzugt) oder WMMX2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 600MHz oder schneller.
- 128 MB RAM.

Softwareanforderungen für RDP

- Für die Verwendung mehrerer Monitore ist RDC 6.0 oder eine neuere Version erforderlich.
- Für Windows XP- und Windows XP Embedded-Systeme ist Microsoft RDC 6.x zu verwenden.
- Windows Vista umfasst RDC 6.x; es wird jedoch RDC 7 empfohlen.
- Windows 7 umfasst RDC 7. Windows 7 SP1 umfasst RDC 7.1.
- Für virtuelle Windows XP-Maschinen müssen Sie die RDP-Patches installieren, die in den Knowledgebase-Artikeln 323497 und 884020 aufgeführt sind. Wenn Sie die RDP-Patches nicht installieren, wird möglicherweise ein Windows Socket-Fehler auf dem Client angezeigt.

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

Die RDC-Versionen stehen auf der Microsoft-Website zum Download zur Verfügung.

Hardwareanforderungen für Desktops im lokalen Modus

Wenn Sie einen View-Desktop zur Verwendung auf Ihrem lokalen Computer auschecken, muss die Hardware auf dem Clientcomputer sowohl das lokale System als auch die virtuelle Maschine unterstützen, die nun darauf ausgeführt wird.

PC-Hardware

Tabelle 1-1 beschreibt die Hardwareanforderungen für verschiedene View-Desktop-Betriebssysteme.

Tabelle 1-1. Prozessoranforderungen

Clientcomputeranforderung	Beschreibung
PC	x86 64-kompatibel LAHF/SAHF-Unterstützung im Long Mode
Anzahl von CPUs	Multiprozessorsysteme werden unterstützt
CPU-Geschwindigkeit	Für einen lokalen Windows XP-Desktop 1,3 GHz oder schneller; 1,6GHz empfohlen Für einen Windows 7- oder 8-Desktop 1,3 GHz oder schneller; für Aero-Effekte 2,0 GHz oder schneller
Intel-Prozessoren	Pentium 4-, Pentium M- (mit PAE), Core-, Core 2-, Core i3-, Core i5- und Core i7-Prozessoren Für Windows 7- oder 8-Aero: Intel-Dual-Core
AMD-Prozessoren	Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom und Phenom II Die AMD-CPU muss im Long Mode über Segmentlimit-Unterstützung verfügen. Für Windows 7- oder 8-Aero: Athlon 4200+ und höher
64-Bit-Betriebssysteme auf View-Desktops	Intel Pentium 4- und Core 2- sowie Core i7-Prozessoren mit EM64T und Intel Virtualization Technology Für die Intel-CPU muss VT-x-Unterstützung im Hostsystem-BIOS aktiviert sein. Die BIOS-Einstellungen, die für die VT-x-Unterstützung aktiviert sein müssen, sind abhängig vom jeweiligen Systemhersteller. Im VMware-Knowledgebase-Artikel http://kb.vmware.com/kb/1003944 finden Sie Informationen darüber, wie Sie bestimmen können, ob die VT-x-Unterstützung aktiviert ist. Die meisten AMD64-Prozessoren (ausgenommen Revision C Opteron-Prozessoren)
Grafikprozessor für Windows 7- oder 8-Aero	nVidia GeForce 8800GT und höher ATI Radeon HD 2600 und höher

Obwohl es sich bei dem Betriebssystem auf dem Clientcomputer um eine 32-Bit- oder 64-Bit-Version handeln kann, muss die Hardware 64-Bit-kompatibel sein und über aktivierte Intel- oder AMD-Technologie zur Virtualisierungsunterstützung verfügen, um einen View-Desktop unter einem 64-Bit-Betriebssystem ausführen zu können. Wenn diese Anforderungen erfüllt sind, sollten Sie einen View-Desktop mit einem 64-Bit-Betriebssystem auf einem Client mit 32-Bit- oder 64-Bit-Betriebssystem ausführen können.

Festplattenspeicher

Bei Verwendung eines Standard-Setups für das Betriebssystem im View-Desktop entsprechen die tatsächlichen Anforderungen an den Festplattenspeicherplatz etwa den Anforderungen für die Installation und die Ausführung von Betriebssystem und Anwendungen auf einem physischen Computer.

Beispielsweise empfiehlt Microsoft 16 GB Festplattenspeicher für einen Computer, auf dem eine 32-Bit-Version von Windows 7 oder 8 ausgeführt wird. Wenn Sie eine 16 GB große virtuelle Festplatte für eine virtuelle Windows 7- oder 8-Maschine mit 32-Bit konfigurieren, wird nur der tatsächlich verwendete Speicherplatz heruntergeladen, wenn Sie den lokalen Desktop auschecken. Für einen Desktop, dem 16 GB zugewiesen sind, beträgt die tatsächliche Downloadgröße möglicherweise 7 GB.

Nach dem Download des Desktops kann die Menge des verwendeten Speicherplatzes auf bis zu 16 GB ansteigen, wenn Sie eine Festplatte mit 16 GB konfiguriert haben. Da während der Replikation ein Snapshot erstellt wird, wird zusätzlich eine gleich große Menge an Speicherplatz benötigt. Wenn beispielsweise aktuell 7 GB Speicherplatz für den lokalen Desktop verwendet werden, belegt der Snapshot zusätzliche 7 GB auf dem Clientcomputer.

IDE- und SCSI-Festplattenlaufwerke werden unterstützt.

Arbeitsspeicher

Sie benötigen ausreichend Arbeitsspeicher zum Ausführen des Hostbetriebssystems auf dem Clientcomputer sowie die erforderliche Arbeitsspeicherkapazität für das Betriebssystem des View-Desktops sowie für Anwendungen auf dem Clientcomputer und auf dem View-Desktop. VMware empfiehlt für Windows XP und Windows Vista 2 GB oder mehr, für Windows 7 oder 8 werden 3 GB oder mehr empfohlen. Weitere Informationen zu den Arbeitsspeicheranforderungen finden Sie in der Dokumentation zu Ihrem Gastbetriebssystem sowie in der Anwendungsdokumentation.

Die Arbeitsspeichergröße, die Sie allen virtuellen Maschinen auf einem einzelnen Computer insgesamt zuweisen können, wird allein durch die RAM-Größe auf dem Computer begrenzt. Die maximale Arbeitsspeichergröße für jeden View-Desktop beträgt auf 64-Bit-Computern 32 GB.

Grafik

Es wird ein 32-Bit-Anzeigeadapter empfohlen. 3D-Benchmarks, z.B. 3DMark '06, werden möglicherweise nicht ordnungsgemäß oder überhaupt nicht gerendert, wenn virtuelle Windows Vista- oder Windows 7- oder 8-Maschinen auf einigen Grafikhardwareprodukten ausgeführt werden.

View Client with Local Mode unterstützt DirectX9c, welches auf Clientsystemen mit unterstützungsfähigen Grafikprozessoren automatisch aktiviert wird. DirectX9c umfasst verschiedene 3D-Funktionen, so zum Beispiel Google Earth mit aktivierter 3D-Konstruktion, Windows 7- oder 8 Aero-Effekte und einige 3D-Spiele.

Zur Wiedergabe von Videos mit 720p oder mehr ist ein Multiprozessorsystem erforderlich.

Die CPU- und Grafikprozessoranforderungen zur Unterstützung von Windows 7- oder 8-Aero sind unter [Tabelle 1-1](#) aufgeführt.

Voraussetzungen für die Verwendung der Multimedia-Umleitung (MMR)

Die MMR-Funktion (Multimedia Redirection) sendet Multimediadaten unter Verwendung eines virtuellen Kanals direkt an den Client.

Mit MMR wird der Multimediadatenstrom auf dem Clientsystem verarbeitet, d. h. verschlüsselt und entschlüsselt. Lokale Hardware wird formatiert und gibt Medieninhalte wieder, wobei die Nachfragelast auf den ESX/ESXi-Host gelegt wird.

View Client und View Client with Local Mode unterstützen MMR auf den folgenden Betriebssystemen:

- Windows XP

- Windows XP Embedded
- Windows Vista

Die MMR-Funktion unterstützt die Mediendateiformate, die das Clientsystem unterstützt, da auf dem Client lokale Decoder vorhanden sein müssen. Dateiformate sind unter anderem MPEG2-1, MPEG-2, MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3 und WAV.

Arbeiten Sie mit Windows Media Player 10 oder höher, und installieren Sie das Programm sowohl auf dem lokalen Computer als auch dem Clientzugriffsgesetz sowie dem View-Desktop.

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

HINWEIS Die View Client-Hardware zur Videoanzeige muss Overlay-Unterstützung bieten, damit MMR ordnungsgemäß funktioniert.

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

Unterstützte View-Desktop-Betriebssysteme

Administratoren erstellen virtuelle Maschinen mit einem Gastbetriebssystem und installieren View Agent auf diesem Gastbetriebssystem. Die Endbenutzer können sich an diesen virtuellen Maschinen von einem Client-Gerät aus anmelden.

Eine Liste mit unterstützten Gastbetriebssystemen finden Sie unter dem Thema „Unterstützte Betriebssysteme für View Agent“ in der Dokumentation Installation von Horizon View 4.6.x oder 5.x.

Voraussetzungen für die Verwendung von Microsoft Lync mit Horizon View Client

Mit Horizon View 5.2 können Kunden jetzt einen Microsoft Lync 2013-Client auf ihren View-Desktops einsetzen, um an Unified Communications (UC) VoIP (Voice over IP) und Video-Chats mit Lync-zertifizierten USB-Audio- und Videogeräten teilzunehmen. Die Verwendung eines speziellen IP-Telefons ist nicht mehr erforderlich.

Für diese neue Architektur ist die Installation eines Microsoft Lync 2013-Clients auf dem View-Desktop und einem Microsoft Lync VDI-Plug-In auf dem Clientendpunkt erforderlich. Kunden können den Microsoft Lync 2013-Client für Präsenz, Instant Messaging, Webkonferenz und Microsoft Office-Funktionen verwenden.

Sobald ein Lync VoIP-Anruf oder Video-Chat eintrifft, nimmt das Lync-VDI-Plug-In die gesamte Medienverarbeitung vom Rechenzentrumsserver auf den Clientendpunkt und codiert alle Medien in Lync-optimierten Audio- und Videocodern. 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.

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

Für diese Funktion gelten die folgenden Anforderungen.

Betriebssystem

- Client-Betriebssystem: Volle Unterstützung für 32- oder 64-Bit-Windows 7 SP1
- 32-Bit- und 64-Bit-Windows 8 ist ein Tech-Preview.

	<ul style="list-style-type: none">■ Betriebssystem der virtuellen Maschine (Agent): 32- oder 64-Bit-Windows 7 SP1
Software des Clientsystems	<ul style="list-style-type: none">■ Horizon View Client für Windows 5.3■ 32-Bit-Version des Microsoft Lync VDI-Plug-Ins <hr/> <p>WICHTIG Die 64-Bit-Version von Microsoft Office muss nicht auf dem Clientcomputer installiert werden. Das erforderliche 32-Bit-Microsoft Lync VDI-Plug-In ist nicht mit der 64-Bit-Version von Microsoft Office 2013 kompatibel.</p> <hr/>
	<ul style="list-style-type: none">■ Das Sicherheitszertifikat, das während der Bereitstellung von Microsoft Lync Server 2013 erzeugt wird, muss in das Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen importiert werden
Software für den View-Desktop (Agent)	<ul style="list-style-type: none">■ Horizon View Agent 5.2■ Microsoft Lync 2013-Client <p>Die Bit-Version des Lync 2013-Clients sollte der Bit-Version des Betriebssystems der virtuellen Maschine entsprechen.</p> <ul style="list-style-type: none">■ Das Sicherheitszertifikat, das während der Bereitstellung von Microsoft Lync Server 2013 erzeugt wird, muss in das Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen importiert werden
Erforderliche Server	<ul style="list-style-type: none">■ Ein Server, auf dem View-Verbindungsserver 5.2 ausgeführt wird■ Ein Server, auf dem Microsoft Lync Server 2013 ausgeführt wird■ Eine vSphere-Infrastruktur zur Aufnahme der virtuellen Maschinen <p>Auf dem vCenter Server und den ESXi-Hosts muss vSphere 5.0 oder höher ausgeführt werden.</p>
Hardware	<ul style="list-style-type: none">■ Hardware, die alle der zuvor genannten erforderlichen Softwarekomponenten unterstützt■ Clientendpunkt: 1,5 GHz oder schnellere CPU und mindestens 2 GB RAM für das Microsoft Lync 2013-Plug-In

Clientbrowseranforderungen für View Portal

Von einem Clientsystem aus können Sie einen Browser öffnen und zu einer bestimmten View-Verbindungsserver-Instanz navigieren. Die erscheinende Webseite trägt den Namen View Portal und enthält Links zum Herunterladen der Installationsprogrammdatei für View Client.

Zur Verwendung von View Portal müssen Sie über einen der folgenden Webbrowser verfügen:

- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10 (von einem Windows 8-System im Desktop-Modus)
- Firefox 6 und höher
- Safari 5 (auf einem Mac)
- Chrome 14 oder später

Anforderungen für die Smartcard-Authentifizierung

Clientsysteme, die eine Smartcard für die Benutzerauthentifizierung verwenden, müssen bestimmte Anforderungen erfüllen.

Für jedes Clientsystem, das zur Benutzerauthentifizierung eine Smartcard verwendet, gelten die folgenden Software- und Hardwareanforderungen:

- View Client
- Ein Windows-kompatibler Smartcard-Leser
- Smartcard-Middleware
- Produktspezifische Anwendungstreiber

Sie müssen auf den View-Desktops zusätzlich produktspezifische Anwendungstreiber installieren.

VMware View unterstützt Smartcards und Smartcard-Leser, die einen PKCS#11- oder Microsoft CryptoAPI-Anbieter verwenden. Optional können Sie das ActivClient-Softwarepaket von ActivIdentity installieren, das Tools zur Interaktion mit Smartcards bereitstellt.

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über ein Smartcard- oder USB-Smartcard-Token verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten.

Zum Installieren von Zertifikaten auf einer Smartcard müssen Sie einen Computer einrichten, der als Registrierungsstelle fungiert. Dieser Computer muss Smartcard-Zertifikate für Benutzer ausgeben können und Mitglied der Domäne sein, für die Sie Zertifikate ausgeben.

WICHTIG Wenn Sie eine Smartcard anmelden, können Sie die Schlüsselgröße des resultierenden Zertifikats auswählen. Zur Verwendung von Smartcards auf lokalen Desktops müssen Sie bei der Smartcard-Registrierung eine Schlüsselgröße von 1024 Bit oder 2048 Bit auswählen. Zertifikate mit 512-Bit-Schlüsseln werden nicht unterstützt.

Die Microsoft TechNet-Website enthält ausführliche Informationen zu Planung und Implementierung der Smartcard-Authentifizierung für Windows-Systeme.

Neben der Einhaltung dieser Anforderungen für View Client-Systeme müssen andere View-Komponenten bestimmte Anforderungen an die Konfiguration zur Unterstützung von Smartcards erfüllen:

- Informationen zur Konfiguration von View-Servern für die Nutzung von Smartcards finden Sie unter dem Thema „Konfigurieren der Smartcard-Authentifizierung“ im Dokument *Verwaltung von VMware Horizon View*.
- Informationen zu den Aufgaben, die Sie womöglich in Active Directory zur Implementierung der Smartcard-Authentifizierung durchführen müssen, finden Sie in den Hilfethemen zur Vorbereitung von Active Directory für die Smartcard-Authentifizierung im Dokument *Installation von VMware Horizon View*.

Vorbereitung von View-Verbindungsserver für View Client

Administratoren müssen bestimmte Aufgaben durchführen, um Endbenutzern die Verbindung zu den View-Desktops zu ermöglichen.

Bevor die Endbenutzer eine Verbindung mit dem View-Verbindungsserver oder einem Sicherheitsserver herstellen und auf einen View-Desktop zugreifen können, müssen bestimmte Pool- und Sicherheitseinstellungen konfiguriert werden:

- Stellen Sie bei Verwendung eines Sicherheitsservers, wie von VMware empfohlen, sicher, dass ein View-Verbindungsserver der Version 4.6.1 oder höher und ein View-Sicherheitsserver der Version 4.6.1 oder höher verwendet werden. Siehe die Dokumentation *Installation von VMware Horizon View*.

- Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für den View-Verbindungsserver oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.
 Navigieren Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in View Administrator auf das Dialogfeld View-Verbindungsserver-Einstellungen bearbeiten und setzen Sie einen Haken in das Kontrollkästchen **[Sichere Tunnelverbindung zum Desktop verwenden]** .
- Vergewissern Sie sich, dass ein virtueller Desktop-Pool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen View-Desktop verfügt. Siehe die Hilfetemen zur Erstellung von Desktop-Pools in der Dokumentation *Verwaltung von VMware Horizon View*.
- Zum Verwenden der zweistufigen Authentifizierung für View Client, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, müssen Sie diese Funktion auf dem View-Verbindungsserver aktivieren. Die RADIUS-Authentifizierung ist bei View-Verbindungsservern mit View 5.1 oder höher verfügbar. Weitere Informationen finden Sie in den Themen über zweistufige Authentifizierung in der Dokumentation *Verwaltung von VMware Horizon View*.

Durch VMware gesammelte View Client-Daten

Wenn Ihr Unternehmen am Programm zur Verbesserung der Benutzerfreundlichkeit teilnimmt, erhebt VMware Daten aus bestimmten Horizon View Client-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

HINWEIS Diese Funktion ist nur verfügbar, wenn Ihre Horizon View-Bereitstellung den View-Verbindungsserver der Version 5.1 oder einer höheren Version verwendet. Client-Informationen werden für Clients mit View Client 2.0 und höher gesendet.

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein Administrator Ihres Unternehmens zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit entscheidet, sammelt VMware anonyme Daten über Ihre Bereitstellung, um die Reaktion von VMware auf die Kundenanforderungen verbessern zu können. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten. Die View Client-Informationen werden erst an den Horizon View-Server und dann an VMware gesendet, zusammen mit den Daten der View-Server, Desktop-Pools und View-Desktops.

Auch wenn die Informationen bei der Übertragung an den View-Verbindungsserver verschlüsselt werden, werden die Informationen des Clientensystems unverschlüsselt in einem benutzerspezifischen Verzeichnis protokolliert. Die Protokolle enthalten jedoch keine personen- oder unternehmensbezogenen Informationen.

Zur Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit kann der Administrator, der die Installation des View-Verbindungservers durchführt, bei der Ausführung des Installations-Assistenten für den View-Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in View Administrator festlegen.

Tabelle 1-2. Von den View Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, welches die View Client-Anwendung entwickelte	No (Nein)	VMware
Produktname	No (Nein)	VMware Horizon View Client
Client-Produktversion	No (Nein)	Das Format lautet <i>x.x.x-yy/yyyy</i> , wobei <i>x.x.x</i> für die Client-Versionnummer und <i>yy/yyyy</i> für die Build-Nummer steht.

Tabelle 1-2. Von den View Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit (Fortsetzung)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Client-Binärarchitektur	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ i386 ■ x86_64 ■ arm
Client-Build-Name	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ VMware-wswc-viewclient-x86_64 ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android
Host-Betriebssystem	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Windows 7, 64-Bit Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.7.5 (11G63)
Host-Betriebssystemkernel	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unknown (unbekannt) (für Windows Store)
Host-Betriebssystemarchitektur	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unknown (unbekannt) (für iPad)
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	No (Nein)	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ 4096 ■ unknown (unbekannt) (für Windows Store)

Installation von View Client für Windows

2

Sie können das Windows-basierte View Client-Installationsprogramm entweder von der VMware-Website oder über View Portal abrufen, einer Seite für den Webzugriff, die von View-Verbindungsserver bereitgestellt wird. Nach der Installation von View Client können Sie verschiedene Startoptionen für die Endbenutzer festlegen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Installieren von View Client \(Windows-basiert\) oder View Client with Local Mode“](#), auf Seite 17
- [„Installieren von View Client unter Verwendung von View Portal“](#), auf Seite 19
- [„Konfigurieren der im View Portal angezeigten View Client-Download-Links“](#), auf Seite 20
- [„Unbeaufsichtigte Installation von View Client“](#), auf Seite 21

Installieren von View Client (Windows-basiert) oder View Client with Local Mode

Endbenutzer öffnen View Client, um von einem physischen Computer eine Verbindung mit ihren virtuellen Desktops herzustellen. Sie können eine Windows-basierte Installationsdatei zum Installieren sämtlicher Komponenten von View Client ausführen.

View Client with Local Mode ermöglicht Endbenutzern das Herunterladen einer Kopie ihres virtuellen Desktops auf ihren lokalen Computer. Anschließend können die Endbenutzer den virtuellen Desktop sogar verwenden, wenn keine Netzwerkverbindung vorhanden ist. Die Latenz wird minimiert und die Leistung wird verbessert.

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

Dieser Vorgang beschreibt die Installation von View Client über einen interaktiven Installationsassistenten. Wenn Sie stattdessen die Befehlszeilenoption bzw. die Option zur unbeaufsichtigten Installation des Microsoft Windows Installer (MSI) verwenden möchten, finden Sie weitere Informationen unter [„Unbeaufsichtigte Installation von View Client“](#), auf Seite 22.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe [„Systemanforderungen für Windows-Clients“](#), auf Seite 7.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Voraussetzungen für den lokalen Modus:
 - Stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst.

- Stellen Sie sicher, dass keines der folgenden Produkte installiert ist: VMware Horizon View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Voraussetzungen für die USB-Umleitung:
 - Bestimmen Sie, ob der Benutzer des Clientgeräts von einem virtuellen Desktop auf lokal verbundene USB-Geräte zugreifen darf. Ist dies nicht der Fall, können Sie entweder die vom Assistenten vorgelegte Komponente **[USB-Umleitung]** deaktivieren oder die Komponente installieren, sie jedoch unter Verwendung von Gruppenrichtlinienobjekten deaktivieren.

VMware empfiehlt, die Komponente **[USB-Umleitung]** immer zu installieren und Gruppenrichtlinienobjekte zur Steuerung des USB-Zugriffs zu verwenden. Auf diese Weise müssen Sie View Client nicht noch einmal neu installieren, wenn Sie die USB-Umleitung für einen Client zu einem späteren Zeitpunkt aktivieren möchten. Weitere Informationen finden Sie unter dem Thema „Einstellungen für die ADM-Vorlage der View Client-Konfiguration“ im Kapitel über die Konfigurationsrichtlinien im Dokument *Verwaltung von VMware Horizon View*.
 - Wenn Sie die Komponente **[USB-Umleitung]** installieren möchten, stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.
- Bestimmen Sie, ob die Funktion verwendet werden soll, mit der Endbenutzer sich bei View Client und ihrem virtuellen Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View-Verbindungsserver-Instanz und schließlich an den virtuellen Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Wenn Sie nicht möchten, dass die Endbenutzer den vollqualifizierten Domänennamen (FQDN) der View-Verbindungsserver-Instanz eingeben müssen, die ihre virtuelle Maschine hostet, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Vorgehensweise

- 1 Melden Sie sich als Benutzer mit Administratorberechtigungen am Clientsystem an.
- 2 Laden Sie auf dem Clientsystem die View Client-Installationsdatei von der VMware-Download-Seite unter Horizon View Client <http://www.vmware.com/products/http://www.vmware.com/go/viewclients> herunter.

Wählen Sie die entsprechende Installationsdatei aus, wobei *xxxxxx* die Build-Nummer und *y.y.y* die Versionsnummer ist.

Option	Aufgabe
View Client auf 64-Bit-Betriebssystemen	Wählen Sie die Datei <i>VMware-viewclient-x86_64-y.y.y-xxxxxx.exe</i> für View Client. Wählen Sie die Datei <i>VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe</i> für View Client mit lokalem Modus.
View Client auf 32-Bit-Betriebssystemen	Wählen Sie <i>VMware-viewclient-y.y.y-xxxxxx.exe</i> für View Client. Wählen Sie <i>VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe</i> für View Client mit lokalem Modus.

- 3 Zum Starten des View Client-Installationsprogramms doppelklicken Sie auf die Installationsdatei.
- 4 Folgen Sie den Anweisungen zum Installieren der gewünschten Komponenten.

Der VMware View Client-Dienst wird auf dem Windows-Clientcomputer installiert. Der Dienstname für View Client lautet *wsm*. Die Dienstnamen für die USB-Komponenten sind *VMUSBArbService* und *vmware-view-usbd*.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Anmeldung an einem View-Desktop“, auf Seite 39 oder „Installieren von View Client unter Verwendung von View Portal“, auf Seite 19.

Installieren von View Client unter Verwendung von View Portal

Eine bequeme Methode zum Herunterladen und Installieren von View Client oder View Client mit Local Mode besteht darin, einen Browser zu öffnen und zur View Portal-Webseite zu wechseln. Sie können über View Portal das vollständige Installationsprogramm für View Client herunterladen, sowohl für Windows- als auch für Mac-Clientcomputer.

Als Alternative zum Suchen einer VMware-Downloadseite für das Herunterladen von View Client können Sie nach einer View-Verbindungsserver-URL suchen. Sie können die Einstellungen auch so konfigurieren, dass die Links auf View Portal auf einen anderen Standort als die VMware-Downloadseite zeigen.

Voraussetzungen

- Wenn die Links auf View Portal auf einen anderen Zielort als die VMware-Downloadseite zeigen müssen, siehe „[Konfigurieren der im View Portal angezeigten View Client-Download-Links](#)“, auf Seite 20.
- Stellen Sie sicher, dass Sie über die URL für die View-Verbindungsserver-Instanz verfügen.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „[Systemanforderungen für Windows-Clients](#)“, auf Seite 7.
- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Voraussetzungen für den lokalen Modus:
 - Stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst.
 - Stellen Sie sicher, dass keines der folgenden Produkte installiert ist: VMware Horizon View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Voraussetzungen für die USB-Umleitung:
 - Bestimmen Sie, ob der Benutzer des Clientgeräts von einem virtuellen Desktop auf lokal verbundene USB-Geräte zugreifen darf. Ist dies nicht der Fall, können Sie entweder die vom Assistenten vorgelegte Komponente **[USB-Umleitung]** deaktivieren oder die Komponente installieren, sie jedoch unter Verwendung von Gruppenrichtlinienobjekten deaktivieren.

VMware empfiehlt, die Komponente **[USB-Umleitung]** immer zu installieren und Gruppenrichtlinienobjekte zur Steuerung des USB-Zugriffs zu verwenden. Auf diese Weise müssen Sie View Client nicht noch einmal neu installieren, wenn Sie die USB-Umleitung für einen Client zu einem späteren Zeitpunkt aktivieren möchten. Weitere Informationen finden Sie unter dem Thema „Einstellungen für die ADM-Vorlage der View Client-Konfiguration“ im Kapitel über die Konfigurationsrichtlinien im Dokument *Verwaltung von VMware Horizon View*.
 - Wenn Sie die Komponente **[USB-Umleitung]** installieren möchten, stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.

Vorgehensweise

- 1 Melden Sie sich als Benutzer mit Administratorberechtigungen am Clientsystem an.
- 2 Öffnen Sie einen Browser und geben Sie die URL der View-Verbindungsserver-Instanz ein, die Zugriff auf den virtuellen Desktop bietet.

Vergewissern Sie sich, dass Sie bei der URL `https` anstelle von `http` verwenden.
- 3 Klicken Sie den entsprechenden Link für Ihren Betriebssystemtyp (32-Bit oder 64-Bit) und den zu installierenden View Client-Typ (mit oder ohne lokalen Modus).
- 4 Wenn Sie dazu aufgefordert werden, speichern Sie die Installationsdatei in Ihrem Clientsystem.
- 5 Zum Starten des View Client-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

- 6 Folgen Sie den Anweisungen zum Installieren der gewünschten Komponenten.

Weiter

Stellen Sie eine Verbindung mit dem View-Desktop her. Siehe „[Anmeldung an einem View-Desktop](#)“, auf Seite 39.

Konfigurieren der im View Portal angezeigten View Client-Download-Links

Normalerweise enthält die View Portal-Seite, die erscheint, wenn Sie einen Browser öffnen und die URL einer View-Verbindungsserver-Instanz eingeben, Links zur VMware Downloads-Website zum Herunterladen des View Client. Das Standardverhalten kann geändert werden.

Die standardmäßigen View Client-Links in View Portal stellen sicher, dass Sie zu den aktuellsten kompatiblen View Client-Installationsprogrammen geleitet werden. In einigen Fällen jedoch möchten Sie vielleicht, dass die Links auf einen internen Webserver verweisen, oder Sie möchten bestimmten Client-Versionen auf Ihren eigenen View-Verbindungsserver zur Verfügung stellen. Sie können die Seite neu konfigurieren, sodass sie auf eine andere URL verweist.

WICHTIG Wenn Sie die View Portal-Links anpassen, wie in diesem Thema beschrieben, und später VMware Horizon View HTML Access auf dem Server installieren, wird Ihre benutzerdefinierte View Portal-Seite durch eine HTML-Zugriff-Seite ersetzt.

Voraussetzungen

- Laden Sie die Installationsdateien für die View Client-Typen herunter, die Sie in Ihrer Umgebung einsetzen möchten. Die URL für die View Client-Download-Seite ist <https://www.vmware.com/go/viewclients>.
- Legen Sie fest, auf welchem HTTP-Server die Installationsdateien liegen sollen. Die Dateien können sich auf einer View-Verbindungsserver-Instanz oder auf einem anderen HTTP-Server befinden.

Vorgehensweise

- 1 Erstellen Sie auf dem HTTP-Server, auf dem sich die Installationsdateien befinden sollen, einen Ordner für die Dateien des Installationsprogramms.

Um die Dateien beispielsweise in einen Ordner `downloads` im Standardinstallationsverzeichnis auf dem View-Verbindungsserver-Host zu stellen, verwenden Sie den folgenden Pfad:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Die Links zu den Dateien würden dann URLs mit dem Format `https://Servername/downloads/Client-Installer-Dateiname` verwenden. Ein Server mit dem Namen `view.mycompany.com` würde die folgende URL für View Client für Windows benutzen: `https://view.mycompany.com/downloads/VMware-viewclient.exe`. Bei diesem Beispiel befindet sich der Ordner mit dem Namen `downloads` im Stammordner `webapps`.

- 2 Kopieren Sie die View Client-Installationsdateien in den Ordner.

Wenn sich der Ordner auf einem View-Verbindungsserver-Dienst neu befindet, können Sie alle Dateien in diesem Ordner ersetzen, ohne den VMware View-Verbindungsserver-Dienst neu starten zu müssen.

- 3 Kopieren Sie auf dem View-Verbindungsserver die Datei `portal-links.properties` und die Datei `portal.properties`, die sich unter `Installationspfad\Server\Extras\PortalExamples` befinden.
- 4 Legen Sie einen Ordner `portal` im Verzeichnis `C:\ProgramData\VMware\VDM` an, und kopieren Sie die Dateien `portal-links.properties` und `portal.properties` in den Ordner `portal`.

- 5 Bearbeiten Sie die Datei `C:\ProgramData\VMware\VDM\portal\portal-links.properties` so, dass sie auf den neuen Speicherort der Installationsdateien verweist.

Sie können die Zeilen in dieser Datei bearbeiten und ihnen weitere hinzufügen, falls Sie weitere Links erstellen müssen. Sie können auch Zeilen löschen.

Die folgenden Beispiele zeigen Eigenschaften zum Erstellen von zwei Links für View Client für Windows und zwei Links für View Client für Linux:

```
link.win=https://server-name/downloads/VMware-viewclient-x86_64-y.y.y-XXXX.exe#win
link.win.1=https://server-name/downloads/VMware-viewclient-y.y.y-XXXX.exe#win
link.linux=https://server-name/downloads/VMware-viewclient-x86_64-y.y.y-XXXX.rpm#linux
link.linux.1=https://server-name/downloads/VMware-viewclient-y.y.y-XXXX.tar.gz#linux
```

Bei diesem Beispiel gibt `y.y.y-XXXX` die Versions- und Build-Nummer an. Der Text `win` am Ende der Zeile weist darauf hin, dass dieser Link im Browser angezeigt werden soll, wenn der Client über ein Windows-Betriebssystem verfügt. Verwenden Sie `win` für Windows, `linux` für Linux und `mac` für Mac OS X.

- 6 Bearbeiten Sie für Text die Datei `C:\ProgramData\VMware\VDM\portal\portal.properties` so, dass sie den anzuzeigenden Text für die Links angibt.

Diese Zeilen stehen im Abschnitt der Datei namens `# keys based on key names in portal-links.properties` zur Verfügung.

Das folgende Beispiel zeigt den Text, der den für `link.win` und `link.win.1` angegebenen Links entspricht:

```
text.win=View Client for Windows 32 bit Client users
text.win.1=View Client for Windows 64 bit Client users
```

- 7 Starten Sie den VMware View-Verbindungsserver-Dienst neu.

Wenn Endbenutzer den View-Verbindungsserver öffnen, sehen sie Links mit dem von Ihnen angegebenen Text. Die Links verweisen auf die von Ihnen angegebenen Stellen.

Unbeaufsichtigte Installation von View Client

Sie können eine unbeaufsichtigte Installation von View Client durchführen, indem Sie den Namen der Installationsdatei sowie die gewünschten Installationsoptionen an der Befehlszeile eingeben. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Festlegen von Gruppenrichtlinien zum Zulassen einer unbeaufsichtigten Installation von View Client with Local Mode

Bevor Sie eine unbeaufsichtigte Installation von View Client with Local Mode ausführen können, müssen Sie Microsoft Windows-Gruppenrichtlinien konfigurieren, um eine Installation mit erhöhten Rechten zuzulassen.

Zur unbeaufsichtigten Installation von View Client ist das Festlegen dieser Gruppenrichtlinien nicht erforderlich. Diese Richtlinien werden nur für View Client with Local Mode benötigt.

Sie müssen Windows Installer-Gruppenrichtlinien für Computer und Benutzer auf dem Clientcomputer festlegen.

Voraussetzungen

Stellen Sie sicher, dass Sie auf dem Windows-Clientcomputer, auf dem Sie View Client with Local Mode installieren möchten, über Administratorberechtigungen verfügen.

Vorgehensweise

- 1 Melden Sie sich am Clientcomputer an und klicken Sie auf **[Start (Starten)] > [Run (Ausführen)]** .
- 2 Geben Sie `gpedit.msc` ein und klicken Sie auf **[OK]** .

- 3 Klicken Sie im Gruppenrichtlinienobjekt-Editor auf **[Local Computer Policy (Richtlinie für 'Lokaler Computer')] > [Computer Configuration (Computerkonfiguration)]** .
- 4 Erweitern Sie **[Administrative Templates (Administrative Vorlagen)]** und **[Windows Components (Windows-Komponenten)]** . Öffnen Sie dann den Ordner **[Windows Installer]** und doppelklicken Sie auf **[Always install with elevated privileges (Immer mit erhöhten Rechten installieren)]** .
- 5 Klicken Sie im Fenster **[Always Install with Elevated Privileges Properties (Eigenschaften von 'Immer mit erhöhten Rechten installieren')]** auf **[Enabled (Aktiviert)]** und anschließend auf **[OK]** .
- 6 Klicken Sie im linken Fensterbereich auf **[User Configuration (Benutzerkonfiguration)]** .
- 7 Erweitern Sie **[Administrative Templates (Administrative Vorlagen)]** und **[Windows Components (Windows-Komponenten)]** . Öffnen Sie dann den Ordner **[Windows Installer]** und doppelklicken Sie auf **[Always install with elevated privileges (Immer mit erhöhten Rechten installieren)]** .
- 8 Klicken Sie im Fenster **[Always Install with Elevated Privileges Properties (Eigenschaften von 'Immer mit erhöhten Rechten installieren')]** auf **[Enabled (Aktiviert)]** und anschließend auf **[OK]** .

Weiter

Führen Sie eine unbeaufsichtigte Installation von View Client with Local Mode aus.

Unbeaufsichtigte Installation von View Client

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, View Client oder View Client with Local Mode auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe [„Systemanforderungen für Windows-Clients“](#), auf Seite 7.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Voraussetzungen für den lokalen Modus:
 - Stellen Sie sicher, dass die für die unbeaufsichtigte Installation erforderlichen Windows Installer-Gruppenrichtlinien auf dem Clientcomputer konfiguriert sind. Siehe [„Festlegen von Gruppenrichtlinien zum Zulassen einer unbeaufsichtigten Installation von View Client with Local Mode“](#), auf Seite 21.
 - Stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst.
 - Stellen Sie sicher, dass keines der folgenden Produkte installiert ist: VMware Horizon View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Bestimmen Sie, ob die Funktion verwendet werden soll, mit der Endbenutzer sich bei View Client und ihrem virtuellen Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View-Verbindungsserver-Instanz und schließlich an den virtuellen Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe [„Microsoft Windows Installer-Befehlszeilenoptionen“](#), auf Seite 25.
- Machen Sie sich mit den verfügbaren MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client vertraut. Siehe [„Eigenschaften für die unbeaufsichtigte Installation von View Client“](#), auf Seite 23.

- Legen Sie fest, ob Sie Endbenutzern von ihren virtuellen Desktops aus den Zugriff auf lokal angeschlossene USB-Geräte gestatten möchten. Falls nicht, legen Sie über die MSI-Eigenschaft ADDLOCAL die Liste der relevanten Funktionen fest und lassen Sie die USB-Funktion aus. Weitere Informationen finden Sie unter „Eigenschaften für die unbeaufsichtigte Installation von View Client“, auf Seite 23.
- Wenn Sie nicht möchten, dass die Endbenutzer den vollqualifizierten Domänennamen (FQDN) der View-Verbindungsserver-Instanz eingeben müssen, die ihre virtuelle Maschine hostet, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Vorgehensweise

- 1 Laden Sie die View Client-Installationsdatei von der VMware-Produktseite unter <http://www.vmware.com/de/products/> auf das Clientsystem herunter.

Wählen Sie die entsprechende Installationsdatei aus, wobei *xxxxxx* die Build-Nummer und *y.y.y* die Versionsnummer ist.

Option	Aufgabe
View Client auf 64-Bit-Betriebssystemen	Wählen Sie die Datei <code>VMware-viewclient-x86_64-y.y.y-xxxxxx.exe</code> für View Client. Wählen Sie die Datei <code>VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe</code> für View Client mit lokalem Modus.
View Client auf 32-Bit-Betriebssystemen	Wählen Sie <code>VMware-viewclient-y.y.y-xxxxxx.exe</code> für View Client. Wählen Sie <code>VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe</code> für View Client mit lokalem Modus.

- 2 Öffnen Sie auf dem Windows-Clientcomputer eine Eingabeaufforderung.
- 3 Geben Sie den Installationsbefehl in einer Zeile ein.

Im folgenden Beispiel wird View Client mit SSO (Single Sign-On) und USB-Umleitung installiert. Für die View Client-Benutzer wird eine standardmäßige View-Verbindungsserver-Instanz konfiguriert: `VMware-viewclient-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,TSSO,USB"`

In diesem Beispiel wird View Client with Local Mode installiert: `VMware-viewclientwithlocal-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"`

HINWEIS Die Funktion Core ist verbindlich.

Der VMware View Client-Dienst wird auf dem Windows-Clientcomputer installiert.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Anmeldung an einem View-Desktop“, auf Seite 39 oder „Installieren von View Client unter Verwendung von View Portal“, auf Seite 19.

Eigenschaften für die unbeaufsichtigte Installation von View Client

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation von View Client über die Befehlszeile ausführen. Sie müssen hierbei das Format `EIGENSCHAFT=Wert` einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

[Tabelle 2-1](#) zeigt die Eigenschaften für eine unbeaufsichtigte Installation von View Client, die Sie an der Befehlszeile verwenden können.

Tabelle 2-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Client-Software installiert wird. Beispiel: INSTALLDIR=""D:\abc\Mein Ordner"" Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen als gültigen Teil des Pfads interpretiert. Diese MSI-Eigenschaft ist optional.	%ProgramFiles %\VMware\VMware View\Client
VDM_SERVER	Der vollqualifizierte Domänenname (FQDN) der View-Verbindungsserver-Instanz, mit der View Client-Benutzer standardmäßig eine Verbindung herstellen. Wenn Sie diese Eigenschaft konfigurieren, müssen View Client-Benutzer diesen FQDN nicht angeben. Beispiel: VDM_SERVER=cs1.companydomain.com Diese MSI-Eigenschaft ist optional.	Kein
DESKTOP_SHORTCUT	Konfiguriert eine Desktop-Verknüpfung für View Client. Bei Verwendung des Werts 1 wird eine Verknüpfung erstellt. Bei Verwendung des Werts 0 wird keine Verknüpfung erstellt. Diese MSI-Eigenschaft ist optional.	1
QUICKLAUNCH_SHORTCUT	Konfiguriert ein Verknüpfungssymbol für View Client in der Schnellstartleiste. Bei Verwendung des Werts 1 wird eine Verknüpfung erstellt. Bei Verwendung des Werts 0 wird keine Verknüpfung erstellt. Diese MSI-Eigenschaft ist optional.	1
STARTMENU_SHORTCUT	Konfiguriert eine Verknüpfung für View Client im Startmenü. Bei Verwendung des Werts 1 wird eine Verknüpfung erstellt. Bei Verwendung des Werts 0 wird keine Verknüpfung erstellt. Diese MSI-Eigenschaft ist optional.	1

In einem Befehl für die unbeaufsichtigte Installation können Sie mit der MSI-Eigenschaft ADDLOCAL= Funktionen angeben, die das View Client-Installationsprogramm konfiguriert. Jede Funktion für die unbeaufsichtigte Installation entspricht einer Setup-Option, die Sie während einer interaktiven Installation auswählen können.

[Tabelle 2-2](#) zeigt die View Client-Funktionen, die Sie an der Befehlszeile angeben können, sowie die entsprechenden Optionen in einer interaktiven Installation.

Tabelle 2-2. Funktionen für die unbeaufsichtigte View Client-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setup-Option bei einer interaktiven Installation
Core Wenn Sie mithilfe der MSI-Eigenschaft ADDLOCAL= einzelne Funktionen angeben, müssen Sie Core einschließen. Bei Verwendung der Eigenschaft ADDLOCAL=ALL werden alle Funktionen für View Client und View Client with Local Mode, einschließlich Core, installiert.	– Bei einer interaktiven Installation werden die View Client-Hauptfunktionen standardmäßig installiert.
MVDI Verwenden Sie diese Funktion, wenn Sie View Client with Local Mode installieren und mit ADDLOCAL= einzelne Funktionen angeben. Bei Verwendung der Eigenschaft ADDLOCAL=ALL werden alle Funktionen für View Client with Local Mode, einschließlich MVDI, installiert.	– Wenn Sie View Client with Local Mode interaktiv installieren, werden die MVDI-Funktionen standardmäßig installiert. Wenn Sie View Client interaktiv installieren, stehen die MVDI-Funktionen nicht zur Verfügung.
ThinPrint	Virtueller Druck

Tabelle 2-2. Funktionen für die unbeaufsichtigte View Client-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation (Fortsetzung)

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setup-Option bei einer interaktiven Installation
TSSO	Einmalige Anmeldung (Single Sign-On, SSO)
USB	USB-Umleitung

Microsoft Windows Installer-Befehlszeilenoptionen

Zur unbeaufsichtigten Installation von View-Komponenten müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für View-Komponenten sind MSI-Programme und verwenden standardmäßige MSI-Funktionen. Sie können auch MSI-Befehlszeilenoptionen zum unbeaufsichtigten Deinstallieren von View-Komponenten verwenden.

Weitere Informationen zum Microsoft Windows Installer (MSI) finden Sie auf der Microsoft-Website. Informationen zu MSI-Befehlszeilenoptionen erhalten Sie, wenn Sie auf der Microsoft Developer Network (MSDN) Library-Website nach MSI-Befehlszeilenoptionen suchen. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Computer mit der View-Komponente eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation einer View-Komponente deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

[Tabelle 2-3](#) zeigt die Befehlszeilenoptionen, die das Bootstrap-Programm des Installationsprogramms steuern.

Tabelle 2-3. Befehlszeilenoptionen für das Bootstrap-Programm einer View-Komponente

Option	Beschreibung
<code>/s</code>	Deaktiviert den Bootstrap-Begrüßungsbildschirm und das Dialogfeld für das Extrahieren, sodass keine interaktiven Dialogfenster angezeigt werden. Beispiel: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code> Die Option <code>/s</code> ist erforderlich, um eine unbeaufsichtigte Installation auszuführen. In den Beispielen steht <code>xxxxxx</code> für die Build-Nummer und <code>y.y.y</code> für die Versionsnummer.
<code>/v" MSI-Befehlszeilenoptionen"</code>	Weist das Installationsprogramm an, die in doppelte Anführungszeichen eingeschlossene Zeichenfolge, die an der Befehlszeile eingegeben wurde, als MSI-Optionssatz auszuwerten. Sie müssen die Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Platzieren Sie ein doppeltes Anführungszeichen nach <code>/v</code> und am Ende der Befehlszeile. Beispiel: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"</code> Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten die View-Komponente in einem Pfad installieren, dessen Name Leerzeichen enthält. Beispiel: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder""</code> In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen. Die Option <code>/v" Befehlszeilenoptionen"</code> ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.

Sie steuern den verbleibenden Teil einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaften an das MSI-Installationsprogramm (`msiexec.exe`) übergeben. Das MSI-Installationsprogramm umfasst den Installationscode der View-Komponente. Der Installer verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für die View-Komponente spezifischen Setup-Optionen auszuwerten.

[Tabelle 2-4](#) zeigt die Befehlszeilenoptionen und MSI-Eigenschaftenwerte, die an das MSI-Installationsprogramm übergeben werden.

Tabelle 2-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
/qn	<p>Weist das MSI-Installationsprogramm an, keine Seiten des Installations-Assistenten anzuzeigen.</p> <p>Angenommen, Sie möchten View Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</code></p> <p>In den Beispielen steht <code>xxxxxx</code> für die Build-Nummer und <code>y.y.y</code> für die Versionsnummer. Alternativ können Sie die Option /qb verwenden, um die Assistentenseiten in einer nicht interaktiven, automatisierten Installation anzuzeigen. Im Verlauf der Installation werden die Assistentenseiten angezeigt, eine Eingabe ist jedoch nicht möglich.</p> <p>Die Option /qn oder /qb ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.</p>
INSTALLDIR	<p>Gibt einen alternativen Installationspfad für die View-Komponente an.</p> <p>Verwenden Sie das Format <code>INSTALLDIR=Pfad</code>, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie die View-Komponente im Standardpfad installieren möchten.</p> <p>Diese MSI-Eigenschaft ist optional.</p>
ADDLOCAL	<p>Legt die komponentenspezifischen Funktionen fest, die installiert werden sollen. In einer interaktiven Installation zeigt das View-Installationsprogramm Auswahloptionen für das benutzerdefinierte Setup an. Mithilfe der MSI-Eigenschaft ADDLOCAL können Sie diese Setup-Optionen an der Befehlszeile angeben.</p> <p>Um alle verfügbaren Optionen für ein benutzerdefiniertes Setup zu installieren, geben Sie <code>ADDLOCAL=ALL</code> ein.</p> <p>Beispiel: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></p> <p>Wenn Sie die MSI-Eigenschaft ADDLOCAL nicht verwenden, werden die standardmäßigen Setup-Optionen installiert.</p> <p>Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format <code>ADDLOCAL=Wert,Wert,Wert...</code></p> <p>Angenommen, Sie möchten View Agent mit den View Composer-Agent- und PCoIP-Funktionen in einem Gastbetriebssystem installieren: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP"</code></p> <p>HINWEIS Die Funktion Core ist in View Agent erforderlich.</p> <p>Diese MSI-Eigenschaft ist optional.</p>
REBOOT	<p>Sie können die Option <code>REBOOT=ReallySuppress</code> verwenden, um zuzulassen, dass Systemkonfigurationsaufgaben vor einem Neustart des Systems ausgeführt werden dürfen.</p> <p>Diese MSI-Eigenschaft ist optional.</p>
/l*v <i>Protokolldatei</i>	<p>Schreibt Protokollinformationen in die angegebene Protokolldatei. Hierbei ist eine ausführliche Ausgabe festgelegt.</p> <p>Beispiel: <code>/l*v ""%TEMP%\vmmsi.log""</code></p> <p>In diesem Beispiel wird eine ausführliche Protokolldatei ähnlich dem Protokoll generiert, das bei einer interaktiven Installation erstellt wird.</p> <p>Sie können mit dieser Option benutzerdefinierte Funktionen erfassen, die möglicherweise nur für Ihre Installation gelten. Sie können die protokollierten Informationen verwenden, um Installationsfunktionen in zukünftigen unbeaufsichtigten Installationen anzugeben.</p> <p>Die Option /l*v ist optional.</p>

Konfigurieren von View Client für die Endbenutzer

3

View Client bietet mehrere Konfigurationsmechanismen zur Vereinfachung der Anmeldung und Desktopauswahl und Verbesserung der Benutzererfahrung, jedoch auch zur Durchsetzung der Sicherheitsrichtlinien.

Dieses Kapitel behandelt die folgenden Themen:

- [„Verwenden von URIs zur Konfiguration von View Client“](#), auf Seite 27
- [„Konfigurieren der Zertifikatsprüfungen für Endbenutzer“](#), auf Seite 32
- [„Ausführen von View Client über die Befehlszeile“](#), auf Seite 34

Verwenden von URIs zur Konfiguration von View Client

Unter Verwendung sogenannter Uniform Resource Identifiers (URIs) können Sie eine Webseite oder E-Mail mit verschiedenen Verknüpfungen erstellen, auf die die Endbenutzer zum Start von View Client, zur Verbindung mit dem View-Verbindungsserver oder zum Start eines bestimmten Desktops mit bestimmten Konfigurationsoptionen klicken.

Sie können die Anmeldung am View-Desktop durch Erstellen von Web- oder E-Mail-Verknüpfungen für die Endbenutzer deutlich vereinfachen. Diese Verknüpfungen werden durch die Generierung von URIs erstellt, die einige oder alle der folgenden Informationen bereitstellen, sodass die Endbenutzer diese nicht angeben müssen:

- Adresse des View-Verbindungsservers
- Portnummer für den View-Verbindungsserver
- Active Directory-Benutzername
- RADIUS- oder RSA SecurID-Benutzername, falls dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Desktopanzeigename
- Fenstergröße
- Desktopaktionen, darunter „Zurücksetzen“, „Abmelden“ und „Rollback ausführen“
- Anzeigeprotokoll
- Optionen zur Umleitung von USB-Geräten

WICHTIG Um diese Funktion nutzen zu können, müssen Sie über View Client 5.1 oder höher verfügen.

Verwenden Sie zur Generierung eines URI das URI-Schema `vmware-view` mit View Client-spezifischen Pfad- und Abfrageteilen.

HINWEIS Sie können URIs nur zum Start von View Client verwenden, wenn View Client bereits auf den Clientcomputern der Endbenutzer installiert ist.

Syntax für die Erstellung von `vmware-view`-URIs

Die Syntax umfasst das URI-Schema `vmware-view`, einen Pfadauszug zur Angabe des Desktops sowie optional eine Abfrage zur Angabe der Desktopaktionen oder Konfigurationsoptionen.

Spezifikationen für VMware View-URIs

Verwenden Sie zum Generieren von URIs für den Start von View Client die folgende Syntax:

```
vmware-view://[authority-part][/path-part][?query-part]
```

Das einzig erforderliche Element ist das URI-Schema `vmware-view`. Für einige Versionen bestimmter Client-betriebssysteme muss für den Namen des Schemas die Groß- und Kleinschreibung beachtet werden. Verwenden Sie daher `vmware-view`.

WICHTIG In allen Teilen müssen Nicht-ASCII-Zeichen vorab gemäß UTF-8 codiert werden [STD63]. Anschließend muss jedes Oktett der entsprechenden UTF-8-Sequenz als Prozentwert codiert werden, damit es als URI-Zeichen dargestellt werden kann.

Informationen zur Codierung von ASCII-Zeichen finden Sie in der URL-Codierungsreferenz unter http://www.w3schools.com/tags/ref_urlencode.asp.

authority-part

Gibt die Serveradresse und optional einen Benutzernamen, eine nicht standardmäßige Portnummer oder beides an. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax:

```
user1@server-address
```

Beachten Sie dabei, dass Sie keine UPN-Adresse angeben können. Hierzu zählt auch die Domäne. Zur Angabe des Domänennamens können Sie den Abfrageteil `domainName` im URI verwenden.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

```
server-address:port-number
```

path-part

Gibt den Desktop an. Verwenden Sie den Anzeigenamen des Desktops. Weist der Anzeigename ein Leerzeichen auf, müssen Sie den Codierungsmechanismus `%20` verwenden, um das Leerzeichen darzustellen.

query-part

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführen Desktopaktionen an. Für die Abfragen muss die Groß- und Kleinschreibung nicht beachtet werden. Verwenden Sie für den Einsatz mehrerer Abfragen das kaufmännische Und-Zeichen (&) zwischen den Abfragen. Sollten die Abfragen miteinander in Konflikt stehen, wird die letzte Abfrage in der Liste verwendet. Verwenden Sie die folgende Syntax:

```
query1=value1[&query2=value2. . .]
```

Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für diesen View Client-Typ unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktopclients oder mobile Clients, finden Sie für jede Art Clientsystem weitere Anweisungen im Handbuch *Verwendung von VMware Horizon View Client*.

action

Tabelle 3-1. Werte, die mit der Abfrage „action“ verwendet werden können

Wert	Beschreibung
browse	Zeigt eine Liste der verfügbaren, auf dem angegebenen Server gehosteten Desktops an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop angeben.
start-session	Startet den angegebenen Desktop. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktopname angegeben wird, ist <code>start-session</code> die Standardaktion.
zurücksetzen	Führt den angegebenen Desktop herunter und startet ihn neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines View-Desktops kommt dem Betätigen der Schaltfläche „Zurücksetzen“ auf einem physischen PC gleich.
logoff	Meldet den Benutzer vom Gastbetriebssystem auf dem View-Desktop ab.
rollback	Verwirft die Änderungen, die am angegebenen Desktop vorgenommen wurden, während dieser zur Verwendung im lokalen Modus auf einem Windows-PC oder Laptop ausgecheckt wurde.

connectUSBOnInsert

Verbindet ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten Desktop. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf `start-session` setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **Yes** und **No**. Ein Beispiel für die Syntax ist etwa `connectUSBOnInsert=yes`.

connectUSBOnStartup

Leitet alle aktuell mit dem Clientsystem verbundenen USB-Geräte an den Desktop um. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf `start-session` setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **Yes** und **No**. Ein Beispiel für die Syntax ist etwa `connectUSBOnStartup=yes`.

desktopLayout

Legt die Größe des Fensters für die Anzeige des View-Desktops fest. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf `start-session` setzen oder ohne die Abfrage `action` arbeiten.

Tabelle 3-2. Gültige Werte für desktopLayout-Abfrage

Wert	Beschreibung
fullscreen	Vollbild auf einem Monitor. Hierbei handelt es sich um die Standardeinstellung.
multimonitor	Vollbild auf allen Monitoren.
windowLarge	Großes Fenster.

Tabelle 3-2. Gültige Werte für desktopLayout-Abfrage (Fortsetzung)

Wert	Beschreibung
windowSmall	Kleines Fenster.
WxH	Benutzerdefinierte Auflösung, bei der Sie die Breite mal Höhe in Pixel angeben. Ein Beispiel für die Syntax ist etwa desktopLayout=1280x800 .

desktopProtocol	Gültige Werte sind RDP und PCoIP . Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax desktopProtocol=PCoIP .
domainName	Die Domäne, die mit dem Benutzer verknüpft ist, der sich mit dem View-Desktop verbindet.
tokenUserName	Gibt den RSA- oder RADIUS-Benutzernamen an. Verwenden Sie diese Abfrage nur, wenn der RSA- oder RADIUS-Benutzername nicht mit dem Active Directory-Benutzernamen identisch ist. Wenn Sie diese Abfrage nicht angeben und die RSA- oder RADIUS-Authentifizierung erforderlich ist, wird der Windows-Benutzername verwendet. Die Syntax lautet tokenUserName=name .
unattended	Erstellt eine Serververbindung im Kioskmodus. Geben Sie keine Benutzerinformationen an, wenn Sie diese Abfrage verwenden.

Beispiele für vmware-view-URIs

Sie können Hypertext-Links oder Schaltflächen mit dem URI-Schema `vmware-view` erstellen und diese Links in E-Mails oder auf einer Webseite einbinden. Ihre Endbenutzer können dann auf diese Links klicken, um beispielsweise einen bestimmten View-Desktop mit den von Ihnen angegebenen Startoptionen zu starten.

URI-Syntaxbeispiele

Nach jedem URI-Beispiel finden Sie eine Beschreibung, was der Endbenutzer nach Anklicken des URI-Links sieht.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **[Primary Desktop]** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

HINWEIS Die Standardvorgaben für das Anzeigeprotokoll und die Fenstergröße werden verwendet. Das Standardanzeigeprotokoll ist PCoIP. Die Standardfenstergröße ist Vollbild.

2 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Dieser URI hat die gleiche Wirkung wie im vorherigen Beispiel, außer dass er den nicht standardmäßigen Port 7555 für den View-Verbindungsserver verwendet. (Der standardmäßige Port lautet 443.) Da eine Desktop-ID bereitgestellt wird, wird der Desktop gestartet, obwohl die Aktion `start-session` nicht im URI enthalten ist.

3 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCoIP`

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird das Textfeld **[Benutzername]** mit dem Namen **[fred]** gefüllt. Der Benutzer muss den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **[Finance Desktop]** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet. Die Verbindung nutzt das PCoIP-Anzeigeprotokoll.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird das Textfeld **[Benutzername]** mit dem Namen **[fred]** und das Textfeld **[Domäne]** mit **[mycompany]** gefüllt. Der Benutzer muss das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **[Finance Desktop]** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

5 `vmware-view://view.mycompany.com/`

View Client wird gestartet und der Benutzer wird zur Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` geleitet.

6 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt View Client ein Dialogfeld, in dem der Benutzer aufgefordert wird, das Zurücksetzen für „Primary Desktop“ zu bestätigen. Nach dem Zurücksetzen kann der Benutzer je nach View Client-Typ eine Meldung sehen, die über den Erfolg des Zurücksetzens informiert.

HINWEIS Diese Aktion ist nur verfügbar, wenn die Funktion vom View-Administrator für den Endbenutzer aktiviert wurde.

7 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSB0nStartup=true`

Dieser URI hat die gleiche Wirkung wie das erste Beispiel, und alle an das Clientsystem angeschlossenen USB-Geräte werden an den neuen View-Desktop umgeleitet.

8 `vmware-view://`

View Client wird gestartet und der Benutzer wird zu der Seite geleitet, auf der die Adresse einer View-Verbindungsserver-Instanz eingegeben werden kann.

Beispiel für HTML-Code

Sie können URIs verwenden, um Hypertext-Links und Schaltflächen zu erstellen, die in E-Mails oder auf Webseiten eingebunden werden können. Die folgenden Beispiele veranschaulichen, wie Sie den URI aus dem ersten Beispiel verwenden, um einen Hypertext-Link mit dem Text **[Test Link]** besagt und eine Schaltfläche mit dem Text **[TestButton]** zu codieren.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Text
Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Konfigurieren der Zertifikatsprüfungen für Endbenutzer

Administratoren können den Zertifikatüberprüfungsmodus so konfigurieren, dass beispielsweise immer die vollständige Überprüfung durchgeführt wird.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen View-Verbindungsserver und View Client durchgeführt. Die Administratoren können den Überprüfungsmodus so konfigurieren, dass eine der folgenden Strategien verwendet wird:

- Die Endbenutzer wählen selbst den Überprüfungsmodus. In der restlichen Liste werden die drei Überprüfungsmodi beschrieben.
- (Keine Überprüfung) Es werden keine Zertifikatsprüfungen durchgeführt.
- (Warnen) Die Endbenutzer werden gewarnt, wenn der Server ein selbstsigniertes Zertifikat vorlegt. Die Benutzer können dann selbst entscheiden, ob sie diesen Verbindungstyp zulassen.
- (Volle Sicherheit) Es wird eine vollständige Überprüfung durchgeführt. Die Verbindungen, für die diese Prüfung nicht erfolgreich verläuft, werden abgelehnt.

Einzelheiten zu den verschiedenen Arten der durchgeführten Überprüfungen finden Sie unter [„Zertifikatsprüfungsmodi für View Client“](#), auf Seite 32.

Verwenden Sie die ADM-Vorlagendatei zur Client-Konfiguration, um den Überprüfungsmodus einzustellen. Die ADM-Vorlagendateien für View-Komponenten sind im Verzeichnis *Installationsverzeichnis\VMware\VMware View\Server\Extras\GroupPolicyFiles* auf Ihrem View-Verbindungsserver-Host installiert. Informationen zum Verwenden dieser Vorlagen zum Festlegen der GPO-Einstellungen finden Sie im Dokument *Verwaltung von VMware Horizon View*.

Wenn Sie diese Einstellung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatsprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zu einem der folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren:

- 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Verwenden Sie die folgenden Werte im Registrierungsschlüssel:

- `0` implementiert Server-Identitätszertifikate nicht überprüfen.
- `1` implementiert Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben.
- `2` implementiert Nie mit nicht vertrauenswürdigen Servern verbinden.

Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschleuseinstellung.

Zertifikatsprüfungsmodi für View Client

Administratoren und manchmal auch Endbenutzer können über eine Konfiguration festlegen, ob Client-Verbindungen abgelehnt werden sollen, wenn bei Zertifikatsüberprüfungen Fehler auftreten.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen View-Verbindungsserver und View Client durchgeführt. Die Zertifikatsüberprüfung umfasst die folgenden Checks:

- Wurde das Zertifikat widerrufen?
- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?

- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?
- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich View Client auf einen Server mit einem Zertifikat umleitet, das nicht mit dem in View Client eingegebenen Hostnamen übereinstimmt. Ein weiterer möglicher Grund für eine fehlende Übereinstimmung ist die Eingabe einer IP-Adresse statt eines Hostnamens im Client.
- Ist das Zertifikat von einer unbekanntenen oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

Um diese Prüfung zu bestehen, muss die Vertrauenskette des Zertifikats bis in den Zertifikatspeicher des Geräts zurückverfolgt werden können.

HINWEIS Anweisungen zur Verbreitung eines selbstsignierten Stammzertifikats an alle Windows-Clientsysteme in einer Domäne finden Sie unter dem Thema „Stammzertifikat zu den vertrauenswürdigen Zertifizierungsstellen hinzufügen“ im Dokument *Installation von VMware Horizon View*.

Wenn Ihr Administrator Ihnen die Verwendung von View Client bei der Anmeldung an einem Desktop ermöglicht hat, können Sie auf **[SSL konfigurieren]** klicken und den Zertifikatsprüfungsmodus einstellen. Sie haben drei Auswahlmöglichkeiten:

- **[Nie mit nicht vertrauenswürdigen Servern verbinden]** . Sollte eine beliebige der Zertifikatsprüfungen fehlschlagen, kann der Client keine Verbindung mit dem Server herstellen. Die nicht bestandenen Prüfungen werden in einer Fehlermeldung aufgelistet.
- **[Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben]** . Wenn eine Zertifikatsprüfung fehlschlägt, weil der Server ein selbstsigniertes Zertifikat verwendet, können Sie auf **[Weiter]** klicken, um die Warnung zu ignorieren. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Namen des View-Verbindungsservers übereinstimmen, den Sie in View Client eingegeben haben.

Möglicherweise erhalten Sie auch eine Warnung, wenn das Zertifikat abgelaufen ist.

- **[Server-Identitätszertifikate nicht überprüfen]** . Bei Aktivierung dieser Option führt View keine Zertifikatsüberprüfung durch.

Ist der Zertifikatsprüfungsmodus auf **[Warnen]** gesetzt, können Sie immer noch Verbindung mit einer View-Verbindungsserver-Instanz herstellen, die ein selbstsigniertes Zertifikat verwendet.

Installiert ein Administrator später ein Sicherheitszertifikat von einer vertrauenswürdigen Zertifikatsautorität, sodass alle Zertifikatsüberprüfungen bei der Verbindungsherstellung bestanden werden, wird diese vertrauenswürdige Verbindung für diesen speziellen Server vorgemerkt. Legt dieser Server in Zukunft wieder ein selbstsigniertes Zertifikat vor, schlägt die Verbindung fehl. Nachdem ein bestimmter Server ein vollständig überprüfbares Zertifikat vorgelegt hat, muss er dies auch in Zukunft immer so handhaben.

WICHTIG Wenn Sie einen ausgecheckten View-Desktop auf Ihrem lokalen System verwenden und mit dem Firmennetzwerk verbunden sind, wird die Zertifikatsüberprüfung wie bei der Anmeldung an Ihrem View-Desktop beschrieben vorgenommen. Wenn Sie nicht mit dem Firmennetzwerk verbunden sind, kann auch keine Zertifikatsüberprüfung vorgenommen werden. Der View-Desktop wird dann so ausgeführt, als ob die Zertifikatsüberprüfung erfolgreich bestanden worden wäre.

Ausführen von View Client über die Befehlszeile

View Client für Windows kann über die Befehlszeile oder über Skripts ausgeführt werden. Dies kann bei Implementierung einer Kiosk-basierten Anwendung sinnvoll sein, über die Endbenutzer auf Desktop-Anwendungen zugreifen können.

Verwenden Sie den Befehl `wswc`, um View Client für Windows über die Befehlszeile auszuführen. Der Befehl umfasst Optionen, mit denen sich das Verhalten von View Client ändern lässt.

Verwenden von View Client-Befehlen

Die Syntax des Befehls `wswc` bestimmt, wie View Client ausgeführt wird.

Verwenden Sie den Befehl `wswc` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
wswc [command_line_option [argument]] ...
```

Der Pfad zur ausführbaren Datei des Befehls `wswc` lautet standardmäßig `C:\Program Files\VMware\VMware View\Client\bin`. Zur Vereinfachung fügen Sie diesen Pfad zu Ihrer Umgebungsvariable `PATH` hinzu.

[Tabelle 3-3](#) zeigt die Befehlszeilenoptionen, die mit dem Befehl `wswc` verwendet werden können.

Tabelle 3-3. View Client-Befehlszeilenoptionen

Option	Beschreibung								
<code>/?</code>	Zeigt die Liste der Befehlsoptionen an.								
<code>-checkin</code>	(Nur lokaler Desktop) Checkt den angegebenen Desktop ein und entspermt die Online-Version. Diese Option erfordert, dass Sie auch die Option <code>-desktopName</code> festlegen.								
<code>-checkout</code>	(Nur lokaler Desktop) Checkt den angegebenen Desktop aus und sperrt die Online-Version. Diese Option erfordert, dass Sie auch die Option <code>-desktopName</code> festlegen.								
<code>-confirmRollback</code>	(Nur lokaler Desktop) Unterdrückt das Bestätigungsdialogfeld, das bei Verwendung der Option <code>-rollback</code> angezeigt wird. Um das Rollback im nicht interaktiven Modus auszuführen, geben Sie auch die Option <code>-nonInteractive</code> an.								
<code>-connectUSB0nStartup</code>	Wenn hier <code>true</code> angegeben ist, werden alle gegenwärtig mit dem Host verbundenen USB-Geräte an den Desktop umgeleitet. Diese Option wird bei Angabe der Option <code>-unattended</code> implizit festgelegt. Die Standardeinstellung ist <code>false</code> .								
<code>-connectUSB0nInsert</code>	Wenn hier <code>true</code> angegeben ist, wird ein USB-Gerät mit dem Desktop im Vordergrund verbunden, wenn Sie das Gerät anschließen. Diese Option wird bei Angabe der Option <code>-unattended</code> implizit festgelegt. Die Standardeinstellung ist <code>false</code> .								
<code>-desktopLayout</code> <i>Fenstergröße</i>	Gibt an, wie das Desktop-Fenster angezeigt wird: <table border="0" style="margin-left: 20px;"> <tr> <td>fullscreen</td> <td>Anzeige im Vollbildmodus</td> </tr> <tr> <td>multimonitor</td> <td>Anzeige auf mehreren Monitoren</td> </tr> <tr> <td>windowLarge</td> <td>Großes Fenster</td> </tr> <tr> <td>windowSmall</td> <td>Kleines Fenster</td> </tr> </table>	fullscreen	Anzeige im Vollbildmodus	multimonitor	Anzeige auf mehreren Monitoren	windowLarge	Großes Fenster	windowSmall	Kleines Fenster
fullscreen	Anzeige im Vollbildmodus								
multimonitor	Anzeige auf mehreren Monitoren								
windowLarge	Großes Fenster								
windowSmall	Kleines Fenster								
<code>-desktopName</code> <i>Desktop-Name</i>	Gibt den Namen des Desktops an, der im Dialogfeld zur Desktop-Auswahl angezeigt wird. Dies ist der Anzeigename des Desktops im Dialogfeld zur Desktop-Auswahl.								
<code>-desktopProtocol</code> <i>Protokoll</i>	Gibt den Namen des zu verwendenden Protokolls an, der im Dialogfeld zur Desktop-Auswahl angezeigt wird. Das Protokoll kann PCOIP oder RDP sein.								

Tabelle 3-3. View Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
<code>-domainName</code> <i>Domänenname</i>	Gibt die Domäne an, die der Endbenutzer zur Anmeldung an View Client verwendet.
<code>-file</code> <i>Dateipfad</i>	Gibt den Pfad einer Konfigurationsdatei mit zusätzlichen Befehlsoptionen und -argumenten an. Siehe „ View Client-Konfigurationsdatei “, auf Seite 36.
<code>-languageId</code> <i>Gebietsschema-ID</i>	Bietet Lokalisierungsunterstützung für verschiedene Sprachen in View Client. Wenn eine Ressourcenbibliothek verfügbar ist, geben Sie die zu verwendende Gebietsschema-ID (Locale ID, LCID) an. Für Englisch (USA) geben Sie 0x409 ein.
<code>-localDirectory</code> <i>Verzeichnispfad</i>	(Nur lokaler Desktop) Gibt an, welches Verzeichnis auf dem lokalen System zum Herunterladen des lokalen Desktops verwendet werden soll. Die heruntergeladenen lokalen Dateien werden direkt im angegebenen Verzeichnis gespeichert. Wird im Gegensatz dazu das lokale Verzeichnis in View Client ausgewählt, wird ein Unterordner mit dem Desktop-Namen im ausgewählten Verzeichnis erstellt und die lokalen Dateien werden in diesem Unterordner gespeichert. Diese Option erfordert, dass Sie auch die Option <code>-desktopName</code> festlegen.
<code>-logInAsCurrentUser</code>	Wenn hier <code>true</code> angegeben ist, werden die Anmeldeinformationen des Endbenutzers, die dieser zur Anmeldung am Clientssystem eingegeben hat, an die View-Verbindungsserver-Instanz und schließlich an den View-Desktop übergeben. Die Standardeinstellung ist <code>false</code> .
<code>-nonInteractive</code>	Unterdrückt Fehlermeldungen beim Starten von View Client über ein Skript. Diese Option wird bei Angabe der Option <code>-unattended</code> implizit festgelegt.
<code>-password</code> <i>Kenntwort</i>	Gibt das Kennwort an, das der Endbenutzer zur Anmeldung an View Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn das Kennwort automatisch generiert wird.
<code>-printEnvironmentInfo</code>	Zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.
<code>-rollback</code>	(Nur lokaler Desktop) Entsperrt die Online-Version eines ausgecheckten Desktops und verwirft die lokale Sitzung. Diese Option erfordert, dass Sie auch die Option <code>-desktopName</code> festlegen. Um das Rollback im nicht interaktiven Modus auszuführen, geben Sie auch die Optionen <code>-nonInteractive</code> und <code>-confirmRollback</code> an.
<code>-serverURL</code> <i>Verbindungsserver</i>	Gibt die URL, die IP-Adresse oder den FQDN der View-Verbindungsserver-Instanz an.
<code>-smartCardPIN</code> <i>PIN</i>	Gibt die PIN an, wenn ein Endbenutzer eine Smartcard zur Anmeldung einführt.
<code>-standalone</code>	Startet eine zweite Instanz von View Client, die mit demselben oder einem anderen View-Verbindungsserver über PCoIP verbunden werden kann. Für mehrere Desktopverbindungen zu demselben Server wird keine sichere Tunnelverbindung unterstützt. Für mehrere Desktopverbindungen zu verschiedenen Servern wird die sichere Tunnelverbindung unterstützt. HINWEIS Die zweite Desktopverbindung hat möglicherweise keinen Zugriff auf die lokale Hardware, wie USB-Geräte, Smartcards, Drucker und mehrere Monitore.

Tabelle 3-3. View Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
<code>-unattended</code>	<p>Führt View Client im nicht interaktiven Modus aus, der sich für Clients im Kiosk-Modus eignet. Zusätzlich müssen folgende Informationen angegeben werden:</p> <ul style="list-style-type: none"> ■ Der Kontoname des Clients, wenn dieser nicht über die MAC-Adresse des Clientgeräts generiert wurde. Der Name muss mit der Zeichenfolge „custom-“ oder einem alternativen Präfix beginnen, das Sie in ADAM konfiguriert haben. ■ Das Kennwort des Clients, wenn dieses nicht automatisch beim Einrichten des Clientkontos generiert wurde. <p>Über die Option <code>-unattended</code> werden die Optionen <code>-nonInteractive</code>, <code>-connectUSBOnStartup</code> und <code>-connectUSBOnInsert</code> implizit festgelegt.</p>
<code>-userName</code> <i>Benutzername</i>	Gibt den Kontonamen an, den der Endbenutzer zur Anmeldung an View Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn der Kontoname über die MAC-Adresse des Clientgeräts generiert wird.

Über die Befehlszeile oder in der Konfigurationsdatei angegebene Optionen haben Vorrang vor globalen Systemrichtlinien, die wiederum Benutzerrichtlinien außer Kraft setzen.

Mit Ausnahme von `-checkin`, `-checkout`, `-file`, `-languageId`, `-localDirectory`, `-printEnvironmentInfo`, `-rollback`, `-smartCardPIN` und `-unattended` können alle Optionen über Active Directory-Gruppenrichtlinien angegeben werden.

View Client-Konfigurationsdatei

Die Befehlszeilenoptionen für View Client können einer Konfigurationsdatei entnommen werden.

Der Pfad zur Konfigurationsdatei kann als Argument der Option `-f` des `wswc`-Befehls angegeben werden. Die Datei muss als Unicode- (UTF-16) oder ASCII-Textdatei vorliegen.

Beispiel: Beispiel einer Konfigurationsdatei für eine nicht interaktive Anwendung

Das folgende Beispiel zeigt den Inhalt einer Konfigurationsdatei für eine nicht interaktive Anwendung.

```
-serverURL https://view.yourcompany.com
-userName autouser
-password auto123
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

Beispiel: Beispiel einer Konfigurationsdatei für einen Client im Kiosk-Modus

Das folgende Beispiel zeigt einen Client im Kiosk-Modus, dessen Kontoname auf seiner MAC-Adresse basiert. Der Client verfügt über ein automatisch generiertes Kennwort.

```
-serverURL 145.124.24.100
-unattended
```

View Client-Registrierungseinstellungen

Sie können Standardeinstellungen für View Client in der Windows-Registrierung definieren, sodass diese nicht über die Befehlszeile angegeben werden müssen.

[Tabelle 3-4](#) zeigt die Registrierungseinstellungen für View Client. Diese Einstellungen befinden sich in der Registrierung unter HKLM\Software\VMware, Inc.\VMware VDM\Client\.

Richtlinieneinträge haben Vorrang vor Registrierungseinstellungen und Befehlszeileneinstellungen haben Vorrang vor Richtlinieneinstellungen.

Tabelle 3-4. View Client-Registrierungseinstellungen

Registrierungseinstellung	Beschreibung
DomainName	Gibt den standardmäßigen Domännennamen an.
EnableShade	Gibt an, ob die Menüleiste (Schatten) im oberen Bereich des View Client-Fensters aktiviert ist. Die Menüleiste ist standardmäßig aktiviert, ausgenommen für Clients im Kiosk-Modus. Bei Festlegung von [false] wird die Menüleiste deaktiviert.
Password	Gibt das standardmäßige Kennwort an.
ServerURL	Gibt die standardmäßige View-Verbindungsserver-Instanz über die URL, die IP-Adresse oder den FQDN an.
UserName	Gibt den standardmäßigen Benutzernamen an.

View Client-Exitcodes

Die Befehlszeilenschnittstelle für View Client kann Exitcodes mit Informationen zu Fehlern zurückgeben, die von View Client ermittelt werden.

[Tabelle 3-5](#) zeigt die Exitcodes, die vom Befehl wswc zurückgegeben werden können.

Tabelle 3-5. View Client-Exitcodes

Exitcode	Beschreibung
-1	Schwerwiegender Fehler im Kiosk-Modus.
0	Vorgang erfolgreich.
1	Verbindung fehlgeschlagen.
2	Anmeldung fehlgeschlagen.
3	Desktop konnte nicht gestartet werden.
4	RDP konnte nicht gestartet werden.
5	RDP-Vorgang fehlgeschlagen.
6	Tunnelverbindung unterbrochen.
7	Fehler beim Übertragen des lokalen Desktops.
8	Fehler beim Einchecken des lokalen Desktops.
9	Fehler beim Auschecken des lokalen Desktops.
10	Fehler beim Rollback des lokalen Desktops.
11	Unbekanntes Ergebnis während der Authentifizierung.
12	Authentifizierungsfehler.
13	Anforderung zur Verwendung einer unbekanntes Authentifizierungsmethode empfangen.
14	Ungültige Serverantwort.

Tabelle 3-5. View Client-Exitcodes (Fortsetzung)

Exitcode	Beschreibung
15	Desktop wurde getrennt.
16	Tunnel wurde getrennt.
17	Für zukünftige Entwicklung reserviert.
18	Für zukünftige Entwicklung reserviert.
19	Nicht unterstützter Kiosk-Vorgang.
20	RMKS-Verbindungsfehler (Remote Mouse, Keyboard, or Screen).
21	PIN-Fehler.
22	Keine Übereinstimmung für PIN.
23	Keine Übereinstimmung für Kennwort.
24	View-Verbindungsserver-Fehler.
25	Desktop war nicht verfügbar.

Verwaltung der Serververbindungen und Desktops

4

Verwenden Sie View Client, um eine Verbindung zu View-Verbindungsserver oder einem Sicherheitsserver herzustellen und sich an einem View-Desktop an- bzw. von diesem abzumelden. Für die Problembeseitigung können Sie den Ihnen zugewiesenen View-Desktop zurücksetzen und für einen ausgecheckten Desktop ein Rollback durchführen.

Je nachdem, wie der Administrator die Richtlinien für View-Desktops festlegt, können die Endbenutzer viele verschiedene Vorgänge auf ihren Desktops durchführen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Anmeldung an einem View-Desktop“](#), auf Seite 39
- [„Wechseln zwischen Desktops“](#), auf Seite 42
- [„Abmelden oder Trennen von Desktops“](#), auf Seite 42

Anmeldung an einem View-Desktop

Bevor Sie den Endbenutzern Zugriff auf ihre virtuellen Desktops gewähren, sollten Sie sicherstellen, dass Sie sich von einem Clientgerät aus an einem virtuellen Desktop anmelden können. Sie können View Client über das Menü **[Start]** oder eine Desktop-Verknüpfung auf dem Clientsystem starten.

In Umgebungen, in denen eine Netzwerkverbindung verfügbar ist, wird die Benutzersitzung von View-Verbindungsserver authentifiziert.

Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Benutzernamen und das Kennwort, den RSA SecurID-Benutzernamen und das Kennwort, den RADIUS-Authentifizierungsbennennamen oder -Passcode oder die Smartcard-PIN.
- Besorgen Sie sich den Domännennamen für die Anmeldung.
- Durchführen der unter [„Vorbereitung von View-Verbindungsserver für View Client“](#), auf Seite 13.
- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den virtuellen Desktop keinen Sicherheitsserver verwenden, stellen Sie sicher, dass Ihr Clientgerät für die Verwendung einer VPN-Verbindung konfiguriert ist, und aktivieren Sie diese Verbindung.

WICHTIG VMware empfiehlt die Verwendung eines Sicherheitsservers anstelle eines VPNs.

- Stellen Sie sicher, dass Sie über den vollqualifizierten Domännennamen (FQDN) des Servers verfügen, der Zugriff auf diesen virtuellen Desktop gewährt. Sie benötigen zudem auch die Portnummer, wenn es sich beim Port nicht um 443 handelt.

- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem View-Desktop zu verwenden, müssen Sie sicherstellen, dass die View Agent-Gruppenrichtlinieneinstellung Allow-DirectRDP aktiviert ist.
- Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus für das von View-Verbindungsserver vorgelegte SSL-Zertifikat konfigurieren.

Informationen zur Bestimmung des zu verwendenden Modus finden Sie unter „[Zertifikatsprüfungsmodi für View Client](#)“, auf Seite 32.

Vorgehensweise

- 1 Doppelklicken Sie auf die Desktop-Verknüpfung **[VMware Horizon View Client]** oder klicken Sie auf **[Start] > [Programme] > [VMware] > [VMware Horizon View Client]**.
- 2 Geben Sie im Dropdown-Menü **[Verbindungsserver]** den Hostnamen für View-Verbindungsserver oder einen Sicherheitsserver ein.
- 3 Stellen Sie sicher, dass die weiteren optionalen Einstellungen im Dialogfeld Ihrer Konfiguration entsprechen.

Option	Beschreibung
Log in as current user (Anmelden als aktueller Benutzer)	Dieses Kontrollkästchen wird gemäß der globalen Einstellung in View Administrator angezeigt oder ausgeblendet. Aktivieren Sie dieses Kontrollkästchen nicht, wenn Sie den View-Desktop für die Verwendung im lokalen Modus auschecken möchten.
Port	Wenn Sie dieses Feld leer lassen, wird der standardmäßige Port 443 verwendet.
Automatische Verbindungsherstellung	Wenn Sie dieses Kontrollkästchen aktivieren, ist das Feld [Verbindungsserver] beim nächsten Start von View Client deaktiviert und Sie werden mit dem Server verbunden, den Sie bei Aktivierung des Kontrollkästchens [Automatische Verbindungsherstellung] angegeben haben. Zur Deaktivierung dieses Kontrollkästchens schließen Sie das nächste Dialogfeld und klicken Sie auf [Optionen] , um diese Einstellung anzuzeigen und zu ändern.
SSL konfigurieren	Wenn Ihr View-Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus durch Klicken auf diese Verknüpfung festlegen, wie unter den Voraussetzungen für diesen Vorgang beschrieben.

- 4 Klicken Sie auf **[Verbinden]**.
Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfenster erscheint.
- 5 Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungs-Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und den Passcode ein und klicken Sie auf **[Weiter]**.
- 6 Geben Sie die Anmeldeinformationen eines Benutzers ein, der für die Verwendung von mindestens einem Desktop-Pool berechtigt ist, wählen Sie die Domäne aus und klicken Sie auf **[Anmelden]**.

Wenn Sie den Benutzernamen mit dem Format **Benutzer@Domaene** eingeben, wird er aufgrund des At-Zeichens (@) als Benutzerprinzipalname (User Principal Name, UPN) behandelt, und das Dropdown-Menü für die Domäne wird ausgeblendet dargestellt.

Informationen zur Erstellung von Desktop-Pools und zum Zuweisen von Benutzerberechtigungen für Pools finden Sie im Dokument *Verwaltung von VMware Horizon View*.

- 7 Wählen Sie einen Desktop aus der eingeblendeten Liste der Desktops.
- a (Optional) Wählen Sie im Dropdown-Menü **[Anzeige]** die Fenstergröße für die Anzeige des View-Desktops.
Die Anzeigeeinstellung wird beim nächsten Öffnen des Desktops als Standardeinstellung beibehalten.
 - b (Optional) Zur Auswahl eines Anzeigeprotokolls klicken Sie auf den nach unten weisenden Pfeil neben einem Desktop in der Liste, klicken Sie auf **[Anzeigeprotokoll]** und wählen Sie das gewünschte Protokoll.

Diese Auswahl ist nur verfügbar, wenn sie durch View Administrator aktiviert wurde. PCoIP bietet ein optimiertes PC-Benutzererlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten im LAN oder WAN.

HINWEIS Wenn Sie Smartcard-Informationen zur Anmeldung verwenden und Sie die Protokolle wechseln möchten, müssen Sie sich abmelden und anschließend wieder anmelden.

Die Protokolleinstellung wird beim nächsten Öffnen des Desktops als Standardeinstellung beibehalten.

- 8 Klicken Sie auf **[Verbinden]**.

Sie werden mit dem Desktop verbunden.

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt.

Wenn keine Authentifizierung gegenüber View-Verbindungsserver möglich ist oder View Client keine Verbindung mit einem Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der View-Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. View Client erfordert SSL-Verbindungen. Prüfen Sie, ob die globale Einstellung in View Administrator für das Kontrollkästchen **[SSL für Client-Verbindungen verwenden]** deaktiviert ist. Ist dies der Fall, müssen Sie entweder das Kontrollkästchen markieren, sodass SSL verwendet wird, oder Ihre Umgebung so einrichten, dass die Clients eine Verbindung zu einem HTTPS-fähigen Lastenausgleich oder einem anderen Zwischengerät herstellen können, das zur Herstellung einer HTTP-Verbindung zum View-Verbindungsserver konfiguriert ist.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für den View-Verbindungsserver sicher. Wenn dies nicht zutrifft, wird in View Administrator möglicherweise angezeigt, dass View Agent in Desktops nicht erreichbar ist, und über den Übertragungsserver-Status wird angezeigt, dass die Komponente nicht bereit ist. Dies sind Hinweise auf zusätzliche Verbindungsprobleme, die durch Zertifikatprobleme verursacht werden.
- Stellen Sie sicher, dass die für die View-Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem View-Desktop verwenden, müssen Sie bestätigen, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Weiter

- Konfigurieren Sie Startoptionen.

Wenn Sie nicht möchten, dass Endbenutzer den Hostnamen von View-Verbindungsserver eingeben müssen, oder wenn Sie andere Startoptionen konfigurieren möchten, verwenden Sie die View Client-Befehlszeilenoptionen, um eine Desktop-Verknüpfung zu erstellen.

Siehe „[Ausführen von View Client über die Befehlszeile](#)“, auf Seite 34.

- Checken Sie einen Desktop aus, der im lokalen Modus verwendet werden kann.

Endbenutzer können feststellen, ob ein Desktop ausgecheckt werden kann, indem sie in der von View Client with Local Mode bereitgestellten Liste auf den nach unten weisenden Pfeil neben dem Desktop klicken. Wenn der Desktop im lokalen Modus verwendet werden kann, wird die Option **[Auschecken]** im Kontextmenü angezeigt. Nur der Benutzer, der den Desktop auscheckt, kann auf den Desktop zugreifen. Dies gilt selbst dann, wenn einer Gruppe von Benutzern Berechtigungen für den Desktop erteilt wurden.

Wechseln zwischen Desktops

Wenn Sie mit einem Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln.

Vorgehensweise

- ◆ Wählen Sie in der View-Desktop-Menüleiste **[Optionen] > [Desktop wechseln]** und wählen Sie den Desktop aus, der angezeigt werden soll.

Option	Aktion
Einen View-Desktop auf demselben Server auswählen	Wird der Desktop-Name nicht gelistet, müssen Sie [Anderer Desktop] wählen und sich für einen anderen Desktop aus der Liste zur Desktop-Auswahl entscheiden.
Einen View-Desktop auf einem anderen Server auswählen	Befindet sich der von Ihnen gewünschte Desktop nicht auf demselben Server, müssen Sie View Client beenden und anschließend neu starten, um eine Verbindung mit einem anderen Server herzustellen.

Abmelden oder Trennen von Desktops

Wenn Sie die Verbindung zu einem View-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen geöffnet.

Selbst wenn Sie keinen View-Desktop geöffnet haben, können Sie sich vom View-Desktop-Betriebssystem abmelden. Die Verwendung dieser Option hat dieselbe Funktion, wie wenn Sie die Tastenkombination Ctrl+Alt+Delete drücken und anschließend auf **[Abmelden]** klicken.

HINWEIS Die Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für View-Desktops nicht unterstützt. Wählen Sie, um dieselben Resultate wie bei einer Betätigung von Strg+Alt+Entf zu erzielen, die Optionen **[Desktop] > [Strg+Alt+Entf senden]** aus der Menüleiste.

Alternativ können Sie auch die Tastenkombination Strg+Alt+Einfg betätigen.

Wenn Sie einen View-Desktop im lokalen Modus verwenden, können Sie den Desktop stattdessen anhalten oder herunterfahren, wie hier beschrieben: „[Herunterfahren oder Anhalten eines lokalen Desktops](#)“, auf Seite 56.

Vorgehensweise

- Trennen Sie die Verbindung, ohne sich abzumelden.

Option	Aktion
View Client ebenfalls beenden	Klicken Sie auf die Schaltfläche [Schließen] in der Ecke des Fensters oder wählen Sie [Optionen] > [Trennen] aus der Menüleiste aus.
Einen anderen View-Desktop auf demselben Server auswählen	Wählen Sie [Optionen] > [Desktop wechseln] aus der Menüleiste.
Einen View-Desktop auf einem anderen Server auswählen	Beenden Sie View Client und starten Sie die Anwendung neu, um die Verbindung mit einem anderen Server herzustellen.

HINWEIS Der View-Administrator kann Ihren Desktop so konfigurieren, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall werden alle geöffneten Programme auf Ihrem Desktop angehalten.

- Melden Sie sich ab und trennen Sie die Verbindung zu einem Desktop.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows- [Start] -Menü ab.
Über die Menüleiste	Wählen Sie [Optionen] > [Trennen und Abmelden] . Bei Verwendung dieser Option werden alle Dateien, die auf dem View-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

- Melden Sie sich ab, wenn kein View-Desktop geöffnet ist.

Bei Verwendung dieser Option werden alle Dateien, die auf dem View-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

- Starten Sie View Client, stellen Sie eine Verbindung mit der View-Verbindungsserver-Instanz her, die Zugriff auf den View-Desktop bietet, und geben Sie Ihre Anmeldeinformationen für die Authentifizierung an.
- Klicken Sie bei Anzeige der Liste zur Desktop-Auswahl auf den nach unten weisenden Pfeil neben dem Desktop und wählen Sie **[Abmelden]** .

Arbeiten auf einem View-Desktop

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

Dieses Kapitel behandelt die folgenden Themen:

- „[Funktionsunterstützungs-Matrix](#)“, auf Seite 45
- „[Internationalisierung](#)“, auf Seite 47
- „[Verbinden von USB-Geräten](#)“, auf Seite 47
- „[Konfigurieren von Clients zur erneuten Verbindung beim Neustart der USB-Geräte](#)“, auf Seite 49
- „[Kopieren und Einfügen von Text und Bildern](#)“, auf Seite 50
- „[Drucken auf einem View-Desktop](#)“, auf Seite 51
- „[Steuern der Adobe Flash-Anzeige](#)“, auf Seite 52
- „[Verwenden der Funktion der relativen Mausbewegung für CAD- und 3D-Anwendungen](#)“, auf Seite 53

Funktionsunterstützungs-Matrix

Viele Funktionen wie z. B. die RSA SecurID-Authentifizierung, das standortbasierte Drucken und das PCoIP-Protokoll werden auf den meisten Clientbetriebssystemen unterstützt. Zudem muss berücksichtigt werden, ob die Funktion im Betriebssystem des View-Desktops unterstützt wird.

Halten Sie sich bei der Planung der Anzeigeprotokolle und Funktionen, die Sie Ihren Benutzern zur Verfügung stellen möchten, an die folgenden Informationen, um zu bestimmen, welche Betriebssysteme von Client und Agent (View-Desktop) die jeweilige Funktion unterstützen.

Die Typen und Editionen des unterstützten Gastbetriebssystems hängen von der Windows-Version ab.

Tabelle 5-1. Betriebssystemunterstützung für View Agent

Gastbetriebssystem	Version	Edition	Service Pack
Windows 8	64-Bit und 32-Bit	Enterprise und Professional	–
Windows 7	64-Bit und 32-Bit	Enterprise und Professional	Keine und SP1
Windows Vista	32-Bit	Business und Enterprise	SP1 und SP2
Windows XP	32-Bit	Professional	SP3

Tabelle 5-1. Betriebssystemunterstützung für View Agent (Fortsetzung)

Gastbetriebssystem	Version	Edition	Service Pack
Windows 2008 R2 Terminal Server	64-Bit	Standard	SP1
Windows 2008 Terminal Server	64-Bit	Standard	SP2

Tabelle 5-2. Unterstützte Funktionen unter Betriebssystemen für View-Desktops (in denen View Agent installiert ist)

Funktion	Windows XP	Windows Vista	Windows 7	Windows 2008	Windows 8
USB-Zugriff	X	X	X		X
RDP-Anzeigeprotokoll	X	X	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X		X
Persona-Verwaltung	X	X	X		X
Wyse MMR	X	X			
Standortbasiertes Drucken	X	X	X		X
Virtuelles Drucken	X	X	X		X
Smartcards	X	X	X	X	X
RSA SecurID oder RADIUS	X	X	X	–	X
Einmaliges Anmelden	X	X	X	X	X
Mehrere Monitore	X	X	X	Mit RDP 7	X
Lokaler Modus	X	X	X		X

Tabelle 5-3. Auf Windows-basierten View Client-Instanzen unterstützte Funktionen

Funktion	Windows XP	Windows Vista	Windows 7	Windows 8
USB-Zugriff	X	X	X	X
RDP-Anzeigeprotokoll	X	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X	X
Persona-Verwaltung	X (nicht mit lokalem Modus)	X (nicht mit lokalem Modus)	X (nicht mit lokalem Modus)	X (nicht mit lokalem Modus)
Wyse MMR	X	X		
Standortbasiertes Drucken	X	X	X	X
Virtuelles Drucken	X	X	X	X
Smartcards	X	X	X	X
RSA SecurID oder RADIUS	X	X	X	X
Einmaliges Anmelden	X	X	X	X
Mehrere Monitore	X	X	X	X
Lokaler Modus	X	X	X	X

Informationen zu den unterstützten Editionen der einzelnen Clientbetriebssysteme bzw. zu den unterstützten Service Packs finden Sie in den Themen zu den Systemanforderungen.

Weitere Erläuterungen für diese Funktionen und deren Einschränkungen finden Sie im Dokument *Planung der VMware Horizon View--Architektur*.

Internationalisierung

Die Benutzeroberfläche und die Dokumentation sind in den Sprachen Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch und Koreanisch verfügbar.

Verbinden von USB-Geräten

Sie können lokal angeschlossene USB-Geräte, zum Beispiel Thumb Drive-Flashlaufwerke, Kameras oder Drucker, von einem View-Desktop aus verwenden. Diese Funktion wird als USB-Umleitung bezeichnet.

Bei Verwendung dieser Funktion werden die meisten an das lokale Clientsystem angeschlossenen USB-Geräte aus einem Menü in View Client heraus verfügbar. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

Bei der Verwendung von USB-Geräten mit View-Desktops gelten folgende Einschränkungen:

- Bei Zugriff auf ein USB-Gerät von einem Menü in View Client und Verwendung des Geräts in einem View-Desktop können Sie nicht auf dem lokalen Computer auf das Gerät zugreifen.

WICHTIG Aus diesem Grund sollten Sie keine Geräte wie USB-Ethernet-Geräte und Touchscreen-Geräte umleiten. Wenn Sie beispielsweise ein USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk. Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der View-Desktop Eingaben vom Touchscreen und nicht von der Tastatur.

- Zu den USB-Geräten, die nicht im Menü angezeigt werden, aber auf dem View-Desktop verfügbar sind, zählen Eingabegeräte (Human Interface Devices) wie zum Beispiel Tastaturen und Zeigergeräte. Der View-Desktop und der lokale Computer verwenden diese Geräte zur gleichen Zeit. Die Interaktion mit diesen Geräten kann aufgrund der Netzwerklatenz manchmal recht langsam sein.
- Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Desktop angezeigt werden.
- Manche USB-Geräte erfordern bestimmte Treiber. Wenn der erforderliche Treiber nicht bereits auf dem View-Desktop installiert ist, werden Sie möglicherweise bei Verbindung des USB-Geräts mit dem View-Desktop zu Installation dieses Treibers aufgefordert.
- Wenn Sie USB-Geräte verbinden möchten, die MTP-Treiber verwenden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets, müssen Sie View Client so einstellen, dass es die USB-Geräte automatisch mit Ihrem View-Desktop verbindet. Anderenfalls wird das USB-Gerät beim Versuch der manuellen Umleitung über ein Menüelement nur umgeleitet, wenn Sie das Gerät trennen und es anschließend wieder verbinden.
- Webcams werden für die USB-Umleitung nicht unterstützt.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz.

Sie können USB-Geräte sowohl manuell als auch automatisch mit einem View-Desktop verbinden.

HINWEIS Leiten Sie keine USB-Geräte wie USB-Ethernet-Geräte und Touchscreen-Geräte an den virtuellen Desktop um. Wenn Sie ein USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk. Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der View-Desktop Eingaben vom Touchscreen und nicht von der Tastatur. Wenn Sie Ihren virtuellen Desktop zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie Richtlinien konfigurieren, um bestimmte Geräte auszuschießen. Siehe Thema "Konfiguration der Filterrichtlinieneinstellungen für USB-Geräte" im Dokument *Verwaltung von VMware Horizon View*.

WICHTIG In diesem Vorgang wird die Verwendung des VMware Horizon View Client-Menüelements zur Konfiguration der automatischen Verbindung von USB-Geräten mit dem View-Desktop erläutert. Sie können die automatische Verbindung auch konfigurieren, indem Sie die View Client-Befehlszeilenschnittstelle verwenden oder eine Gruppenrichtlinie erstellen.

Weitere Informationen über die Befehlszeilenschnittstelle finden Sie unter „[Ausführen von View Client über die Befehlszeile](#)“, auf Seite 34. Weitere Informationen zur Erstellung von Gruppenrichtlinien finden Sie im Dokument *Verwaltung von VMware Horizon View*.

Voraussetzungen

- Um USB-Geräte mit einem View-Desktop verwenden zu können, muss der View-Administrator die USB-Funktion für den View-Desktop aktiviert haben.

Diese Aufgabe umfasst die Installation der Komponente **[USB-Umleitung]** in View Agent. Weitere Informationen und Anweisungen finden Sie im Kapitel über die Erstellung und Vorbereitung der virtuellen Maschinen im Dokument *Verwaltung von VMware Horizon View*.

Die Aufgabe kann zudem auch das Festlegen von Gruppenrichtlinien zur Zulassung der USB-Umleitung umfassen. Weitere Informationen finden Sie in den Abschnitten „USB-Einstellungen für View Agent“, „USB-Einstellungen für View Client“, „Konfiguration der Geräteaufschlüsselungs-Richtlinieneinstellungen für USB-Verbundgeräte“ und „Konfiguration der Filterrichtlinieneinstellungen für USB-Geräte“ im Dokument *Verwaltung von VMware Horizon View*.

- Bei der Installation von View Client muss die Komponente **[USB-Umleitung]** mit installiert werden. Wenn Sie diese Komponente nicht in die Installation eingeschlossen haben, sollten Sie das Installationsprogramm erneut ausführen, die Komponenten ändern und die Komponente **[USB-Umleitung]** einschließen.

Vorgehensweise

- Verbinden Sie das USB-Gerät manuell mit einem View-Desktop.
 - a Schließen Sie das USB-Gerät an Ihr lokales Clientsystem an.
 - b Klicken Sie in der VMware Horizon View Client-Menüleiste auf **[USB-Gerät verbinden]**.
 - c Wählen Sie das USB-Gerät aus.

Das Gerät wird manuell vom lokalen System an den View-Desktop umgeleitet.

- Konfigurieren Sie View Client dahingehend, dass USB-Geräte automatisch mit dem View-Desktop verbunden werden, wenn Sie diese an das lokale System anschließen.

Verwenden Sie diese Funktion zur automatischen Verbindungsherstellung unbedingt dann, wenn Sie Geräte mit MTP-Treibern verwenden möchten, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets.

- a Bevor Sie das USB-Gerät anschließen, starten Sie View Client und stellen Sie die Verbindung mit einem View-Desktop her.
- b Wählen Sie in der VMware Horizon View Client-Menüleiste **[USB-Gerät verbinden] > [USB-Geräte automatisch verbinden]** .
- c Schließen Sie das USB-Gerät an.

Das USB-Gerät wird auf dem Desktop angezeigt. Dieser Vorgang kann bis zu 20 Sekunden dauern. Bei erstmaliger Verbindung von Gerät und Desktop werden Sie eventuell dazu aufgefordert, bestimmte Treiber zu installieren.

Wird das USB-Gerät auch nach mehreren Minuten nicht auf dem Desktop angezeigt, sollten Sie die Verbindung trennen und das Gerät anschließend neu mit dem Clientcomputer verbinden.

Weiter

Bei Problemen mit der USB-Umleitung finden Sie weitere Informationen im Kapitel über die Behebung von Problemen bei der USB-Umleitung im Dokument *Verwaltung von VMware Horizon View*-.

Konfigurieren von Clients zur erneuten Verbindung beim Neustart der USB-Geräte

Wenn Sie View Client nicht zur automatischen Verbindung der USB-Geräte mit Ihrem View-Desktop konfigurieren, können Sie immer noch festlegen, dass View Client mit bestimmten Geräten, die gelegentlich neu starten, wieder eine Verbindung herstellt. Anderenfalls verbindet sich das Gerät bei einem Neustart während eines Upgrades nicht mit dem View-Desktop, sondern mit dem lokalen System.

Wenn Sie als USB-Gerät zum Beispiel ein Smartphone oder ein Tablet verbinden möchten, welches bei Betriebssystem-Upgrades automatisch neu gestartet wird, können Sie View Client dazu anweisen, das bestimmte Gerät erneut mit dem View-Desktop zu verbinden. Zum Durchführen dieser Aufgabe muss die Konfigurationsdatei auf dem Client bearbeitet werden.

Wenn Sie die Option **[USB-Geräte automatisch verbinden]** in View Client verwenden, werden alle Geräte, die Sie am Clientsystem anschließen, an den View-Desktop umgeleitet. Wenn Sie nicht möchten, dass alle Geräte verbunden werden, sollten Sie die folgende Vorgehensweise zur Konfiguration von View Client anwenden, sodass nur bestimmte USB-Geräte automatisch neu verbunden werden.

Voraussetzungen

Ermitteln Sie das hexadezimale Format der Hersteller-ID (VID) und der Produkt-ID (PID) des Geräts. Anweisungen hierzu finden Sie im VMware KB-Artikel <http://kb.vmware.com/kb/1011600>.

Vorgehensweise

- 1 Öffnen Sie die Datei `config.ini` in einem Text-Editor auf dem Client.

Betriebssystemversion	Dateipfad
Windows 7	C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini
Windows XP	C:\Documents and Settings\All Users\Application Data\VMware\VMware USB Arbitration Service\config.ini

- 2 Legen Sie die Eigenschaft `slow-reconnect` für das bestimmte Gerät oder die Geräte fest.

```
usb.quirks.device0 = "vid:pid slow-reconnect"
```

Hier stehen `vid:pid` jeweils für die Hersteller- und die Produkt-ID (im hexadezimalen Format) des Geräts. Die folgenden Zeilen legen diese Eigenschaft beispielsweise für zwei USB-Geräte fest:

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
```

```
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

Geben Sie die Geräteeigenschaften `usb.quirks.deviceN` in der richtigen Reihenfolge, beginnend bei 0, an. Folgt auf die Zeile `usb.quirks.device0` zum Beispiel nicht eine Zeile mit `usb.quirks.device1`, sondern eine Zeile mit `usb.quirks.device2`, wird nur die erste Zeile gelesen.

Wenn nun für Geräte wie Smartphones oder Tablets ein Upgrade der Firmware oder des Betriebssystems durchgeführt wird, verläuft das Upgrade erfolgreich, da das Gerät neu startet und die Verbindung zu dem View-Desktop herstellt, welcher das Gerät verwaltet.

Kopieren und Einfügen von Text und Bildern

Wenn Ihr Administrator die Funktion aktiviert, können Sie formatierten Text und Bilder zwischen einem Remote-View-Desktop und Ihrem Clientsystem oder zwischen zwei View-Desktops kopieren und einfügen. Hierfür gelten allerdings einige Einschränkungen.

Wenn Sie das PCoIP-Anzeigeprotokoll sowie einen View-Desktop vom Typ 5.x oder eine neuere Version verwenden, kann Ihr View-Administrator diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem auf einen View-Desktop oder nur von einem View-Desktop zu Ihrem Clientsystem oder beide Vorgänge zugelassen werden bzw. keiner der beiden Vorgänge zugelassen wird.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinienobjekten (GPOs), die View Agent auf den View-Desktops zugeordnet sind. Weitere Informationen finden Sie unter dem Thema über allgemeine Sitzungsvariablen von View PCoIP im Dokument *Verwaltung von VMware Horizon View* - im Kapitel über die Konfigurationsrichtlinien.

Zu den unterstützten Dateiformaten gehören Text, Bilder und RTF (Rich Text Format). In der Zwischenablage können bis zu 1 MB an Daten für Kopier- und Einfügevorgänge gespeichert werden. Wenn Sie formatierten Text kopieren, handelt es sich bei den Daten teilweise um Text und teilweise um Formatierungsinformationen. Ein Dokument mit einer Größe von 800 KB kann beim Kopieren eine Datenmenge von mehr als 1 MB besitzen, da mehr als 200 KB an RTF-Daten in der Zwischenablage gespeichert werden.

Wenn Sie daher eine große Menge an formatiertem Text oder Text und ein Bild kopieren, kann es beim Einfügen dazu kommen, dass Sie den Text ganz oder teilweise sehen, nicht aber die Formatierung oder das Bild. Dies liegt daran, dass die drei Arten von Daten separat gespeichert werden können. Je nach Art des Dokuments, von dem aus Sie kopieren, können Bilder möglicherweise als Bilder oder als RTF-Daten gespeichert werden.

Beträgt die Gesamtmenge von Text und RTF weniger als 1 MB, wird der formatierte Text eingefügt. Es ist häufig der Fall, dass die RTF-Daten nicht gekürzt werden können, sodass die RTF-Daten verworfen und nur der reine Text eingefügt wird, sollten Text und Formatierung zusammen mehr als 1 MB umfassen.

Sollten Sie nicht in der Lage sein, den gesamten formatierten Text und die von Ihnen ausgewählten Bilder einzufügen, versuchen Sie geringere Teilmengen zu speichern und einzufügen.

Das Kopieren und Einfügen von Dateien zwischen einem View-Desktop und dem Dateisystem auf Ihrem Client-Computer ist nicht möglich.

Drucken auf einem View-Desktop

Sie können von einem View-Desktop aus Dokumente auf einem virtuellen Drucker oder einem USB-Drucker ausdrucken, der mit Ihrem Clientcomputer verbunden ist. Die virtuelle Druckfunktion und das Drucken mit USB-Umleitung können ohne Konflikte gemeinsam eingesetzt werden.

Festlegen von Voreinstellungen für die virtuelle Druckfunktion auf Windows-Clients

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

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

WICHTIG Diese Funktion steht für die folgenden Druckertypen nicht zur Verfügung:

- USB-Drucker, die die USB-Umleitungsfunktion zur Verbindung mit einem virtuellen USB-Port im View-Desktop verwenden

Sie müssen den USB-Drucker im View-Desktop trennen, um die virtuelle Druckfunktion verwenden zu können.
 - Die Windows-Funktion für die Ausgabe in einer Datei

Das Kontrollkästchen **[Ausgabe in Datei]** im Dialogfeld **[Drucken]** kann nicht ausgewählt werden. Ein Druckertreiber, über den eine Datei erstellt wird, kann verwendet werden. Beispielsweise können Sie einen PDF-Writer zum Drucken einer PDF-Datei verwenden.
-

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Druckfunktion von View Agent auf dem View-Desktop installiert ist. Die Treiber befinden sich im View-Desktop-Dateisystem unter `C:\Programme\Gemeinsame Dateien\VMware\Drivers\Virtual Printer`.

Die Installation von View Agent ist eine der Aufgaben, die im Rahmen der Vorbereitung einer virtuellen Maschine auf die Verwendung als View-Desktop durchgeführt werden muss. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.

Vorgehensweise

- 1 Klicken Sie im View-Desktop auf **[Start] > [Settings (Einstellungen)] > [Drucker und Faxgeräte]** .
- 2 Klicken Sie im Fenster **[Drucker und Faxgeräte]** mit der rechten Maustaste auf einen der lokal verfügbaren Drucker und wählen Sie **[Eigenschaften]** .

Auf Windows 7- und 8-Desktops wird möglicherweise nur der Standarddrucker angezeigt, selbst wenn weitere Drucker verfügbar sind. Zum Anzeigen der anderen Drucker klicken Sie mit der rechten Maustaste auf den Standarddrucker und zeigen auf **[Druckereigenschaften]** .

Auf dem View-Desktop werden virtuelle Drucker als `<Druckername>#:<Nummer>` angezeigt.
- 3 Klicken Sie im Fenster mit den Druckereigenschaften auf die Registerkarte **[ThinPrint-Geräteeinrichtung]** und geben Sie die zu verwendenden Einstellungen an.
- 4 Klicken Sie auf der Registerkarte **[Allgemein]** auf **[Druckereinstellungen]** und bearbeiten Sie die Seiten- und Farbeinstellungen.

- 5 Auf der Registerkarte **[Erweitert]** legen Sie die Einstellungen für den doppelseitigen Druck und das Druckformat (Hochformat oder Querformat) fest.
- 6 Zur Anzeige einer Druckvorschau auf dem Host aktivieren Sie **[Vor dem Druck Vorschau auf Client anzeigen]**.
Aus dieser Vorschau können Sie auf einen beliebigen Drucker mit allen verfügbaren Eigenschaften zugreifen.
- 7 Auf der Registerkarte **[Anpassung]** können Sie die Optionen für die automatische Druckanpassung überprüfen.
VMware empfiehlt die Beibehaltung der Standardeinstellungen.
- 8 Klicken Sie auf **[OK]**.

Verwenden von USB-Druckern

In einer View-Umgebung können virtuelle Drucker und umgeleitete USB-Drucker konfliktfrei zusammen eingesetzt werden.

Ein USB-Drucker ist ein Drucker, der über einen USB-Port an das lokale Clientsystem angeschlossen ist. Um Druckaufträge an einen USB-Drucker zu senden, können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion nutzen. In Abhängigkeit von den Netzwerkbedingungen werden Druckaufträge mit USB-Umleitung möglicherweise schneller gedruckt als über die virtuelle Druckfunktion.

- Sie können die USB-Umleitungsfunktion verwenden, um einen USB-Drucker über einen virtuellen USB-Port an den View-Desktop anzuschließen, wenn die erforderlichen Treiber ebenfalls auf dem View-Desktop installiert sind.

Bei Verwendung dieser Umleitungsfunktion ist der Drucker nicht mehr mit dem physischen USB-Port am Client verbunden, sodass der USB-Drucker nicht in der Liste der lokalen Drucker aufgeführt wird, die über die virtuelle Druckfunktion angezeigt wird. Dies bedeutet auch, dass Sie vom View-Desktop auf dem USB-Drucker drucken können, jedoch nicht von der lokalen Clientmaschine.

Auf dem View-Desktop werden USB-Drucker als *<Druckername>* angezeigt.

Weitere Informationen zum Anschluss eines USB-Druckers finden Sie unter „[Verbinden von USB-Geräten](#)“, auf Seite 47.

- Auf Windows-Clients können Sie alternativ die virtuelle Druckfunktion verwenden, um Druckaufträge an einen USB-Drucker zu senden. Bei Verwendung der virtuellen Druckfunktion können Sie sowohl vom View-Desktop als auch vom lokalen Client auf dem USB-Drucker drucken, ohne Druckertreiber im View-Desktop installieren zu müssen.

Steuern der Adobe Flash-Anzeige

Der View-Administrator kann die Wiedergabe von Adobe Flash-Inhalten im View-Desktop so festlegen, dass Rechenressourcen eingespart werden. In einigen Fällen können diese Einstellungen zu einer verringerten Wiedergabequalität führen. Mithilfe des Mauszeigers können Sie die Adobe Flash-Einstellungen außer Kraft setzen, die Ihr View-Administrator festlegt.

Die Steuerung der Adobe Flash-Anzeige ist ausschließlich für Internet Explorer-Sitzungen unter Windows sowie für Adobe Flash 9 und 10 verfügbar. Zur Steuerung der Adobe Flash-Anzeigequalität darf Adobe Flash nicht im Vollbildmodus ausgeführt werden.

Vorgehensweise

- 1 Navigieren Sie im Internet Explorer des View-Desktops zu den gewünschten Adobe Flash-Inhalten und starten Sie diese, falls erforderlich.

Je nach Konfiguration der Adobe Flash-Einstellungen durch Ihren View-Administrator ist die Wiedergabequalität möglicherweise verringert.

- 2 Bewegen Sie den Mauszeiger während der Wiedergabe in die Adobe Flash-Inhalte.

Die Anzeigequalität wird verbessert, solange sich der Cursor innerhalb der Adobe Flash-Inhalte befindet.

- 3 Doppelklicken Sie in die Adobe Flash-Inhalte, um die verbesserte Wiedergabequalität beizubehalten.

Verwenden der Funktion der relativen Mausbewegung für CAD- und 3D-Anwendungen

Wenn Sie das PCoIP-Anzeigeprotokoll bei CAD- oder 3D-Anwendungen in einem Horizon View 5.2-Desktop verwenden, können Sie die Mausleistung durch Aktivierung der Funktion für die relative Mausbewegung verbessern.

In den meisten Fällen, wenn Sie Anwendungen verwenden, die kein 3D-Rendering erfordern, überträgt View Client Informationen über die Mauszeigerbewegungen mithilfe von absoluten Koordinaten. Bei der Verwendung von absoluten Koordinaten rendert der Client die Mausbewegungen lokal, wodurch die Leistung insbesondere dann verbessert wird, wenn Sie sich außerhalb des Firmennetzwerks befinden.

Bei der Arbeit mit grafikintensiven Anwendungen wie AutoCAD oder bei Videospielen können Sie die Mausleistung verbessern, indem Sie die Funktion für die relative Mausbewegung aktivieren. Diese Funktion verwendet relative statt absoluter Koordinaten. Um diese Funktion zu verwenden, wählen Sie **[Optionen] > [Relative Maus aktivieren]** in der View Client-Menüleiste.

HINWEIS Wenn Sie View Client im Fenstermodus und nicht im Vollbildmodus verwenden und die Funktion der relativen Mausbewegung aktiviert ist, können Sie möglicherweise den Mauszeiger nicht auf die View Client-Menüoptionen oder aus dem View Client-Fenster hinaus bewegen. Um diese Situation zu beheben, drücken Sie Ctrl+Alt.

Wenn die Funktion der relativen Mausbewegung aktiviert ist, kann die Performance langsam sein, wenn Sie sich außerhalb des Firmennetzwerks in einem WAN befinden.

WICHTIG Für diese Funktion wird ein Horizon View 5.2-Desktop benötigt, und Sie müssen das 3D-Rendering für den Desktop-Pool einschalten. Weitere Informationen zu Pool-Einstellungen und den Optionen für 3D-Rendering finden Sie im Dokument *Verwaltung von VMware Horizon View*.

Arbeiten mit Desktops im lokalen Modus

6

View-Desktops im lokalen Modus verhalten sich genauso wie ihre Remot-Desktop-Gegenstücke. Jedoch können sie die lokalen Ressourcen nutzen und benötigen keine Netzwerkverbindung.

Wenn Sie einen View-Desktop auschecken, wird der Desktop auf Ihren Clientcomputer heruntergeladen, so dass er lokal ausgeführt werden kann. Wenn ein Desktop ausgecheckt ist, können Sie ihn auf dem Server sichern, um die Änderungen zu speichern, die Sie am lokalen Desktop vornehmen.

Falls Sie einen lokalen Desktop nicht mehr verwenden, können Sie ihn beenden oder anhalten. Nach Abschluss der Arbeit mit dem lokalen Desktop können Sie ihn wieder beim Server einchecken. Alternativ können Sie ein Rollback für den Desktop durchführen, um die Änderungen zu verwerfen, die Sie vorgenommen haben.

Weitere Informationen über die Vorteile von View Client mit dem lokalen Modus finden Sie im Dokument *Planung der VMware Horizon View--Architektur*.

Dieses Kapitel behandelt die folgenden Themen:

- [„Erstmaliges Auschecken eines Desktops im lokalen Modus“](#), auf Seite 55
- [„Herunterfahren oder Anhalten eines lokalen Desktops“](#), auf Seite 56
- [„Backup eines Desktops“](#), auf Seite 56
- [„Einchecken eines Desktops“](#), auf Seite 57
- [„Rollback eines Desktops“](#), auf Seite 58
- [„Konfigurieren der Ressourcennutzung für Endpunkte“](#), auf Seite 58

Erstmaliges Auschecken eines Desktops im lokalen Modus

Wenn ein Endbenutzer einen View-Desktop erstmalig zur Verwendung im lokalen Modus auscheckt, umfasst der Vorgang zum Auschecken und Herunterladen mehrere Phasen und diese Schritte dauern länger als bei nachfolgenden Auscheckvorgängen.

Wenn sich ein Endbenutzer bei View Client anmeldet und eine Liste mit Desktops angezeigt wird, kann der Benutzer sich entweder mit einem Desktop verbinden und diesen auschecken oder den Desktop auschecken, ohne zunächst eine Remote-Verbindung herzustellen.

WICHTIG Sie können einen Desktop nicht auschecken, wenn Sie bei der Anmeldung die Funktion **[Anmelden als aktueller Benutzer]** gewählt haben. Sie müssen View Client schließen, erneut starten und das Kontrollkästchen **[Anmelden als aktueller Benutzer]** deaktivieren.

Wenn der Endbenutzer eine Verbindung mit dem Desktop herstellt und diesen auscheckt, wird der Benutzer vom Remote-Desktop abgemeldet, die virtuelle Maschine im Rechenzentrum wird gesperrt und eine Kopie der virtuellen Maschine wird für den Endbenutzer heruntergeladen.

Nach dem Herunterladen werden beim erstmaligen Einschalten des lokalen Desktops durch den Endbenutzer verschiedene Treiber auf dem lokalen Desktop installiert. Welche Treiber installiert werden, hängt vom Betriebssystem des View-Desktops sowie von der Hardware und vom Betriebssystem des lokalen Computers ab. Während der Treiberinstallation ist die Leistung des View-Desktops beeinträchtigt. Dies gilt insbesondere, wenn auf dem View-Desktop ein Windows XP-Betriebssystem ausgeführt wird.

Im Anschluss an die Treiberinstallation wird der Endbenutzer zum Neustart des lokalen Desktops aufgefordert.

HINWEIS Wenn Sie beim Starten oder Herunterfahren des Gastbetriebssystems in ein View-Desktop-Fenster klicken, kann es vorkommen, dass die Zeigersteuerung im Fenster verbleibt. Nachdem alle Startvorgänge abgeschlossen sind und die VMware Tools ausgeführt werden, wird der Zeiger freigegeben. Wenn die Zeigersteuerung weiterhin im Desktop-Fenster verbleibt, können Sie den Zeiger durch Drücken von Strg+Alt freigegeben.

Die RAM-Größe und die Anzahl an CPUs, die der lokale View-Desktop nutzt, richtet sich nach der Kapazität des lokalen Computers. Da der View-Desktop NAT verwendet, werden die IP- und MAC-Adressen des lokalen Computers gemeinsam verwendet. Weitere Informationen finden Sie unter „[Konfigurieren der Ressourcennutzung für Endpunkte](#)“, auf Seite 58.

Herunterfahren oder Anhalten eines lokalen Desktops

Wenn Sie einen lokalen Desktop nicht verwenden, können Sie ihn schließen. Ein lokaler Desktop kann heruntergefahren oder angehalten werden.

Voraussetzungen

Falls Dateien im Desktop geöffnet sind, speichern und schließen Sie diese.

Vorgehensweise

- ◆ Wählen Sie im Menü **[Optionen]** des View-Desktops, wie der Desktop geschlossen werden soll.

Option	Beschreibung
Anhalten	Schließt View Client und lässt alle geöffneten Programme im aktuellen Zustand. Beim Wiederherstellen der Verbindung zu dem Desktop werden die Programme im selben Zustand fortgesetzt, in dem sie waren. HINWEIS Das Anhalten des Desktops dauert länger als das Herunterfahren des Desktops.
Gast herunterfahren	Schließt View Client und beendet alle geöffneten Programme. Nicht gespeicherte Daten gehen verloren. Diese Option hat dieselbe Funktion, wie wenn Sie die Tastenkombination Strg+Alt+Entf drücken und anschließend auf [Herunterfahren] klicken.

Beim Klicken auf die Schaltfläche **[Schließen]** in der Titelleiste wird der Desktop abhängig davon, wie Ihr View-Administrator den Desktop konfiguriert hat, entweder angehalten oder heruntergefahren.

Backup eines Desktops

Sie können einen Desktop auf dem Server sichern, um die Änderungen zu speichern, die Sie am lokalen Desktop vornehmen.

Sie können den Desktop nur sichern, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Voraussetzungen

- Der Desktop muss ausgecheckt sein.
- Sie müssen über eine Netzwerkverbindung verfügen.

Vorgehensweise

- ◆ Sichern Sie den Desktop.

Option	Aktion
Vom View-Desktop aus	Doppelklicken Sie auf das Symbol [VMware View] in der Taskleiste, um das Dialogfeld der Sicherung zu öffnen, und klicken Sie auf [Backup anfordern] .
In der Desktop-Auswahlliste	Klicken Sie neben dem zu sichernden Desktop auf den Dropdown-Pfeil und wählen Sie [Backup]

Um eine laufende Sicherung zu unterbrechen, klicken Sie auf **[Backup verschieben]**. Sie können das Desktop-Backup nur anhalten, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Um ein angehaltenes Backup fortzusetzen, klicken Sie auf **[Verschobenes Backup fortsetzen]**.

Um Toastbenachrichtigungen zu deaktivieren, die den Sicherungsstatus anzeigen, klicken Sie mit der rechten Maustaste auf das Taskleistensymbol **[VMware Horizon View]** und wählen Sie **[Backup-Benachrichtigungen deaktivieren]**.

Einchecken eines Desktops

Wenn Sie die Verwendung eines lokalen Desktops beendet haben, können Sie ihn wieder auf dem Server einchecken.

Sie können einen View-Desktop nur einchecken, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Während des Eincheckens können Sie nicht auf den Desktop zugreifen.

Voraussetzungen

- Der Desktop muss ausgecheckt sein.
- Sie müssen über eine Netzwerkverbindung verfügen.

Vorgehensweise

- ◆ So checken Sie den Desktop ein

Option	Aufgabe
Auf dem View-Desktop	Wählen Sie in der Titelleiste [Optionen] > [Einchecken] .
Über die Liste zur Desktop-Auswahl	Klicken Sie auf den nach unten weisenden Pfeil neben dem Desktop, den Sie einchecken möchten, und wählen Sie [Einchecken] .

Zum Anhalten eines laufenden Eincheckvorgangs wählen Sie **[Einchecken anhalten]**. Um einen angehaltenen Eincheckvorgang fortzusetzen, wählen Sie **[Einchecken fortsetzen]**. Zum Abbrechen eines laufenden Eincheckvorgangs wählen Sie **[Einchecken abbrechen]**.

Der Desktop wird wieder auf dem Server eingechekkt und steht für ein Auschecken durch andere autorisierte Benutzer zur Verfügung.

Durch das Einchecken eines Desktops werden die Dateien des lokalen Desktops nicht von der Festplatte Ihres Clientcomputers entfernt.

Rollback eines Desktops

Beim Ausführen eines Rollbacks für einen lokalen Desktop werden Änderungen verworfen, die am Desktop vorgenommen wurden. Alle Daten, die seit dem letzten Auscheckvorgang oder der letzten Server-Sicherung aktualisiert wurden, gehen dabei verloren.

Sie können ein Rollback für einen Desktop nur durchführen, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Während des Rollbacks können Sie nicht auf den Desktop zugreifen.

Voraussetzungen

- Der Desktop muss ausgecheckt sein.
- Sie müssen über eine Netzwerkverbindung verfügen.

Vorgehensweise

- ◆ So führen Sie ein Rollback für den Desktop aus

Option	Aufgabe
Auf dem View-Desktop	Wählen Sie in der Titelleiste [Optionen] > [Rollback] .
Über die Liste zur Desktop-Auswahl	Klicken Sie auf den nach unten weisenden Pfeil neben dem Desktop, für den ein Rollback ausgeführt werden soll, und wählen Sie [Rollback] .

Der Desktop wird nicht mehr lokal ausgeführt.

Durch das Rollback eines Desktops werden die Dateien des lokalen Desktops nicht von der Festplatte Ihres Clientcomputers entfernt.

Konfigurieren der Ressourcennutzung für Endpunkte

Für die Verwendung auf einem lokalen System ausgecheckte View-Desktops nutzen standardmäßig die Arbeitsspeicher- und CPU-Optionen dieses Hosts. Die virtuellen Netzwerkkarten des Desktops verwenden NAT, um die IP- und MAC-Adressen des Hosts gemeinsam zu verwenden. Dieses Standardverhalten kann geändert werden.

Außerkräftsetzen der lokalen Nutzung von Arbeitsspeicher- und CPU-Ressourcen

Nachdem ein lokaler Desktop ausgecheckt ist, nutzt er die Arbeitsspeicher- und CPU-Ressourcen des lokalen Systems unabhängig von den Arbeitsspeicher- und CPU-Einstellungen für die virtuelle Maschine in vCenter Server. Dieses Standardverhalten kann außer Kraft gesetzt werden.

Die RAM-Größe, die einem zur Verwendung im lokalen Modus ausgecheckten View-Desktop zugewiesen ist, wird standardmäßig automatisch an eine bestimmte Größe des RAM auf dem Clienthost angepasst.

In der Formel wird berücksichtigt, wie viel Arbeitsspeicher verfügbar ist, um diesen zwischen Host und lokalem View-Desktop aufzuteilen. Für ein Windows XP-Betriebssystem sind mindestens 512 MB Arbeitsspeicher erforderlich. Für ein Windows 8-, Windows 7- oder Windows Vista-Betriebssystem mit 32-Bit ist mindestens 1 GB Arbeitsspeicher erforderlich. Die verfügbare Arbeitsspeichergröße, die aufgeteilt werden kann, ist der gesamte RAM auf dem Host abzüglich der Mindestanforderungen an den RAM für Host- und Gastbetriebssysteme.

Tabelle 6-2. Für lokale View-Desktops vorgesehener Arbeitsspeicher

Arbeitsspeicherzuweisung	Windows XP-Gastsysteme	Windows 8-, Windows 7- und Windows Vista-Gäste
Minimal	512 MB	1 GB
Best Effort	512 MB + (verfügbarer RAM/2)	1 GB + (verfügbarer RAM/2)
Maximal	2 GB	4 GB

Wenn ein Windows 7-Host beispielsweise über insgesamt 2 GB Arbeitsspeicher verfügt, würde die lokale Ausführung eines View-Desktops mit Windows 7 2 GB Arbeitsspeicher erfordern, wobei 1 GB Arbeitsspeicher dem Host und 1 GB Arbeitsspeicher dem lokalen View-Desktop zugewiesen wird. Wenn der Host über 3 GB Arbeitsspeicher verfügen würde, würden 1,5 GB Arbeitsspeicher dem Host und 1,5 GB Arbeitsspeicher dem lokalen View-Desktop zugewiesen werden.

HINWEIS Bei der automatischen Anpassung der Arbeitsspeicherzuweisung wird für den Arbeitsspeicher des lokalen Desktops nie ein niedrigerer Wert als der in vCenter Server konfigurierte Wert festgelegt.

Gleichermaßen kann der lokale View-Desktop bis zu zwei CPUs nutzen, die auf dem Clienthost verfügbar sind, wenn auf dem View-Desktop Windows Vista oder ein höheres Betriebssystem ausgeführt wird.

Sie können die Standardwerte ändern und den Geltungsbereich der Einstellung festlegen. Die Einstellung kann auf alle lokalen Desktops auf dem Client oder, abhängig von der Einstellung, auf einen bestimmten Desktop bzw. auf alle Desktops einer bestimmten View-Verbindungsserver-Instanz angewendet werden, zu deren Verwendung ein spezifischer Benutzer auf dem Client berechtigt ist.

Zum Ändern dieser Standardwerte müssen Sie die Windows-Registrierungseinstellungen konfigurieren. Zur Bereitstellung dieser Registrierungseinstellungen können Sie standardmäßige Windows-Tools wie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) verwenden.

Voraussetzungen

- Wenn Sie eine bestimmte Anzahl an CPUs festlegen möchten, die der lokale Desktop verwenden kann, schalten Sie den lokalen Desktop aus.
- Da Sie den Geltungsbereich der Einstellung in vielen Fällen angeben können, bestimmen Sie die IDs, die Sie festlegen müssen.

Tabelle 6-1. In den Registrierungseinstellungen verwendete IDs für die Ressourcennutzung im lokalen Modus

Geltungsbereich	Bezeichnung der Variablen	Beschreibung
Serverspezifisch	<i>Broker-GUID</i>	GUID (Globally Unique Identifier) für die View-Verbindungsserver-Instanz oder -Gruppe. Legen Sie die GUID über den Befehl <code>vdmadmin -C</code> fest.
Server- und benutzerspezifisch	<i>Remote-Benutzer_SID</i>	Die Sicherheits-ID des Endbenutzers. Verwenden Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Host und suchen Sie nach dem Wert des Felds <code>[pae-SIDString]</code> von <code>[CN=Maschinen-CN,OU=Servers,DC=vdi,DC=vmware,DC=int]</code> .
Server-, benutzer- und desktopspezifisch	<i>Desktop-ID</i>	Die ID des View-Desktops. Verwenden Sie das Dienstprogramm ADSI-Editor auf einem View-Verbindungsserver-Host. Die ID ist in <code>[OU=Applications]</code> von <code>[DC=vdi,DC=vmware,DC=int]</code> aufgeführt. Die Desktop-ID ist der Distinguished Name, der den Anzeigenamen des Desktop-Pools verwendet: <code>[CN=Pool-Anzeigename,OU=Applications,DC=vdi,DC=vmware,DC=int]</code> .

Die Broker-GUID können Sie auch in der Datei `mvd1.lst` auf Ihrem Clientcomputer finden. Unter Windows XP befindet sich die Datei im Ordner `C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\VMware\VDM`. Öffnen Sie die Datei und suchen Sie nach `brokerGUID`. Die Sicherheits-ID des Remote-Benutzers ist ebenfalls in dieser Datei aufgelistet. Öffnen Sie die Datei und suchen Sie nach `user-sid`.

Vorgehensweise

- Um das Standardverhalten außer Kraft zu setzen, sodass der lokale Desktop lediglich die in vCenter Server konfigurierte Arbeitsspeichergröße verwendet, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel hinzuzufügen, und stellen Sie das GPO bereit. Setzen Sie den Schlüssel auf 1.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopMemoryScaleup
Server- und benutzerspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\disableOfflineDesktopMemoryScaleup

Der Wert 1 gibt an, dass `disableOfflineDesktopMemoryScaleup` aktiviert ist, der Wert 0 weist darauf hin, dass die Einstellung deaktiviert ist.

- Um eine bestimmte Arbeitsspeichergröße für den View-Desktop festzulegen, wenn dieser lokal ausgeführt wird, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel zur Angabe eines Werts in MB (bis zu 32 GB) hinzuzufügen, und stellen Sie das GPO bereit.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultMemoryScaleupValue
Serverspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopDefaultMemoryScaleupValue
Server- und benutzerspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\offlineDesktopDefaultMemoryScaleupValue
Server-, benutzer- und desktopspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\Desktop-ID\offlineDesktopDefaultMemoryScaleupValue

Bei Angabe eines zu hohen Werts kann der lokale Desktop nicht eingeschaltet werden und es wird eine Fehlermeldung angezeigt.

- Um einen Desktop auszuwachen, der so konfiguriert wurde, dass er mehr Arbeitsspeicher benötigt als auf dem Clienthost verfügbar ist, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um den folgenden Registrierungsschlüssel zur Angabe eines Werts für die zu berichtende Arbeitsspeichergröße des lokalen Clients in MB hinzuzufügen, und stellen Sie das GPO bereit.

HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue

Die Einstellung dieses Wertes auf größer oder gleich dem vom View-Desktop geforderten Speicher ermöglicht es Ihnen, den View-Desktop auszuwachen und auszuführen, wenn auf dem Client genug Speicher vorhanden ist, um die virtuelle Maschine auszuführen.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue
Serverspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopReportedHostMemoryValue

Geltungsbereich der Einstellung	Pfad
Server- und benutzerspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\offlineDesktopReportedHostMemoryValue
Server-, benutzer- und desktopspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopReportedHostMemoryValue

Wenn der Client nicht über ausreichend Speicher verfügt, können Sie die Einstellung `offlineDesktopDefaultMemoryScaleupValue` in Verbindung mit der Einstellung `offlineDesktopReportedHostMemoryValue` verwenden.

Wenn Ihr Clientsystem z. B. 2 GB Speicher hat und der View-Desktop laut Konfiguration 2 GB Speicher erfordert, können Sie den View-Desktop nicht auschecken, da ein gewisser Anteil des Speichers für vom Client gehostete Virtualisierung notwendig ist. Sie können jedoch die Registrierungseinstellung `offlineDesktopReportedHostMemoryValue = 2048` verwenden, damit Sie den Desktop auschecken können, und die Registrierungseinstellung `offlineDesktopDefaultMemoryScaleupValue = 1024` verwenden, damit der View-Desktop nur 1 GB Speicher verwendet, wenn er lokal ausgeführt wird.

- Um das Standardverhalten außer Kraft zu setzen, sodass der lokale Desktop lediglich die in vCenter Server konfigurierte Anzahl an CPUs verwendet, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel hinzuzufügen, und stellen Sie das GPO bereit. Setzen Sie den Schlüssel auf 1.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopCPUScaleup
Server- und benutzerspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\disableOfflineDesktopCPUScaleup

Der Wert 1 gibt an, dass `disableOfflineDesktopCPUScaleup` aktiviert ist, der Wert 0 weist darauf hin, dass die Einstellung deaktiviert ist.

- Um eine bestimmte Anzahl an CPUs für den View-Desktop festzulegen, wenn dieser lokal ausgeführt wird, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel zur Angabe der Anzahl an CPUs (bis zu 2) hinzuzufügen, und stellen Sie das GPO bereit.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultCPUScaleupValue
Serverspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopDefaultCPUScaleupValue
Server- und benutzerspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\offlineDesktopDefaultCPUScaleupValue
Server-, benutzer- und desktopspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\Broker-GUID\Remote-Benutzer-SID\Desktop-ID\offlineDesktopDefaultCPUScaleupValue

Bei Angabe eines ungültigen Werts wird dieser ignoriert und der Standardwert verwendet. Wenn Sie mehr CPUs festlegen, als auf dem Host verfügbar sind, wird der lokale Desktop nicht gestartet und es wird eine Fehlermeldung angezeigt. Wenn Sie einen höheren Wert als 2 festlegen, wird der Wert 2 verwendet.

Mit Ausnahme der Einstellung, über welche die erforderliche Arbeitsspeichergröße geringer sein darf als der festgelegte Wert in vCenter Server, werden die Einstellungen übernommen, wenn der lokale Desktop gestartet wird. Diese Einstellung ist bei einem ausgecheckten Desktop schreibgeschützt.

Ändern des Netzwerktyps von NAT in Bridged

Der virtuelle Netzwerktyp eines View-Desktops wird standardmäßig in NAT (Network Address Translation) geändert, wenn der Desktop zur Verwendung auf einem lokalen System ausgecheckt wird. Sie können dieses Verhalten außer Kraft setzen und ein Bridged-Netzwerk verwenden, sodass der View-Desktop über eine eigene Netzwerkidentität verfügt.

Bei einem Bridged-Netzwerk wird der virtuelle Netzwerkadapter im View-Desktop mit dem physischen Netzwerkadapter im Hostcomputer verbunden. In einem Bridged-Netzwerk ist der View-Desktop für andere Computer im Netzwerk sichtbar und der Desktop muss über eine eigene IP-Adresse verfügen.

Bei NAT wird eine virtuelle Maschine für die gemeinsame Verwendung der IP- und MAC-Adressen des Hosts konfiguriert. Der View-Desktop und der Clienthost verwenden eine einzige Netzwerkidentität innerhalb des Netzwerks.

Um diese Standardeinstellungen für alle lokalen Desktops oder für bestimmte lokale Desktops auf einem Clienthost zu ändern, müssen Windows-Registrierungseinstellungen konfiguriert werden. Zur Bereitstellung dieser Registrierungseinstellungen können Sie standardmäßige Windows-Tools wie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) verwenden.

Voraussetzungen

- Da Sie den Geltungsbereich der Einstellung in vielen Fällen angeben können, bestimmen Sie die IDs, die Sie festlegen müssen.

Tabelle 6-3. In den Registrierungseinstellungen verwendete IDs für die Ressourcennutzung im lokalen Modus

Geltungsbereich	Bezeichnung der Variablen	Beschreibung
Serverspezifisch	<i>Broker-GUID</i>	GUID (Globally Unique Identifier) für die View-Verbindungsserver-Instanz oder -Gruppe. Legen Sie die GUID über den Befehl <code>vdmadmin -C</code> fest.
Server- und benutzerspezifisch	<i>Remote-Benutzer_SID</i>	Die Sicherheits-ID des Endbenutzers. Verwenden Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Host und suchen Sie nach dem Wert des Felds <code>[pae-SIDString]</code> von <code>[CN=Maschinen-CN,OU=Servers,DC=vdi,DC=vmware,DC=int]</code> .
Server-, benutzer- und desktopspezifisch	<i>Desktop-ID</i>	Die ID des View-Desktops. Verwenden Sie das Dienstprogramm ADSI-Editor auf einem View-Verbindungsserver-Host. Die ID ist in <code>[OU=Applications]</code> von <code>[DC=vdi,DC=vmware,DC=int]</code> aufgeführt. Die Desktop-ID ist der Distinguished Name, der den Anzeigenamen des Desktop-Pools verwendet: <code>[CN=Pool-Anzeigename,OU=Applications,DC=vdi,DC=vmware,DC=int]</code>

Die Broker-GUID können Sie auch in der Datei `mvdi.lst` auf Ihrem Clientcomputer finden. Unter Windows XP befindet sich die Datei im Ordner `C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\VMware\VDM`. Öffnen Sie die Datei und suchen Sie nach `brokerGUID`. Die Sicherheits-ID des Remote-Benutzers ist ebenfalls in dieser Datei aufgelistet. Öffnen Sie die Datei und suchen Sie nach `user-sid`.

Vorgehensweise

- ◆ Um das Standardverhalten außer Kraft zu setzen, sodass der lokale Desktop ein Bridged-Netzwerk verwendet, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel hinzuzufügen, und stellen Sie das GPO bereit. Setzen Sie den Schlüssel auf 1.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopUseBridgedNetworking
Server- und benutzerspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\ <i>Broker-GUID</i> \Remote-Benutzer-SID\offlineDesktopUseBridgedNetworking
Server-, benutzer- und desktopspezifisch	HKCU\Software\VMware, Inc.\VMware VDM\Client\ <i>Broker-GUID</i> \Remote-Benutzer-SID\Desktop-ID\offlineDesktopUseBridgedNetworking

Durch den Wert 1 wird festgelegt, dass der Desktop den Bridged-Netzwerktyp verwendet. Der Wert 0 legt die Verwendung von NAT fest (Standardeinstellung).

Diese Einstellung wird angewendet, wenn der Endbenutzer den lokalen Desktop einschaltet.

Fehlerbehebung für View Client

Sie können die meisten Probleme mit View Client lösen, indem Sie den Desktop zurücksetzen oder die VMware Horizon View Client-Anwendung neu installieren.

Dieses Kapitel behandelt die folgenden Themen:

- [„Vorgehensweise, wenn View Client unerwartet beendet wird“](#), auf Seite 65
- [„Zurücksetzen eines Desktops“](#), auf Seite 65
- [„Deinstallieren von View Client“](#), auf Seite 66

Vorgehensweise, wenn View Client unerwartet beendet wird

View Client wird möglicherweise beendet, selbst wenn Sie die Anwendung nicht schließen.

Problem

View Client wird möglicherweise unerwartet beendet. Abhängig von Ihrer View-Verbindungsserver-Konfiguration kann eine Meldung wie die folgende angezeigt werden: Es besteht keine sichere Verbindung mit View-Verbindungsserver. In manchen Fällen wird jedoch keine Meldung angezeigt.

Ursache

Dieses Problem tritt auf, wenn die Verbindung zu View-Verbindungsserver getrennt wird.

Lösung

- ◆ Starten Sie View Client neu. Sobald View-Verbindungsserver wieder ausgeführt wird, können Sie erfolgreich eine Verbindung herstellen. Sollten weiterhin Probleme mit der Verbindung bestehen, wenden Sie sich an Ihren View-Administrator.

Zurücksetzen eines Desktops

Eventuell muss der Desktop zurückgesetzt werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Beim Zurücksetzen wird der Desktop heruntergefahren und neu gestartet. Nicht gespeicherte Daten gehen verloren.

Das Zurücksetzen eines Desktops entspricht dem Betätigen der Taste „Zurücksetzen“ auf einem physischen Computer, mit der der Neustart des Computers erzwungen wird. Alle Dateien, die auf dem View-Desktop geöffnet sind, werden ohne vorheriges Speichern geschlossen.

Sie können den Desktop nur zurücksetzen, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Vorgehensweise

- ◆ Verwenden Sie den **[Desktop zurücksetzen]**-Befehl.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Wählen Sie [Optionen] > [Desktop zurücksetzen] aus der Menüleiste.
In der Desktop-Auswahlliste	<ul style="list-style-type: none">a Starten Sie View Client, stellen Sie eine Verbindung mit der View-Verbindungsserver-Instanz her, die Zugriff auf den View-Desktop bietet, und geben Sie Ihre Anmeldeinformationen für die Authentifizierung an.b Klicken Sie bei Anzeige der Liste zur Desktop-Auswahl auf den nach unten weisenden Pfeil neben dem Desktop und wählen Sie [Desktop zurücksetzen].

Das Betriebssystem im View-Desktop wird neu gestartet. View Client wird vom Desktop getrennt.

Weiter

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend, eine Verbindung zum View-Desktop herzustellen.

Deinstallieren von View Client

Sie können manche Probleme mit dem View Client lösen, indem Sie die VMware Horizon View Client-Anwendung deinstallieren und anschließend neu installieren.

Die Vorgehensweise beim Deinstallieren von View Client entspricht der Vorgehensweise bei der Deinstallation anderer Anwendungen.

Verwenden Sie beispielsweise das Applet **[Software]** Ihres Windows-Betriebssystems, um die VMware Horizon View Client-Anwendung zu entfernen.

Nachdem Sie die Deinstallation durchgeführt haben, können Sie die Anwendung von neuem installieren.

Siehe [Kapitel 2, „Installation von View Client für Windows“](#), auf Seite 17.

Index

Zahlen

3D-Anwendungen **53**

A

Abmeldung **42**

Adobe Flash-Video, steuern **52**

Anforderungen für Windows 7 und 8, Desktops im lokalen Modus **9**

Anhalten eines Desktops **56**

Anmelden als aktueller Benutzer, Funktion **39**

Anzeigeanforderungen, Desktops im lokalen Modus **9**

Anzeigeprotokolle

Microsoft RDP **45**

View PCoIP **45**

Arbeitsspeichieranforderungen, Desktops im lokalen Modus **9**

automatische Verbindung von USB-Geräten **47**

B

Backup eines Desktops **56**

Betriebssysteme, Unterstützung auf View Agent **11**

Bilder, kopieren **50**

Bridged-Netzwerke für lokale Desktops **62**

Browseranforderungen **12**

C

CAD-Anwendungen **53**

Clientsoftwareanforderungen **7**

CPU-Anforderungen, Desktops im lokalen Modus **9**

D

Deinstallieren von View Client **66**

Desktop

Abmelden **42**

anhalten **56**

Backup **56**

herunterfahren **56**

lokal **55**

reset **65**

wechseln **42**

Desktop zurücksetzen **65**

Desktop-Backup anhalten **56**

Desktop-Backup fortsetzen **56**

Desktop-Backup verschieben **56**

Drucken über einen Desktop **51**

Drucker, einrichten **51**

E

Einchecken eines View-Desktops **57**

Endpunkte, Ressourcennutzung, konfigurieren **58**

F

Firefox, unterstützte Versionen **12**

Funktionsunterstützungs-Matrix **45**

G

Geräten, Verbinden von USB- **47, 49**

H

Hardwareanforderungen

Desktops im lokalen Modus **9**

für Windows-Systeme **7**

Smartcard-Authentifizierung **13**

Herunterfahren eines Desktops **56**

I

Internet Explorer, unterstützte Versionen **12**

L

Lokale Arbeitsspeichernutzung, Außerkraftsetzung **58**

Lokale CPU-Nutzung, Außerkraftsetzung **58**

Lokale Desktops, Konfiguration, Ändern des Netzwerktyps in Bridged **62**

lokaler Desktop **55**

Lokaler Desktop, Konfiguration, Hardwareanforderungen **9**

Lokaler Desktop, Verwendung, Auschecken **55**

M

Maussteuerung in Desktop-Fenster **55**

Mediendateiformate, unterstützte **10**

Menübefehl Strg+Alt+Entf senden **42**

Microsoft Lync-Unterstützung **11**

Microsoft RDP **45**

Microsoft Windows Installer

Befehlszeilenoptionen für die unbeaufsichtigte Installation **25**

Eigenschaften für View Client **23**

Multimedia-Umleitung (MMR) **10**

N

NAT bei lokalen Desktops **62**

Netzwerkkarten **62**

P

PCoIP **45**

Programm zur Verbesserung der Benutzerfreundlichkeit, Desktop-Pool-Daten **14**

R

Registrierung

Einstellungen für den wswc-Befehl **37**

Einstellungen für View Client **37**

relative Maus **53**

Remote-Desktops, Abmelden **55**

Rollback eines View-Desktops **58**

S

Serververbindungen **39**

Sicherheitsserver **13**

Smartcard-Authentifizierung, Anforderungen **13**

SSL-Zertifikate, Überprüfen **32**

steuern, Adobe Flash-Videoanzeige **52**

Streaming von Multimedia **10**

Strg+Alt zur Freigabe des Mauszeigers **55**

Strg+Alt+Entf **42**

Systemanforderungen, für Windows **7**

T

Text, kopieren **50**

Text und Bilder einfügen **50**

Text und Bilder kopieren **50**

Thin Client-Unterstützung **45**

ThinPrint-Einrichtung **51**

Treiber, Installierte Treiber auf Clientsystemen für lokale Desktops **55**

Trennen der Verbindung mit einem View-Desktop **42**

U

Überprüfung des Serverzertifikats **32**

Überprüfungsmodi für die Zertifikatsprüfung **32**

unbeaufsichtigte Installation, View Client **21**

Unbeaufsichtigte Installation

Gruppenrichtlinien zum Zulassen der Installation **21**

View Client **22**

View Client with Local Mode **22**

Unified Communications **11**

UPNs

View Client **39**

View Client with Local Mode **39**

URI-Beispiele **30**

URI-Syntax für View Clients **28**

URIs (Uniform Resource Identifier) **27**

USB-Drucker **51, 52**

USB-Geräte, Verwendung mit View-Desktops **45**

V

Verbinden, USB-Geräte **47, 49**

View Agent, Installationsanforderungen **11**

View Client

Ausführen über die Befehlszeile **34**

Befehlssyntax **34**

Download über View Portal **20**

Fehlerbehebung **65**

Installation auf einem Windows-PC oder -Laptop **17**

Installation über View Portal **19**

Installationsübersicht **17**

Konfiguration von **27**

Konfigurationsdatei **36**

Registrierungseinstellungen **37**

starten **17, 39**

Systemanforderungen für Windows **7**

Trennen der Verbindung mit einem Desktop **42**

Unbeaufsichtigte Installation auf einem Windows-PC oder -Laptop **21, 22**

Unbeaufsichtigte Installation, Eigenschaften **23**

unerwartetes Beenden **65**

View Client with Local Mode, Gruppenrichtlinien für die unbeaufsichtigte Installation **21**

View Portal, Browseranforderungen **12**

View-Desktop

einchecken **57**

Rollback **58**

View-Komponenten, Befehlszeilenoptionen für die unbeaufsichtigte Installation **25**

View-Verbindungsserver **13**

virtuelle Drucker **51**

virtuelle Druckfunktion **45, 51**

virtuelle Profile **45**

VoIP (Voice over IP) **11**

Voraussetzungen für Clientgeräte **13**

W

Webbrowseranforderungen **12**

Wechseln zwischen Desktops **42**

Windows, Installation von View Client auf **7**

Windows-Computer, View Client-Installation **17**

wswc, Befehl

Exitcodes **37**

Konfigurationsdatei **36**
Syntax **34**
Wyse MMR **10, 45**

Z

Zeigersteuerung in Desktop-Fenster **55**
Zertifikate, Ignorieren von Problemen **32**

