vmware®

Release Notes for VMware Horizon 7 version 7.9

Released 02 July 2019

These release notes include the following topics:

- [What's New in This Release](#)
- [Before You Begin](#)
- [Internationalization](#)
- [Compatibility Notes](#)
- [Supported Windows 10 Operating Systems](#)
- [Support for Red Hat Enterprise Linux Workstation](#)
- [Prior Releases of Horizon 7](#)
- [Known Issues](#)
- [Resolved Issues](#)

What's New in This Release

VMware Horizon 7 version 7.9 provides the following new features and enhancements. This information is grouped by installable component.

- [Product Enhancements](#)
- [Horizon Connection Server On-Premises](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO Bundle](#)
- [Horizon Client](#)
- [Horizon 7 Cloud Connector](#)
- [Horizon 7 Deployed on VMware Cloud on AWS](#)

For information about the issues that are resolved in this release, see[Resolved Issues](#).

Product Enhancements

The VMware Horizon 7 version 7.9 release includes many new features and enhancements to Horizon Connection Server and Horizon Agent including continuing to build on the feature parity of Horizon Console, the HTML5-based web console that will eventually replace Horizon Administrator.

Horizon Connection Server On-Premises

- **Horizon Console (HTML5-based Web Interface)**
  There are several enhancements to Horizon Console. These include:
    - Add, edit, or remove an instant-clone domain administrator.
    - View the number of published desktop sessions for farms or registered machines.
    - Configure event reporting and monitor events.
    - Monitor published desktop and application sessions.
    - Configure smart card authentication.
    - Perform enhanced role-based delegated administration including privileges and roles for custom roles in Horizon Console.
    - The Horizon Console user interface contains updated icons.
    - View the image, pending image, and task columns for an RDS host for a farm.
    - Configure the multi-session mode feature for published applications.
    - Configure global settings that affect client sessions and connections and set global security settings for client sessions and connections in Horizon Console.
    - Select whether and when to refresh the OS disks when creating an instant-clone desktop pool.
    - Determine whether to allow ESXi hosts to reclaim unused disk space on instant clones that are created in space-efficient disk format when creating an instant-clone desktop pool. The space reclamation feature reduces the total storage space required for instant clone desktops.
    - Publish and launch Universal Windows Platform (UWP) applications.
    - Change or remove the icon of a published application.
- **Horizon Administrator**
    - You can use Horizon Administrator to configure additional options such as "Always", "Log to file on error (default)", and "Never" to enable event log messages to be generated and stored in Syslog format in log files. These options are not available in Horizon Console.
- **Cloud Pod Architecture**
    - The **Home Site Override** tab is separated from the **Users and Groups** tab in Horizon Console. To configure a home site override in Horizon Console in Horizon 7 version 7.9, select **Inventory > Global Entitlements**, select the name of the global entitlement to associate with the home site, and click the **Home Site Override** tab.
    - You can use the **Search Sessions** feature in Horizon Console to view desktop and application sessions across the pod federation.
- **Published Desktops and Applications**
    - You can publish and launch Universal Windows Platform (UWP) applications.
- **Virtual Desktops**
    - When creating an instant clone, you can select whether and when to refresh the OS disks.
    - When creating an instant clone, you can determine whether to allow ESXi hosts to reclaim unused disk space on instant clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for instant clone desktops.

Horizon Agent for Linux

- **Expanded OS support for smart card redirection**
  Smart card redirection allows client users to authenticate into a Linux desktop using a smart card reader connected to the client system. Horizon 7 version 7.9 supports smart card

redirection on Linux desktops running the following distributions:
- Ubuntu 18.04
- Ubuntu 16.04
- SLED 12 SP3
- SLES 12 SP3
- SLED 11 SP4

- **Enhanced system performance with single-thread architecture for user sessions**
Beginning with version 7.9, Horizon Agent for Linux features a Java NIO solution that uses a single thread to handle all connection sessions to the desktop. Previous versions opened a separate thread for each session. The new single-thread architecture improves performance by reducing the use of system resources.

Horizon Agent

- **Remoting Protocols**
  - Horizon 7 version 7.9 is required to support Microsoft Media Server (MMS) and Real Time Streaming Protocol (RTSP).
  - NVIDIA Tesla T4 GPUs are now validated and supported with Horizon 7 across Windows 10 VDI, Windows Server 2016 and 2019. Blast Extreme can offload H.264, H.265, and graphics to the T4 GPUs.
  - Blast log files rotation has been improved to take up less disk space and reduce production issues.

- **Remote Experience**
  - Microsoft Teams application has been validated and works with Real-Time Audio-Video. For a good experience, you need a minimum setting of 4vCPU 4GB RAM as a published desktop configuration and RTAV video resolution configured with 640 x 480p.
  - You can redirect biometric devices, specifically fingerprint scanners, that are plugged into a USB port on a Windows client system, to virtual desktops.
  - You can redirect card readers that are plugged into a USB port over PCoIP virtual channel on a Windows client system to virtual desktops.
  - Several enhancements have been made to VMware Virtualization Pack for Skype for Business. These include:
    - Proxy support for Win 7 Clients
    - Improved audio quality in fallback mode for RDSH 2016 and 2019 terminal service sessions
    - Support for Skype for Business 2019 Server
    - Support for Mac Client IPV6
  - VMware Integrated Printing supports more Universal Print Driver (UPD) print settings for redirected UPD printers from Windows client machines.
  - You can use VMware Integrated Printing with Horizon Client 5.1 for Linux and Horizon Client 5.1 for Mac.
  - The following Wacom signature pads are supported in this release:
    - Wacom STU-520A
    - Wacom STU-530G
    - Wacom STU-500
    - Wacom DTU-1031
    - Wacom Intuos Pro

- Updated Windows display specifications require Windows 10 version 1803 or later for six monitor support.
- Windows 10 notifications can be redirected to the client in an application session.
- You can use HTML5 Multimedia Redirection with Horizon Client 5.1 for Linux.

Horizon GPO Bundle

- The VMware View Agent Configuration ADMX template file (vdm_agent.admx) contains a new VMware Virtualization Pack for Skype for Business group policy setting, **Disable extended filter for acoustic echo cancellation in VMware Virtualization Pack for Skype for Business**.
- The VMware Horizon Client Drive Redirection ADMX template file (vdm_agent_cdr.admx) contains two new Device Filtering group policy settings, **Exclude Vid/Pid Device** and **Include Vid/Pid Device**. You can use these settings to exclude or include devices that have specific vendor and product IDs when users use the client drive redirection feature.
- The Horizon PCoIP ADMX template file (pcoip.admx) and VMware Blast ADMX template file (vdm_blast.admx) contain two new group policy settings, **Configure drag and drop formats** and **Configure drag and drop size threshold**, to configure drag and drop behavior.

Horizon Client

For information about new features in Horizon Client 5.1, including HTML Access 5.1, see the release notes on the [Horizon Clients Documentation](#) page.

Horizon 7 Cloud Connector

This is a required component for Horizon 7.6 and later to support the following new features:

- Subscription licenses as part of a Workspace One Enterprise bundle See the *Horizon 7 Installation* guide on the [Horizon 7 Documentation](#) page.
- Cloud Monitoring Services (CMS) features as part of Horizon Cloud Service. See the *Horizon Cloud Administration Guide* on the [Horizon Cloud Service Documentation](#) page. New CMS features include:
  - Report for users, applications, desktop, and utilization for cloud-connected Horizon 7 pods
  - 7-day session history for the Help Desk Tool
  - Horizon cloud-connected session metrics and health status

Horizon 7 Deployed on VMware Cloud on AWS

- Manual desktop pools are now supported for vSphere virtual machines running Windows or Linux.
- Horizon 7 suppports the use of SDDC1.7.
- Horizon 7 supports the use of the following AWS services:
  - AWS Directory Service for Microsoft Active Directory
  - Events database on the Amazon Relational Database Service
- For a list of Horizon 7 features supported on VMware Cloud on AWS, see the [VMware Knowledge Base article 58539.](#)

Before You Begin

- **Important note about installing VMware View Composer**
  If you plan to install or upgrade to View Composer 7.2 or later, you must upgrade the Microsoft .NET framework to version 4.6.1. Otherwise, the installation will fail.
- **Important note about installing VMware Tools**
  If you plan to install a version of VMware Tools downloaded from VMware Product Downloads, rather than the default version provided with vSphere, make sure that the VMware Tools version is supported. To determine which VMware Tools versions are supported, go to the [VMware Product Interoperability Matrix](#), select the solution **VMware Horizon View** and the version, then select **VMware Tools (downloadable only)**.
- If you want to install View Composer silently, see the VMware Knowledge Base (KB) article 2148204, [Microsoft Windows Installer Command-Line Options for Horizon Composer](#).
- This Horizon 7 release includes new configuration requirements that differ from some earlier releases. See the *Horizon 7 Upgrades* document for upgrade instructions.
- Horizon 7.5.1 is an Extended Service Branch (ESB) that will receive periodic service pack (SP) updates, which include cumulative, critical bug fixes, and security fixes. See the VMware Knowledge Base (KB) article 52845 [FAQ: Horizon 7, App Volumes, UEM Extended Service Branches (ESB)](#) for detailed information of ESB. See the *Horizon 7 Upgrades* document for upgrading to SPs.
- If you intend to upgrade a pre-6.2 installation of Horizon 7, and the Connection Server, security server, or View Composer server uses the self-signed certificate that was installed by default, you must remove the existing self-signed certificate before you perform the upgrade. Connections might not work if the existing self-signed certificates remain in place. During an upgrade, the installer does not replace any existing certificate. Removing the old self-signed certificate ensures that a new certificate is installed. The self-signed certificate in this release has a longer RSA key (2048 bits instead of 1024) and a stronger signature (SHA-256 with RSA instead of SHA-1 with RSA) than in pre-6.2 releases. Note that self-signed certificates are insecure and should be replaced by CA-signed certificates as soon as possible, and that SHA-1 certificates are no longer considered secure and should be replaced by SHA-2 certificates.
  Do not remove CA-signed certificates that were installed for production use, as recommended by VMware. CA-signed certificates will continue to work after you upgrade to this release.
- To take advantage of Horizon 7 features such as Virtual SAN 6.1, GRID vGPU, and Virtual Volumes, install vSphere 6.0 and subsequent patch releases.
- After you have performed a fresh install or upgraded all Connection Server instances to Horizon 7 version 7.2 or later, you cannot downgrade the Connection Server instances to a version earlier than Horizon 7 version 7.2 because the keys used to protect LDAP data have changed. To keep the possibility of downgrading Connection Server instances while planning an upgrade to Horizon 7 version 7.2 or later, you must perform an LDAP backup before starting the upgrade. If you need to downgrade the Connection Server instances, you must downgrade all Connection Server instances and then apply the LDAP backup to the last Connection Server that is downgraded.
- Selecting the Scanner Redirection setup option with Horizon Agent installation can significantly affect the host consolidation ratio. To ensure the optimal host consolidation, make sure that the Scanner Redirection setup option is only selected for those users who need it. (By default, the Scanner Redirection option is not selected when you install Horizon

Agent.) For users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.

- Horizon 7 uses only TLSv1.1 and TLSv1.2. In FIPS mode, it uses only TLSv1.2. You might not be able to connect to vSphere unless you apply vSphere patches. For information about re-enabling TLSv1.0, see Enable TLSv1 on vCenter Connections from Connection Server and Enable TLSv1 on vCenter and ESXi Connections from View Composer in the *Horizon 7 Upgrades* document.
- FIPS mode is not supported on releases earlier than 6.2. If you enable FIPS mode in Windows and upgrade Horizon Composer or Horizon Agent from a release earlier than Horizon View 6.2 to Horizon 7 version 7.2 or later, the FIPS mode option is not shown. You must do a fresh install instead to install Horizon 7 version 7.2 or later in FIPS mode.
- Linux desktops use port 22443 for the VMware Blast display protocol.
- Starting with Horizon 7 version 7.2, it is possible that the ordering of cipher suites can be enforced by Connection Server. For more information, see the *Horizon 7 Security* document.
- Starting with Horizon 7 version 7.2, Connection Server must be able to communicate on port 32111 with other Connection Servers in the same pod. If this traffic is blocked during installation or upgrade, installation will not succeed.
- Starting with Horizon 7 version 7.3.2, TLS handshakes on port 443 must complete within 10 seconds, or within 100 seconds if smart card authentication is enabled. In previous releases of Horizon 7, TLS handshakes on port 443 were allowed 100 seconds to complete in all situations. You can adjust the time for TLS handshakes on port 443 by setting the configuration property handshakeLifetime. Optionally, the client that is responsible for an over-running TLS handshake can be automatically added to a blacklist. New connections from blacklisted clients are delayed for a configurable period before being processed so that connections from other clients take priority. You can enable this feature by setting the configuration property secureHandshakeDelay. For more information about setting configuration properties, see the *Horizon 7 Security* document.

Top of Page

Internationalization

The Horizon Administrator and Horizon Console user interface, Horizon Administrator and Horizon Console online help, and Horizon 7 product documentation are available in Japanese, French, German, Spanish, simplified Chinese, traditional Chinese, and Korean. For the documentation, see the Documentation Center for VMware Horizon 7.

Top of Page

Compatibility Notes

- For the supported guest operating systems for Horizon Agent on single-user machines and RDS hosts, see VMware Knowledge Base (KB) article 2150295, Supported Windows Versions for Remote Desktop Systems for Horizon Agent.
- If you use Horizon 7 servers with a version of View Agent older than 6.2, you will need to enable TLSv1.0 for PCoIP connections. View Agent versions that are older than 6.2 support the security protocol TLSv1.0 only for PCoIP. Horizon 7 servers, including connection

servers and security servers, have TLSv1.0 disabled by default. You can enable TLSv1.0 for PCoIP connections on these servers by following the instructions in VMware Knowledge Base (KB) article 2130798, Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later.

- For the supported Linux guest operating systems for Horizon Agent, seeSystem Requirements for Horizon 7 for Linux in the *Setting Up Horizon 7 for Linux Desktops* document.

- For the supported operating systems for Connection Server, security server, and View Composer, see System Requirements for Server Components in the *Horizon 7 Installation* document.

- Horizon 7 functionality is enhanced by an updated set of Horizon Clients provided with this release. For example, Horizon Client 4.0 or later is required for VMware Blast Extreme connections. See the VMware Horizon Clients Documentation page for information about supported Horizon Clients.

- The instant clones feature requires vSphere 6.0 Update 1 or later.

- Windows 7 and Windows 10 are supported for instant clones, but not Windows 8 or Windows 8.1.

- See the VMware Product Interoperability Matrix for information about the compatibility of Horizon 7 with current and previous versions of vSphere.

- For the supported Active Directory Domain Services (AD DS) domain functional levels, see Preparing Active Directory in the *Horizon 7 Installation* document.

- For more system requirements, such as the supported browsers for Horizon Administrator, see the *Horizon 7 Installation* document.

- RC4, SSLv3, and TLSv1.0 are disabled by default in Horizon 7 components, in accordance with 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", and SP800-52r1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations." If you need to re-enable RC4, SSLv3, or TLSv1.0 on a Connection Server, security server, View Composer, or Horizon Agent machine, see Older Protocols and Ciphers Disabled in View in the *Horizon 7 Security* document.

- If a PCoIP Secure Gateway (PSG) has been deployed for PCoIP connections, zero client firmware must be version 4.0 or later.

- When using Client Drive Redirection (CDR), deploy Horizon Client 3.5 or later and View Agent 6.2 or later to ensure that CDR data is sent over an encrypted virtual channel from an external client device to the PCoIP security server and from the security server to the remote desktop. If you deploy earlier versions of Horizon Client or Horizon Agent, external connections to the PCoIP security server are encrypted, but within the corporate network, the data is sent from the security server to the remote desktop without encryption. You can disable CDR by configuring a Microsoft Remote Desktop Services group policy setting in Active Directory. For details, see Managing Access to Client Drive Redirection in the *Configuring Remote Desktop Features in Horizon 7*document.

- The USB Redirection setup option in the Horizon Agent installer is deselected by default. You must select this option to install the USB redirection feature. For guidance on using USB redirection securely, see Deploying USB Devices in a Secure View Environment in the *Horizon 7 Security* document.

- The Global Policy, Multimedia redirection (MMR), defaults to**Deny**. To use MMR, you must open Horizon Administrator, edit Global Policies, and explicitly set this value to **Allow**. To control access to MMR, you can enable or disable the Multimedia redirection (MMR) policy globally or for an individual pool or user. Multimedia Redirection (MMR) data is sent across

- the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.
- Before you set the level of Transparent Page Sharing (TPS) in Horizon Administrator, VMware recommends that the security implications be understood. For guidance, see the VMware Knowledge Base (KB) article 2080735, Security considerations and disallowing inter-Virtual Machine Transparent Page Sharing.
- To use View Storage Accelerator in a vSphere 5.5 or later environment, a desktop virtual machine must be 512GB or smaller. View Storage Accelerator is disabled on virtual machines that are larger than 512GB. Virtual machine size is defined by the total VMDK capacity. For example, one VMDK file might be 512GB or a set of VMDK files might total 512GB. This requirement also applies to virtual machines that were created in an earlier vSphere release and upgraded to vSphere 5.5.
- Horizon 7 does not support vSphere Flash Read Cache (formerly known as vFlash).
- In Horizon (with View) version 6.0 and later releases, the View PowerCLI cmdlets Get-TerminalServer, Add-TerminalServerPool, and Update-TerminalServerPool have been deprecated.
- Screen DMA is disabled by default in virtual machines that are created in vSphere 6.0 and later. View requires screen DMA to be enabled. If screen DMA is disabled, users see a black screen when they connect to the remote desktop. When Horizon 7 provisions a desktop pool, it automatically enables screen DMA for all vCenter Server-managed virtual machines in the pool. However, if Horizon Agent is installed in a virtual machine in unmanaged mode (VDM_VC_MANAGED_AGENT=0), screen DMA is not enabled. For information about manually enabling screen DMA, see VMware Knowledge Base (KB) article 2144475, Manually enabling screen DMA in a virtual machine
- vGPU enabled instant clone desktop pools are supported for vSphere 2016 and later.
- Microsoft Windows Server requires a dynamic range of ports to be open between all Connection Servers in the Horizon 7 environment. These ports are required by Microsoft Windows for the normal operation of Remote Procedure Call (RPC) and Active Directory replication. For more information about the dynamic range of ports, see the Microsoft Windows Server documentation.
- In Horizon 7 version 7.2 or later, the viewDBChk tool will not have access to vCenter or View Composer credentials and will prompt for this information when needed.
- The forwarding rules for HTTP requests received by Connection Server instances and security servers have changed at this release. If you have defined custom frontMapping entries in locked.properties, you should remove them before upgrading. If you wish to disallow administrator connections to certain Connection Server instances, then instead of defining custom frontMapping entries, add this entry to locked.properties:

  frontServiceWhitelist = tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot

  On security servers, this entry is applied automatically and does not need to be set in locked.properties.
- Horizon Persona Management is not compatible with User Writable Volumes created with the UIA + Profile template.
- In Horizon 7 version 7.0.3 or later, internal validation checks determine if the instant clone and internal template have valid IP addresses and a network connection. If a virtual machine has a NIC that cannot be assigned an IP address during provisioning, instant-clone provisioning fails.
- NVIDIA GPU cards V100 and P100 are supported.

- AMD v340 graphics cards are supported.
- Real-Time Audio-Video (RTAV) is supported in an IPv6 environment.
- See the VMware Product Interoperability Matrix for information about the compatibility of Horizon 7 with the latest versions of VMware Unified Access Gateway, VMware Identity Manager, VMware App Volumes, VMware User Environment Manager, and VMware Tools.
- On VMware Cloud on AWS, instant-clone desktop pools and desktop pools that contain full virtual machines are limited to 1000 desktops because of an NSX-t limitation on logical switches.

Top of Page

Supported Windows 10 Operating Systems

For an updated list of supported Windows 10 operating systems, see VMware Knowledge Base (KB) article 2149393, Supported Versions of Windows 10 on Horizon 7.
For more information on upgrade requirements for Windows 10 operating systems, see VMware Knowledge Base (KB) article 2148176, Upgrade Requirements for Windows 10 Operating Systems here.

Top of Page

Support for Red Hat Enterprise Linux Workstation

Horizon Agent for Linux supports installation on systems running Red Hat Enterprise Linux Workstation. Red Hat Enterprise Linux Server is not supported.

In the Setting Up Horizon 7 for Linux Desktops document, all occurrences of "Red Hat Enterprise Linux" and "RHEL" refer to Red Hat Enterprise Linux Workstation only.

For the list of supported versions of Red Hat Enterprise Linux Workstation, seeSystem Requirements For Horizon 7 for Linux.

Top of Page

Prior Releases of Horizon 7

Features that were introduced in prior releases are described in the release notes for each release, along with existing known issues.

Top of Page

Resolved Issues

- 1614429: For RDS host farms that are created with VMware Blast display protocol support, enabling the UDP network protocol for VMware Blast sessions reduces Blast Secure Gateway scale and sessions might fall back to the TCP network protocol.
- 1911437: When you set a timeout value for HKLM\Software\VMware, Inc.\VMware VDM\Agent\USB\UemTimeouts, it fails to take effect.

- 1995561: Horizon Console does not have the icons to indicate a shared or local data store for an automated desktop pool or automated farm.

- 2293188: In Horizon Console, attaching a persistent disk shows machines that the administrator does not have permissions to manage.

- 2252570: You cannot use smart card authentication in Horizon Console.

- 2294241: In Horizon Console, editing Horizon Composer does not work when you change from the Standalone Horizon Composer Server selection to the Horizon Composer co-installed with the vCenter Server selection.

- 2294801: In Horizon Console, when you add a Standalone Horizon Composer server and then change the Horizon Composer server username and password, an error message appears on the Ready to Complete page.

- 2293423: While restoring a linked clone in Horizon Console, if you change the value of a data center in the Import from vCenter window, you cannot select the first desktop pool entry.

- 2294138: In Horizon Console, if you remove the last permission from the last role that is listed in Settings > Administrators > Role Permissions, a loading icon appears that does not vanish.

- 2310781: When you use the Internet Explorer Web browser to add a SAML 2.0 authenticator in Horizon Console, the certificate to accept and successfully add a SAML 2.0 authenticator does not appear.

- 2313771: In Horizon Console, if a group is entitled to a global entitlement (desktop or application), the users in that group can be added to a home site override only if the users are explicitly entitled to that global entitlement.

- 2273138: There is a discrepancy between the user session status that is displayed in Horizon Administrator and the user session status that is displayed on the RDS host.

- 2320364: The event database captures virtual machines GUIDs instead of virtual machines names in the logs.

- 2319428: Connection Server does not perform the scheduled push image operation on some virtual machines in the instant-clone desktop pool since forced logoff is not triggered.

- 2318790: Security server becomes unresponsive because PCOIP secure gateway consumes 100% CPU usage and users are unable to connect.

- 2337476: HTML Access is not installed when upgrading Connection Server from Horizon 7 version 7.2.0 or later.

- 234799: After upgrading, not all pools are presented in the sidebar and launcher in HTML Access in a Cloud Pod Architecture environment.

- 2347998: In a mixed-mode Cloud Pod Architecture environment where Connection Server instances are running different versions of Horizon 7, remote desktop launch can fail in

Horizon Client.

- 2310349: After upgrading pods from Horizon 7 version 7.5.1 to Horizon 7 version 7.7.0, a Server Error occurs when you select **Catalog > Global Entitlements** in Horizon Administrator. After upgrading pods from Horizon 7 version 7.5.1 to Horizon 7 version 7.7.0 or 7.8.0, "Internal error occurred" appears when you select **Inventory > Machines** in Horizon Console. After upgrading pods from Horizon 7 version 7.5.1 to Horizon 7 version 7.7.0 or 7.8.0, when stale users are present, "EntityNotFound" appears when you use the Horizon PowerCLI Get-HVMachineSummary cmdlet.

- 1655461, 1659128, 1661027: After a brief network outage and the VMware Blast session between Horizon Client and a remote desktop has recovered or has been reconnected, certain features might stop working, such as:

  - Smart card
  - Client Drive Redirection (CDR) and File Association
  - Multimedia Redirection (MMR)
  - Lync/Skype for Business

- 2329564: Reloading published applications causes more than one instance of the application to start for the end user.

- 2261193: Some Horizon 7 configurations are not restored by importing the backed up .ldf file.

- 2225252: In the Horizon Administrator dashboard, the View Composer status is green but the SSL certificate status is unknown.

- 2328222: In Horizon Administrator, when you click Send Message on the Sessions tab, the message cannot be sent to all selected virtual machines in active sessions.

- 2274553: When you use a published application in Horizon Client, sub-windows, such as popup menus, are not visible.

- 2256633: Computer-based GPOs do not get applied to instant clones in Horizon 7 version 7.9.

- 2316930: The Horizon Administrator page does not load properly when smart card authentication is used to login.

- 2269220: Creating linked-clone farms does not work if the if the linked-clone farm domain is a one-way trust domain that is externally trusted by the Connection Server domain.

- 2289635: After a push image operation, a few instant-clone virtual machines still have the old snapshot instead of the updated snapshot.

- 2320685: Some users failed to connect to an existing application session.

Known Issues

The known issues are grouped as follows.

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

Horizon Persona Management

- After every login, Persona Management takes a long time to replicate the first user persona on a guest operating system that uses the "v6" version of the user profile.
- When you log in to a Windows 10 LTSB machine using a persona profile and try to access redirected folders from Quick Access, such as Downloads or My Documents, you get this error:

  C:\Users\vdiuser7\Downloads is unavailable. Microsoft doesn't provide the API to add folder or file to Quick Access.
  Workaround: None

- When you log into a VM configured with Persona Management for the second time, the Microsoft Edge browser crashes and an error message that states the OneDrive application has never been used appears. Additionally, the files and folders cannot be replicated properly. This issue occurs with Windows 10 build 1703 and later.
  Workaround: Disable the Persona Management setting **Roam Local Settings Folders**. When you disable this setting, the Microsoft Edge browser works properly but the OneDrive application is only available when you log in for the first time.

- Offline icons are not displayed for files on a Windows Server 2012 virtual machine with Horizon Persona Management setting enabled.
  Workaround: None known.

- After a successful initial login to a virtual machine with Horizon Agent installed on Windows 10 version 1703 CBB system and with Persona Management enabled, the "OneDrive -Bad Image error" message is displayed during subsequent login attempts.

  Workaround: Do not use OneDrive on your Windows 10 version 1703 CBB system. In the Group Policy Management Editor, disable the "Roam local settings folders" setting in the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Persona Management > Roaming & Synchronization** folder.

View Composer

- When you run View Composer installer on Windows Server 2016 with the latest Windows update from command line, you get a Microsoft .NET 4.6 framework error. This issue occurs because the CLI installer is not able to recognize latest version of Microsoft .NET 4.7.
  Workaround: Use the View Composer installer user interface to run the installer.

- Creating or recomposing desktop pools fails after you upgrade the parent virtual machine

from build 1511 to build 1607 of the Windows 10 operating system. Build 1607 is the Windows 10 Anniversary Update operating system.

Workaround:
- Option 1. Perform a fresh installation of Windows 10 Build 1607 on the parent virtual machine.
- Option 2. Do not select "Redirect disposable files"in the desktop pool creation wizard.

- Connection to View Composer fails when you run the following command: viewdbchk.cmd –findMachine
Workaround: Import the self-signed certificate for View Composer into Connection Server's keystore or use a custom CA certificate.

- Due to recent changes to the Guest Customization utility on vSphere 6.7, during an Horizon 7 upgrade to version 7.5 you cannot use View Composer 7.5 with an earlier version of Horizon Agent for provisioning and recomposing linked-clone pools using the Sysprep customization method. The linked-clone desktops and farms get stuck indefinitely in the customization state during provisioning or recomposing operations.
Workaround: Upgrade to the latest version of VMware Tools and upgrade Horizon Agent to version 7.5 on the parent virtual machine and take a snapshot of the upgraded parent virtual machine. Then, provision or recompose linked-clone desktop pools using the Sysprep customization method on vSphere 6.7.

- Linked clones get stuck in the customizing state for Win2k12 Standard and Datacenter versions.
Workaround: For more information on how to fix this issue, see the VMware KB article https://kb.vmware.com/s/article/57348.

Horizon Connection Server

- During provisioning of an instant-clone desktop pool, if there is not enough space available on the data stores, the error message that is displayed in Horizon Administrator is "Cloning of VM <VM name> has failed -VC_FAULT_FATAL: Failed to extend swap file from 0 KB to 2097152 KB." This message does not clearly indicate the root cause of the problem.
Workaround: Not required.

- In Horizon Administrator, if you go to**Catalog> Desktop Pools**, double-click an instant-clone desktop pool, go to the **Inventory** tab and click **Machines (Instant Clone Details)**, the window displays details of the instant clones. However, the OS Disk data store column displays no information.
Workaround: None

- In a large scale environment, some of the desktops in an instant-clone desktop pool might go into the Invalid IP state.
Workaround: In Horizon Administrator, go to**Pool Inventory**, select the desktops in the **Invalid IP** state and click **Recover**.

- When you restart or reset a virtual machine for which an end user session exists in a desktop pool from vCenter Server or from the Windows Operating System menu, the virtual machine restarts but the status of the virtual machine might appear in the "Already Used" state in Horizon Administrator.
This problem can occur for the following pool types:
  - Instant-clone desktop pools.
  - Linked-clone floating desktop pools with "Delete on log Off" enabled.

- Linked-clone floating desktop pools with "Refresh on log Off" enabled.
  - Full-clone floating desktop pools with "Delete on log Off" enabled.

  Workaround: Use Horizon Administrator or Horizon Client to restart or reset the virtual machine in the instant-clone desktop pool. If the virtual machine is already in the "Already Used" state, remove the virtual machine. This action automatically creates a new virtual machine based on the pool provisioning settings.

- If you provision instant clones on local datastores, the corresponding hosts cannot be put into maintenance mode. This occurs because the internal VMs and the instant clones are stored on local datastores so they cannot be migrated.
  Workaround: Delete the instant-clone desktop pool. This will delete the related VMs and enable the corresponding hosts to enter maintenance mode.

- ESXi host remediation that uses VUM fails if the instant-clone Parent VM is present on the host in a powered-on state
  Workaround: For more information,see the VMware Knowledge Base (KB) article 2144808, [Entering and exiting maintenance mode for an ESXi host that has Horizon instant clones](#).

- Windows Universal apps are not supported in Windows Server 2016 RDS host and Windows Server 2019 RDS host.

- For True SSO, the connectivity status between the Connection Server instance and the enrollment server is displayed only on the System Health Status dashboard for the connection server that you are using to access Horizon Administrator. For example, if you are using https://server1.example.com/admin for Horizon Administrator, the connectivity status to the enrollment server is collected only for the server1.example.comconnection server. You might see one or both of the following messages:
  - The primary enrollment server cannot be contacted to manage sessions on this connection server.
  - The secondary enrollment server cannot be contacted to manage sessions on this connection server.

  It is mandatory to configure one enrollment server as primary. Configuring a secondary enrollment server is optional. If you have only one enrollment server, you will see only the first message (on error). If you have both a primary and a secondary enrollment server and both have connectivity issues, you will see both messages.

- When you set up True SSO in an environment with CAs and SubCAs with different templates setup on each of them, you are allowed to configure True SSO with a combination of template from a CA or SubCA with another CA or SubCA. As a result, the dashboard might display the status of True SSO as green. However, it fails when you try to use True SSO.

- In Horizon Help Desk Tool, the pod name does not appear if the session is a local session or a session running in the local pod.
  Workaround: Set up the Cloud Pod Architecture environment to view pod names in Horizon Help Desk Tool.

- The Workspace ONE mode setting does not get reflected in the replica server from Workspace ONE.
  Workaround: Configure the Workspace ONE mode in Connection Server.

- When you create full-clone desktop pools, sometimes wrong templates are displayed and valid templates are hidden due to a cache issue.

Workaround: Restart Connection Server.

- VMware does not recommend creating more than one URL content redirection setting in this release.

- When you try to add a SAML authenticator in Horizon Administrator, the **Add** button is disabled on the Manage SAML Authenticators page.
  Workaround: Log in to Horizon Administrator as a user who has the Administrators or Local Administrators role.
- In a Cloud Pod Architecture environment, pre-launched application sessions from global application entitlements are not shown in **Inventory > Search Sessions** in Horizon Administrator.
  Workaround: Log in to the Horizon Administrator user interface for a Connection Server instance in the hosting pod and select **Monitoring > Events** to view pre-launched session information.

- Users that are assigned to 20 to 50 Cloud Pod Architecture global application entitlements have a 20 to 30 second delay while being authenticated to Horizon 7 when connecting through any version of Horizon Client.
  Note: In Horizon 7 version 7.2, this connection time is slightly improved.
  Workaround: None.

- For Intel vDGA, only the Haswell and Broadwell series of Intel integrated GPUs are supported. Broadwell integrated GPUs are supported only on vSphere 6 Update 1b and later. Haswell integrated GPUs are supported on vSphere 5.5 and later. The GPU must be enabled in the BIOS before it can be recognized by ESXi. For more information, see the documentation for your specific ESXi host. Intel recommends leaving the graphics memory settings in the BIOS set to their default values. If you choose to change the settings, keep the aperture setting at its default (256M).
- Provisioning of virtual machines based on View Composer desktop pools configured to use NVIDIA GRID vGPU fails with the following error: The amount of graphics resource available in the parent resource pool is insufficient for the operation.
  Workaround: Use a single vGPU profile for all virtual desktops configured for 3D rendering in a cluster.

- For vCenter Server 6.0 U3 or later, including vCenter Server 6.5, internal parent VMs migrate to another host during failure. This migration causes an issue because unnecessary parent VMs reside on the destination host.
  Workaround: Manually remove these parent VMs. For more information, see the *Setting Up Virtual Desktops in Horizon 7* document.

- To reduce the possibility of memory exhaustion, vGPU profiles with 512 MB or less of frame buffer support only one virtual display head on a Windows 10 guest operating system.

  The following vGPU profiles have 512 Mbytes or less of frame buffer:

    - Tesla M6-0B, M6-0Q
    - Tesla M10-0B, M10-0Q
    - Tesla M60-0B, M60-0Q
    - GRID K100, K120Q
    - GRID K200, K220Q

- **Workaround:** Use a profile that supports more than one virtual display head and has at least one GB of frame buffer.

- Published desktops and application pools fail to launch if they have the client restriction feature enabled and are entitled to a domain that is configured with a one-way AD trust.
  Workaround: None

- After an upgrade, the option to add a farm is grayed out if you have a role with the "Manage Farms and Desktops and Application Pools" (object-specific privilege).
  Workaround: Edit the role or create the role again with the "Manage Farms and Desktops and Application Pools" privilege, which also adds the "Manage Global Configuration and Policies" privilege.

- After an upgrade, the bookmarks do not appear in Workspace ONE.
  Workaround: Add the bookmarks from the catalog in Workspace ONE again.

- After you disconnect and reconnect the network cable and click "Disconnect and Log Off" on the client machine, the remote desktop does not disconnect and log off.

  Workaround: Manually close the window of the remote desktop and disconnect from the remote session.

- In Horizon Administrator, the ready to complete step does not does not display values for many fields during the cloning process for an automated pool containing full virtual machines. However, the cloning operation succeeds.
  Workaround: None.

- When you create linked clones and full clones with the Sysprep customization method, customization and domain joining sometimes fails on Windows 10 guest operating systems.
  Workaround: This occurs because of a Microsoft Windows issue. To resolve this issue, follow the steps in the Microsoft Knowledge Base (KB) article: https://support.microsoft.com/en-us/help/2769827.

- You cannot create a linked-clone desktop pool or farm in Horizon Console if there is no Horizon 7 license configured.
  Workaround: Use Horizon Administrator to create a linked-clone desktop pool or farm without a Horizon 7 license.

- Log in to Horizon Console fails from the Microsoft Edge browser and log in to Horizon Console from the Internet Explorer browser displays only keywords instead of icons. This issue occurs when you connect to a Connection Server or security server using an IP address instead of a DNS name.
  Workaround: Use a DNS name instead of an IP address when connecting. For more information, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/2150307.

- When you use Safari version 10.1.1 as the Web browser to log in to Horizon Console with a Fully Qualified Domain Name, user interface issues such as the bottom panels appearing blank can occur.
  Workaround: Safari version 10.1.1 is not a supported Web browser version for Horizon Console. Use a Safari version earlier than version 10.1.1 or version 11.0.2 and later to log

in to Horizon Console.

- The following user interface issues occur in Horizon Help Desk Tool for global Linux sessions in a Cloud Pod Architecture deployment:

  - An internal error occurred message appears, the Skype for Business status is not displayed, and the operating system version displays as "-" when you click the session details on the Details tab.
  - A "failed to get Remote Assistance ticket" message appears when you click Remote Assistance.
  - An internal error occurred message appears when you click the Applications tab.

  Workaround: None. Horizon Help Desk does not support the following user interface features for Linux desktops: Skype for Business status, Remote Assistance, Applications tab, and the session idle status.

- Horizon Administrator does not update the space reclamation information for a vCenter Server on vSphere version 6.7 that uses the VMFS6 with the automatic UNMAP feature.
  Workaround: None.

- After an upgrade to Horizon 7 version 7.5, only the first Connection Server that was installed can connect to the enrollment server.
  Workaround: Stop the Horizon Connection Server service, remove certificates with the friendly name "vdm.ec" from the VMware Horizon View Certificates store, and restart the Horizon Connection Server service.

- Single Sign-On does not work if you access Horizon Administrator in a timed out tab of Horizon Console and then click the Horizon Console link from Horizon Administrator.
  Workaround: Clear the website data in the browser and restart the browser.

- Login to Horizon Console fails if you use the IP address to login to Horizon Console on a Google Chrome, Microsoft Edge, or Safari Web browser.
  Workaround: Use the Fully Qualified Doman Name (FQDN) to login to Horizon Console. For more information on using FQDN to log in to Web applications, see the *Horizon 7 Security* document.

- Horizon Administrator displays null/null in the user name column in the Users and Groups page for the following users: Account Operators, Incoming Forest Trust Builders, Terminal Server License Servers, Windows Authorization Access Group, Server Operators, and Pre-Windows 2000 Compatible Access.
  Workaround: None.

- After an upgrade to vSphere 6.7, you cannot use the custom specification created with a vSphere version earlier than 6.7.
  Workaround: After an upgrade to vSphere 6.7, create a new custom specification and use this specification for pool provisioning.

- Horizon Help Desk Tool displays the logon time for both the brokering pod and the hosting pod but does not display the logon time for a pod that is neither the brokering pod nor the hosting pod. Horizon Help Desk Tool displays the logon time after a few minutes for the hosting pod if the brokering pod is a remote pod.
  Workaround: If Horizon Help Desk Tool does not display the logon time for the hosting

pod, close the page that displays session details, wait 7-8 mins and navigate to the Details tab to view the session details again.

- VMware Identity Manager sometimes fails to launch desktops. When you save SAML configuration details for the first time in VMware Identity Manager with SAML enabled on Connection Server, desktops do not start.
  Workaround: Save the profile again and perform a sync operation on the new profile. The sync operation can occur every hour or day, as set by the administrator.

- Horizon Administrator on Chrome in incognito mode displays an error when you try to export a table's contents as CSV: **The file cannot be exported because a file of the same name is currently open. Close the file and try again or use a different file name.**
  Workaround: Use Horizon Administrator on Chrome in normal mode to export the table.

- When you use Sysprep to customize Windows 10 linked clones on vCenter Server 6.7, the linked-clone desktops get stuck indefinitely in the customization state during provisioning or recomposing operations.
  Workaround: Use vCenter Server 6.5 U2 or earlier. If you must use vCenter Server 6.7, then use the Quickprep customization method.

- In Horizon Console, an internal error occurs if you use a non-ASCII character in the "Specify names manually" field for a desktop pool that contains full virtual machines.
  Workaround: Use only alphanumeric characters, spaces, underscores, and dashes in the "Specify names manually" field for a desktop pool that contains full virtual machines.

- When you use Horizon Console with the Internet Explorer Web browser, the button texts in the Desktops page disappear after reloading the Desktops page. This issue occurs in Internet Explorer version 11.966.15063.0, Update version: 11.0.56.
  Workaround: Use another browser such as Chrome, Microsoft Edge, Safari, or Firefox that does not have this issue. Or, navigate to another page in Internet Explorer and then navigate back to the Desktops page to fix this issue.

- In Horizon Administrator, you can add a remote access user as an unauthenticated access user. However, unauthenticated access users cannot get remote access from external gateways. The user will not be able to access virtual desktops and can only launch applications as an unauthenticated access user. If the user tries to login with normal access, an "Incorrect authentication type requested" error message appears.
  Workaround: None.

- In Horizon Console, the session timeout value does not match the session timeout value added in the Horizon Administrator interface in View Configuration > Global Settings.
  Workaround: None.

- Horizon Single Sign On fails when the scope of the trust authentication setting is set to "Selective Authentication".
  Workaround: Use one of the following workarounds to resolve this issue.

    - Use domain-wide authentication.
    - Continue to use the "Selective Authentication" security setting, but explicitly grant each Horizon Connection Server host (local system) accounts the "Allowed to Authenticate" permission on all the domain controllers of the computer objects

(resource computers) that reside in the trusting domain or forest. For information on how to grant the "Allowed to Authenticate" permission, see the Microsoft article Grant the Allowed to Authenticate permission on computers in the trusting domain or forest."

- With the Cloud Pod Architecture feature, in certain circumstances RDS licensing servers issue multiple permanent licences to the same client in a mixed-mode licensing environment.

  Workaround: None. This problem is a third-party issue and is inline with the way Microsoft RDS license servers issue licenses, even without Horizon 7.

- In Horizon Administrator, the "Use VMware Virtual vSAN" option does not appear as selected in the Storage Optimization step during the cloning process for a linked clone pool or an automated pool containing full virtual machines created on a vSAN datastore. However, the cloning operation is successful.
  Workaround: None.

- The following issues occur when you browse the datastore while editing an automated desktop pool that contains full virtual machines:

  - On the vCenter Settings tab, click "Browse Datastore", the minimum recommended GB value is displayed.
  - On the Provisioning Settings tab, increase the maximum number of machines, then select the vCenter Settings tab, and click "Browse Datastore." The minimum recommended GB value increases but gets added to the existing value.
  - For a desktop pool that contains three machines with one available and one still in the customizing or provisioning phase, edit the desktop pool and then select the vCenter Settings tab, and click "Browse Datastore." The minimum recommended GB value is displayed for the total of three machines.

  Workaround: Use Horizon Administrator to browse for a datastore while editing an automated desktop pool that contains full virtual machines to see the correct value for the minimum recommended GB storage.

- The following issues occur when you browse the datastore while editing instant-clone desktop pools:

  - After an instant-clone desktop pool has all the machines in the available state, edit the desktop pool, on the vCenter Settings tab, click "Browse Datastore". The Minimum Recommended (GB), Maximum Recommended (GB), and 50% Utilization values have positive values.
  - After an instant-clone desktop pool has all the machines in the available state, edit the desktop pool, on the Provisioning Settings tab, increase the maximum number of machines, then on the vCenter Settings tab click "Browse Datastore". The Minimum Recommended (GB), Maximum Recommended (GB), and 50% Utilization values increase but get added to the existing value.
  - For a desktop pool that contains three machines with one available and one still in the customizing or provisioning phase, edit the desktop pool and then select the vCenter Settings tab, and click "Browse Datastore." The Minimum Recommended (GB), Maximum Recommended (GB), and 50% Utilization values are shown for all three machines.

  Workaround: Use Horizon Administrator to browse for a datastore while editing instant-

clone desktop pools to see the correct Minimum Recommended (GB), Maximum Recommended (GB), and 50% Utilization values.

- After you create an automated desktop pool that contains full virtual machines with two or more names with the "#Unassigned machines kept powered on" value less than the actual names specified and then edit the pool, the "#Unassigned machines kept powered on" field does not accept a value equal to the total number of names specified during the pool creation process and displays an incorrect error message.
  Workaround: Use Horizon Administrator to edit the automated desktop pool that contains full virtual machines with two or more names to update the "#Unassigned machines kept powered on" field value correctly.

- Attempts to connect to the HTML Access portal or one of the administration consoles using an IP address or CNAME fails for most browsers without additional configuration. In the majority of these cases, an error is reported but sometimes a blank error message is displayed.
  Workaround: To resolve this issue, see "Origin Checking" in the *Horizon 7 Security* document.

- When configuring Skype for Business, there is an optional feature to enable Media Bypass which bypasses the Mediation Server.
  For Skype for Business optimized calls to and from PSTN users, media will always route through the Mediation Server regardless if Media Bypass is enabled.

  Workaround: None. Media Bypass is not supported with the Virtualization Pack for Skype for Business. See https://kb.vmware.com/s/article/56977

- If the same user exists in both Connection Server pods that need to be paired in a Cloud Pod Architecture environment, Horizon Administrator displays the value for "Source Pods" as 2 and sources the user from both pods. An administrator can edit the user from both pods, which might cause inconsistencies in user configuration during hybrid logon. Additionally, hybrid logon for the user cannot be disabled.
  Workaround: You must delete the user from both pods and then recreate the user and configure the user for hybrid logon.

- In Horizon Administrator, the Logoff Session and Disconnect Session buttons are not disabled for remote sessions started from vCenter Server.
  Workaround: Use Horizon Console for remote sessions started from vCenter Server to get the functionality for disabled Logoff Session and Disconnect Session buttons. However, this does not work when you navigate to Inventory > Desktops, select a desktop pool and click the Machines tab or Machines (Instant Clone Details) tab or Machines (View Composer Details) tab.

- Core-dump error messages are generated while adding Virtual Volumes datastores on nested ESXi or nested virtual ESXi.
  Workaround: None.

- When you open Horizon Console in the Internet Explorer and Microsoft Edge browsers, the long text does not wrap around in the user interface columns.
  Workaround: Use Horizon Console with a different Web browser.

- Both Horizon Administrator and Horizon Console display the internal folder names instead of the actual folder names when you browse a vSAN datastore to import a persistent disk. **Workaround:** None.

- In both Horizon Administrator and Horizon Console, custom roles with the Manage Help Desk (Read Only) privilege are shown as being applicable to access groups. **Workaround:** None.

- Users that have the Administrators (Read Only) role cannot see **View Configuration > Cloud Pod Architecture** in Horizon Administrator. **Workaround**: Use Horizon Console.

- In Horizon Administrator, when you add or edit a linked-clone farm that uses vSAN datastores, Blackout Times is disabled. **Workaround:** Use Horizon console to set blackout times for a linked-clone farm that uses vSAN datastores.

- The Horizon Console user interface does not list more than 1,000 published application pools. **Workaround:** Use Horizon Administrator to view and access more than 1,000 published application pools.

- In the Microsoft Edge Web browser, validation does not occur when you use the 'x' icon to clear a mandatory input field value. **Workaround:** Use another Web browser such as Internet Explorer.

- When you use Horizon Console in the Internet Explorer Web browser and add a vCenter Server, the vCenter Server and Horizon Composer certification details displays an empty certificate. **Workaround:** Use another Web browser to view the vCenter Server and Horizon Composer certificate details.

- In Horizon Administrator, the Rebuild button does not work in the machine summary of an automated desktop pool that contains full virtual machines. **Workaround:** In Horizon Administrator, use the rebuild functionality from Machines > vCenter Server.

- When you add a vCenter Server to Connection Server using an existing PowerShell script, the following error message appears: Failed to add vc instance: No enum constant com.vmware.vdi.commonutils.Thumbprint.Algorithm.SHA-1. This issue occurs because the certificateEncoding property that indicates a certificate override for self-signed certificates is added in Horizon 7 version 7.8. Therefore, earlier versions of VMware PowerCLI scripts that have an incorrect value of SHA-1 fail. **Workaround:** Update the PowerShell scripts to use the property value DER_BASE64_PEM instead of SHA-1. For example, set $certificate_override.sslCertThumbprintAlgorithm = 'DER_BASE64_PEM'.

- When a Universal Windows Platform (UWP) application is upgraded, the path containing the version changes, and the application is unreachable by the original path. The app status is **Unavailable** in Horizon Administrator and a user cannot launch the app.

Workaround: Update the app path in Horizon Administrator after an upgrade and verify the app status is **Available**. Alternatively, do not upgrade the app.

- When device filtering is configured for the client drive redirection feature, and a user uses the RDP display protocol to connect, device filtering does not work.

  Workaround: When device filtering is configured for client drive redirection, configure Connection Server so that RDP connections are not allowed.

- The True SSO desktop unlock feature is supported in PCoIP and Blast protocols, but not in Remote Desktop Protocol (RDP).

- In Horizon Console, the user or group summary fails to load due to domain trust issues in the following cases:

  - When users and groups belong to a one-way trust domain and the logged in administrator has the necessary permissions from a one-way trust domain.
  - When users and groups belong to a two-way trust domain and the logged in administrator has the necessary permissions from a two-way trust domain.
  - When users and groups belong to a one-way or two-way trust domain and the logged in administrator is from the child domain and has the necessary permissions.

  Workaround: Use Horizon Administrator to access the user or group summary.

- Updating the certificate information for an existing SAML authenticator fails in Horizon Console.
  Workaround: Use Horizon Administrator to update the certificate information for an existing SAML authenticator.

- Horizon Console does not display "Show all networks" when you browse networks for instant-clone desktop pools and farms.
  Workaround: Use Horizon Administrator to view all networks including unsupported networks.

- In Horizon Console, some events might not be listed because the Connection Server time is set incorrectly with respect to the Connection Server time zone.
  Workaround: Use Horizon Administrator to view all events.

- In Horizon Console, administrators who can view desktop pools but cannot entitle users or groups to the pool, cannot view the application entitlements in User or Group Summary > Application Entitlements.
  Workaround: Use Horizon Administrator to view the application entitlements for a user or group.

- You can recover an instant-clone virtual machine with an active session. This occurs in both Horizon Administrator and Horizon Console.
  Workaround: None.

- In Horizon Console, you cannot add a SAML authenticator URL that contains numbers.
  Workaround: Use Horizon Administrator to add a SAML authenticator URL that contains numbers.

Horizon Agent for Linux

This section describes issues that might occur with Horizon Agent for Linux or when you configure a Linux desktop.

- Sometimes the Collaboration window might not appear after you connect to a remote desktop and click the Collaboration UI icon.

  Workaround: Resize the desktop window or reconnect to the remote desktop.

- Configuring four monitors at 2560x1600 resolution on RHEL 6.6 or CentOS 6.6 virtual machines in vSphere 6.0 is not supported.
  Workaround: Use 2048x1536 resolution or deploy this configuration in vSphere 5.5.

- The Linux agent's keyboard layout and locale do not synchronize with the client if the Keyboard Input Method System is set to fcitx.
  Workaround: Set the Keyboard Input Method System to iBus.

- Single Sign On (SSO) does not work well on a RHEL/CentOS 7.2 desktop when you add a domain using System Security Services Daemon (SSSD).
  Workaround: After you add a domain using SSSD, modify the /etc/pam.d/password-auth file using the information in the VMware Knowledge Base article 2150330 [SSO configuration changes required when using SSSD to join AD on RHEL/CentOS 7.2 Desktops](#).

- **When a client user authenticating with smart card redirection connects to an Ubuntu 18.04/16.04 or SLED/SLES 12 SP 3 desktop and removes or reinserts the smart card before entering the PIN, the desktop does not appear to recognize the change.**
  The desktop will only detect a change in the smart card's state after the user closes the prompt asking for the PIN.

  Workaround: At the prompt, enter the smart card PIN and click OK. Or click Cancel to dismiss the prompt without entering a PIN.

- **When a client user connects to an Ubuntu 18.04/16.04, SLED/SLES 12 SP 3, or SLED 11 SP4 desktop, "Error 2306: No suitable token available" appears on the login screen.**
  This error message indicates that a smart card has been removed from the client system. The user can log in to the desktop by entering the user password or reinserting the smart card.

- On Ubuntu 16.04, if the administrator attempts to disable smart card redirection by setting VVC.ScRedir.Enable to "FALSE" in the /etc/vmware/config configuration file, the desktop will hang at the login screen.

- **When a client user disconnects from and then reconnects to a SLED 11 SP4 desktop using smart card authentication, the desktop login screen prompts for the user password instead of the smart card PIN.**
  The user can enter the password or the smart card PIN. Either method allows the user to log in to the desktop.

- **When connecting to a SLED 11 SP4 desktop configured for single sign-on (SSO), the client user encounters a smart card prompt.**

When SSO is enabled and a smart card is inserted at the client system, the smart card prompt often appears. The user can click OK to close the prompt and allow SSO authentication to proceed. The user can log in with SSO and does not need to enter the smart card PIN.

- To enable both SSO and smart card redirection for a SLED 11 SP4 desktop, configure the PAM settings for smart card redirection in the configuration file /etc/pam.d/gdm after installing Horizon Agent. Otherwise, client users can use only one of these methods for authentication.

- **After connecting to an Ubuntu 16.04 desktop and entering the wrong PIN for smart card authentication, the client user encounters a login prompt to enter the user password instead of the smart card PIN.**
  The client user can click OK to close the user password prompt. A new prompt appears asking the user to enter the smart card PIN.

- **On Ubuntu 18.04/16.04 and SLED/SLES 12 SP3, the desktop screensaver does not lock as expected when the user removes a smart card from the client system.**
  By default, the desktop screensaver does not lock even after the client user removes the smart card used to authenticate into the desktop. To lock the screensaver under these conditions, you must configure pkcs11_eventmgr on the desktop.

  Workaround: Configure pkcs11_eventmgr to specify the correct screensaver behavior in response to smart card events.

- After you install Horizon Agent with smart card redirection enabled (-m parameter set to "yes") on a RHEL 7.0 desktop, Horizon Administrator, Horizon Console, or vSphere may display a black screen. Smart card redirection is supported on desktops running RHEL 7.1 or later. The feature is not supported on RHEL 7.0 desktops.

  Workaround: Install Horizon Agent with smart card redirection enabled on a desktop running RHEL 7.1 or later.

- If you configure two monitors with different resolutions, and the resolution of the primary screen is lower than that of the secondary screen, you might not be able to move the mouse or drag application windows to certain areas of the screen.
  Workaround: Make sure that the primary monitor's resolution is at least as large as the secondary monitor's.

- When you use a smart card on a RHEL 7 desktop and enable the option to lock the screen upon removal of the card, the screen may lock immediately after you log in with the smart card. This is a known issue with RHEL 7.

  Workaround: To access the desktop, unlock the screen after logging in with the smart card.

Horizon Agent

- In FIPS mode, Horizon Agent fails to pair with Connection Server and the pool status is not available when Horizon Agent is installed to a drive other than the C drive.
  Workaround: When operating in the FIPS mode, install Horizon Agent on the C drive.

- A warning message about applications in use appears when you uninstall Horizon Agent on Windows Server 2016.
  Workaround: Click "Ignore" in the dialog box that appears when you use Windows Add or Remove Programs to uninstall Horizon Agent. If you uninstall Horizon Agent from the command line, use the command msiexec /x /qn {GUID of Agent} instead of the command msiexec /x {GUID of Agent}.
- When you uninstall the Horizon Agent, the mouse speed becomes slow and jerky. Uninstalling Horizon Agent also uninstalls the vmkbd.sys driver.
  Workaround: Repair VMware Tools on the Horizon Agent virtual machine.

- When upgrading from Horizon Agent 7.1 to Horizon Agent 7.2 on a Windows 7 guest operating system, a "Files in Use" dialog appears. The dialog states that the VMware Horizon Agent application is using files that need to be updated by the setup.
  Workaround: Click "Ignore" to proceed with the upgrade.

- Windows 10 32-bit Horizon Agent installation throws "the arguments are invalid" exception and the installation continues after you click OK. This error occurs because the print spooler service is disabled.
  Workaround: Enable the print spooler service for the installation to work as expected.
- With the Session Collaboration feature, if a session owner grants control to a collaborator, and the collaborator experiences connection loss and network recovery while the session owner is attempting to regain control of the session, both the session owner and collaborator might have input control of the session at the same time.

  Workaround: Disconnect and reconnect the collaborative session, or toggle the input check box in the Session Collaboration user interface.

- The HTML5 Multimedia Redirection feature cannot redirect HTML multimedia content from http://huffingtonpost.com. The HTML5 Multimedia Redirection feature can redirect HTML5 multimedia content from http://www.yahoo.com, but you might see a "Page Unresponsive" message.

  Workaround: None.

- If a session owner is watching a video that has been accelerated using MMR during a collaboration session, the collaborators see a black screen instead of the video.

  Workaround: As a session owner, if you need to play a video during a collaboration session, do not use Windows Media Player or Internet Explorer to play the video, or disable MMR on pools where collaboration is enabled.

- If a collaborator joins a multimonitor session and enables relative mouse mode on their client, it is possible for the mouse to move to a secondary monitor that the collaborator cannot see.

  Workaround: Move the mouse back on to the screen. Alternatively, don't use relative mouse mode in a multimonitor session.

- If you use Chrome with URL Content Redirection, and you set ".*.google.*" for the https protocol in filtering rules and you set Google as your home page in Chrome, redirection to google.com occurs each time you open a new tab.

Workaround: Change the home page or the filtering rules.

- When setting up a collaborative session, adding a collaborator by the email address from a two-way trusted domain fails.

  Workaround: Add the collaborator by using domain\user.

- If you include the URL of a Microsoft Edge trusted site in the list of websites in the **Enable URL list for VMware HTML5 Multimedia Redirection** group policy setting, HTML5 Multimedia Redirection does not work for that URL. To view trusted sites, select **Internet options**, click the **Security** tab, click **Trusted sites**, and click **Sites**.

  Workaround: Run the command CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe", which makes the host less secure.

- With the Microsoft Edge browser, the HTML5 Multimedia Redirection feature cannot redirect HTML multimedia content from websites that use the m3u8 video format, such as ted.com.

  Workaround: Use the Chrome browser.

- With the HTML5 Multimedia Redirection feature, if a user plays an HTML5 video that uses a static video URL in a remote desktop, their client machine does not have access to the static URL and the playback falls back to the remote desktop.

  Workaround: None. This issue is a network limitation.

- With the HTML5 Multimedia Redirection feature, when the Scanner Redirection setup option is enabled in Horizon Agent in a remote desktop, the VMware Horizon HTML5 Redirection Extension for Edge extension sometimes crashes after the Microsoft Edge browser is launched in the remote desktop. This issue typically occurs in large-monitor environments and under stress.

  Workaround: Close the launched Microsoft Edge browser and launch the Microsoft Edge browser again.

- HTML5 Multimedia Redirection works for Edge in a pre-1803 Windows 10 virtual desktop, but after updating to the latest Windows 10 1803 version, such as 17133, redirection does not work, particularly for websites that use autoplay, such as youtube.com.

  Workaround: Force restart the Windows 10 virtual desktop.

- When you connect to Horizon Client using a Unified Access Gateway appliance and configure the appliance using a non-English locale or an arbitrary name such as "UAG 2" instead of the machine's FQDN, then the field does not map to a URL. During a session collaboration, the generated URI invite has the wrong hostname.
  Workaround: When you configure the Unified Access Gateway name, use English and FQDN.

- Published applications do not get disconnected when the client session is idle, even when Idle Session Timeout is set with MaxIdleTime using the GPO or non-GPO method. A disconnect warning message appears, but the application is not disconnected.

- HTML5 Multimedia Redirection does not support 360 videos. The HTML5 Multimedia Redirection extension icon is marked with the REDR badge, even though the video is not supported.

  Workaround: None.

- After you perform a seek operation of streaming media using Multimedia Redirection, the audio and video are not smooth.

  Workaround: Wait for a few minutes or reopen the current streaming media.

Horizon GPO Bundle

- Computer-based global policy objects (GPOs) that require a reboot to take effect are not applied on instant clones.
  Workaround: See the VMware Knowledge Base (KB) article,[2150495](#).

- A GSSAPI_ERROR message appears when you initially login with username and password and try to recursively unlock using smart card authentication to login to a local machine that has the group policy setting "Unlock remote sessions when the client machine is unlocked" enabled, and then Log In As Current User from Horizon Client.
  Workaround: Disable Log In As Current User from Horizon Client and manually unlock the virtual desktop using the username and password.

- In a nested mode configuration where the first-level desktop (the machine where Horizon Client and Horizon Agent are installed) is a virtual desktop and the second-level desktop is a published desktop, the "Specify a filter in redirecting client printers" group policy setting does not affect the second-level desktop if you configure it in the first-level virtual desktop.

  Workaround: If you want to filter printers for the second-level desktop, configure the "Specify a filter in redirecting client printers" group policy in the second-level desktop.

Horizon Client

This section describes problems that end users might encounter when using Horizon Client or HTML Access to connect to remote desktops and applications. For problems that occur only in a specific Horizon Client platform, see the Horizon Client release notes on the [Horizon Clients Documentation page](#).

- Customized application icons with the .ico file extension do not appear on the Shortcut and Start Menu on a Windows desktop.
  Workaround: Use the .png file extension when you save the customized application icon.
- The profile data is missing for multiple user sessions on RDS hosts. This issue occurs when the sessions are in the disconnected state but the task manager on the RDS host still shows these sessions.
  Workaround: Delete the sessions from the RDS host or log the user off from the published desktop or application.

- When you log in to Workspace ONE, the pre-launch application session is not triggered. Pre-launch sessions are triggered only when there is a successful login to Connection Server from Horizon Client.

Workaround: Manually start an application or desktop from Workspace ONE to trigger the applications enabled for pre-launch to be started.

- Using the VMware Blast display protocol and with Blast Secure Gateway (BSG) disabled, Horizon Client sometimes cannot recover from a brief (about 1 minute) network outage and the connection to the desktop is disconnected. This issue does not occur when BSG is enabled.
  Workaround: Reconnect the session.
- Sometimes, when using Lync VDI to make a video call, the local image is not displayed.
  Workaround: Update Microsoft Lync VDI to the latest version.
- Skype for Busines VDI optimized solution is not compatible for inter-operatibility with Lync 2010 clients.

- The RDS host stores only one set of application data for the first application launch of a session. Any subsequent application launch data is lost.
  Workaround: Log off the session and launch another application to store that data.

- Desktops fail to start when you use HTML Access from Internet Explorer or Microsoft Edge Web browsers to connect to Connection Server, security server, or replica server on a Windows 10 client operating system. This issue affects desktops with Windows 10 N, Windows 10 KN, Windows 7 N and Windows 7 KN guest operating systems.
  Workaround: Use Firefox or Google Chrome Web browsers for HTML Access.

- Sometimes after a call ends, you might see a message:
  Skype for Business has stopped working.

  Workaround: Apply Skype for Business updates. See https://support.microsoft.com/en-us/help/3158521/lync--skype-for-business--or-outlook-2016-or-2013-crash for details.

- For Intel vDGA, multiple-monitor support is limited to no more than 3 monitors. The Intel driver supports only up to 3 monitors with a resolution of up to 3840 X 2160. If you try to connect with 4 monitors, the connection shows 3 black screens with just one screen working.
- With NVIDIA M60 GPU and driver version 361.89 or 361.94, users might see a blur red screen when they first connect to the Windows desktop, or when they right click on the desktop and then select **NVIDIA Control Panel > System Information**.
  Workaround: Changing the resolution of the display or changing to full-screen mode fixes the problem and you can revert to the original resolution or screen mode. The problem disappears after the first time it occurs. Also, the problem does not occur with NVIDIA driver 361.51.
- If a VDI desktop is in a remote location and experiencing high network latency, then a recursive unlock using smart card authentication might not work.
  Workaround: Unlock the desktop manually.

- If a user of a Windows 8 remote desktop logs in using Kerberos authentication, and the desktop is locked, the user account for unlocking the desktop that Windows 8 shows the user by default is the related Windows Active Directory account, not the original account from the Kerberos domain. The user does not see the account he or she logged in with. This is a Windows 8 issue, not directly a Horizon 7 issue. This issue could, but does not usually, occur in Windows 7.

Workaround: The user must unlock the desktop by selecting "Other user." Windows then shows the correct Kerberos domain and the user can log in using the Kerberos identity.

- When you use the Ambir Image Scan Pro 490i to perform a scan on a remote desktop or application, the dialog box always displays "Scanning…" and does not complete.
  Workaround: Perform a scan on the client. The client scan calibrates the scanner. After the calibrate operation is finished, run the scan within the remote desktop or application.
- Unicode keyboard input does not work correctly with HTML Access in Horizon 7 for Linux Desktops.

- When you connect to a Linux desktop, some keyboard inputs do not work. For example, if you are using a non-English IME on both the client device and the remote desktop, some non-English keys are not displayed correctly.
  Workaround: Set the English IME on the client device and set the non-English IME on the remote desktop.
- Sometimes an audio call does not start correctly from Skype to Skype for Business. The call status is "Connecting call..." on the Skype for Business client.

  Workaround: None.

- If you use Skype for Business inside a non-persistent desktop, you might reach the Skype for Business limit of 16 device certificates. When this limit is reached and Skype for Business attempts a new logon, a new certificate will be issued and the oldest assigned certificate will be revoked.

- Microsoft Skype for Business 2016 Client displays a black screen instead of the shared desktop when a second user shares a desktop. The first user sees a black screen and an error message: Someone else started presenting, which ended your presentation.

  Workaround: None.

- If a user starts a Co-Author Office session in Office 365 during a Skype for Business video call, Microsoft Skype for Business 2016 Client displays a black screen instead of the second user's video display.

  Workaround: None.

- If you launch Horizon Client for Linux 4.8 or earlier with FIPS mode enabled, and you try to connect to a Horizon Agent 7.6 or Horizon Connection Server 7.6 with FIPS mode enabled, the error message "Invalid license info for rds-license: Missing client id" is displayed.

  Workaround: To use Horizon Client for Linux with FIPS mode enabled to connect to Horizon Agent 7.6 or later or Horizon Connection Server 7.6 or later with FIPS mode enabled, use Horizon Client for Linux 4.9 or later.

- Changing the ringer volume level in audio settings of Skype for Business (in optimized mode) does not change the ringing volume when receiving a call in Windows, Mac, and Linux Horizon Clients.

  Workaround: When you receive a call, manually change the volume of the output device or speaker connected to the Horizon Client to change the output volume.

Horizon JMP Server and JMP Integrated Workflow

- In an environment where multiple JMP servers are installed, conflicts might occur when creating or deleting JMP assignments if more than one JMP server refers to the same User Environment Manager configuration share.

  Workaround: None.

- If you configured your JMP settings to use only one VMware App Volumes Manager and if during a JMP assignment creation you selected a desktop pool whose Horizon Agent is not pointing to that configured App Volumes Manager, you can still select AppStacks from the App Volumes Manager instance that is pointed to by the desktop pool's Horizon Agent. Also, if you configured your JMP Settings to use multiple App Volumes Manager instances, even if you select a desktop pool whose Horizon Agent points to one of those App Volumes Manager instances, you can still select the AppStacks from the other App Volumes Manager instances configured in your JMP settings. However, when the desktop pool is launched, the AppStacks selected from that other App Volumes Manager are unavailable.

  Workaround: None.

- If an AppStack that is currently used by an existing JMP assignment is renamed using the App Volumes Manager or by editing the JMP assignment, the summary page of existing JMP assignments does not get updated with the new AppStack name.

  Workaround: None.

- If you have two Horizon 7 instances that are registered with the same JMP Server instance and use the same App Volumes Manager, deleting a JMP assignment from one Horizon 7 instance can delete the AppStacks assignments used by another JMP assignment in the other Horizon 7 instance.

  Workaround: None.

- When adding or editing Active Directory information in the JMP Settings page, the operation fails if the value entered for **Bind User Name** contains one or more of a range of 30 triple-byte Chinese characters, such as the ' ' character, that cause the Active Directory authentication to fail.

  Workaround: Use another bind user name from your Active Directory that has administrative privileges and does not contain any of the 30 triple-byte Chinese characters. such as the ' ' character.

- When adding or editing App Volumes Manager instance information in the JMP Settings page, the operation fails if the value entered for **Service Account User Name** contains one or more of a range of 30 triple-byte Chinese characters, such as the ' ' character, that causes the App Volumes Manager instance authentication to fail.

  Workaround: Use another bind user name from your App Volumes Manager instance that has administrative privileges and does not contain any of the 30 triple-byte Chinese characters, such as the ' ' character.

- The Drive Mapping settings that were mapped using VMware User Environment Manager

version 9.2.1 are not visible when Windows 10 1703 desktop pool is launched.

Workaround: After the Windows 10 1703 desktop pool is launched, execute the following command.

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

See the VMware Knowledge Base (KB) articlehttps://kb.vmware.com/s/article/2113657 for additional information.

- If you access Horizon Console using localhost, the error message "JMP server is not reachable at the moment." is displayed on the JMP Settings pane of Horizon Console.

  Workaround: Access Horizon Console using a fully qualified domain name (FQDN) only, instead of using localhost.

- While creating a new JMP assignment, the following warning message might appear in the **Applications** tab: "The App Volumes instance associated with the selected desktop pool does not match any of the registered App Volumes instances." This issue occurs when one of the following is true:

    - The App Volumes Agent used in the desktop pool was installed using an IP address instead of a fully qualified domain name (FQDN)
    - The App Volumes Agent used in the desktop pool was installed using an FQDN, but the App Volumes Manager instance's IP address was registered in the JMP settings instead.

  Workaround: Re-install the App Volumes Agent using an FQDN and use the FQDN when registering the App Volumes Manager instance in the **Settings (JMP) > App Volumes** tab.

- While installing VMware Horizon JMP Server, the JMP Server installer failed to continue because McAfee Antivirus detected NSSM.EXE as a threat.

  Workaround: Add the following files to the McAfee Antivirus exclusion list before you reinstall JMP Server.
      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

- If you selected the **Authorize the local Administrator group** option during the Horizon 7 Connection Server installation, which creates a BUILTIN\Administrators group instead of *<domainName>*\Administrator, adding the JMP Server information using Horizon Console fails with the error message "Insufficient Horizon Privileges".

  Workaround: Using Horizon Administrator, register *<domainName>*/administrator with full administrator access. Log back in to Horizon Console and add the JMP Server information.

- While you are creating a JMP assignment and you hover over an instant-clone desktop pool, the value shown for the 3D Renderer option is **Disabled** instead of **Manage using vSphere Client**.

  Workaround: None.

- JMP Server registration fails when the scope of the trust authentication setting is set to "Selective Authentication."

  Workaround: Use one of the following workarounds to resolve this issue.

  - Use domain-wide authentication.
  - Continue to use the "Selective Authentication" security setting, but explicitly grant each Horizon Connection Server host (local system) accounts the "Allowed to Authenticate" permission on all the domain controllers of the computer objects (resource computers) that reside in the trusting domain or forest. For information on how to grant the "Allowed to Authenticate" permission, see the Microsoft article [Grant the Allowed to Authenticate permission on computers in the trusting domain or forest](#).

- JMP assignments do not work as expected because information about the App Volume Manager used by the desktop pool and the User Environment Manager version used by JMP Server could not be determined.

  Workaround: When configuring a desktop pool, set the **Number of spare (powered on) machines** value to 1 or more in the Desktop Pool Sizing section of the Provisioning Settings pane. In addition, if you selected the **Provision machines on demand** option in the Provisioning Timing section, set the **Min number of machines** value to 1 or more.

- When the JMP Server version 1.0.2.x installer file is run on a host that currently has JMP Server version 1.0.0.516 installed, the installation process does not proceed.

  Workaround: Use the Control Panel to uninstall JMP Server version 1.0.0.516. Run the installation file for JMP Server version 1.0.2.x and follow the wizard to complete the installation. Provide the same SQL Server database information during the installation process to preserve any data you had with the JMP Server version 1.0.0.516 installation.

- In the following scenarios, your JMP Server instance becomes unusable after you attempt to upgrade your current installation using JMP Server installer version 1.1.0.xxx, the upgrade fails, and the installation rolls back.

  - The SQL Server database certificate is missing in your JMP Server installation and the **Enable SSL** check box is selected during the upgrade.
  - The JMP Server upgrade is done by choosing the Windows Authentication connection mode, but a SQL Server login account was not created for the JMP Server host system.
  - You cancelled the upgrade operation by clicking **Cancel.**

  Workaround: Try upgrading again by re-running the JMP Server installer version 1.1.0.xxx. You must re-enter the same SQL Server database information that you used to install the previous JMP Sever version. After a successful upgrade, verify that all the certificates that you had configured for JMP Server are still intact. Depending on when the installation failure or cancellation occurred, the certificates might have been altered.

- When you attempt to add a User Environment Manager (UEM) configuration share, the following error may appear: **runOne] Error running file_share.createFileShare { code: 400,\n took: 221,\n data: {},\n error: 'Unable to create file share <fileshare-unc-path>.'**

  Adding a UEM configuration share fails when the password for the UEM configuration share contains one of the following characters: " #+,;<>=\~

Workaround: Use a different password containing one of these allowed characters: !$%&'()*-./:?@[]^_`{|}

Horizon Cloud Connector

- When you use the HTML5-based vSphere Web client to deploy the Horizon Cloud Connector virtual appliance OVA file, the following error occurs: "Invalid value 'false' specified for property proxySsl. Failed to deploy OVF package."
  Workaround: Use the Flex-based or the Flash-based vSphere Web Client to deploy the Horizon Cloud Connector virtual appliance OVA file.

- **When starting Horizon Cloud Connector, you encounter the message "[FAILED] Failed to start Wait for Network to be Configured. See 'systemctl status systemd-networkd-wait-online.service' for details."**
  This message is displayed incorrectly and does not indicate an actual problem with the network. You can disregard the message and continue to use Horizon Cloud Connector as usual.