

Versionshinweise zu VMware Horizon 7, Version 7.11

Veröffentlicht am 12. Dezember 2019

Diese Versionshinweise behandeln die folgenden Themen:

- [Neuheiten in dieser Version](#)
- [Bevor Sie beginnen](#)
- [Internationalisierung](#)
- [Kompatibilitätshinweise](#)
- [Unterstützte Windows 10-Betriebssysteme](#)
- [Unterstützung für Red Hat Enterprise Linux Workstation](#)
- [Vorgängerversionen von Horizon 7](#)
- [Bekannte Probleme](#)
- [Behobene Probleme](#)

Neuheiten in dieser Version

VMware Horizon 7, Version 7.11, weist die folgenden neuen Funktionen und Verbesserungen auf. Diese Informationen werden nach installierbarer Komponente gruppiert.

- [Produktverbesserungen](#)
- [Horizon Connection Server lokal](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon-GPO-Bundle](#)
- [Horizon Client](#)
- [Horizon 7 Cloud Connector](#)
- [Horizon 7 mit Bereitstellung auf VMware Cloud on AWS](#)

Informationen zu den in dieser Version behobenen Problemen erhalten Sie unter [Behobene Probleme](#).

Produktverbesserungen

VMware Horizon 7, Version 7.11 enthält viele neue Funktionen und Verbesserungen für Horizon Connection Server und den Horizon Agent, einschließlich Fortführung der Funktionsparität von Horizon Console, der HTML5-basierten Webkonsole, die Horizon Administrator irgendwann ersetzt. Dieser wird Anfang 2020 außer Kraft gesetzt.

Horizon Connection Server lokal

- **Horizon Console (HTML5-basierte Webschnittstelle)**
Horizon Console wurde um mehrere Verbesserungen ergänzt. Dazu gehören:
 - Horizon Console ist nun die primäre und empfohlene Webschnittstelle für Horizon 7. Die vorhandene flashbasierte Horizon Administrator-Webschnittstelle wird weiterhin unterstützt, jedoch Anfang 2020 außer Kraft gesetzt. Weitere Informationen finden Sie im Thema [Anmelden bei Horizon Console](#) im Dokument *Verwaltung der VMware Horizon Console*.
 - Das Horizon Help Desk Tool ist jetzt besser sichtbar in die Horizon Console integriert. Klicken

Sie in der Horizon Console auf „Überwachen“ > „Help Desk“, um das Horizon Help Desk Tool zu öffnen. Weitere Informationen finden Sie im Thema [Starten des Horizon Help Desk Tools in der Horizon Console](#) im Dokument *Verwaltung der VMware Horizon Console*.

- Sie können den Benutzernamen und die Kennwortbezeichnungen anpassen, die im Dialogfeld „Anmeldung mit RADIUS-Zwei-Faktor-Authentifizierung“ angezeigt werden. Weitere Informationen finden Sie im Thema [Aktivieren der Zwei-Faktor-Authentifizierung in der Horizon Console](#) im Dokument *Verwaltung der VMware Horizon Console*.
- Sie können globale Client-Einschränkungseinstellungen konfigurieren, um Client-Sitzungsverbindungen auf Desktops und veröffentlichten Anwendungen für nicht unterstützte Horizon Client-Versionen einzuschränken. Weitere Informationen finden Sie im Thema [Globale Client-Einschränkungseinstellungen für Clientsitzungen in der Horizon Console](#) im Dokument *Verwaltung der VMware Horizon Console*.
- Sie können die CPU- und Arbeitsspeichernutzung für jeden Verbindungsserver in der Horizon Console anzeigen. Weitere Informationen finden Sie im Thema [Überwachen des Laststatus von Horizon Connection Servers](#) im Dokument *Verwaltung der VMware Horizon Console*.
- Das Recht „Composer-Desktop-Pool-Image verwalten“ wird in „Verwalten von Wartungsvorgängen auf automatisierten Desktops und Farmen“ umbenannt. Mit diesem Recht können Sie einen Push-Image-Vorgang für einen Instant-Clone-Desktop-Pool oder eine Instant-Clone-Desktop-Farm durchführen. Weitere Informationen finden Sie unter [Objektspezifische Berechtigungen](#) im Dokument *Verwaltung der VMware Horizon Console*.
- Sie können die Namen der veröffentlichten Anwendungen anzeigen, die einer Sitzung zugeordnet sind, wenn Sie die Sitzungsinformationen für eine Farm anzeigen. Weitere Informationen finden Sie im Thema [Verwalten veröffentlichter Desktop- und Anwendungssitzungen in der Horizon Console](#) im Dokument *Verwaltung der VMware Horizon Console*.

• Cloud-Pod-Architektur

- Für Horizon 7 Version 7.11 wurden 12.000 Sitzungen pro Pod validiert:
- Für die Anzeige der globalen Desktopberechtigung, die einen bestimmten Desktop-Pool umfasst, können Sie [Bestandsliste auswählen](#)>Desktops in der Horizon Console. Der Name der globalen Desktop-Berechtigung, die den Desktop-Pool enthält, wird in der Spalte „Globale Berechtigung“ für diesen Desktop-Pool auf der Seite „Desktop-Pools“ angezeigt. Sie können auch auf der Seite „Desktop-Pools“ auf den Namen eines Desktop-Pools klicken und den Namen der globalen Desktop-Berechtigung auf der Registerkarte Übersicht anzeigen.
- Sie können globale Sicherungsberechtigungen konfigurieren. Eine globale Sicherungsberechtigung stellt Remote-Desktops oder veröffentlichte Anwendungen bereit, wenn die primäre globale Berechtigung eine Sitzung aufgrund von Problemen wie unzureichender Poolkapazität oder nicht verfügbarer Pods nicht starten kann. Eine globale Sicherungsberechtigung kann Pools aus jedem Pod im Pod-Verbund enthalten. Weitere Informationen finden Sie im Thema [Implementieren von globalen Sicherungsberechtigungen](#) im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

• Veröffentlichte Desktops und Anwendungen

- Horizon 7 unterstützt Anwendungen der universellen Windows-Plattform (UWP), die auf Windows 10 Virtual Desktop(WVD)-Hosts oder einen Desktop-Pool ausgeführt werden. Weitere Informationen finden Sie im Thema [Remote-Desktop-Diensthubs](#) im Dokument *Einrichten veröffentlichter Desktops und Anwendungen in der Horizon Console*.

• Virtuelle Desktops

- Ein Fortschrittsbalken gibt den ausstehenden Image-Status einer virtuellen Master-Maschine und eines Snapshots an, der zum ersten Mal für einen Instant Clone-Pool veröffentlicht wird.

• True SSO

- Sie können einen externen Identitätsanbieter verwenden, der eine Unified Access Gateway-Appliance mit der True SSO-Funktion verwendet. Weitere Informationen finden Sie im Thema [Einrichten von True SSO](#) im Dokument *Horizon 7-Verwaltung*.

• Lastausgleich

- VMware Avi Networks unterstützt den Lastausgleich für Verbindungsserver, Unified Access Gateway-Appliances und App Volumes Manager.

Horizon Agent for Linux

- **Unterstützte Distributionen**

Horizon Agent for Linux unterstützt jetzt folgende Betriebssysteme für Linux-Remote-Desktops. Weitere Informationen finden Sie im Thema [Systemanforderungen für Horizon 7 for Linux](#) im Dokument *Einrichten von Horizon 7 for Linux-Desktops*.

- RHEL 7.7
- CentOS 7,7
- CentOS 8,0

- **True SSO auf RHEL/CentOS 8-Desktops**

Die True SSO-Funktion wird auf manuellen und automatisierten Full-Clone-Desktops unterstützt, auf denen die RHEL/CentOS 8-Distribution ausgeführt wird. Instant-Clone RHEL 8-Desktops unterstützen True SSO nicht. Weitere Informationen finden Sie im Thema [Konfigurieren von True SSO auf RHEL/CentOS 8-Desktops](#) im Dokument *Einrichten von Horizon 7 for Linux-Desktops*.

Horizon Agent

- **Remoting-Protokolle**

- Mit einem dynamischen Encoder-Switch können Sie zwischen einem für Video optimierten Encoder (H.264 4:2:0 oder H.264 4:4:4) und einem für Text optimierten Encoder (Blast-Codec oder Adaptive) wechseln. Mit diesem Switch erhalten Sie gestochen scharfe Texte und Videos bei geringer Bandbreitennutzung. Weitere Informationen finden Sie im Thema [VMware Blast Extreme](#) im Dokument *Planung der Horizon 7-Architektur*.
- Der HW-Encoder unterstützt mindestens fünf Monitore.
- Ausstehende Mails werden zusammengefasst und in größeren Paketen gesendet, wodurch die Bandbreitennutzung für die Datenübertragung reduziert wird.

- **Remote-Nutzung**

- Administratoren können eine Registrierungsschlüssel-Zeichenfolge verwenden oder die GPO-Einstellung „VMware AppTap-Konfiguration“ für Anwendungen und Prozesse festlegen, sodass die Anwendungen und Prozesse ignoriert werden, die eine Remotesitzung verhindern, wenn sich ein Benutzer von einer Remotesitzung abmeldet. Die GPO-Einstellung wird im Thema [ADMX-Vorlageneinstellungen für die VMware View Agent-Konfiguration](#) im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7* aufgeführt.
- Wenn Sie ein Desktop- oder RDSH-Image für die Verwendung im geschachtelten Modus vorbereiten, können Sie Horizon Agent und Horizon Client in beliebiger Reihenfolge installieren.
- Das Horizon Agent-Installationsprogramm unterstützt LSA-fähige Maschinen. Weitere Informationen finden Sie im Thema [Installieren von Horizon Agent auf einer virtuellen Maschine](#) im Dokument *Einrichten von virtuellen Desktops in Horizon Console*.

Horizon-GPO-Bundle

- Die ADMX-Vorlagendatei für die Konfiguration von VMware View Agent (vdm_agent.admx) enthält die folgenden neuen Einstellungen:
 - Aktivieren der Akkustandsumleitung
 - Aktivieren der UWP-Unterstützung auf RDSH-Plattformen
 - VMware AppTap-Konfiguration
- Die ADMX-Vorlagendatei für die Konfiguration von VMware Horizon Client (vdm_client.admx) enthält die folgenden neuen Einstellungen:
 - Auflösung und DPI-Wert auf Server speichern

Horizon Client

Informationen zu neuen Funktionen in Horizon Client 5.3, einschließlich HTML Access 5.3, finden Sie in den Versionshinweisen auf der Seite [Horizon Clients-Dokumentation](#).

Horizon 7 Cloud Connector

Gilt für Kunden mit universellen VMware Horizon-Lizenzen. Die virtuelle Horizon Cloud Connector-Appliance ist eine erforderliche Komponente für Horizon 7 Version 7.6 und höher, um die Verwaltung von Horizon 7-Pods mithilfe von Horizon Cloud Service zu unterstützen.

Horizon 7 mit Bereitstellung auf VMware Cloud on AWS

Eine Liste der Horizon 7-Funktionen, die von VMware Cloud on AWS unterstützt werden, finden Sie im [VMware-Knowledgebase-Artikel 58539](#).

Bevor Sie beginnen

- **Wichtiger Hinweis zur Installation von VMware View Composer**

Wenn Sie View Composer 7.2 oder höher installieren oder ein Upgrade auf diese Version durchführen möchten, müssen Sie das Microsoft.NET-Framework auf Version 4.6.1 aktualisieren. Andernfalls schlägt die Installation fehl.

- **Wichtiger Hinweis zur Installation von VMware Tools**

Wenn Sie eine von der VMware-Download-Site heruntergeladene Version von VMware Tools und nicht die mit vSphere bereitgestellte Standardversion installieren möchten, müssen Sie prüfen, ob diese VMware Tools-Version unterstützt wird. Dazu wechseln Sie zur [Interoperabilitätstabelle für VMware-Produkte](#), wählen VMware Horizon View und die Version aus und anschließend VMware Tools (nur zum Herunterladen).

- Wenn Sie View Composer unbeaufsichtigt installieren möchten, finden Sie entsprechende Erläuterungen im VMware-Knowledgebase-Artikel 2148204, [Microsoft Windows Installer Command-Line Options for Horizon Composer](#) (Befehlszeilenoptionen des Microsoft Windows-Installationsprogramms für Horizon Composer).
- In dieser Horizon 7-Version gibt es neue Konfigurationsanforderungen, die von einigen früheren Versionen abweichen. Anleitungen zum Upgrade finden Sie im Dokument *Horizon 7-Upgrades*.
- Wenn Sie für eine vor der Version 6.2 installierte Version von Horizon 7 ein Upgrade durchführen möchten und der Verbindungsserver, der Sicherheitsserver oder der View Composer-Server das standardmäßig installierte selbstsignierte Zertifikat verwenden, müssen Sie dieses Zertifikat vor der Durchführung des Upgrades entfernen. Wenn die vorhandenen selbstsignierten Zertifikate bestehen bleiben, funktionieren Verbindungen möglicherweise nicht. Während eines Upgrades ersetzt das Installationsprogramm kein vorhandenes Zertifikat. Mit dem Entfernen des alten selbstsignierten Zertifikats wird sichergestellt, dass ein neues Zertifikat installiert wird. Das selbstsignierte Zertifikat in dieser Version besitzt einen längeren RSA-Schlüssel (2048 Bit statt 1024) und eine stärkere Signatur (SHA-256 mit RSA statt SHA-1 mit RSA) als in Releases vor Version 6.2. Beachten Sie, dass selbstsignierte Zertifikate unsicher sind und so schnell wie möglich durch von einer Zertifizierungsstelle signierte Zertifikate ersetzt werden müssen. Außerdem sollten SHA-1-Zertifikate nicht länger als sicher betrachtet und durch SHA-2-Zertifikate ersetzt werden. Entfernen Sie keine Zertifikate, die von einer Zertifizierungsstelle signiert wurden und die für die Verwendung in der Produktion installiert wurden, wie von VMware empfohlen. Von einer Zertifizierungsstelle signierte Zertifikate funktionieren auch nach dem Upgrade auf dieses Release.
- Nachdem Sie eine Neuinstallation durchgeführt oder alle Verbindungsserver-Instanzen auf Horizon 7 Version 7.2 oder höher aktualisiert haben, können Sie die Verbindungsserver-Instanzen nicht mehr auf eine frühere Version als Horizon 7 Version 7.2 herabstufen, da sich die zum Schutz der LDAP-Daten verwendeten Schlüssel geändert haben. Um die Möglichkeit eines Downgrades der Verbindungsserver-Instanzen beim Planen eines Upgrades auf Horizon 7 Version 7.2 oder höher beizubehalten, müssen Sie eine LDAP-Sicherung vor Beginn des Upgrades durchführen. Wenn Sie ein Downgrade der Verbindungsserver-Instanzen durchführen müssen, müssen Sie alle Verbindungsserver-Instanzen herabstufen und dann die LDAP-Sicherung des letzten herabzustufenden Verbindungsservers anwenden.
- Die Auswahl der Setup-Option für die Scannerumleitung bei der Horizon Agent-Installation kann erhebliche Auswirkungen auf das Host-Konsolidierungsverhältnis haben. Um die optimale Hostkonsolidierung sicherzustellen, sollte die Setup-Option für die Scannerumleitung nur für jene Benutzer ausgewählt werden, die diese Funktion wirklich benötigen. (Die Setup-Option für die Scannerumleitung ist standardmäßig nicht ausgewählt, wenn Sie Horizon Agent installieren.)

Konfigurieren Sie für Benutzer, die die Scannerumleitungsfunktion benötigen, einen separaten Desktop-Pool und wählen Sie die Setup-Option nur in diesem Pool aus.

- Horizon 7 verwendet nur TLSv1.1 und TLSv1.2. Im FIPS-Modus wird nur TLSv1.2 verwendet. Sie können möglicherweise nur durch Anwenden von vSphere-Patches eine Verbindung mit vSphere herstellen. Informationen zum erneuten Aktivieren von TLSv1.0 finden Sie unter [Aktivieren von TLSv1 für vCenter-Verbindungen vom Verbindungsserver](#) und [Aktivieren von TLSv1 für vCenter- und ESXi-Verbindungen von View Composer](#) im Dokument *Horizon 7-Upgrades*.
- Der FIPS-Modus wird in den Versionen vor 6.2 nicht unterstützt. Wenn Sie den FIPS-Modus in Windows aktivieren und für Horizon Composer oder für Horizon Agent ein Upgrade von einer Version vor Horizon View 6.2 auf Horizon 7 Version 7.2 oder höher durchführen, wird die Option für den FIPS-Modus nicht angezeigt. Sie müssen stattdessen für die Installation von Horizon 7 Version 7.2 oder höher im FIPS-Modus eine Neuinstallation durchführen.
- Linux-Desktops verwenden Port 22443 für das VMware Blast-Anzeigeprotokoll.
- Ab Horizon 7 Version 7.2 kann die Reihenfolge von Verschlüsselungs-Suites vom Verbindungsserver erzwungen werden. Weitere Informationen finden Sie im Dokument *Horizon 7-Sicherheit*.
- Ab Horizon 7 Version 7.2 muss der Verbindungsserver mit anderen Verbindungsserver-Instanzen im selben Pod über Port 32111 kommunizieren können. Wenn dieser Datenverkehr während der Installation oder während des Upgrades blockiert wird, wird die Installation nicht erfolgreich abgeschlossen.
- Ab Horizon 7 Version 7.3.2 müssen TLS-Handshakes auf Port 443 innerhalb von 10 Sekunden bzw. bei aktivierter Smartcard-Authentifizierung innerhalb von 100 Sekunden abgeschlossen werden. In früheren Versionen von Horizon 7 mussten TLS-Handshakes auf Port 443 in sämtlichen Situationen innerhalb von 100 Sekunden abgeschlossen werden. Sie können die Zeit für die TLS-Handshakes auf Port 443 mithilfe der Konfigurationseigenschaft `handshakeLifetime` anpassen. Optional kann der Client, der für einen zu lange andauernden TLS-Handshake verantwortlich ist, automatisch auf eine schwarze Liste gesetzt werden. Neue Verbindungen von auf der schwarzen Liste stehenden Clients werden vor ihrer Verarbeitung für einen konfigurierbaren Zeitraum lang verzögert, sodass Verbindungen von anderen Clients Vorrang haben. Sie können diese Funktion mithilfe der Konfigurationseigenschaft `secureHandshakeDelay` aktivieren. Weitere Informationen zum Festlegen von Konfigurationseigenschaften finden Sie im Dokument *Horizon 7-Sicherheit*.
- Wenn die Rolle „Remote-Desktop-Dienste“ nicht vorhanden ist, werden Sie vom Horizon Agent-Installationsprogramm aufgefordert, Horizon Agent im RDS- oder Desktop-Modus zu installieren.

Internationalisierung

Die Horizon Administrator- und Horizon Console-Benutzeroberfläche, die Horizon Administrator- und Horizon Console-Onlinehilfe und die Produktdokumentation zu Horizon 7 sind auf Japanisch, Französisch, Deutsch, Spanisch, Chinesisch (vereinfacht), Chinesisch (traditionell) und Koreanisch verfügbar. Die Dokumentation finden Sie im [Dokumentationscenter für VMware Horizon 7](#).

Kompatibilitätshinweise

- Die unterstützten Gastbetriebssysteme für Horizon Agent auf Einzelbenutzermaschinen und RDS-Hosts finden Sie im VMware Knowledgebase-Artikel 2150295 [Supported Windows Versions for Remote Desktop Systems for Horizon Agent](#) (Unterstützte Windows-Versionen für Remote-Desktop-Systeme für Horizon Agent).
- Wenn Sie Horizon 7-Server mit einer älteren View Agent-Version als 6.2 verwenden, müssen Sie TLSv1.0 für PCoIP-Verbindungen aktivieren. View Agent-Versionen vor View Agent 6.2 unterstützen das Sicherheitsprotokoll TLSv1.0 nur für PCoIP. Bei Horizon 7-Servern, einschließlich Verbindungsserver und Sicherheitsserver, ist TLSv1.0 standardmäßig deaktiviert. Sie können TLSv1.0 für PCoIP-Verbindungen auf diesen Servern mithilfe der im VMware-Knowledgebase-Artikel 2130798 [Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later](#) (Konfigurieren von Sicherheitsprotokollen für Horizon 6 Version 6.2 und höher sowie für Horizon Client 3.5 und höher) dargestellten Anweisungen aktivieren.
- Zu den unterstützten Linux-Gastbetriebssystemen für Horizon Agent finden Sie weitere

Informationen unter [Systemanforderungen für Horizon 7 für Linux](#) im Dokument *Einrichten von Horizon 7 für Linux-Desktops*.

- Informationen zu den unterstützten Betriebssystemen für Verbindungsserver, Sicherheitsserver und View Composer finden Sie unter [Systemanforderungen für Serverkomponenten](#) im Dokument *Horizon 7-Installation*.
- Die Horizon 7-Funktionalität wird durch einen aktualisierten Satz von Horizon Clients verbessert, die in dieser Version enthalten sind. Für VMware Blast Extreme-Verbindungen ist z. B. Horizon Client 4.0 oder höher erforderlich. Auf der Webseite [VMware Horizon Clients-Dokumentation](#) finden Sie Informationen zu unterstützten Horizon Clients.
- Für die Funktion Instant Clones ist vSphere 6.0 Update 1 erforderlich.
- Windows 7 und Windows 10 werden für Instant Clones unterstützt. Das gilt nicht für Windows 8 und Windows 8.1.
- In der [Interoperabilitätstabelle für VMware-Produkte](#) finden Sie weitere Einzelheiten zur Kompatibilität von Horizon 7 mit aktuellen und früheren Versionen von vSphere.
- Informationen zu den unterstützten Domänenfunktionsebenen der Active Directory-Domänendienste (AD DS) finden Sie unter [Vorbereiten von Active Directory](#) im Dokument *Horizon 7-Installation*.
- Informationen zu weiteren Systemanforderungen, beispielsweise unterstützte Browser für Horizon Administrator, finden Sie im Dokument *Horizon 7-Installation*.
- RC4, SSLv3 und TLSv1.0 sind in Horizon 7-Komponenten standardmäßig deaktiviert gemäß RFC 7465, „Prohibiting RC4 Cipher Suites“, RFC 7568, „Deprecating Secure Sockets Layer Version 3.0“, PCI-DSS 3.1, „Payment Card Industry (PCI) Data Security Standard“ und SP800-52r1, „Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations“. Wenn Sie RC4 oder SSLv3 oder TLSv1.0 auf einem Verbindungsserver, Sicherheitsserver, in View Composer oder auf einer Horizon Agent-Maschine wieder aktivieren möchten, lesen Sie [Ältere Protokolle und in View deaktivierte Verschlüsselungen](#) im Dokument *Horizon 7-Sicherheit*.
- Falls ein PCoIP Secure Gateway (PSG) für PCoIP-Verbindungen bereitgestellt wurde, muss Zero-Client-Firmware die Version 4.0 oder höher aufweisen.
- Stellen Sie bei Verwendung der Clientlaufwerksumleitung (Client Drive Redirection, CDR) Horizon Client 3.5 oder höher und View Agent 6.2 oder höher bereit, um sicherzustellen, dass CDR-Daten über einen verschlüsselten virtuellen Channel von einem externen Clientgerät an den PCoIP-Sicherheitsserver und vom Sicherheitsserver an den Remote-Desktop gesendet werden. Wenn Sie frühere Versionen von Horizon Client oder Horizon Agent bereitstellen, werden externe Verbindungen mit dem PCoIP-Sicherheitsserver verschlüsselt, aber innerhalb des Unternehmensnetzwerks werden die Daten ohne Verschlüsselung vom Sicherheitsserver an den Remote-Desktop gesendet. Sie können die Clientlaufwerksumleitung durch Konfiguration einer RDS-Gruppenrichtlinieneinstellung (Microsoft-Remote-Desktop-Dienste) in Active Directory deaktivieren. Weitere Informationen dazu finden Sie unter [Verwalten des Zugriffs auf die Clientlaufwerksumleitung](#) im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.
- Die Setup-Option für die USB-Umleitung im Horizon Agent-Installationsprogramm ist standardmäßig deaktiviert. Sie müssen diese Option auswählen, um die USB-Umleitungsfunktion zu installieren. Anleitungen zur sicheren Verwendung der USB-Umleitung finden Sie unter [Bereitstellen von USB-Geräten in einer sicheren View-Umgebung](#) im Dokument *Horizon 7-Sicherheit*.
- Die globale Richtlinie für die Multimedia-Umleitung (Multimedia Redirection, MMR) ist standardmäßig auf **Verweigern** eingestellt. Um MMR zu nutzen, müssen Sie Horizon Administrator öffnen, die globalen Richtlinien bearbeiten und diesen Wert explizit auf **Zulassen** setzen. Um den Zugriff auf MMR zu steuern, können Sie die MMR-Richtlinie global oder für einzelne Pools oder Benutzer aktivieren bzw. deaktivieren. MMR-Daten (Multimedia Redirection, Multimediaumleitung) werden über das Netzwerk ohne anwendungsbasierte Verschlüsselung gesendet und können sensitive Daten enthalten, abhängig vom umgeleiteten Inhalt. Um sicherzustellen, dass diese Daten nicht auf dem Netzwerk nachverfolgt werden können, sollten Sie MMR nur auf einem sicheren Netzwerk verwenden.
- VMware empfiehlt, dass Sie sich vor der Festlegung des Umfangs der transparenten gemeinsamen Seitennutzung (Transparent Page Sharing, TPS) in Horizon Administrator mit den Auswirkungen auf

die Sicherheit befassen. Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel 2080735 [Sicherheitsüberlegungen und Verweigern der transparenten gemeinsamen Seitennutzung zwischen virtuellen Maschinen](#).

- Um View-Speicherbeschleunigung in vSphere 5.5 oder in einer späteren Umgebung verwenden zu können, muss eine virtuelle Maschine des Desktops 512 GB oder weniger umfassen. View-Speicherbeschleunigung wird auf virtuellen Maschinen, die größer als 512 GB sind, deaktiviert. Die Größe der virtuellen Maschine wird durch die gesamte VMDK-Kapazität festgelegt. Beispielsweise kann eine VMDK-Datei 512 GB groß sein oder eine Reihe von VMDK-Dateien kann zusammen 512 GB umfassen. Diese Anforderung ist auch für virtuelle Maschinen gültig, die in früheren Versionen von vSphere erstellt und auf vSphere 5.5 aktualisiert wurden.
- vSphere Flash Read Cache (früher als „vFlash“ bezeichnet) wird von Horizon 7 nicht unterstützt.
- In Horizon (mit View) Version 6.0 und höheren Releases werden die View PowerCLI-Cmdlets „Get-TerminalServer“, „Add-TerminalServerPool“ und „Update-TerminalServerPool“ als veraltet behandelt.
- Die Bildschirm-DMA-Funktion ist auf virtuellen Maschinen, die in vSphere 6.0 und höher erstellt wurden, standardmäßig deaktiviert. Für View muss die Bildschirm-DMA-Funktion aktiviert sein. Wenn die Bildschirm-DMA-Funktion deaktiviert ist, sehen die Benutzer beim Herstellen einer Verbindung mit dem Remote-Desktop einen schwarzen Bildschirm. Wenn Horizon 7 einen Desktop-Pool bereitstellt, wird die Bildschirm-DMA-Funktion automatisch für alle von vCenter Server verwalteten Maschinen im Pool aktiviert. Wenn Horizon Agent auf einer virtuellen Maschine im nicht verwalteten Modus installiert ist (VDM_VC_MANAGED_AGENT=0), ist die Bildschirm-DMA-Funktion nicht aktiviert. Informationen zum manuellen Aktivieren der Bildschirm-DMA-Funktion finden Sie im VMware-Knowledgebase-Artikel 2144475, [Manuelles Aktivieren der Bildschirm-DMA-Funktion auf einer virtuellen Maschine](#).
- Es werden vGPU-fähige Instant-Clone-Desktop-Pools für vSphere 2016 und höher unterstützt.
- Microsoft Windows Server erfordert einen dynamischen Bereich von Ports, die zwischen allen Verbindungsservern in der Horizon 7-Umgebung geöffnet sind. Microsoft Windows benötigt diese Ports für die herkömmliche Ausführung des Remoteprozeduraufrufs (Remote Procedure Call, RPC) und der Active Directory-Replizierung. Weitere Informationen zum dynamischen Portbereich finden Sie in der Microsoft Windows Server-Dokumentation.
- In Horizon 7 Version 7.2 oder höher verfügt das Tool ViewDBChk über keinen Zugriff auf vCenter- oder View Composer-Anmeldedaten und fordert diese Informationen bei Bedarf an.
- Die Regeln für die Weiterleitung von HTTP-Anforderungen, die von Verbindungsserver-Instanzen und Sicherheitsservern empfangen werden, wurden in dieser Version geändert. Wenn Sie benutzerdefinierte `frontMapping`-Einträge in `locked.properties` definiert haben, sollten Sie sie vor dem Upgrade entfernen. Wenn Sie Administrator-Verbindungen zu bestimmten Verbindungsserver-Instanzen als nicht zulässig festlegen möchten, definieren Sie keine benutzerdefinierten `frontMapping`-Einträge, sondern fügen Sie den folgenden Eintrag zu `locked.properties` hinzu:
`frontServiceWhitelist = tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot`

Auf Sicherheitsservern wird dieser Eintrag automatisch angewendet und muss nicht in `locked.properties` festgelegt werden.

- Horizon Persona Management ist nicht mit durch Benutzer beschreibbaren Volumes kompatibel, die mit der „UIA + Profil“-Vorlage erstellt wurden.
- In Horizon 7-Version 7.0.3 oder höher bestimmen interne Validierungsprüfungen, ob die Instant-Clone- und interne Vorlage über gültige IP-Adressen und eine Netzwerkverbindung verfügen. Wenn eine virtuelle Maschine über eine Netzwerkkarte (NIC) verfügt, der während des Provisioning keine IP-Adresse zugewiesen werden kann, schlägt das Instant-Clone-Provisioning fehl.
- Informationen zu den Modellen von NVIDIA GPU-Karten, die von Horizon 7 unterstützt werden, finden Sie unter <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.
- AMD v340-Grafikkarten werden unterstützt.
- Echtzeit-Audio und -Video (RTAV) wird in einer IPv6-Umgebung unterstützt.
- In der [Interoperabilitätstabelle für VMware-Produkte](#) finden Sie Informationen zur Kompatibilität von Horizon 7 mit den neuesten Versionen von VMware Unified Access Gateway, VMware Identity Manager, VMware App Volumes, VMware User Environment Manager und VMware Tools.

- JMP Server unterstützt VMware App Volumes 2.14 oder höher, aber nicht App Volumes 4.0. Um JMP Server zu verwenden, müssen Sie App Volumes ab 2.xx-Version 2.14 oder höher installieren.
- Bei VMware Cloud on AWS sind Instant-Clone-Desktop-Pools und Desktop-Pools mit vollständigen virtuellen Maschinen aufgrund einer NSX-t-Beschränkung für logische Switches auf 1.000 Desktops beschränkt.
- PCoIP wird für RDSH-Instant-Clone-Pools in einer IPv6-Umgebung nicht unterstützt. PCoIP wird für Remote-Desktops in einer IPv6-Umgebung unterstützt.
- Ab Version 18.2.7 unterstützt Avi Networks (VMware NSX Advanced Load Balancer) den Load Balancer für Verbindungsserver, Unified Access Gateway-Appliances und App Volumes Manager.

Unterstützte Windows 10-Betriebssysteme

Eine aktualisierte Liste der unterstützten Windows 10-Betriebssysteme finden Sie im VMware-Knowledgebase-Artikel 2149393, [Supported Versions of Windows 10 on Horizon View](#) (Unterstützte Versionen von Windows 10 auf Horizon 7).

Weitere Informationen zu den Upgrade-Anforderungen für Windows 10-Betriebssysteme erhalten Sie im VMware-Knowledgebase-Artikel 2148176, [Upgrade Requirements for Windows 10 Operating Systems](#) (Upgrade-Anforderungen für Windows 10-Betriebssysteme).

Unterstützung für Red Hat Enterprise Linux Workstation

Horizon Agent for Linux unterstützt die Installation auf Systemen, auf denen Red Hat Enterprise Linux Workstation ausgeführt wird. Red Hat Enterprise Linux Server wird nicht unterstützt.

Im Dokument [Einrichten von Horizon 7 for Linux-Desktops](#) beziehen sich alle Vorkommen von „Red Hat Enterprise Linux“ und „RHEL“ nur auf Red Hat Enterprise Linux Workstation.

Eine Liste der unterstützten Versionen von Red Hat Enterprise Linux Workstation finden Sie unter [Systemanforderungen für Horizon 7 for Linux](#).

Vorgängerversionen von Horizon 7

Funktionen aus Vorgängerversionen werden zusammen mit bekannten Problemen in den Versionshinweisen zur jeweiligen Version erläutert.

Behobene Probleme

- 1864296: Eine GSSAPI_ERROR-Meldung wird angezeigt, wenn Sie sich anfänglich mit Benutzername und Kennwort angemeldet haben, versuchen, eine rekursive Entsperrung mithilfe der Smartcard-Authentifizierung für die Anmeldung bei einem lokalen Computer mit aktivierter Gruppenrichtlinieneinstellung „Remotesitzungen entsperren, wenn der Clientcomputer entsperrt wird“ durchzuführen, und sich dann von Horizon Client aus als aktueller Benutzer anmelden.
- 2260206: Windows-VM wird nicht heruntergefahren, weil kein Callback-Aufruf zum Entladen des Treibers an Persona gesendet wurde.
- 2344754: Bei der Synchronisierung von Persona Management tritt aufgrund der Verweigerungsberechtigung bei jeder Replikationsintervallzeit ein Fehler auf.
- 2373674: Wenn sich ein Benutzer bei einem Remote-Desktop mit aktivierter Deep Security anmeldet, hängt die Maschine, wenn Persona große Dateien kopiert.
- 2414242: Wenn Deep Security aktiviert ist, können Dateien, die aus der Dateifreigabe auf die lokale Festplatte kopiert wurden, nicht gelöscht werden.

- 2403057: BSOD REGISTRY_FILTER_DRIVER_EXCEPTION (135) tritt bei der Kombination von Persona und Deep Security auf.
- 2373808: Bei der Installation von Adobe Acrobat Reader stürzte die Windows-Maschine mit aktiviertem Persona mit BSOD (BugCheck 3B) ab.
- 2403061: Das Synchronisieren von Benutzerprofilen funktioniert nicht ordnungsgemäß für Dokumente, die mit dem japanischen Textverarbeitungsprogramm Ichitaro verfasst wurden.
- 2292092: Wenn sich der Desktop im Abmeldevorgang befindet, können sich Benutzer, die sich bereits abgemeldet haben, bei demselben Desktop anmelden.
- 2412281: Bei Verbindung mit einem veröffentlichten Windows 2016-Desktop mithilfe von Blast oder PCoIP können Benutzer die Einstellung „Desktop-Sprachleiste verwenden, wenn sie verfügbar ist“ nicht speichern.

Bekannte Probleme

Die bekannten Probleme werden in folgende Kategorien unterteilt:

- [Horizon Persona Management](#)
- [View Composer](#)
- [Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon-GPO-Bundle](#)
- [Horizon Client](#)
- [Horizon JMP Server und JMP Integrated Workflow](#)
- [Horizon Cloud Connector](#)

Horizon Persona Management

- Nach jeder Anmeldung benötigt Persona-Verwaltung eine gewisse Zeit, um die erste Benutzer-Persona auf einem Gastbetriebssystem zu replizieren, das die Version „v6“ des Benutzerprofils verwendet.
- Wenn Sie sich bei einer Windows 10-LTSB-Maschine mithilfe eines Persona-Profiles anmelden und versuchen über den Schnellzugriff (z. B. „Downloads“ oder „Dokumente“) auf umgeleitete Ordner zuzugreifen, erhalten Sie diese Fehlermeldung:

C:\Users\vdiuser7\Downloads ist nicht verfügbar. Microsoft stellt die Programmierschnittstelle (API) zum Hinzufügen eines Ordners oder einer Datei zum Schnellzugriff nicht bereit.

Problemumgehung: Keine

- Wenn Sie sich zum zweiten Mal bei einer mit Persona-Verwaltung konfigurierten VM anmelden, stürzt der Microsoft Edge-Browser ab und eine Fehlermeldung wird angezeigt, die besagt, dass die OneDrive-Anwendung noch nie verwendet wurde. Darüber hinaus können die Dateien und Ordner nicht ordnungsgemäß repliziert werden. Dieses Problem tritt bei Windows 10 Build 1703 und höher auf.
Problemumgehung: Deaktivieren Sie die Persona-Verwaltung-Einstellung **Ordner mit den lokalen Einstellungen auf dem Server speichern**. Wenn Sie diese Einstellung deaktivieren, funktioniert der Microsoft Edge-Browser ordnungsgemäß, doch die OneDrive-Anwendung ist nur verfügbar, wenn Sie sich zum ersten Mal anmelden.
- Offline-Symbole werden nicht für Dateien auf einer virtuellen Windows Server 2012-Maschine angezeigt, wenn die Horizon Persona Management-Einstellung aktiviert ist.
Problemumgehung: Keine bekannt.

- Nach einer erfolgreichen ersten Anmeldung an einer virtuellen Maschine mit installiertem Horizon Agent auf einem CBB-System unter Windows 10 Version 1703 und mit aktivierter Persona-Verwaltung wird die Fehlermeldung „OneDrive – Fehlerhaftes Bild“ während aufeinanderfolgenden Anmeldeversuchen angezeigt.

Problemumgehung: Verwenden Sie OneDrive nicht auf Ihrem CBB-System unter Windows 10 Version 1703. Deaktivieren Sie im Gruppenrichtlinienverwaltungs-Editor die Einstellung „Ordner mit den lokalen Einstellungen auf dem Server speichern“ im Ordner

Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > Persona-Verwaltung > Serverspeicherung und Synchronisierung.

View Composer

- Wenn Sie das View Composer-Installationsprogramm auf Windows Server 2016 mit dem neuesten Windows-Update von der Befehlszeile aus ausführen, erhalten Sie einen Microsoft .NET 4.6-Framework-Fehler. Dieses Problem tritt auf, weil das CLI-Installationsprogramm die neueste Version von Microsoft .NET 4.7 nicht erkennt.
Problemumgehung: Verwenden Sie die Benutzeroberfläche des View Composer-Installationsprogramms zum Ausführen des Installationsprogramms.
- Die Erstellung oder Neuzusammenstellung von Desktop-Pools ist nicht möglich, nachdem Sie für die übergeordnete virtuelle Maschine ein Upgrade von Build 1511 auf Build 1607 des Betriebssystems Windows 10 durchgeführt haben. Build 1607 stellt das Betriebssystem Windows 10 Anniversary Update dar.
Problemumgehung:
 - Option 1: Führen Sie eine neue Installation von Windows 10 Build 1607 auf der übergeordneten virtuellen Maschine durch.
 - Option 2: Wählen Sie im Assistenten zur Erstellung eines Desktop-Pools nicht die Option „Löschbare Dateien nicht umleiten“ aus.
- Verbindung zu View Composer schlägt fehl, wenn Sie den folgenden Befehl ausführen:
viewdbchk.cmd – findMachine
Problemumgehung: Importieren Sie das selbstsignierte Zertifikat für View Composer in den Keystore des Verbindungsservers oder verwenden Sie ein benutzerdefiniertes CA-Zertifikat.
- Aufgrund von Änderungen, die vor Kurzem im Rahmen eines Upgrades von Horizon 7 auf Version 7.5 am Dienstprogramm für die Gastanpassung von vSphere 6.7 vorgenommen wurden, können Sie View Composer 7.5 nicht mit einer früheren Version von Horizon Agent für die Bereitstellung und Neuzusammenstellung von Linked-Clone-Pools mit der Sysprep-Anpassungsmethode verwenden. Die Linked-Clone-Desktops und -Farmen verbleiben während der Bereitstellungs- oder Neuzusammenstellungsvorgänge auf unbestimmte Zeit im Zustand „Anpassung“.
Problemumgehung: Führen Sie ein Upgrade auf die neueste Version von VMware Tools sowie für Horizon Agent ein Upgrade auf Version 7.5 auf der übergeordneten virtuellen Maschine durch. Erstellen Sie einen Snapshot von der übergeordneten virtuellen Maschine, für die Sie das Upgrade durchgeführt haben. Stellen Sie Linked-Clone-Desktop-Pools dann mit der Sysprep-Anpassungsmethode auf vSphere 6.7 bereit oder stellen Sie diese neu zusammen.
- Linked Clones verbleiben im Status „Wird angepasst“ in Win2k12 Standard- und Datacenter-Versionen.
Problemumgehung: Weitere Informationen zum Beheben des Problems finden Sie im VMware-KB-Artikel <https://kb.vmware.com/s/article/57348>.

Horizon Connection Server

- Wenn während der Bereitstellung eines Instant-Clone-Desktop-Pools nicht genügend Speicherplatz auf den Datenspeichern verfügbar ist, wird in Horizon Administrator eine Fehlermeldung wie „Klonen von VM <VM-Name> ist fehlgeschlagen – VC_FAULT_FATAL: Fehler beim Erweitern der Auslagerungsdatei von 0 KB auf 2.097.152 KB.“ angezeigt. Diese Fehlermeldung gibt die Hauptursache des Problems nicht eindeutig an.

Problemumgehung: Nicht erforderlich.

- Wenn Sie in Horizon Administrator **Katalog > Desktop-Pools** aufrufen, auf einen Instant-Clone Desktop-Pool doppelklicken, die Registerkarte **Bestand** öffnen und auf **Maschinen (Instant Clone-Details)** klicken, werden Details der Instant Clones im Fenster angezeigt. In der Spalte für den Datenspeicher der Betriebssystemfestplatte sind jedoch keine Informationen enthalten.

Problemumgehung: Keine

- In einer umfangreichen Umgebung gilt für einige Desktops in einem Instant-Clone-Desktop-Pool eventuell der Status „Ungültige IP“.

Problemumgehung: Wechseln Sie in Horizon Administrator zu **Poolbestand**, wählen Sie die Desktops mit dem Status **Ungültige IP** aus und klicken Sie auf **Wiederherstellen**.

- Wenn Sie eine virtuelle Maschine neu starten oder zurücksetzen, für die eine Endbenutzersitzung in einem Desktop-Pool des vCenter Server oder des Windows-Betriebssystemmenüs vorhanden ist, wird diese zwar gestartet, der Status der virtuellen Maschine wird aber in Horizon Administrator eventuell als „Bereits verwendet“ angezeigt.

Dieses Problem kann für folgende Pooltypen auftreten:

- Instant-Clone-Desktop-Pools.
- Dynamische Linked-Clone-Desktop-Pools mit aktivierter Einstellung „Delete on log Off“ (Beim Abmelden löschen)
- Dynamische Linked-Clone-Desktop-Pools mit aktivierter Einstellung „Refresh on log Off“ (Beim Abmelden aktualisieren)
- Dynamische Full-Clone-Desktop-Pools mit aktivierter Einstellung „Delete on log Off“ (Beim Abmelden löschen)

Problemumgehung: Starten Sie mit Horizon Administrator oder Horizon Client die virtuelle Maschine im Instant-Clone-Desktop-Pool erneut oder setzen Sie sie zurück. Wenn die virtuelle Maschine bereits den Status „Bereits verwendet“ aufweist, entfernen Sie die virtuelle Maschine. Mit dieser Aktion wird automatisch eine neue virtuelle Maschine auf der Basis der Bereitstellungseinstellungen des Pools erstellt.

- Wenn Sie Instant Clones auf lokalen Datenspeichern bereitstellen, können die entsprechenden Hosts nicht in den Wartungsmodus versetzt werden. Dies tritt auf, weil die internen VMs und die Instant Clones in lokalen Datenspeichern gespeichert sind, sodass diese nicht migriert werden können.

Problemumgehung: Löschen Sie die Instant-Clone-Desktop-Pools. Dadurch werden die zugehörigen virtuellen Maschinen gelöscht, und die entsprechenden Hosts können in den Wartungsmodus versetzt werden.

- Eine ESXi-Hostwartung, die VUM verwendet, kann nicht durchgeführt werden, wenn die übergeordnete VM des Instant Clone auf dem Host eingeschaltet ist.

Problemumgehung: Weitere Informationen dazu finden Sie im VMware Knowledgebase-Artikel 2144808 [Entering and exiting maintenance mode for an ESXi host that has Horizon instant clones](#) (Aufrufen und Beenden des Wartungsmodus für einen ESXi-Host mit Horizon-Instant-Clones).

- Anwendungen der universellen Windows-Plattform (UWP) werden auf RDS-Hosts mit Windows Server 2016 und Windows Server 2019 nicht als veröffentlichte Anwendungen unterstützt.
- Für True SSO wird der Konnektivitätsstatus zwischen der Verbindungsserver-Instanz und dem Registrierungsserver nur auf dem Systemzustand-Dashboard für den Verbindungsserver angezeigt, mit dem Sie auf Horizon Administrator zugreifen. Wenn Sie z. B.

<https://server1.example.com/admin> für Horizon Administrator verwenden, wird der Konnektivitätsstatus des Registrierungsservers nur für den Verbindungsserver

server1.example.com erfasst. Es werden eine oder beide der folgenden Meldungen angezeigt:

- Mit dem primären Registrierungsserver kann zur Verwaltung von Sitzungen auf diesem Verbindungsserver kein Kontakt aufgenommen werden.
- Mit dem sekundären Registrierungsserver kann zur Verwaltung von Sitzungen auf diesem Verbindungsserver kein Kontakt aufgenommen werden.

Ein Registrierungsserver muss als primärer Server konfiguriert werden. Optional kann ein sekundärer Registrierungsserver konfiguriert werden. Wenn nur ein Registrierungsserver vorhanden ist, wird nur die erste Meldung bei einem Fehler angezeigt. Ist sowohl ein primärer als auch ein sekundärer Registrierungsserver vorhanden und bei beiden bestehen

Konnektivitätsprobleme, erscheinen beide Meldungen.

- Wenn Sie True SSO in einer Umgebung mit CAs und SubCAs mit jeweils unterschiedlichen Vorlagen einrichten, können Sie True SSO mit einer Kombination einer Vorlage eines CA oder SubCA mit einem anderen CA oder SubCA konfigurieren. Der True SSO-Status wird daraufhin im Dashboard möglicherweise grün angezeigt. Es tritt jedoch ein Fehler auf, wenn Sie versuchen, True SSO zu verwenden.

- Im Horizon Help Desk Tool wird der Pod-Name nicht angezeigt, wenn die lokale Sitzung oder eine Sitzung im lokalen Pod ausgeführt wird.

Problemumgehung: Richten Sie die Cloud-Pod-Architektur-Umgebung ein, um die Pod-Namen im Horizon Help Desk Tool anzuzeigen.

- Die Einstellung für den Workspace ONE-Modus wird nicht für den Replikatserver von Workspace ONE übernommen.

Problemumgehung: Konfigurieren Sie den Workspace ONE-Modus im Verbindungsserver.

- Für das Erstellen von Full-Clone-Desktop-Pools werden manchmal falsche Vorlagen dargestellt. Die gültigen Vorlagen werden aufgrund eines Cache-Problems nicht angezeigt.

Problemumgehung: Starten Sie den Verbindungsserver neu.

- Wenn Sie versuchen, einen SAML-Authentifikator in Horizon Administrator hinzuzufügen, wird die Schaltfläche **Hinzufügen** auf der Seite „SAML-Authentifikatoren verwalten“ deaktiviert.

Problemumgehung: Melden Sie sich bei Horizon Administrator als Benutzer mit der Administrator- oder lokalen Administratorrolle an.

- In einer Cloud-Pod-Architektur-Umgebung werden mit globalen Anwendungsberechtigungen vorab gestartete Sitzungssitzungen nicht in **Bestandsliste > Sitzungen** suchen in Horizon Administrator angezeigt.

Problemumgehung: Melden Sie sich bei der Horizon Administrator-Benutzeroberfläche für eine Verbindungsserver-Instanz in dem Host-Pod an und wählen Sie **Überwachung > Ereignisse**, um vorab gestartete Sitzungsinformationen anzuzeigen.

- Bei Benutzern, die 20 bis 50 globalen Anwendungsberechtigungen der Cloud-Pod-Architektur zugewiesen sind, kommt es bei der Authentifizierung bei Horizon 7 zu einer Verzögerung von 20 bis 30 Sekunden, wenn eine Verbindung über eine beliebige Version von Horizon Client hergestellt wird.

Hinweis: In Horizon 7 Version 7.2 fällt diese Verzögerung etwas geringer aus.

Problemumgehung: Keine.

- Für Intel vDGA werden nur die integrierten Intel-GPUs der Serien Haswell und Broadwell unterstützt. Die integrierten Broadwell-GPUs werden nur für vSphere 6 Update 1b und höher unterstützt. Die integrierten Haswell-GPUs werden nur für vSphere 5.5 und höher unterstützt. Die GPU muss im BIOS aktiviert werden, damit sie von ESXi erkannt wird. Weitere Informationen finden Sie in der Dokumentation Ihres spezifischen ESXi-Hosts. Intel empfiehlt, für die Einstellungen des Grafikspeichers im BIOS die Standardwerte zu übernehmen. Wenn Sie diese Einstellungen ändern, lassen Sie den Standardwert (256M) für die Blendeneinstellung unverändert.

- Die Bereitstellung von virtuellen Maschinen auf der Basis von View Composer-Desktop-Pools, die für die Verwendung von NVIDIA GRID vGPU konfiguriert wurden, kann mit folgender Fehlermeldung nicht durchgeführt werden: Die im übergeordneten Ressourcenpool verfügbaren Grafikressourcen sind für diesen Vorgang nicht ausreichend.

Problemumgehung: Verwenden Sie ein einziges vGPU-Profil für alle virtuellen Desktops, die für das 3D-Rendering in einem Cluster konfiguriert wurden.

- Bei vCenter Server 6.0 U3 oder höher, einschließlich vCenter Server 6.5, migrieren interne übergeordnete virtuelle Maschinen beim Fehlschlagen auf einen anderen Host. Diese Migration führt zu einem Problem, da sich auf dem Zielhost nicht benötigte übergeordnete virtuelle Maschinen befinden.

Problemumgehung: Entfernen Sie diese übergeordneten virtuellen Maschinen manuell. Weitere Informationen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

- Um die Wahrscheinlichkeit eines Mangels an Arbeitsspeicher zu verringern, unterstützen vGPU-Profile mit jeweils 512 MB oder weniger Bildspeicher nur ein virtuelles Anzeigegerät auf einem Windows 10-Gastbetriebssystem.

Die folgenden vGPU-Profile verfügen über 512 MB oder weniger Bildspeicher:

- Tesla M6-OB, M6-OQ
- Tesla M10-OB, M10-OQ
- Tesla M60-OB, M60-OQ
- GRID K100, K120Q
- GRID K200, K220Q

Problemumgehung: Verwenden Sie ein Profil, das mehr als ein virtuelles Anzeigegerät unterstützt und über mindestens 1 GB Bildspeicher verfügt.

- Veröffentlichte Desktops und Anwendungspools können nicht gestartet werden, wenn die Funktion für die Clienteinschränkung aktiviert ist und sie eine Berechtigung für eine Domäne haben, die mit einer Ein-Weg-AD-Vertrauensstellung konfiguriert ist.

Problemumgehung: Keine

- Nach einem Upgrade wird die Option zum Hinzufügen einer Farm abgeblendet dargestellt, wenn Sie über eine Rolle mit der Berechtigung „Farmen, Desktop- und Anwendungspools verwalten“ verfügen (objektspezifische Berechtigung).

Problemumgehung: Bearbeiten Sie die Rolle oder erstellen Sie sie erneut mit der Berechtigung „Farmen, Desktop- und Anwendungspools verwalten“. Dabei wird auch die Berechtigung „Globale Konfiguration und Globale Richtlinien verwalten“ hinzugefügt.

- Nach einem Upgrade werden die Lesezeichen nicht in Workspace ONE angezeigt.

Problemumgehung: Fügen Sie die Lesezeichen aus dem Katalog in Workspace ONE erneut hinzu.

- Wenn Sie das Netzkabel entfernen und wieder anschließen und auf dem Clientcomputer auf „Verbindung trennen und abmelden“ klicken, trennt der Remote-Desktop die Verbindung nicht und es erfolgt keine Abmeldung.

Problemumgehung: Schließen Sie das Fenster des Remote-Desktops und beenden Sie die Remote-Sitzung manuell.

- In Horizon Administrator werden beim Schritt „Bereit zum Abschließen“ die Werte für viele Felder nicht angezeigt, während der Klonvorgang für einen automatisierten Pool mit vollständigen virtuellen Maschinen ausgeführt wird. Der Klonvorgang ist jedoch erfolgreich.

Problemumgehung: Keine.

- Bei der Erstellung verknüpfter und vollständiger Klone mit der Sysprep-Anpassungsmethode treten auf Windows 10-Gastbetriebssystemen möglicherweise Fehler bei der Anpassung und beim Domänenbeitritt auf.

Problemumgehung: Dies geschieht aufgrund eines Problems Microsoft Windows. Um dieses Problem zu beheben, befolgen Sie die Schritte im Microsoft Knowledge Base-Artikel: <https://support.microsoft.com/en-us/help/2769827>.

- Sie können keinen Linked-Clone-Desktop-Pool bzw. keine Farm in Horizon Console erstellen, wenn keine Horizon 7-Lizenz konfiguriert ist.

Problemumgehung: Verwenden Sie Horizon Administrator zur Erstellung eines Linked-Clone-Desktop-Pools oder einer Farm ohne Horizon 7-Lizenz.

- Bei der Anmeldung bei der Horizon Console im Internet Explorer-Browser werden anstelle von Symbolen nur Schlüsselwörter angezeigt. Dieses Problem tritt auf, wenn Sie eine Verbindung zu einem Verbindungs- oder Sicherheitsserver mit einer IP-Adresse anstelle eines DNS-Namens herstellen.
Problemumgehung: Verwenden Sie beim Herstellen einer Verbindung einen DNS-Namen anstelle einer IP-Adresse. Weitere Informationen finden Sie im VMware-KB-Artikel <https://kb.vmware.com/s/article/2150307>.
- Wenn Sie die Safari-Version 10.1.1 als Webbrowser für die Anmeldung bei der Horizon Console mit einem vollqualifizierten Domännennamen verwenden, können Schnittstellenprobleme wie eine leere Anzeige in den unteren Fensterbereichen auftreten.
Problemumgehung: Die Safari-Version 10.1.1 ist keine unterstützte Webbrowserversion für die Horizon Console. Verwenden Sie eine Safari-Version vor 10.1.1 oder 11.0.2 und höher, um sich bei der Horizon Console anzumelden.
- Folgende Schnittstellenprobleme treten im Horizon Help Desk Tool für globale Linux-Sitzungen in einer Cloud-Pod-Architekturbereitstellung auf:
 - Eine Meldung zu einem internen Fehler wird angezeigt, der Skype for Business-Status wird nicht angezeigt und die Betriebssystemversion wird als „-“ angezeigt, wenn Sie auf die Sitzungsdetails auf der Registerkarte „Details“ klicken.
 - Wenn Sie auf die Remotehilfe klicken, wird die Meldung „Fehler beim Abrufen des Remotehilfe-Tickets“ angezeigt.
 - Eine Meldung zu einem internen Fehler wird angezeigt, wenn Sie auf die Registerkarte „Anwendungen“ klicken.**Problemumgehung:** Keine. Folgende Schnittstellenfunktionen für Linux-Desktops werden nicht von Horizon-Helpdesk unterstützt: Skype for Business-Status, Remotehilfe, Registerkarte „Anwendungen“ und Status „Sitzung im Leerlauf“.
- Horizon Administrator aktualisiert die Informationen für die Rückforderung von Speicherplatz für einen vCenter Server auf der vSphere-Version 6.7 nicht, der VMFS6 mit der automatischen UNMAP-Funktion verwendet.
Problemumgehung: Keine.
- Nach einem Upgrade auf Horizon 7-Version 7.5 kann nur für den ersten Verbindungsserver, der installiert wurde, eine Verbindung mit dem Registrierungsserver hergestellt werden.
Problemumgehung: Beenden Sie den Horizon Connection Server-Dienst, entfernen Sie Zertifikate mit dem Anzeigenamen „vdm.ec“ aus dem VMware Horizon View-Zertifikatsspeicher und starten Sie den Horizon Connection Server-Dienst neu.
- Single Sign-on funktioniert nicht, wenn Sie in einer Registerkarte der Horizon Console mit Zeitüberschreitung auf Horizon Administrator zugreifen und dann über Horizon Administrator auf den Horizon Console-Link klicken.
Problemumgehung: Löschen Sie die Websitedaten im Browser und starten Sie ihn neu.
- Die Anmeldung bei der Horizon Console schlägt fehl, wenn Sie für die Anmeldung bei der Horizon Console mit einem Firefox-, Google Chrome-, Microsoft Edge- oder Safari-Webbrowser die IP-Adresse verwenden.
Problemumgehung: Verwenden Sie den vollqualifizierten Domännennamen (FQDN für englisch Fully Qualified Domain Name) für die Anmeldung bei der Horizon Console. Weitere Informationen zur Verwendung des FQDN für die Anmeldung bei Webanwendungen finden Sie im Dokument *Horizon 7-Sicherheit*.
- Horizon Administrator zeigt in der Spalte mit dem Benutzernamen auf der Seite „Benutzer und Gruppen“ für folgende Benutzer Null/Null an: Kontobetreiber, Incoming Forest Trust-Ersteller, Terminal Server-Lizenzserver, Zugriffsgruppe für Windows-Autorisierung, Serverbetreiber und kompatibler Zugriff vor Windows 2000.
Problemumgehung: Keine.

- Nach einem Upgrade auf vSphere 6.7 können Sie die benutzerdefinierten Spezifikation, die mit einer vSphere-Version vor 6.7 erstellt wurde, nicht verwenden.
Problemumgehung: Erstellen Sie nach einem Upgrade auf vSphere 6.7 eine neue benutzerdefinierte Spezifikation und verwenden Sie diese für das Pool-Provisioning.
- Das Horizon Help Desk Tool zeigt die Anmeldezeit sowohl für den Brokering- als auch den Hosting-Pod an, jedoch nicht für einen Pod, der weder Brokering- noch Hosting-Pod ist. Das Horizon Help Desk Tool zeigt die Anmeldezeit nach einigen Minuten für den Hosting-Pod an, wenn der Brokering-Pod ein Remote-Pod ist.
Problemumgehung: Wenn das Horizon Help Desk Tool die Anmeldezeit für den Hosting-Pod nicht anzeigt, schließen Sie die Seite mit den Sitzungsdetails, warten Sie 7–8 Minuten und navigieren Sie zur Registerkarte „Details“, um die Sitzungsdetails erneut anzuzeigen.
- VMware Identity Manager kann Desktops manchmal nicht starten. Wenn Sie SAML-Konfigurationsdetails zum ersten Mal in VMware Identity Manager mit auf dem Verbindungsserver aktiviertem SAML speichern, können Desktops nicht gestartet werden.
Problemumgehung: Speichern Sie das Profil erneut und führen Sie einen Synchronisierungsvorgang für das neue Profil aus. Der Synchronisierungsvorgang kann jede Stunde oder jeden Tag ausgeführt werden, je nach Einstellung vom Administrator.
- Horizon Administrator zeigt in Chrome im Inkognito-Modus eine Fehlermeldung an, wenn Sie versuchen, den Inhalt einer Tabelle als CSV-Datei zu exportieren: **Die Datei kann nicht exportiert werden, da eine Datei mit demselben Namen aktuell geöffnet ist. Schließen Sie die Datei und versuchen Sie es erneut oder verwenden Sie einen anderen Dateinamen.**
Problemumgehung: Verwenden Sie Horizon Administrator in Chrome im normalen Modus, um die Tabelle zu exportieren.
- Bei Verwendung von Sysprep zum Anpassen von Windows 10-Linked-Clones bei vCenter Server 6.7 verbleiben die Linked-Clone-Desktops während der Bereitstellungs- oder Neuzusammenstellungsvorgänge auf unbestimmte Zeit im Zustand „Anpassung“.
Problemumgehung: Verwenden Sie vCenter Server 6.5 U2 oder früher. Wenn Sie vCenter Server 6.7 verwenden müssen, nutzen Sie die Methode der Quickprep-Anpassung.
- In Horizon Administrator können Sie einen Benutzer mit Remotezugriff als Benutzer mit nicht authentifiziertem Zugriff hinzufügen. Allerdings erhalten Benutzer mit nicht authentifiziertem Zugriff keinen Remotezugriff von externen Gateways. Der Benutzer kann nicht auf virtuelle Desktops zugreifen und kann Anwendungen nur als Benutzer mit nicht authentifiziertem Zugriff starten. Wenn der Benutzer versucht, sich mit normalem Zugriff anzumelden, wird die Fehlermeldung „Falscher Authentifizierungstyp angefordert“ angezeigt.
Problemumgehung: Keine.
- Horizon-Single Sign-On schlägt fehl, wenn als Authentifizierungseinstellung der Vertrauensstellung „Ausgewählte Authentifizierung“ festgelegt ist.
Problemumgehung: Verwenden Sie eine der folgenden Umgehungen, um dieses Problem zu beheben.
 - Verwenden Sie domänenweite Authentifizierung.
 - Verwenden Sie weiterhin die Sicherheitseinstellung „Ausgewählte Authentifizierung“, doch erteilen Sie für alle Horizon Connection Server-Hostkonten (lokale Systeme) explizit die Berechtigung „Authentifizierung zulassen“ auf allen Domänencontrollern der Computerobjekte (Ressourcencomputer), die sich in der vertrauenden Domäne oder in der Gesamtstruktur befinden. Weitere Informationen zum Erteilen der Berechtigung „Authentifizierung zulassen“ finden Sie im Microsoft-Artikel „Grant the Allowed to Authenticate permission on computers in the trusting domain or forest“.
- Mit der Funktion „Cloud-Pod-Architektur“ geben RDS-Lizenzierungsserver unter bestimmten Umständen mehrere permanente Lizenzen an denselben Client in einer Lizenzierungsumgebung mit gemischtem Modus aus.

Problemumgehung: Keine. Dieses Problem ist ein Drittanbieter-Problem und durch die Art und Weise bedingt, wie Microsoft RDS-Lizenzserver Lizenzen ausstellen, unabhängig von Horizon 7.

- In Horizon Administrator wird während des Klonvorgangs für einen Linked Clone-Pool oder einen automatisierten Pool mit vollständigen virtuellen Maschinen, die in einem vSAN-Datenspeicher erstellt wurden, im Schritt „Speicheroptimierung“ die Option „VMware Virtual vSAN verwenden“ nicht als ausgewählt angezeigt. Der Klonvorgang ist jedoch erfolgreich.

Problemumgehung: Keine.

- Die folgenden Probleme treten auf, wenn Sie den Datenspeicher bei der Bearbeitung eines automatisierten Desktop-Pools mit vollständigen virtuellen Maschinen durchsuchen:
 - Wenn Sie auf der Registerkarte „vCenter-Einstellungen“ auf „Datenspeicher durchsuchen“ klicken, wird der GB-Wert für das empfohlene Minimum angezeigt.
 - Erhöhen Sie auf der Registerkarte „Bereitstellungseinstellungen“ die maximale Anzahl von Maschinen, wählen Sie anschließend die Registerkarte „vCenter-Einstellungen“ aus und klicken Sie auf „Datenspeicher durchsuchen“. Der GB-Wert für das empfohlene Minimum wird erhöht, wird jedoch dem vorhandenen Wert hinzugefügt.
 - Für einen Desktop-Pool mit drei Maschinen, von denen eine verfügbar ist, eine andere sich jedoch noch in der Anpassungs- oder Bereitstellungsphase befindet, bearbeiten Sie den Desktop-Pool, wählen die Registerkarte „vCenter-Einstellungen“ aus und klicken auf „Datenspeicher durchsuchen“. Der GB-Wert für das empfohlene Minimum wird für die Summe der drei Maschinen angezeigt.

Problemumgehung: Verwenden Sie Horizon Administrator, um bei Bearbeitung eines automatisierten Desktop-Pools mit vollständigen virtuellen Maschinen einen Datenspeicher zu suchen, damit Sie den korrekten GB-Wert für den empfohlenen minimalen Speicher sehen.

- Die folgenden Probleme treten auf, wenn Sie bei der Bearbeitung des Instant-Clone-Desktop-Pools den Datenspeicher durchsuchen:
 - Nachdem sich alle Maschinen in einem Instant-Clone-Desktop-Pool im Status „Verfügbar“ befinden, bearbeiten Sie den Desktop-Pool und klicken auf der Registerkarte „vCenter-Einstellungen“ auf „Datenspeicher durchsuchen“. Die GB-Werte für das empfohlene Minimum, das empfohlene Maximum und 50 % der Auslastung sind positiv.
 - Nachdem sich alle Maschinen in einem Instant-Clone-Desktop-Pool im Status „Verfügbar“ befinden, bearbeiten Sie den Desktop-Pool, erhöhen Sie auf der Registerkarte „Bereitstellungseinstellungen“ die maximale Anzahl von Maschinen und klicken Sie dann auf der Registerkarte „vCenter Einstellungen“ auf „Datenspeicher durchsuchen“. Die GB-Werte für das empfohlene Minimum, das empfohlene Maximum und 50 % der Auslastung werden erhöht, werden jedoch dem vorhandenen Wert hinzugefügt.
 - Für einen Desktop-Pool mit drei Maschinen, von denen eine verfügbar ist, eine andere sich jedoch noch in der Anpassungs- oder Bereitstellungsphase befindet, bearbeiten Sie den Desktop-Pool, wählen die Registerkarte „vCenter-Einstellungen“ aus und klicken auf „Datenspeicher durchsuchen“. Die GB-Werte für das empfohlene Minimum, das empfohlene Maximum und 50 % der Auslastung werden für alle drei Maschinen angezeigt.

Problemumgehung: Verwenden Sie Horizon Administrator, um bei der Bearbeitung von Instant-Clone-Desktop-Pools einen Datenspeicher zu suchen, damit Sie die korrekten GB-Werte für das empfohlene Minimum, das empfohlene Maximum und 50 % der Auslastung sehen.

- Wenn nach der Erstellung eines automatisierten Desktop-Pools, der vollständige virtuelle Maschinen mit zwei oder mehr Namen enthält, der Wert für „Anzahl der nicht zugewiesenen Computer, die eingeschaltet bleiben“ kleiner als die Anzahl der tatsächlichen Namen ist, und Sie den Pool bearbeiten, dann akzeptiert das Feld „Anzahl der nicht zugewiesenen Computer, die eingeschaltet bleiben“ keinen Wert, der der Gesamtzahl der bei der Pool-Erstellung angegebenen Namen entspricht und zeigt fälschlicherweise eine Fehlermeldung an.

Problemumgehung: Verwenden Sie Horizon Administrator zum Bearbeiten des automatisierten Desktop-Pools, der vollständige virtuelle Maschinen mit zwei oder mehr Namen enthält, um den Wert des Felds „Anzahl der nicht zugewiesenen Computer, die eingeschaltet bleiben“ korrekt zu aktualisieren.

- Die Anmeldung beim HTML Access-Portal oder bei einer der Administrationskonsolen mit einer IP-Adresse oder CNAME schlägt in den meisten Browsern ohne zusätzliche Konfiguration fehl. In den meisten Fällen wird ein Fehler gemeldet, manchmal wird jedoch nur eine leere Fehlermeldung angezeigt.

Problemumgehung: Um dieses Problem zu beheben, finden Sie weitere Informationen unter „Überprüfen der Herkunft“ im Dokument *Horizon 7-Sicherheit*.

- Wenn Sie Skype for Business konfigurieren, können Sie optional die Medienumgehung aktivieren, um den Vermittlungsserver zu umgehen.

Über Skype for Business optimierte Anrufe für und von PSTN-Benutzern werden immer über den Vermittlungsserver geleitet, auch wenn die Medienumgehung aktiviert ist.

Problemumgehung: Keine. Die Medienumgehung wird vom Virtualization Pack für Skype for Business nicht unterstützt. Weitere Informationen finden Sie unter

<https://kb.vmware.com/s/article/56977>

- Wenn derselbe Benutzer in beiden Verbindungsserver-Pods, die in einer Cloud-Pod-Architektur-Umgebung gekoppelt werden müssen, vorhanden ist, wird in Horizon Administrator für „Quell-Pods“ der Wert „2“ angezeigt, und der Benutzer wird von beiden Pods bezogen. Ein Administrator kann den Benutzer von beiden Pods aus bearbeiten, was zu Inkonsistenzen bei der Benutzerkonfiguration während der Hybrid-Anmeldung führen kann. Darüber hinaus kann die Hybrid-Anmeldung für den Benutzer nicht deaktiviert werden.

Problemumgehung: Sie müssen den Benutzer bei beiden Pods löschen und den Benutzer dann neu erstellen und ihn für die Hybrid-Anmeldung konfigurieren.

- In Horizon Administrator sind die Schaltflächen „Von Sitzung abmelden“ und „Sitzung trennen“ nicht für Remote-Sitzungen deaktiviert, die über vCenter Server gestartet wurden.

Problemumgehung: Verwenden Sie Horizon Console für Remote-Sitzungen, die über vCenter Server gestartet wurden, um die Funktionalität für die deaktivierten Schaltflächen „Von Sitzung abmelden“ und „Sitzung trennen“ abzurufen. Dies funktioniert allerdings nicht, wenn Sie zu „Bestandsliste“ > „Desktops“ navigieren, einen Desktop-Pool auswählen und auf die Registerkarte „Computer“, „Maschinen (Instant Clone-Details)“ oder „Computer (View Composer-Details)“ klicken.

- Kernspeicherfehlermeldungen werden generiert, während Datenspeicher virtueller Volumes in verschachteltem ESXi oder verschachteltem virtuellem ESXi hinzugefügt werden.

Problemumgehung: Keine.

- Sowohl Horizon Administrator als auch Horizon Console zeigen die internen Ordernamen anstelle der tatsächlichen Ordernamen an, wenn Sie einen vSAN-Datenspeicher zum Importieren einer persistenten Festplatte durchsuchen.

Problemumgehung: Keine.

- In Horizon Administrator und Horizon Console werden benutzerdefinierte Rollen mit der Berechtigung „Helpdesk verwalten (schreibgeschützt)“ als für Zugriffsgruppen anwendbar angezeigt.

Problemumgehung: Keine.

- Benutzer mit der Rolle „Administratoren (Nur Lesezugriff)“ können View-Konfiguration > Cloud-Pod-Architektur in Horizon Administrator nicht sehen.
Problemumgehung: Verwenden Sie Horizon Console.
- Wenn Sie in Horizon Administrator eine Linked-Clone-Farm bearbeiten oder hinzufügen, die vSAN-Datenspeicher verwendet, werden die Ausfallzeiten deaktiviert.
Problemumgehung: Legen Sie mit Horizon Console Ausfallzeiten für eine Linked-Clone-Farm fest, die vSAN-Datenspeicher verwendet.
- In Horizon Administrator funktioniert die Schaltfläche „Neu erstellen“ nicht in der Computerübersicht eines automatisierten Desktop-Pools, der vollständige virtuelle Maschinen enthält.
Problemumgehung: Verwenden Sie in Horizon Administrator die Funktionalität zum Neuerstellen über „Computer“ > „vCenter Server“.
- Wenn Sie einen vCenter Server mithilfe eines vorhandenen PowerShell-Skripts zu einem Verbindungsserver hinzufügen, wird die folgende Fehlermeldung angezeigt: VC-Instanz konnte nicht hinzugefügt werden: Enum-Konstante „com.vmware.vdi.commonutils.Thumbprint.Algorithm.SHA-1“ nicht vorhanden. Dieses Problem tritt auf, weil die certificateEncoding-Eigenschaft, die eine Zertifikatsüberschreibung für selbstsignierte Zertifikate angibt, in Horizon 7 Version 7.8 hinzugefügt wird. Aus diesem Grund schlagen frühere Versionen von VMware PowerCLI-Skripten mit einem falschen Wert von SHA-1 fehl.
Problemumgehung: Aktualisieren Sie die PowerShell-Skripte, um den Eigenschaftswert DER_BASE64_PEM anstelle von SHA-1 zu verwenden. Legen Sie z. B. \$certificate _override. sslCertThumbprintAlgorithm = ' DER_BASE64_PEM ' fest.
- Wenn eine Anwendung der universellen Windows-Plattform (UWP) aktualisiert wird, ändert sich der Pfad, der die Version enthält, und die Anwendung ist über den ursprünglichen Pfad nicht erreichbar. Der App-Status in Horizon Administrator lautet **Nicht verfügbar**, und ein Benutzer kann die App nicht starten.
Problemumgehung: Aktualisieren Sie den Pfad der App in Horizon Administrator nach einem Upgrade und überprüfen Sie, ob der App-Status **Verfügbar** lautet. Alternativ können Sie die App nicht aktualisieren.
- Wenn die Gerätefilterung für die Funktion der Clientlaufwerkumleitung konfiguriert ist und ein Benutzer das RDP-Anzeigeprotokoll zum Herstellen einer Verbindung verwendet, funktioniert die Gerätefilterung nicht.
Problemumgehung: Wenn die Gerätefilterung für die Clientlaufwerkumleitung eingestellt ist, dann konfigurieren Sie den Verbindungsserver so, dass RDP-Verbindungen nicht zulässig sind.
- Die True SSO-Desktop-Entsperrfunktion wird in PCoIP- und Blast-Protokollen unterstützt, jedoch nicht in RDP (Remotedesktopprotokoll).
- In der Horizon Console kann die Benutzer- oder Gruppenzusammenfassung aufgrund von Domänenvertrauensproblemen in den folgenden Fällen nicht geladen werden:
 - Wenn Benutzer und Gruppen zu einer unidirektionalen Vertrauensdomäne gehören und der angemeldete Administrator über die erforderlichen Berechtigungen von einer unidirektionalen Vertrauensdomäne verfügt.
 - Wenn Benutzer und Gruppen zu einer bidirektionalen Vertrauensdomäne gehören und der angemeldete Administrator über die erforderlichen Berechtigungen von einer bidirektionalen Vertrauensdomäne verfügt.
 - Wenn Benutzer und Gruppen zu einer unidirektionalen oder bidirektionalen Vertrauensdomäne gehören und der angemeldete Administrator von der untergeordneten Domäne stammt und die erforderlichen Berechtigungen hat.**Problemumgehung:** Verwenden Sie Horizon Administrator, um auf die Benutzer- oder Gruppenzusammenfassung zuzugreifen.

- In Horizon Console werden einige Ereignisse möglicherweise nicht aufgelistet, da die Zeit für den Verbindungsserver in Bezug auf die Zeitzone des Verbindungsservers falsch eingestellt ist.
Problemumgehung: Verwenden Sie Horizon Administrator zum Anzeigen aller Ereignisse.
- Sie können eine virtuelle Instant-Clone-Maschine mit einer aktiven Sitzung wiederherstellen. Dies tritt sowohl in Horizon Administrator als auch in Horizon Console auf.
Problemumgehung: Keine.
- Wenn Sie in Horizon Administrator und Horizon Console die vCenter Server mit getrennten persistenten Festplatten entfernen, zeigt Horizon Administrator weiterhin die Festplatten dieser vCenter an, aber die Festplatten können nicht betrieben werden. In Horizon Console werden keine getrennten Festplatten angezeigt, es werden jedoch interne Fehlerbanner angezeigt.
Problemumgehung: Keine bekannte Problemumgehung. Stellen Sie sicher, dass vor dem Entfernen keine getrennten Festplatten aus dem vCenter Server vorhanden sind.
- Wenn Sie in der Horizon Console einen manuellen Desktop-Pool erstellen, wird das Feld „Zeitüberschreitung bei leerer Sitzung (nur Anwendungen)“ nicht aktualisiert, wenn die Sitzungstypoption „Anwendung“ oder „Desktop und Anwendung“ lautet.
Problemumgehung: Bearbeiten Sie den manuellen Desktop-Pool, um den „Zeitüberschreitung bei leerer Sitzung (nur Anwendungen)“ zu aktualisieren.
- Virtuelle Maschinen, die unter Windows 2019 installiert und durch Auswahl von Windows 2019 OS in vSphere Client für vSphere 7 erstellt wurden, werden in Horizon 7 nicht aufgeführt oder unterstützt.
Problemumgehung: Installieren Sie Windows 2019 auf der virtuellen Maschine, indem Sie die Windows 2016-Betriebssystemversion in vSphere Client auswählen.
- Die Horizon Console gibt den neuen Namen der Portgruppe oder des Segments nicht an, wenn Sie Netzwerke für einen Instant Clone-Desktop-Pool oder eine Instant Clone-Desktop-Farm auswählen und der Segmentname in der VMware Cloud on AWS-Konsole geändert wird.
Problemumgehung: Keine.
- Wenn Sie Horizon Administrator über das Symbol der Horizon 7 Administrator-Konsole starten bzw. `https://localhost/admin` oder `https://localhost/newadmin` in die Adressleiste eines Browsers eingeben, werden Sie zu `https://127.0.0.1/admin` umgeleitet. Diese Umleitung zu einer IP-Adresse kann zu einem Authentifizierungsfehler führen, wie in VMware Knowledgebase(KB)-Artikel 2150307 beschrieben: [Anmeldung bei einer VMware-Webanwendung wie Horizon Administrator oder Horizon Help Desk Tool nicht möglich](#).

Problemumgehung: Um die Umleitung zu einer IP-Adresse zu verhindern, geben Sie `https://localhost/admin/` in die Adressleiste des Browsers ein (stellen Sie sicher, dass „/“ am Ende der URL enthalten ist).

Horizon Agent for Linux

In diesem Abschnitt werden Probleme beschrieben, die bei Horizon Agent for Linux oder dann auftreten können, wenn Sie einen Linux-Desktop konfigurieren.

- Das Fenster „Zusammenarbeit“ wird manchmal nicht angezeigt, nachdem Sie eine Verbindung zu einem Remote-Desktop herstellen und auf das Symbol der Benutzeroberfläche für die Zusammenarbeit klicken.
Problemumgehung: Passen Sie die Größe des Desktopfensters an oder stellen Sie erneut eine Verbindung mit dem Remote-Desktop her.
- Die Konfiguration von vier Monitoren mit einer Auflösung von 2560 x 1600 auf virtuellen RHEL 6.6- oder CentOS 6.6-Maschinen in vSphere 6.0 wird nicht unterstützt.
Problemumgehung: Verwenden Sie die Auflösung 2048 x 1536 oder stellen Sie diese Konfiguration in vSphere 5.5 bereit.
- Das Tastaturlayout und das Gebietsschema eines Linux-Agenten sind nicht mit dem Client

synchronisiert, wenn für „System der Tastatureingabemethode“ `fcitx` festgelegt ist.

Problemumgehung: Legen Sie für „System der Tastatureingabemethode“ `iBus` fest.

- Single Sign-On (SSO) funktioniert nicht ordnungsgemäß auf einem RHEL/CentOS 7.2-Desktop, wenn Sie eine Domäne mithilfe von System Security Services Daemon (SSSD) hinzufügen.

Problemumgehung: Ändern Sie nach dem Hinzufügen einer Domäne mithilfe von SSSD die Datei `/etc/pam.d/password-auth` unter Berücksichtigung der Informationen im VMware-Knowledgebase-Artikel 2150330 [SSO configuration changes required when using SSSD to join AD on RHEL/CentOS 7.2 Desktops](#) (SSO-Konfigurationsänderungen erforderlich, wenn SSSD zum Hinzufügen von AD auf RHEL/CentOS 7.2-Desktops verwendet wird).

- Wenn ein Clientbenutzer, der sich mit der Smartcard-Umleitung authentifiziert, eine Verbindung mit einem Ubuntu 18.04/16.04- oder SLED/SLES 12 SP 3-Desktop herstellt und die Smartcard vor dem Eingeben der PIN entfernt oder erneut einfügt, erkennt der Desktop die Änderung nicht.

Der Desktop erkennt nur eine Änderung des Zustands der Smartcard, nachdem der Benutzer die Eingabeaufforderung für die PIN geschlossen hat.

Problemumgehung: Geben Sie an der Eingabeaufforderung die Smartcard-PIN ein und klicken Sie auf „OK“. Sie können auch auf „Abbrechen“ klicken, um die Eingabeaufforderung ohne Eingabe einer PIN zu schließen.

- Wenn ein Clientbenutzer eine Verbindung mit einem Ubuntu 18.04/16.04- oder SLED/SLES 12 SP 3-Desktop herstellt, wird „Fehler 2306: Kein geeignetes Token verfügbar“ auf dem Anmeldebildschirm angezeigt.

Diese Fehlermeldung weist darauf hin, dass eine Smartcard aus dem Clientsystem entfernt wurde. Der Benutzer kann sich beim Desktop anmelden, indem er das Benutzerkennwort eingibt oder die Smartcard erneut einfügt.

- Wenn der Administrator auf Ubuntu 16.04 versucht, die Smartcard-Umleitung durch Festlegen von `VVC.ScRedir.Enable` auf „FALSE“ in der `/etc/vmware/config`-Konfigurationsdatei zu deaktivieren, bleibt der Desktop auf dem Anmeldebildschirm hängen.
- Nach dem Herstellen einer Verbindung mit einem Ubuntu 16.04-Desktop und Eingabe der falschen PIN für die Smartcard-Authentifizierung stößt der Clientbenutzer auf eine Anmeldeaufforderung, um das Benutzerkennwort anstelle der Smartcard-PIN einzugeben. Der Clientbenutzer kann auf „OK“ klicken, um die Eingabeaufforderung für das Benutzerkennwort zu schließen. Eine neue Eingabeaufforderung wird angezeigt, in der der Benutzer aufgefordert wird, die Smartcard-PIN einzugeben.
- Auf Ubuntu 18.04/16.04 und SLED/SLES 12 SP3 wird der Desktop-Bildschirmschoner nicht wie erwartet gesperrt, wenn der Benutzer eine Smartcard aus dem Clientsystem entfernt. Standardmäßig wird der Desktop-Bildschirmschoner nicht gesperrt, auch wenn der Clientbenutzer die Smartcard entfernt, die zur Authentifizierung beim Desktop verwendet wird. Um den Bildschirmschoner unter diesen Bedingungen zu sperren, müssen Sie `pkcs11_eventmgr` auf dem Desktop konfigurieren.

Problemumgehung: Konfigurieren Sie `pkcs11_eventmgr`, um das richtige Bildschirmschoner-Verhalten als Reaktion auf Smartcard-Ereignisse anzugeben.

- Nach der Installation von Horizon Agent mit aktivierter Smartcard-Umleitung (Parameter „-m“ auf „yes“ gesetzt) auf einem RHEL 7.0-Desktop kann Horizon Administrator, Horizon Console oder vSphere möglicherweise einen schwarzen Bildschirm anzeigen. Die Smartcard-Umleitung wird auf Desktops mit RHEL 7.1 oder höher unterstützt. Auf RHEL 7.0-Desktops wird die Funktion nicht unterstützt.

Problemumgehung: Installieren Sie Horizon Agent mit aktivierter Smartcard-Umleitung auf einem Desktop mit RHEL 7.1 oder höher.

- Wenn Sie zwei Monitore mit unterschiedlicher Auflösung konfigurieren, wobei die Auflösung des primären Bildschirms niedriger ist als die des sekundären, können Sie möglicherweise nicht den Mauszeiger bewegen oder Anwendungsfenster in bestimmte Bereiche des Bildschirms ziehen.
Problemumgehung: Stellen Sie sicher, dass die Auflösung des primären Monitors mindestens ebenso hoch ist wie die des sekundären.
- Wenn Sie eine Smartcard auf einem RHEL 7-Desktop verwenden und die Option zum Sperren des Bildschirms beim Entfernen der Karte aktivieren, kann der Bildschirm sofort nach Anmeldung mit der Smartcard gesperrt werden. Dies ist ein bekanntes Problem bei RHEL 7.

Problemumgehung: Um auf den Desktop zuzugreifen, entsperren Sie den Bildschirm, nachdem Sie sich mit der Smartcard angemeldet haben.

Horizon Agent

- Im FIPS-Modus kann Horizon Agent nicht mit dem Verbindungsserver kombiniert werden. Außerdem ist der Poolstatus nicht verfügbar, wenn View Agent auf einem anderen Laufwerk als Laufwerk C installiert ist.
Problemumgehung: Bei einem Betrieb im FIPS-Modus installieren Sie Horizon Agent auf Laufwerk C.
- Wenn Sie Horizon Agent auf Windows Server 2016 deinstallieren, wird eine Warnmeldung zu den aktuell verwendeten Anwendungen eingeblendet.
Problemumgehung: Klicken Sie im Dialogfeld, das eingeblendet wird, wenn Sie Horizon Agent mit der Windows-Option „Programme hinzufügen oder entfernen“ deinstallieren, auf die Option „Ignorieren“. Für die Deinstallation von Horizon Agent von der Befehlszeile aus verwenden Sie den Befehl `msiexec /x /qn {GUID of Agent}` anstelle des Befehls `msiexec /x {GUID of Agent}`.
- Wenn Sie Horizon Agent deinstallieren, wird die Maus langsam und ruckelt. Beim Deinstallieren von Horizon Agent wird auch der vmkbd.sys-Treiber deinstalliert.
Problemumgehung: Reparieren Sie die VMware Tools auf der virtuellen Horizon Agent-Maschine.
- Beim Aktualisieren von Horizon Agent 7.1 auf Horizon Agent 7.2 auf einem Windows 7-Gastbetriebssystem wird das Dialogfeld „Dateien in Verwendung“ angezeigt. Dieses Dialogfeld zeigt an, dass die VMware Horizon Agent-Anwendung Dateien verwendet, die durch das Setup aktualisiert werden müssen.
Problemumgehung: Klicken Sie auf „Ignorieren“, um das Upgrade fortzusetzen.
- Bevor die Profilverwaltung die Synchronisierung der Benutzerdaten abgeschlossen hat, wird der Desktop aktualisiert oder gelöscht, wenn die Richtlinie zum Aktualisieren oder Löschen beim Abmelden aktiviert ist.

Problemumgehung: Keine

- Die Horizon Agent-Installation für Windows 10 32 Bit löst die Ausnahme „Die Argumente sind ungültig“ aus und die Installation wird nach dem Klicken auf „OK“ fortgesetzt. Dieser Fehler tritt auf, wenn der Druckerspooledienst deaktiviert ist.
Problemumgehung: Aktivieren Sie den Druckerspooledienst, damit die Installation wie vorgesehen durchgeführt werden kann.
- Wenn der Besitzer der Sitzung während einer Zusammenarbeitssitzung ein Video abspielt, das mithilfe einer Multimedia-Umleitung beschleunigt wurde, wird den Teilnehmern anstelle des Videos ein schwarzer Bildschirm angezeigt.

Problemumgehung: Wenn Sie als Besitzer der Sitzung während einer Zusammenarbeitssitzung ein Video abspielen müssen, verwenden Sie dazu weder Windows Media Player noch Internet Explorer, und deaktivieren Sie nicht die Multimedia-Umleitung auf Pools, auf denen die Zusammenarbeit aktiviert ist.

- Wenn ein Teilnehmer einer Sitzung mit mehreren Monitoren beitrifft und den Modus der relativen Maus auf seinem Client aktiviert, kann die Maus auf einen zweiten Monitor bewegt werden, den der Teilnehmer nicht sehen kann.

Problemumgehung: Bewegen Sie die Maus zurück auf den Bildschirm. Alternative: Verwenden Sie in einer Sitzung mit mehreren Monitoren nicht den Modus der relativen Maus.

- Wenn Sie Chrome mit der URL-Inhaltsumleitung verwenden, und „*.google.“ für das Https-Protokoll in den Filterregeln sowie Google als Ihre Startseite in Chrome festlegen, werden Sie bei jedem Öffnen einer neuen Registerkarte zu google.com umgeleitet.

Problemumgehung: Ändern Sie die Startseite oder die Filterregeln.

- Beim Einrichten einer gemeinsamen Sitzung schlägt das Hinzufügen eines Kollaborators über die E-Mail-Adresse aus einer bidirektionalen vertrauenswürdigen Domäne fehl.

Problemumgehung: Fügen Sie den Kollaborator über „Domäne\Benutzer“ hinzu.

- Die HTML5-Multimedia-Umleitung funktioniert für Edge auf einem virtuellen Desktop vor Windows 10 1803, aber nach der Aktualisierung auf die neueste Windows 10 1803-Version, z. B. 17133, funktioniert die Umleitung nicht, besonders für Websites, mit automatischer Wiedergabe wie youtube.com.

Problemumgehung: Erzwingen Sie einen Neustart des virtuellen Windows 10-Desktops.

- Veröffentlichte Anwendungen werden nicht getrennt, wenn die Clientsitzung sich im Leerlauf befindet, selbst wenn eine maximale Leerlaufzeit bis zur Zeitüberschreitung für Sitzungen im Leerlauf mit der GPO-Methode oder einer Nicht-GPO-Methode angegeben wurde. Eine Warnmeldung zur Verbindungstrennung wird angezeigt, doch die Anwendung wird nicht getrennt.
- Nachdem Sie einen Suchvorgang von Streaming-Medien mithilfe der Multimedia-Umleitung durchgeführt haben, werden Audio und Video nicht flüssig wiedergegeben.

Problemumgehung: Warten Sie einige Minuten oder öffnen Sie die aktuellen Streaming-Medien erneut.

- Wenn ein Benutzer die Funktion „HTML5-Multimedia-Umleitung“ verwendet, um ein YouTube-Video im Edge-Browser abzuspielen, wird das Video manchmal gepuffert und es wird kein Bild oder Ton ausgegeben.

Problemumgehung: Aktualisieren Sie die Seite.

- Nachdem Sie eine Verbindung mit einem Remote-Desktop hergestellt haben, auf dem die Funktion „Echtzeit-Audio/Video“ aktiviert ist, wird möglicherweise die folgende Meldung angezeigt: „Ihr PC muss neu gestartet werden, um die Einrichtung dieses Geräts abzuschließen: *Gerätename* (VDI).“

Problemumgehung: Sie können diese Meldung ignorieren, da das Gerät auf dem Remote-Desktop verwendet werden kann. Alternativ können Sie die Benachrichtigung zu Windows-Einstellungen deaktivieren, um zu verhindern, dass die Meldung angezeigt wird.

- Wenn Sie mit einem Desktop mit mehreren hochauflösenden Monitoren (4K) verbunden sind und ein Video im Vollbildmodus mit dem neuen Blast-Codec wiedergeben, ist die Wiedergabeleistung möglicherweise schlecht (niedrige Frame-Rate).

Problemumgehung: Verwenden Sie H.264, um Videos im Vollbildmodus wiedergeben.

- Benutzer können keinen seriellen Drucker mit der Funktion „Umleitung für seriellen Port“ verwenden, wenn Horizon Agent auf einem RDS-Host installiert ist und die Agent-Gruppenrichtlinieneinstellung COM-Port-Isolationsmodus auf Vollständige Isolation (Standardeinstellung) festgelegt ist. Dieses Problem betrifft sowohl Windows- als auch Linux-Clients. Dieses Problem tritt bei virtuellen Desktops nicht auf.

Problemumgehung: Bearbeiten Sie die Gruppenrichtlinieneinstellung COM-Port-Isolationsmodus, ändern Sie den Modus in Isolation deaktiviert und starten Sie Horizon Agent neu. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7* unter dem Thema „Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports“.

- Wenn Sie die VMware Integrated Printing-Funktion verwenden, von einem Windows 7-Clientcomputer aus eine Verbindung mit einem Windows 10-Agent-Computer herstellen und Dokumente, die Delta-Schriftarten enthalten, von einem umgeleiteten Drucker drucken, werden die Schriftarten nicht ordnungsgemäß angezeigt.

Problemumgehung: Keine. Hierbei handelt es sich um ein Drittanbieterproblem.

Horizon-GPO-Bundle

- Computerbasierte globale Richtlinienobjekte (Global Policy Objects, GPOs), die einen Neustart erfordern, um wirksam zu werden, werden auf Instant Clones nicht angewendet.
Problemumgehung: Siehe VMware-Knowledgebase-Artikel [2150495](#).
- Wenn es sich in der Konfiguration mit geschachteltem Modus beim Desktop der ersten Ebene (der Maschine, auf der Horizon Client und Horizon Agent installiert sind) um einen virtuellen Desktop und beim Desktop auf zweiten Ebene um einen veröffentlichten Desktop handelt, gilt die Gruppenrichtlinieneinstellung „Einen Filter bei der Umleitung von Client-Druckern festlegen“ nicht für den Desktop der zweiten Ebene, wenn Sie die Konfiguration auf dem virtuellen Desktop der ersten Ebene vornehmen.

Problemumgehung: Wenn Sie Drucker für den Desktop der zweiten Ebene filtern möchten, konfigurieren Sie die Gruppenrichtlinie „Einen Filter bei der Umleitung von Client-Druckern festlegen“ auf dem Desktop der zweiten Ebene.

Horizon Client

In diesem Abschnitt werden Probleme beschrieben, die bei Endbenutzern auftreten können, wenn sie über Horizon Client oder HTML Access eine Verbindung zu Remote-Desktops und -Anwendungen herstellen. Informationen zu Problemen, die nur bei einer bestimmten Horizon Client-Plattform auftreten, finden Sie in den Versionshinweisen für Horizon Client auf der Seite [Horizon Clients-Dokumentation](#).

- Die Profildaten für mehrere Benutzersitzungen sind auf RDS-Hosts nicht vorhanden. Dieses Problem tritt auf, wenn Sitzungen nicht verbunden sind, aber im Task-Manager auf dem RDS-Host diese Sitzungen weiterhin angezeigt werden.
Problemumgehung: Löschen Sie die Sitzungen auf dem RDS-Host oder melden Sie den Benutzer vom veröffentlichten Desktop oder der veröffentlichten Anwendung ab.
- Wenn Sie sich bei Workspace ONE anmelden, wird die Sitzung der vorab gestarteten Anwendung nicht gestartet. Vorab gestartete Sitzungen werden nur gestartet, wenn eine erfolgreiche Anmeldung am Verbindungsserver von Horizon Client erfolgt ist.
Problemumgehung: Starten Sie eine Anwendung oder einen Desktop aus Workspace ONE manuell, um die für den Vorabstart konfigurierten Anwendungen zu starten.
- Bei Verwendung des VMware Blast-Anzeigeprotokolls und bei deaktiviertem Blast Secure Gateway (BSG) kann Horizon Client nach einem kurzen Netzausfall (ca. 1 Minute) manchmal nicht wiederhergestellt werden und die Verbindung mit dem Desktop wird getrennt. Dieses Problem tritt nicht mit einem aktivierten BSG auf.
Problemumgehung: Stellen Sie erneut eine Verbindung mit der Sitzung her.
- Der RDS-Host speichert nur einen Satz an Anwendungsdaten für den ersten Anwendungsstart einer Sitzung. Alle Daten nachfolgender Anwendungsstarts gehen verloren.
Problemumgehung: Melden Sie sich bei der Sitzung ab und starten Sie eine andere Anwendung, damit deren Daten gespeichert werden.

- Desktops werden nicht gestartet, wenn Sie HTML Access im Internet Explorer- oder Microsoft Edge-Browser verwenden, um eine Verbindung mit dem Verbindungsserver, Sicherheitsserver oder Replikatserver auf einem Windows 10-Client-Betriebssystem herzustellen. Dieses Problem betrifft Desktops mit Windows 10 N-, Windows 10 KN-, Windows 7 N- und Windows 7 KN-Gastbetriebssystemen.

Problemumgehung: Verwenden Sie den Webbrowser Firefox oder Google Chrome für HTML Access.

- Für Intel vDGA wird die Unterstützung mehrerer Monitore auf maximal drei Monitore beschränkt. Der Intel-Treiber unterstützt maximal drei Monitore mit einer Auflösung von bis zu 3840 x 2160. Wenn Sie versuchen, vier Monitore anzuschließen, zeigt die Verbindung drei schwarze Bildschirme, von denen nur einer funktioniert.
 - Wenn sich ein VDI-Desktop in einem Remotespeicherort befindet und eine hohe Netzwerklatenz auftritt, funktioniert möglicherweise das rekursive Entsperren mithilfe einer Smartcard nicht.
- Problemumgehung:** Entsperren Sie den Desktop manuell.

- Wenn sich ein Benutzer auf einem Windows 8-Remote-Desktop anhand der Kerberos-Authentifizierung anmeldet und der Desktop gesperrt ist, ist das Benutzerkonto zum Entsperren des Desktops, das Windows 8 dem Benutzer standardmäßig anzeigt, das zugehörige Windows Active Directory-Konto und nicht das Originalkonto aus der Kerberos-Domäne. Es wird nicht das Konto angezeigt, mit dem sich der Benutzer angemeldet hat. Dieses Problem existiert mit Windows 8 und ist nicht Horizon 7-spezifisch. Dieses Problem kann gelegentlich in Windows 7 auftreten.

Problemumgehung: Der Benutzer muss „Anderer Benutzer“ wählen, um den Desktop zu entsperren. Die korrekte Kerberos-Domäne wird dann in Windows angezeigt und der Benutzer kann sich mit der Kerberos-Identität anmelden.

- Wenn Sie Ambir Image Scan Pro 490i zur Durchführung eines Scanvorgangs auf einem Remote-Desktop oder in einer Remoteanwendung verwenden, wird im Dialogfeld immer „Scanvorgang wird durchgeführt“ angezeigt, ohne dass der Vorgang abgeschlossen wird.
- Problemumgehung:** Führen Sie einen Scanvorgang auf dem Client durch. Der Client-Scan kalibriert den Scanner. Speichern Sie nach Abschluss des Kalibriervorgangs die Kalibrierungsdatei und stellen Sie sie in `ProgramData\AmbirTechnology\ImageScanPro490i` bereit.
- Die Unicode-Tastatureingabe funktioniert mit HTML Access in Horizon 7 for Linux-Desktops nicht ordnungsgemäß.

- Beim Herstellen einer Verbindung mit einem Linux-Desktop funktionieren einige Tastatureingaben nicht. Wenn Sie beispielsweise einen nicht englischsprachigen IME-Editor sowohl auf dem Clientgerät als auch auf dem Remote-Desktop verwenden, werden einige nicht englische Zeichen nicht korrekt dargestellt.

Problemumgehung: Verwenden Sie auf dem Clientgerät den englischsprachigen IME-Editor und auf dem Remote-Desktop den nicht englischsprachigen IME-Editor.

- Manchmal wird ein Audioanruf von Skype an Skype for Business nicht ordnungsgemäß gestartet. Der Aufrufstatus auf dem Skype for Business-Client lautet „Verbindung wird hergestellt...“.

Problemumgehung: Keine.

- Wenn Sie Skype for Business innerhalb eines nicht persistenten Desktops verwenden, erreichen Sie möglicherweise den Skype für Business-Grenzwert von 16 Gerätezertifikaten. Wenn dieser Grenzwert erreicht ist und Skype for Business einen neuen Anmeldeversuch unternimmt, wird ein neues Zertifikat ausgestellt und das älteste zugewiesene Zertifikat wird widerrufen.
- Wenn Sie Horizon Client 4.8 für Linux oder früher mit aktiviertem FIPS-Modus starten und versuchen, eine Verbindung mit Horizon Agent 7.6 oder Horizon Connection Server 7.6 mit aktiviertem FIPS-Modus herzustellen, wird eine Fehlermeldung ähnlich der folgenden angezeigt: „Ungültige Lizenzinformationen für RDS-Lizenz: Fehlende Client-ID“.

Problemumgehung: Verwenden Sie Horizon Client 4.9 für Linux oder höher, um Horizon Client für Linux mit aktiviertem FIPS-Modus dazu zu verwenden, eine Verbindung mit Horizon Agent 7.6 oder höher oder Horizon Connection Server 7.6 oder höher mit aktiviertem FIPS-Modus herzustellen.

- Das auf Unified Access Gateway, Horizon Connection Server und dem Sicherheitsserver generierte standardmäßige selbstsignierte TLS-Serverzertifikat kann möglicherweise nicht von Chrome-Browsern, Safari-Browsern oder VMware Horizon Clients verwendet werden, die unter macOS 10.15, iOS 13 und Chrome OS 76 ausgeführt werden. Dieses Problem kann auftreten, da die Anforderungen für vertrauenswürdige TLS-Serverzertifikate von Apple in diesen Betriebssystemversionen geändert wurden. Die standardmäßigen selbstsignierten Zertifikate erfüllen diese neuen Anforderungen derzeit nicht. Wenn die Verbindung mit Horizon von einem Client über einen Zwischen-Load-Balancer oder -Proxy erfolgt, der TLS beendet, müssen die neuen Zertifikatanforderungen auch auf diesen Geräten erfüllt werden. Auf Horizon Client für Mac unter macOS 10.15 wird der Modus „Warnhinweis vor der Herstellung einer Verbindung mit einem nicht vertrauenswürdigen Server“ möglicherweise nicht fortgesetzt, ohne das selbstsignierte Zertifikat zu überprüfen. Es erscheint das Dialogfeld „Nicht vertrauenswürdige Serververbindung“ mit der Fehlermeldung „VMware Horizon Client kann Ihre Verbindung nicht verifizieren. Wenden Sie sich an Ihren Administrator.“ und nur die Schaltflächen „Zertifikat anzeigen“ und „Nicht verbinden“ sind verfügbar.

Problemumgehung: VMware empfiehlt in der Regel, dass das standardmäßige selbstsignierte TLS-Serverzertifikat auf diesen Produkten durch ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat für die Umgebung ersetzt wird. Diese Empfehlung stellt immer eine gute Sicherheitspraxis dar. In dieser Situation tritt das Problem nicht auf, solange das von der vertrauenswürdigen Zertifizierungsstelle signierte Zertifikat die neuen Apple-Anforderungen erfüllt. Eine alternative Problemumgehung für macOS- und iOS Horizon-Clients besteht darin, die SSL-Konfiguration so festzulegen, dass Serverzertifikate nicht überprüft werden. Weitere Informationen zu den Apple-Zertifikatanforderungen finden Sie unter <https://support.apple.com/de-de/HT210176>

Horizon JMP Server und JMP Integrated Workflow

- In einer Umgebung mit mehreren installierten JMP Servern können beim Erstellen oder Löschen von JMP-Zuweisungen Konflikte auftreten, wenn sich mehr als ein JMP Server auf dieselbe gemeinsame Nutzung der User Environment Manager-Konfiguration bezieht.

Problemumgehung: Keine.

- Wenn Sie Ihre JMP-Einstellungen so konfiguriert haben, dass nur ein VMware App Volumes Manager verwendet wird, und Sie bei der Erstellung einer JMP-Zuweisung einen Desktop-Pool ausgewählt haben, dessen Horizon Agent nicht auf diesen App Volumes Manager verweist, können Sie dennoch AppStacks in der App Volumes Manager-Instanz auswählen, auf die der Horizon Agent des Desktop-Pools verweist. Wenn Sie außerdem Ihre JMP-Einstellungen so konfiguriert haben, dass mehrere App Volumes Manager-Instanzen verwendet werden, können Sie, selbst wenn Sie einen Desktop-Pool auswählen, dessen Horizon Agent auf eine dieser App Volumes Manager-Instanzen verweist, weiterhin die AppStacks aus den anderen App Volumes Manager-Instanzen auswählen, die in Ihren JMP-Einstellungen konfiguriert sind. Wenn der Desktop-Pool jedoch gestartet wird, sind die über diesen anderen App Volumes Manager ausgewählten AppStacks nicht verfügbar.

Problemumgehung: Keine.

- Wird ein AppStack, der derzeit von einer vorhandenen JMP-Zuweisung verwendet wird, mithilfe des App Volumes Manager oder durch Bearbeiten der JMP-Zuweisung umbenannt, wird die Übersichtsseite der vorhandenen JMP-Zuweisungen nicht mit dem neuen AppStack-Namen aktualisiert.

Problemumgehung: Keine.

- Wenn Sie über zwei Horizon 7-Instanzen verfügen, die bei derselben JMP Server-Instanz registriert sind und denselben App Volumes Manager verwenden, können durch das Löschen einer JMP-Zuweisung aus einer Horizon 7-Instanz die Zuweisungen der AppStacks entfernt werden, die von einer anderen JMP-Zuweisung in der anderen Horizon 7-Instanz verwendet werden.

Problemumgehung: Keine.

- Beim Hinzufügen oder Bearbeiten von Active Directory-Informationen auf der Seite „JMP-Einstellungen“ schlägt der Vorgang fehl, wenn der eingegebene Wert für **Verbundener Benutzername** mindestens eins von 30 chinesischen Dreibyte-Zeichen enthält, z. B. das Zeichen „试“, durch die die Active Directory-Authentifizierung fehlschlägt.

Problemumgehung: Verwenden Sie einen anderen verbundenen Benutzernamen aus Ihrem Active Directory, der über Administratorrechte verfügt und keins der 30 chinesischen Dreibyte-Zeichen wie „试“ enthält.

- Beim Hinzufügen oder Bearbeiten von App Volumes Manager-Instanzinformationen auf der Seite „JMP-Einstellungen“ schlägt der Vorgang fehl, wenn der eingegebene Wert für **Dienst-Kontobenutzername** mindestens eins von 30 chinesischen Dreibyte-Zeichen enthält, z. B. „试“, durch die die App Volumes Manager-Instanzauthentifizierung fehlschlägt.

Problemumgehung: Verwenden Sie einen anderen verbundenen Benutzernamen aus Ihrer App Volumes Manager-Instanz, der über Administratorrechte verfügt und keins der 30 chinesischen Dreibyte-Zeichen wie „试“ enthält.

- Die Einstellungen für die Laufwerkszuordnung, die mithilfe der VMware Dynamic Environment Manager-Version 9.2.1 zugeordnet wurden, werden nicht angezeigt, wenn der Windows 10 1703-Desktop-Pool gestartet wird.

Problemumgehung: Nachdem der Desktop-Pool von Windows 10 1703 gestartet wird, führen Sie folgenden Befehl aus.

```
C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe -UemRefreshDrives
```

Weitere Informationen finden Sie im VMware-KB-Artikel <https://kb.vmware.com/s/article/2113657>.

- Wenn Sie über „localhost“ auf die Horizon Console zugreifen, wird die Fehlermeldung „Zugriff auf JMP Server ist derzeit nicht möglich“ im Bereich „JMP-Einstellungen“ der Horizon Console angezeigt.

Problemumgehung: Greifen Sie nur mit einem vollqualifizierten Domännennamen (FQDN) auf die Horizon Console zu, statt mit „localhost“.

- Beim Erstellen einer neuen JMP-Zuweisung wird möglicherweise die folgende Warnmeldung in der Registerkarte **Anwendungen** angezeigt: „Die dem ausgewählten Desktop-Pool zugeordnete App Volumes-Instanz stimmt mit keiner der registrierten App Volumes-Instanzen überein.“ Dieses Problem tritt auf, wenn eines der folgenden Ereignisse eintritt:

- Der im Desktop-Pool verwendete App Volumes Agent wurde mit einer IP-Adresse statt einem vollqualifizierten Domännennamen (FQDN) installiert.
- Der im Desktop-Pool verwendete App Volumes Agent wurde mithilfe eines FQDN installiert, aber die IP-Adresse der App Volumes Manager-Instanz wurde stattdessen in den JMP-Einstellungen registriert.

Problemumgehung: Installieren Sie den App Volumes Agent mithilfe eines FQDN erneut und verwenden Sie den FQDN bei der Registrierung der App Volumes Manager-Instanz auf der Registerkarte **Einstellungen (JMP) > App Volumes**.

- Beim Installieren von VMware Horizon JMP Server konnte das JMP Server-Installationsprogramm nicht fortgesetzt werden, da McAfee Antivirus NSSM.EXE als Bedrohung erkannt hat.

Problemumgehung: Fügen Sie die folgenden Dateien zur Ausnahmeliste von McAfee Antivirus hinzu, bevor Sie JMP Server erneut installieren.

C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe

C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

- Wenn Sie die Option **Autorisieren der lokalen Administratorgruppe** während der Installation des Horizon 7-Verbindungsservers ausgewählt haben, wodurch eine BUILTIN\Administrators-Gruppe statt *<domainName>\Administrator* erstellt wird, schlägt das Hinzufügen der JMP Server-Informationen über die Horizon Console mit der Fehlermeldung „Unzureichende Rechte für Horizon“ fehl.

Problemumgehung: Registrieren Sie bei der Verwendung von Horizon Administrator *<domainName>/administrator* mit vollständigem Administratorzugriff. Melden Sie sich wieder bei der Horizon Console an und fügen Sie die JMP Server-Informationen hinzu.

- Wenn Sie eine JMP-Zuweisung erstellen und über einen Instant-Clone-Desktop-Pool fahren, wird für die Option „3D-Renderer“ der Wert **Deaktiviert** und nicht der Wert **Verwaltung mithilfe des vSphere Client** angezeigt.

Problemumgehung: Keine.

- JMP Server-Registrierung schlägt fehl, wenn als Authentifizierungseinstellung der Vertrauensstellung „Ausgewählte Authentifizierung“ festgelegt ist.

Problemumgehung: Verwenden Sie eine der folgenden Umgehungen, um dieses Problem zu beheben.

- Verwenden Sie domänenweite Authentifizierung.
- Verwenden Sie weiterhin die Sicherheitseinstellung „Ausgewählte Authentifizierung“, doch erteilen Sie für alle Horizon Connection Server-Hostkonten (lokale Systeme) explizit die Berechtigung „Authentifizierung zulassen“ auf allen Domänencontrollern der Computerobjekte (Ressourcencomputer), die sich in der vertrauenden Domäne oder in der Gesamtstruktur befinden. Weitere Informationen zum Erteilen der Berechtigung „Authentifizierung zulassen“ finden Sie im Microsoft-Artikel [Grant the Allowed to Authenticate permission on computers in the trusting domain or forest](#).
- JMP-Zuweisungen funktionieren nicht wie erwartet, weil Informationen über den App Volumes Manager, der vom Desktop-Pool verwendet wird, und die User Environment Manager-Version, die von JMP Server verwendet wird, nicht ermittelt werden konnten.

Problemumgehung: Wenn Sie einen Desktop-Pool konfigurieren, legen Sie im Abschnitt „Größeneinstellung für Desktop-Pool“ des Bereichs „Bereitstellungseinstellungen“ für **Anzahl an (eingeschalteten) Reservecomputern** den Wert 1 oder höher fest. Wenn Sie im Abschnitt „Bereitstellungszeit“ die Option **Computer bei Bedarf bereitstellen** ausgewählt haben, legen Sie zudem für **Mindestanzahl an Computern** den Wert 1 oder höher fest.

- Wenn die Installationsdatei für JMP Server-Version 1.0.2.x auf einem Host ausgeführt wird, auf dem derzeit JMP Server-Version 1.0.0.516 installiert ist, wird der Installationsvorgang nicht fortgesetzt.

Problemumgehung: Verwenden Sie die Systemsteuerung, um JMP Server-Version 1.0.0.516 zu deinstallieren. Führen Sie die Installationsdatei für JMP Server-Version 1.0.2.x aus und befolgen Sie die Anweisungen im Assistenten, um die Installation abzuschließen. Geben Sie die gleichen SQL Server-Datenbankinformationen während des Installationsvorgangs ein, um Daten aus der Installation von JMP Server-Version 1.0.0.516 beizubehalten.

- In den folgenden Szenarien ist Ihre JMP Server-Instanz nicht mehr nutzbar, wenn Sie versuchen, Ihre aktuelle Installation mit dem JMP Server-Installationsprogramm der Version 1.1.0.xxx zu aktualisieren. Das Upgrade schlägt fehl, und die Installation wird zurückgesetzt.
 - Das Zertifikat für die SQL Server-Datenbank fehlt in Ihrer JMP Server-Installation, und während des Upgrades ist das Kontrollkästchen **SSL aktivieren** ausgewählt.

- Beim JMP Server-Upgrade wird der Verbindungsmodus mit Windows-Authentifizierung ausgewählt, für das JMP Server-Hostsystem wurde jedoch kein SQL Server-Anmeldekonto erstellt.
- Sie haben den Upgrade-Vorgang durch Klicken auf **Abbrechen** abgebrochen.

Problemumgehung: Wiederholen Sie das Upgrade mit Version 1.1.0.xxx des JMP Server-Installationsprogramms. Sie müssen dieselben SQL Server-Datenbankinformationen eingeben, die Sie zum Installieren der vorherigen JMP Server-Version verwendet haben. Stellen Sie nach einem erfolgreichen Upgrade sicher, dass alle Zertifikate, die Sie für JMP Server konfiguriert hatten, weiterhin intakt sind. Abhängig vom Zeitpunkt des Installationsfehlers oder -abbruchs können die Zertifikate verändert worden sein.

- Wenn Sie versuchen, eine Konfigurationsfreigabe für Dynamic Environment Manager (DEM) hinzuzufügen, wird möglicherweise sinngemäß die folgende Fehlermeldung angezeigt: `runOne] Error running file_share.createFileShare { code: 400,\n took: 221,\n data: {}},\n error: 'Dateifreigabe <fileshare-unc-path> kann nicht erstellt werden.'`

Das Hinzufügen einer DEM-Konfigurationsfreigabe schlägt fehl, wenn das Kennwort für die DEM-Konfigurationsfreigabe eines der folgenden Zeichen enthält: “ #+,;<>=\~

Problemumgehung: Verwenden Sie ein anderes Kennwort, das eines dieser zulässigen Zeichen enthält: `!$%&'()*-./:~@[]^_`{|}`

Horizon Cloud Connector

- Wenn Sie den HTML5-basierten vSphere Web Client verwenden, um die OVA-Datei für die virtuelle Horizon Cloud Connector-Appliance bereitzustellen, tritt der folgende Fehler auf: „Ungültiger Wert ‚false‘ angegeben für Eigenschaft proxySsl. Bereitstellung des OVF-Pakets ist fehlgeschlagen.“
Problemumgehung: Verwenden Sie den Flex-basierten oder den Flash-basierten vSphere Web Client, um die OVA-Datei für die virtuelle Horizon Cloud Connector-Appliance bereitzustellen.
- Beim Starten von Horizon Cloud Connectors wird die Meldung „[FAILED] Failed to start Wait for Network to be Configured. See 'systemctl status systemd-networkd-wait-online.service' for details.“ angezeigt.
Diese Meldung wird fälschlicherweise angezeigt und weist nicht auf ein tatsächliches Netzwerkproblem hin. Sie können die Meldung ignorieren und Horizon Cloud Connector weiterhin wie gewohnt verwenden.